Homeland Security

Daily Open Source Infrastructure Report for 7 April 2011

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

For information, click here: http://www.dhs.gov

Top Stories

- Bloomberg reports a survey found most energy and utility companies do not use "state-of-the art" technology to defend their networks and are exposing critical infrastructure to sophisticated cyber attacks. (See item **2**)
- According to Food Product Design, federal health officials said the Salmonella strain that sickened 12 people in 10 states and triggered the April 1 recall of 54,960 pounds of Jennie-O turkey burgers may be resistant to antibiotics. (See item **26**)

Fast Jump Menu

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. *April 6, Decatur Herald & Review* – (Illinois) **Gas line rupture forces evacuation of area at Illinois 121 and East Fitzgerald Road.** A hotel was evacuated, and several businesses were shut down for more than 2 hours April 5 after a construction crew opened a gash in a natural gas pipeline in Decatur, Illinois. Before the line was repaired, the escaping gas produced a roar, comparable to a jet engine, as gas was propelled into the atmosphere, the acting battalion chief of the Decatur Fire Department

said. At 9:35 a.m., a construction crew, working on a new access road to the Strand Cinema at Illinois 121 and East Fitzgerald Road, ruptured the underground, 2-inch diameter, high-pressure line. Illinois 121, from Fitzgerald Road north to the parking lot entrance for Steak-N-Shake and other businesses, was closed to traffic until 11:50 a.m. Employees and guests of the Hawthorn Suites hotel were evacuated too. The accident occurred about 30 yards from the southwest corner of the building. Firefighters told employees to evacuate guests and to make sure people did not start cars or light cigarettes because of the risk of explosion.
Source: http://www.herald-review.com/news/local/article_8a356393-375a-5a3f-833a-690ee5bdf338.html

2. *April 6, Bloomberg* – (National) **Energy infrastructure lacks advanced defense from cyber attacks.** A majority of energy and utility companies do not use "state-of-the art" technology to defend their networks and are exposing critical infrastructure to sophisticated cyber attacks, a new industry survey said. Sixty-seven percent of information technology professionals surveyed said their organizations had not deployed the best available security to guard against hackers and Internet viruses, states a report released April 6 by Ponemon Institute LLC, an information-security research group. Of the 291 security practitioners who responded, 71 percent said their companies' top executives do not understand or appreciate the value of information-technology security, according to the report. "One of the big surprises in this survey was that despite increasing cyber attacks on networks, the strategic importance of IT security among C-level executives hasn't increased," said the senior vice president of marketing and channels for Q1 Labs Inc., a software company that sponsored the survey. "It seems that the industry is very reactive in terms of IT security investment." The report follows recent high-profile cyber attacks, including the Stuxnet computer worm, which affects machines sold by Munich-based Siemens AG and can take over networks that run factories and power plants. The Ponemon report also identified shortcomings in adhering to industrywide regulatory initiatives. Seventy-seven percent of survey respondents said compliance with industry security standards did not rank as a priority at their organizations. U.S. regulators currently lack the authority to issue and enforce rules for protecting electric grids from cyberthreats, leaving the industry to follow its own voluntary standards. Those guidelines are set by the North American Electric Reliability Corp., an industry self-regulatory group that helps companies assess their ability to respond to potential attacks.
Source: http://www.bloomberg.com/news/2011-04-06/energy-infrastructure-lacks-advanced-defense-from-cyber-attacks.html

3. *April 6, Attleboro Sun Chronicle* – (Massachusetts) **About 70 South Attleboro homes evacuated after work crew hits gas line.** A construction company replacing a gas line for Columbia Gas ruptured a 2-inch, high-pressure plastic line April 6 in South Attleboro, Massachusetts, forcing officials to evacuate about 70 homes in the area of Robinson and Laurier avenues.The incident occurred around 7:45 a.m., and it took gas company officials about one and a half hours to stop the leak. Firefighters and police evacuated about 70 homes in the neighborhood within 200 feet around the gas line break, fire and gas company officials said. A Columbia Gas spokesman said before the

leak could be stopped, workers had to shut down 133 gas meters on 86 service lines. Some of the lines were to multi-dwelling units, he said. He said a construction company working for Columbia Gas to replace the line somehow struck it, causing the rupture.
Source: http://www.thesunchronicle.com/articles/2011/04/06/news/9132448.txt

4. *April 5, WLTX 19 Columbia* – (South Carolina) **Storms lead to evacuation of 40 people in Columbia.** While light to moderate damage has been reported all across the Midlands, one of the most concentrated areas of destruction from the April 5 storms was a spot off North Main Street in Columbia, South Carolina. Five to seven homes in the Greenview Area off North Main received severe damage, according to the American Red Cross. That led to the evacuation of 40 people. A series of storms rolled through the area, causing downed trees and power lines. At one point, there were approximately 40,000 homes without power in Richland and Lexington counties.
Source: http://www.wltx.com/news/article/131519/2/Storms-Lead-to-Evacuation-of-40-People-in-Columbia

For another story, see item **30**

[Return to top]

Chemical Industry Sector

5. *April 6, WPTV 5 West Palm Beach* – (Florida) **Liquid fertilizer spill shuts intersection of Midway and Glades Cut-Off roads.** Midway Road in St. Lucie County, Florida, remains shut down at Glades-Cut-off Road following a spill of liquid fertilizer. Just before 8:30 a.m. April 6, a tanker truck sprang a leak, sending about 3,800 gallons into the street. The chemical is ammonia polyphosphate solution and is acidic according to the St. Lucie County Fire Department. They said no one is in any immediate danger. The truck was operated by Helena Chemical, which sent a cleanup team to the scene to vacuum up the spill. No one was hurt. Shortly before the noon hour, crews estimated the road would be closed for at least 2 more hours.
Source: http://www.wptv.com/dpp/news/region_st_lucie_county/liquid-fertilizer-spill-shuts-intersection-of-midway-and-glades-cut-off-roads

6. *April 6, Richmond Times-Dispatch* – (Virginia) **I-95 north travel lanes affected by acid spill.** Virginia State Police closed two northbound lanes of Interstate 95 in Richmond for more than 5 hours April 5 because of an acid spill aboard a tractor-trailer. One Richmond firefighter was injured by a piece of equipment inside the tractor-trailer, but his injuries did not appear to be serious. The matter was originally reported as a tractor-trailer fire, but subsequent calls said there may have been a leak of muriatic acid, which has many industrial uses. A Richmond fire lieutenant said the truck's driver had noticed what appeared to be white smoke coming from the vehicle's trailer while he was heading north on 95, so he pulled over to the right shoulder and called authorities. The truck was hauling numerous items, including muriatic acid, acetone, and windshield-washer fluid. The lieutenant said a hazardous-materials crew

that went inside the trailer found a 250-gallon container of muriatic acid had leaked about 200 gallons. The fire lieutenant estimated that 10 to 15 gallons of the acid leaked out of the trailer onto the right shoulder of the interstate. A cleaning contractor was called to remove the spilled acid.
Source: http://www2.timesdispatch.com/news/2011/apr/06/TDMET02-i-95-north-travel-lanes-affected-by-acid-s-ar-952941/

[Return to top]

Nuclear Reactors, Materials and Waste Sector

7. *April 6, Mid Hudson News Network* – (New York) **No need to expand Indian Point emergency planning zone, NRC says.** As the Westchester County, New York Board of Legislators is poised to call on the Nuclear Regulatory Commission (NRC) to expand its 10 mile Emergency Planning Zone (EPZ) around the Indian Point nuclear power plant in Buchanan to 50 miles, the federal agency April 5 announced it sees "no basis at this point" for expanding it. The NRC's statement applies to all U.S. nuclear power plants. The current EPZ has been in use since the 1970s following a federal task force study, an NRC spokesman said. "We're not saying that there couldn't be protective actions beyond that 10 mile radius, but certainly that's where the bulk of the effort should be focused; efforts such as determinations on evacuations, sheltering in place, administration of potassium iodide, the regular testing of sirens," he said. The advice to Americans living within 50 miles of the Fukushima Daiichi plant in Japan was based on calculations done by NRC experts indicating releases from the three hobbled reactors and two fuel pools could possibly exceed conservatively set safe radiation-exposure limits for the public, he said. A Westchester legislator who is leading the local charge for the expanded area said if NRC will not do it for all nuclear power plants in the country, an exemption should be made just for Indian Point.
Source: http://www.midhudsonnews.com/News/2011/April/06/IP_NRC_emer-06Apr11.html

For another story, see item **42**

[Return to top]

Critical Manufacturing Sector

8. *April 6, Aviation Week* – (National) **Analysts mull G650 crash repercussions.** Analysts covering Gulfstream Aerospace's parent General Dynamics predict there will be an up to 6-month delay in certification of the G650, but expect no long-term effect in business jet deliveries after the crash of a test aircraft April 2. The G650 accident may ultimately have little impact on production schedule, a Bernstein Research analyst wrote. "If there is a design issue, delays could extend significantly longer," he wrote. "Certification and green deliveries had been expected later this year, with customer deliveries in 2012." Prior to the accident, the G650 was expected to start delivering in the second half of 2011, with Gulfstream having already completed 1,500

of the 2,200 hours needed for Federal Aviation Administration certification, a Morgan Stanley Research analyst wrote. “We continue to project 12 deliveries in 2011 until more is known,” the analyst added. “Despite a tragic, serious accident, the G650 likely proceeds with potential delay but no change in our view about the underlying business jet demand.”
Source:
http://www.aviationweek.com/aw/generic/story.jsp?id=news/awx/2011/04/05/awx_04_05_2011_p0-306597.xml&headline=Analysts Mull G650 Crash Repercussions&channel=busav

9. *April 5, Reuters* – (International) **Toyota says most Japan plants to stay idle next week.** Toyota Motor Corp said April 6 it would not restart production at most of its idled Japanese vehicle assembly factories the week of April 11, denying a Nikkei newspaper report. The world’s biggest automaker has halted vehicle assembly at all but 2 of the 18 group-wide factories in Japan that build Toyota and Lexus cars since the March 11 earthquake and tsunami disrupted supply of components to automakers globally. “There will be no resumption of production at most of our domestic factories next week [the week of April 10],” a Toyota spokeswoman said. The company will announce its decisions as they are made, she said. Japan’s Nikkei business daily reported Toyota would reopen most of its domestic automobile plants as early as the week of April 10 to start producing a limited number of models. Toyota had lost potential production of about 200,000 vehicles as of April 1, it said, with April 6 marking the 18th day of suspension at most of its Japanese factories. Among other major Japanese automakers, Honda Motor Co. has said it aims to restart production at all domestic plants April 11 at a rate of about half its original plans. Nissan Motor Co. plans to resume normal production with parts procured from suppliers, rather than using inventory, from mid-April at limited operation levels.
Source: http://www.reuters.com/article/2011/04/06/us-toyota-idUSTRE7350DL20110406

10. *April 5, Associated Press* – (Kentucky) **Fire marshal: Victim triggered plant explosion.** The Kentucky state fire marshal’s office has concluded that a man who was killed in an explosion March 31 at a plant in Ashland triggered the explosion when he opened an access panel to a high-pressure gas line. The fire marshal’s office released the finding April 5 and said the 61-year-old from Milton, West Virginia, intended to work on a nearby electrical panel instead at AK Steel’s coke plant. The man worked for a contractor, Dixon Electrical Systems and Contracting. A spokesman from the public protection cabinet, which includes the fire marshal’s office, said the Kentucky Office of Safety and Health Compliance was still investigating. He said he did not know whether the panels were marked.
Source: http://www.wave3.com/story/14391366/copy-fire-marshal-victim-triggered-plant-explosion

11. *April 5, Associated Press* – (International) **Chrysler canceling overtime at plants in Canada and Mexico to conserve parts from Japan.** Chrysler Group LLC is cutting overtime at plants in Canada and Mexico to conserve parts from Japan, Associated

Press reported April 5. Chrysler plants in Brampton, Ontario, and Toluca, Mexico, are affected by the change. The Brampton plant makes the 300 sedan, Dodge Challenger, and Dodge Charger. The Toluca plant makes the Dodge Journey, and Fiat 500. This is the first time Chrysler has linked production cuts to the March 11 earthquake in Japan, which damaged suppliers. Chrysler idled its minivan plant in Windsor, Ontario, the week of April 3 because of parts shortages, but said that was unrelated to the situation in Japan.
Source: http://www.washingtonpost.com/business/chrysler-canceling-overtime-at-plants-in-canada-and-mexico-to-conserve-parts-from-japan/2011/04/05/AFfU7PlC_story.html

[Return to top]

Defense Industrial Base Sector

12. *April 5, Associated Press and msnbc.com* – (Florida) **NASA calls off collision alert for space station.** The three astronauts aboard the International Space Station no longer have to worry about a small piece of space junk heading their way. Mission Control informed the crew April 5 the debris no longer poses a threat. Eight hours earlier, Mission Control told the astronauts they might have to seek shelter in their attached Soyuz capsule. That precaution is no longer needed. The 6-inch piece of debris is from a Chinese satellite that was deliberately destroyed in 2007 as part of a weapons test. Initial estimates put it passing within 3 miles of the space station April 7. But as the afternoon wore on, the threat level went from red to green, due to further refinements in the orbital calculations. The space station had to move out of the way April 1 of an orbiting remnant from a two-satellite collision in 2009. The alert April 5 came too late for an avoidance maneuver, which is why the crew was warned to be ready to take shelter in the Soyuz. Debris is an increasingly serious problem in orbit, because of colliding and destroyed spacecraft. At 5 miles per second, damage can be severe, even from something several inches big. More than 12,500 pieces of debris are orbiting Earth — and those are the ones big enough to track.
Source: http://www.msnbc.msn.com/id/42436198/ns/technology_and_science-space/?GT1=43001

[Return to top]

Banking and Finance Sector

13. *April 6, Newark Star Ledger* – (National) **Two men to face fraud charges in alleged $30M insider trading scheme.** A senior associate at a prominent Washington, D.C. law firm was arrested by the FBI April 6 on federal securities fraud charges in connection with a $30 million scheme that allowed him to trade on insider information related to pending corporate mergers, officials said. The lawyer, who specialized in merger and acquisitions for Wilson Sonsini Goodrich and Rosati, is expected to be arraigned in federal court in Newark, New Jersey, April 6, along with a banker, who allegedly traded on the information the lawyer provided. Officials at the U.S.

Attorney's office said the decades-long scheme involved insider trading based on information stolen from not only Sonsini Goodrich, but also from the law firms of Cravath, Swaine and Moore, and Skadden, Arps, Slate, Meagher and Flom — where the lawyer previously worked.
Source:
http://www.nj.com/news/index.ssf/2011/04/two_men_to_face_fraud_charges.html

14. *April 6, La Crosse Tribune* – (Wisconsin) **La Crosse bank robbery suspect in custody.** Federal prosecutors April 4 charged a 52-year-old Cottage Grove, Wisconsin man with robbing an Associated Bank in a Neenah grocery store January 5 by claiming to have a bomb, according to the complaint filed in U.S. District Court in Milwaukee. The man fled with $2,847 wearing a black hooded sweatshirt pulled over his forehead, according to the criminal complaint. He left behind a brown cardboard box filled with packaging material and wire. DNA recovered from the wire matched the suspect, the complaint states. La Crosse police April 5 asked the district attorney's office to issue an arrest warrant for the March 28 robbery at the Associated Bank in the former Quillin's Foodfest store at 3956 Mormon Coulee Road. A suspect matching the man's description showed a teller a fake bomb of three blue metal canisters taped together and a timer taped to a black and red backpack. He pulled a black hooded sweatshirt over his forehead and fled with $6,300, according to the complaint. The man is also suspected in the February 17 robbery at a Guaranty Bank inside an Oconomowoc grocery store. The suspect is due back in court April 19 for an arraignment. A federal judge in November 2000 sentenced him to 137 months in federal prison and 3 years supervised release for robbing four Wisconsin and Minnesota banks in 2000 after threatening to detonate hoax bombs. He is still on supervised release.
Source: http://lacrossetribune.com/news/local/article_62130f6c-600e-11e0-ae5d-001cc4c03286.html

15. *April 5, Mobile Press-Register* – (International) **Atlanta attorney fifth man arrested in Synergy securities fraud case.** An Atlanta, Georgia attorney has become the fifth man arrested in connection with what investigators called a scam by a Robertsdale, Alabama finance company that stole millions from investors through the sales of bogus securities, Press-Register reported April 5. The man was arrested March 22 in Atlanta by the Fulton County Sheriff's Department on a 17-count indictment. The charges resulted from an Alabama Securities Commission investigation of illegal securities transactions involving Synergy Finance Group LLC, the commission and the Baldwin County District Attorney's Office announced April 4. Charges include 5 counts of sale of securities by an unregistered agent, 1 count of conspiracy to commit securities fraud, 10 counts of securities fraud, and 1 count of first-degree theft of property. According to the indictment, the five men operated a "multi-billion dollar loan brokerage" and solicited money from U.S. and foreign investors seeking large, non-collateralized loans that involved illegal securities transactions, according to the news release. Investors were urged to wire thousands of dollars to Synergy accounts under the promise of multimillion-dollars in returns. Neither Synergy nor any of the indicted men was registered with the commission to conduct securities business in Alabama, according to

the news release.
Source: http://blog.al.com/live/2011/04/atlanta_attorney_fifth_man_arr.html

16. *April 5, Wired.com* – (International) **Conde Nast got hooked by $8 million spear-phishing scam.** A spear-phisher managed to reel in a prize catch in 2010 with a single hook when media giant Conde Nast took the bait and wired $8 million to his bank account after he posed as a legitimate business, according to a lawsuit filed March 30. The alleged swindler failed to withdraw any funds before federal authorities intervened and froze the money, but the case highlights how little effort a scammer needs to invest in order to get a big payday. According to the court document, last November Conde's accounts payable department received an e-mail that purported to come from Quad/Graphics, the company that prints Conde's magazines. The e-mail instructed Conde to send payments for its Quad/Graphics account to a bank account number in the e-mail, and included an electronic payments authorization form. The e-mail said the account was for Quad Graph, a name similar to the real printer's name. Someone at Conde apparently signed the form and sent it back to a fax number in the e-mail, then began making electronic transfer payments to the bank account specified by the scammer. Between November 17 and December 30, the company wired $8 million to the Quad Graph account before a query December 30 from the real printer, Quad/Graphics, asking about outstanding bills, prompted Conde to investigate. The man suspected of perpetrating the attack has yet to be charged with any crime related to the scam, but Forbes found a previous charge against someone with the same name and address who pleaded no contest in December to "terroristic threat of family/household."
Source: http://arstechnica.com/tech-policy/news/2011/04/conde-nast-got-hooked-by-8-million-spear-phishing-scam.ars

17. *April 5, Reno Gazette-Journal* – (Nevada) **Man arrested in Reno bank robbery, suspected in 2 others.** A man accused of robbing a Bank of America office in Reno, Nevada April 5 and suspected in two other bank robberies, was arrested April 5 at a motel in Sparks, Nevada, Reno police reported. The 53-year-old suspect was booked on one federal count of bank robbery, police said. About 2:15 p.m. April 5, a man entered the Bank of America at 700 N. Virginia Street, handed a teller a note demanding money and said he had a weapon, police said. After receiving an undisclosed sum, he fled, authorities reported. Reno and Sparks police and the FBI found the vehicle and suspect in the parking lot of the Aloha Inn in Sparks, police said. When the suspect was taken into custody, unspecified evidence from the Bank of America robbery was found on him, police reported. Detectives and federal agents are continuing their investigation. They anticipate that the suspect will be charged with a March 30 bank robbery in Sparks, and a bank robbery April 1 in Reno, police said.
Source: http://www.rgj.com/article/20110405/NEWS01/110405049/-1/blogs11/Man-arrested-Reno-bank-robbery-suspected-2-others?odyssey=nav|head

[Return to top]

Transportation Sector

18. *April 6, WCVB 5 Boston* – (Massachusetts) **Police: Logan passenger tried to bring guns on plane.** A New Hampshire man was arrested at Logan International Airport in Boston, Massachusetts April 6, police said, after he tried to bring antique firearms on a plane. The suspect, 44, was arrested by Massachusetts State Police at about 7:45 a.m. after he attempted to pass through a security checkpoint with two antique firearms. Police said he did not have proper identification for the weapons. Transportation Security Administration officers stopped the suspect who was heading to a Southwest Airlines gate.
Source: http://www.thebostonchannel.com/r/27451020/detail.html

19. *April 5, Associated Press* – (National) **FAA issues emergency order to inspect airliners.** Federal officials have issued an emergency order requiring inspections of Boeing planes with similar construction to the Southwest Airlines plane that had a 5-foot tear that led to an emergency landing the week of March 28. The Federal Aviation Administration (FAA) order April 5 applies to Boeing 737-300s, 400s and 500s that have a similarly constructed joint where pieces of the plane's skin meet. The joint is at about the midpoint of the passenger cabin. Nearly all of the U.S.-registered planes covered in the order have already been re-inspected. FAA has previously said the order will affect 80 U.S. planes, 78 of which are operated by Southwest. The other two are operated by Alaska Airlines. Southwest has said it has finished their inspections, finding five more planes with similar signs of metal fatigue.
Source: http://www.businessweek.com/ap/financialnews/D9MDNO8G1.htm

20. *April 5, Riverside Brookfield Landmark* – (Illinois) **Brookfield man charged with pointing laser at plane.** Just days after a Chicago, Illinois man was slapped with a 30-day jail sentence for pointing a laser at two aircraft, Brookfield, Illinois police April 4 charged a local man with pointing a laser on several different occasions at a commercial cargo plane flying near Chicago Midway International Airport last year. The suspect, 29, of Brookfield, faces 14 misdemeanor counts of aggravated assault for shining a green laser at a small cargo plane after he was identified by agents from the FBI. The FBI got a huge assist from the plane's pilot, who used Google Earth to pinpoint the general area the light was coming from. A pilot from Ohio, put a video camera in the cockpit of his small cargo plane after someone pointed a laser at his airplane for the first time April 30, 2010. Then he helpfully posted video of the laser shining at his plane and evidence of its location on YouTube. Overlaying a map on the area, he deduced the laser was shining up at him from somewhere in the vicinity of Prairie and Congress Park avenues.
Source:
http://www.rblandmark.com/main.asp?SectionID=1&SubSectionID=1&ArticleID=7372

For more stories, see items **5**, **6**, **35**, **54**, and **59**

[Return to top]

Postal and Shipping Sector

21. *April 5, KTHV 11 Little Rock* – (Arkansas) **U.S. postal worker robbed at gunpoint in Meadowcliff Subdivision.** Little Rock, Arkansas police are after two men who robbed a postal worker at gunpoint April 2. The post office stopped delivery in a couple of neighborhoods in response to the robbery. The post office has indefinitely suspended mail delivery to about 700 homes in the Meadowcliff and Brookview subdivisions. U.S. postal inspectors are looking for robbers who police said targeted a postal carrier. The police report said teen suspects pointed a gun at the mail carrier and robbed him of his pocket knife, dog spray, and a cell phone. A postal inspector said he did not expect the suspension to last long. The crime against the postal worker is a federal offense subject to 25 years in prison.
Source: http://www.todaysthv.com/news/article/152074/2/US-postal-worker-robbed-at-gunpoint-in-Meadowcliff-Subdivision

[Return to top]

Agriculture and Food Sector

22. *April 6, Wall Street Journal* – (National) **U.S. seeks to reassure on contaminated food.** U.S. public-health officials sought April 5 to reassure consumers about the safety of food in the United States, including seafood, amid news that fish contaminated with unusually high levels of radioactive materials had been caught in waters 50 miles from the Fukushima nuclear plant in Japan. No contaminated fish have turned up in the United States, or in U.S. waters, according to experts from the Food and Drug Administration (FDA), Environmental Protection Agency (EPA), and Centers for Disease Control and Prevention (CDC). They expressed confidence that even a single fish sufficiently contaminated to pose a risk to human health would be detected by the U.S. monitoring system. They also dismissed concerns that eating fish contaminated at the levels seen so far in Japan would pose such a risk. The head of the CDC in Atlanta said he expected continued detection of low levels of radioactive elements in the water, air, and food in the United States in coming days, but that readings at those levels "do not indicate any level of public health concern." FDA hinted that further import restrictions could be forthcoming following Japanese authorities' re-evaluation of its own policies. Domestic restrictions on produce in Japan could be expanded to include several more towns.
Source:
http://online.wsj.com/article/SB10001424052748703806304576244973187013008.html?mod=googlenews_wsj

23. *April 6, WRC 4 Washington D.C.* – (Maryland; West Virginia) **Violent Burger King crimes possibly linked.** Police in Maryland and West Virginia are looking into whether Burger Kings across the region are being targeted by the same violent suspects. A Burger King manager was shot and killed March 18 in Frederick, Maryland. The manager had just opened the store at 1302 E. Patrick Street and was shot in a robbery attempt. On April 3, armed robbers hit a Burger King in Hagerstown, Maryland. And a third Burger King was hit by armed robbers in Martinsburg, West Virginia, in January. Now, police in both states are investigating possible links. "There

are some similarities. No. 1: they are all Burger Kings. There could be a possibility that somebody has some inside information on Burger King and some of their practices," a Frederick police lieutenant said. In two of the instances, police said, the suspects hit before the stores opened for the day. In Hagerstown, the burglary happened after the restaurant closed. Police said in each incident, managers were targeted and forced to take money out of a secured vault. All of the Burger Kings targeted were also near a major highway or escape route. In West Virginia and Hagerstown, the robberies may have been committed by two men wearing all black clothing, ski masks and carrying guns, police said. The duo could be traveling up the east coast.
Source: http://www.nbcwashington.com/news/local/119255979.html

24. *April 5, University of Central Florida Today* – (Florida) **Mystery sea creature invading Indian River lagoon, threatens oysters.** An ascidian, better known as a sea squirt, of unknown origins has been found in Indian River Lagoon in Brevard County, Florida. How it got into the lagoon and where it came from has researchers puzzled. The only thing scientists know for sure is it is overgrowing native oysters, a keystone organism for the health of the waterway as well as an important part of the local economy. A University of Central Florida (UCF) biologist has been monitoring the lagoon and helping restore its oyster population for the past 14 years. She has since seen three other non-native species invade the lagoon. If oysters cannot grow because of an invasive species, they cannot clean the lagoon. The oysters also provide refuge to native species such as blue crab, shrimp, and red fish that locals catch and sell. Without them, many other creatures' food sources disappear. In the Indian River Lagoon, the UCF biologist has identified 149 species that rely on native oysters in a balanced ecosystem. It is essential to figure out each species' origins if invaders are to be kept from wrecking havoc on U.S. waterways, researchers say.
Source: http://today.ucf.edu/mystery-sea-creature-invading-indian-river-lagoon-threatens-oysters/

25. *April 5, Associated Press* – (National) **USDA: Delay in meat sales could prevent recalls.** The U.S. President's administration is aiming to prevent meat recalls by withholding meat and poultry products from grocery store shelves until government testing is complete. The Agriculture Department proposed rules April 5 that would force companies to delay shipments to consumers until government inspectors have released tests on the meat. The department's Food Safety and Inspection Service has inspectors in all meat plants that sample for E. coli and other contaminants. Currently, products that are sampled can be shipped before testing results are known, though many companies already have procedures in place to hold the meat. The agency said at least 44 recalls between 2007 and 2009 could have been prevented if the rule had been in place.
Source: http://www.whec.com/news/stories/S2051669.shtml?cat=566

26. *April 5, Food Product Design* – (National) **Drug-resistant Salmonella linked to turkey recall.** The Salmonella strain that sickened 12 people in 10 states and triggered the April 1 recall of 54,960 pounds of Jennie-O turkey burgers may be resistant to antibiotics, the Centers of Disease Control and Prevention (CDC) announced April 4.

According to CDC, Salmonella Hadar is resistant to many commonly prescribed antibiotics, including ampicillin, amoxicillin/clavulanate, cephalothin, and tetracycline, which may increase the risk of hospitalization or possible treatment failure in infected individuals. Jennie-O Turkey Store recalled 4-pound boxes of frozen Jennie-O Turkey Store "All Natural Turkey Burgers with seasonings Lean White Meat" containing 12 individually wrapped one-third pound burgers after they were linked to 12 confirmed cases of Salmonella Hadar in Arizona, California, Colorado, Georgia, Illinois, Mississippi, Missouri, Ohio, Washington, and Wisconsin, with illnesses occurring between December 2010 and March 2011. Three of the patients in Colorado, Ohio, and Wisconsin specifically reported eating this product prior to illness onset and hospitalization; the last of these illnesses was reported March 14.
Source: http://www.foodproductdesign.com/news/2011/04/antibiotic-resistant-salmonella-linked-to-turkey.aspx

27. *April 5, Associated Press* – (Ohio) **24 horses die in Hamilton County barn fire.** Twenty-four horses and a calf died in a barn fire April 5 on a horse breeding farm in Cincinnati, Ohio, fire officials said. About 16 of an estimated 40 horses believed to be in the barn were rescued or escaped from the morning fire, 2 were taken to an animal hospital with severe burns, and 1 had to be euthanized by a veterinarian on the scene, said a captain with the Colerain Township Fire Department. The fire at Oasis Farms was accidental, caused by electrical equipment used inside the barn for warming the newborn calf that died in the fire. The farm provides training, boarding, and breeding services for Crabbet Arabian horses, fire officials said. A passer-by first reported the fire, and the farm owners also called saying horses were trapped, the captain said. Fire crews had to lay down a fire hose about 2,500 feet from the nearest hydrant to the barn, he said. About half of the barn collapsed from the flames that moved rapidly through the open structure. The fire captain said the animals added to the tension of the situation. "We are not professional horse-handlers, and that fact added another level of danger," he said.
Source: http://www.coshoctontribune.com/article/20110405/NEWS01/110405004/24-horses-die-Hamilton-County-barn-fire?odyssey=tab|topnews|text|Frontpage

For another story, see item **59**

[Return to top]

Water Sector

28. *April 6, WACH 57 Columbia* – (South Carolina) **Power outage causes sewage to leak from Midlands treatment plant.** A power outage at the Coventry Woods Wastewater Treatment Plant in Lexington, South Carolina, caused around 272,000 gallons of sewage to spill into Twelve Mile Creek, which flows into the Saluda River, according to health officials. The South Carolina Department of Health and Environmental Control (DHEC) said power was knocked out on Mallard Lakes Drive around 4 a.m. April 5 because of the overnight storm. The outage caused the partially treated water to be discharged from the plant in Lexington. Other sewer line overflows were also

reported along Twelve Mile Creek. An operator discovered the spill around 6 a.m. — 2 hours after power was lost at a pumping station. Power was restored to the pumping station around 1:30 p.m. and the spill has since been stopped, but DHEC officials warned people and pets to stay out of downstream waters from the plant because of high bacteria levels. A DHEC spokesman said no back-up generators were online. Crews are working to clean up the spill.
Source: http://www.midlandsconnect.com/news/story.aspx?id=601426

29. *April 6, WBIR 10 Knoxville* – (Tennessee) **Gatlinburg wastewater plant still offline, still dumping into river.** Officials were working April 6 to determine what caused a raw sewage storage tank at a Gatlinburg, Tennessee wastewater plant to fail April 5, and how to move forward. Two workers were killed, and hundreds of thousands of gallons of untreated waste- and storm-water were dumped into the Little Pigeon River. The first priority is to determine how to get the electrical system back online to power the plant. Then officials will focus on removing debris and getting back online. Until then, Tennessee Department of Environment and Conservation (TDEC) officials said there is no waste coming into the plant. At the site of the old water plant further upstream, they are straining solid waste, but all of the wastewater is being routed directly into the West Prong of the Little Pigeon. They are using a chlorine drip on the water to treat it, but that is not the same as fully treating wastewater in a plant. TDEC urged people to avoid contact with the West Prong of the Little Pigeon due to contamination. Officials noted that the tank release did not likely release any solid waste. Solid waste is strained out of the system before it reaches the tank that ruptured April 5. About 850,000 gallons of wastewater went into the river. TDEC said Gatlinburg normally produces around 2.3 million gallons of wastewater every day, so that means that roughly 2 million gallons of wastewater well directly enter the West Prong of the Little Pigeon daily until the plant gets back up and running. TDEC asked Gatlinburg residents to conserve water. The exact cause of the collapse of the plant's equalization basin wall has not been determined.
Source: http://www.wbir.com/news/article/164827/2/Officials-working-to-determine-cause-of-sewage-spill

30. *April 6, Monroe News Star* – (Louisiana) **Debris-strewn parish picks up.** Tensas Parish, Louisiana is facing a water shortage because the main water treatment plant suffered severe damage after it was hit by a tornado spawned by a severe storm April 4. The National Weather Service in Jackson, Mississippi sent a team to the area and determined an F2 tornado touched down around the Lake Bruin area. The twister knocked down more than 100 power lines, and damaged about 60 homes in the farming community. An F2 tornado is considered a strong tornado with winds between 113-157 mph, according to the weather service. The director of the Tensas Parish Office of Homeland Security and Emergency Preparedness said the two biggest issues facing the area are water and power. The Tensas Water Distribution Association Inc. water treatment plant was severely damaged. He said the $5 million facility is only about 4 years old, and it provides water to three water systems. Those systems are under a boil water order, and water could run out in days, officials said. "The water system is trying to make connections with the town of Newellton and with the town of St. Joseph," he

said. “The Governor’s Office of Homeland Security and Emergency Preparedness contacted the Louisiana National Guard so we have potable water some people will have to use until we can get some of the other systems in place.”
Source: http://www.thenewsstar.com/article/20110406/NEWS01/104060312

31. *April 4, Ozarks First* – (Missouri) **AG files lawsuit against wastewater treatment owner.** Missouri’s attorney general has taken legal action against a Johnson County wastewater treatment owner accused of clean-water violations. A lawsuit filed April 4 alleges infractions against GAAR LLC that include failure to submit an engineering-evaluation report, failure to prevent a bypass of wastewater from the treatment site, discharging wastewater that could pollute a tributary of Devil’s Branch, and failure to renew an operating permit. The attorney general is asking the court to order GAAR to comply with clean-water rules and require it to pay fines and legal costs.
Source: http://ozarksfirst.com/fulltext?nxd_id=433976

[Return to top]

Public Health and Healthcare Sector

32. *April 6, Denver Post* – (Colorado) **Alleged health-insurance scam led to millions in unpaid bills.** The owner of a bankrupt rural health-insurance brokerage, which left dozens of employers and thousands of employees holding millions in unpaid medical bills, has been indicted for embezzlement, fraud, and money laundering. The 59-year-old owner of Centennial, Colorado-based Rural Health Plans Initiative (RHPI) will be arrested on appearance April 6 and faces up to 20 years’ imprisonment and millions in fines, according to a U.S. attorney. The man sold himself and his company as a third-party administrator for small nonprofits and private companies that had trouble finding affordable health insurance for employees. He signed up many school districts, small-town administrations, nursing companies, and others, and promised to handle claims and provide backup insurance for catastrophic illnesses. In the summer and fall of 2010, many of those businesses began hearing their claims with hospitals and doctors had never been paid. The indictment, after joint investigation by the U.S. attorney, the IRS, and the Labor Department, said he and RHPI defrauded employers in at least three states. RHPI’s bankruptcy filing showed it had $8.7 million in revenue in 2009 and was down to $2.9 million through most of 2010. In addition to the individual employees who were told they are liable for their bills, many health care providers have been hurt in the scheme. The HealthOne hospital group has said it had more than $1 million in unpaid bills from patients who thought they were insured through RHPI.
Source: http://www.denverpost.com/news/ci_17780421

33. *April 5, WSBTV 2 Atlanta* – (Georgia) **Barrow Co. Health Department damaged in storms.** The Barrow County Administration Office and the Barrow County Health Department in Georgia suffered heavy damage April 6 due to overnight severe storms. “Heavy winds peeled back a large portion of the roof during the storms,” said a Barrow County Emergency Services lieutenant. “This caused flooding throughout the section of the building also.” The major part of the damage was located over the Barrow County

Health Department. Barrow County firefighters, employees with Barrow County Buildings and Grounds, and officials with the Georgia State Public Health Office worked to remove vaccines and other medicines, as well as to secure all medical records. The health department was closed April 6 due to the extent of the damage. County officials and state public health officials were working together to assess the total damage and decide when the health department can reopen. The section of the administration building that is affected has been shut down to the public, but the county is open for business. County leaders have contacted the insurance company, as well as construction and architectural specialists, to assess the damage and start working on costs of repairs.
Source: http://www.wsbtv.com/news/27439874/detail.html

34. *April 5, Hartford Courant* – (Connecticut) **Hospital records breach involves 93,500 patients.** MidState Medical Center in Connecticut announced April 5 that an employee who wanted to work at home improperly transferred information on 93,500 patients to a personal hard drive. The data transferred outside the hospital's secure computer system included patients' names, addresses, dates of birth, Social Security numbers, and medical record numbers. A spokesman for the hospital, which is affiliated with Hartford Healthcare said the person who took the hard drive was a Hartford Hospital employee and was dismissed following an investigation by a private security firm. The hard drive has not been located, according to MidState, but the hospital has no evidence any of the personal data has been misused. In a statement released with the announcement, MidState's CEO said the hospital does not believe "any information on patient diagnosis or treatment was on the hard drive." The hospital first learned about the incident February 15 and waited to alert the public until it had completed an investigation.
Source: http://articles.courant.com/2011-04-05/health/hc-buck-database-theft-at-midstate-0420110405_1_hard-drive-hartford-healthcare-patients

[Return to top]

Government Facilities Sector

35. *April 6, WPIX 11 New York City* – (New York) **Terror threats made against Long Island school buses.** An anonymous but threatening e-mail was sent April 1 to various New York State offices and state officials, including the speaker of the house. The e-mail referenced threats of violence in state office buildings, against the state legislature, and also made a specific reference to school buses. Because of this, the New York State Education Department issued an e-mail to schools April 4, urging school bus drivers and dispatchers to take extra precautions in checking buses and making sure students are safe. School bus drivers and dispatchers said they had read the e-mail, and that they already receive regular counterterrorism and safety training at the start of each year. New York State Police, the state office of counterterrorism, and the FBI are investigating. The state department of education encourage people involved in school bus transport to remain aware of their surroundings and report suspicious activity.
Source: http://www.wpix.com/wpix-li-bus-threat,0,5006745.story

36. *April 5, WGAL 8 Lancaster* – (Pennsylvania) **State constable accused in DA threat.** A Pennsylvania state constable is accused of threatening to physically harm a Mifflin County district attorney. The 48-year-old suspect made the threats March 30 when the district attorney took a break from his regular musical performance at the Hammermill Bar and Grill in Yeagertown, police said. The suspect confronted the district attorney because the suspect is under investigation for alleged misconduct, investigators said. The suspect appeared to be under the influence of alcohol, according to court documents.
Source: http://www.wgal.com/news/27440242/detail.html

37. *April 4, Steamboat Springs Steamboat Today* – (Colorado) **Man arrested on suspicion of stabbing teen at Bud Werner Memorial Library.** A teenager from Steamboat Springs, Colorado, was taken to the hospital with knife wounds to both hands after police said a man stabbed him April 4 during an altercation at Bud Werner Memorial Library. A Steamboat Springs Police captain said officers arrested a 40-year-old suspect and placed him in custody at Routt County Jail. The injured teen was transported by emergency responders to Yampa Valley Medical Center at about 5 p.m. Both of his hands were bandaged, but he did not appear to suffer any wounds elsewhere to his body. The 14-year-old boy had "stab wounds through and through, one on each hand," the police captain said. The teenager was alert and responsive when responders brought him out of the library. The suspect was on the balcony above the library's teen reading area, and may have been asleep, before the altercation, the police captain said.
Source: http://www.steamboattoday.com/news/2011/apr/04/witness-teen-stabbed-after-altercation-bud-werner-/

38. *April 4, Homeland Security Newswire* – (National) **Safeguarding the private and public sector from insider threats.** A recent panel at the Government Security Convention and Expo in Washington, D.C. dealt with the full range of threats posed by insiders. These types of threats are often the most difficult to detect as they originate from individuals who have already been screened and given access to an organization's critical resources. Businesses, government agencies, and other organizations are vulnerable to a host of threats from insiders including corporate espionage, workplace violence, and the loss of data. Speaking on the panel, the deputy general counsel to the U.S. Senate Homeland Security Committee described the legislative push to secure federal facilities. Currently, the Federal Protective Service (FPS) is charged with overseeing security at 9,000 federal facilities across the nation, but the organization has proven unable to effectively protect employees and prevent illegal materials from being smuggled into buildings. According to the deputy general counsel, Government Accountability Office (GAO) reports and independent investigations by the DHS Inspector General "have documented serious and systematic flaws within the operations of FPS." "These lapses place federal employees and private citizens at risk every day," she said. As evidence, she cited an undercover investigation by GAO in June 2009, where investigators successfully smuggled bomb-making materials into 10 federal facilities and were not detected, even as they assembled the parts.
Source: http://homelandsecuritynewswire.com/safeguarding-private-and-public-sector-insider-threats?page=0,0

For more stories, see items **39** and **40**

[Return to top]

Emergency Services Sector

39. *April 6, Homeland Security Today* – (National) **NORTHCOM striking military emergency response deal with governors.** The Department of Defense (DoD) is negotiating with state governors to set rules for more extensive use of the U..S military during a national disaster, including the activation of Army Reserves, the commander of U.S. Northern Command (NORTHCOM) revealed April 5. DoD has the authority to activate Reserves on an involuntary basis, the U.S. Navy Admiral and NORTHCOM commander said during a hearing of the Senate Armed Services Committee, but state governors have resisted the notion in the past as they like to maintain control of armed forces operating within their states during a disaster. NORTHCOM has been engaging U.S. governors to gain their approval for use of the dual-status structure, which would include a deputy commander acting in federal status, as well as the activation of Reserve forces. The deputy commander, acting under U.S. Code Title 10, would be able to bring federal resources directly to bear against a disaster scenario, an official noted. NORTHCOM also is working with the National Guard to improve its readiness for chemical and biological threat response as well as border security.
Source: http://www.hstoday.us/industry-news/general/single-article/northcom-striking-military-emergency-response-deal-with-governors/4528e3e0e5d9138c438f89f3e3827ebc.html

40. *April 6, National Journal* – (National) **Obama signs policy directive on government's emergency preparedness.** The U.S. President signed a national-security directive the week of March 28 designed to put the administration's imprint on the way the nation responds to major emergencies, including terrorism, National Journal reported. A senior administration official said that congressional committees were briefed April 5 on the Presidential Policy Directive, which bears the title of "National Preparedness." The directive sets government policy as informed by a National Security Staff review completed earlier this year. According to a summary of the directive given to National Journal, the administration preserves core elements of the former U.S. President administration's emergency preparedness plan, which was released in 2003. It makes DHS grants contingent on performance and on how the Homeland Security Secretary assesses need and the quality of response plans. The directive also instructs DHS to set up a "National Preparedness System," which the summary said "will enable the nation to achieve the goal" of maximum preparedness and to undertake "a comprehensive campaign to build and sustain national preparedness; and an annual National Preparedness Report to measure progress in meeting the goal." The directive also calls for closer collaboration with the private sector, and for better and more effective ways for the government to communicate with communities during crises.
Source: http://www.govexec.com/dailyfed/0411/040611emergency-response.htm

41. *April 6, Associated Press* – (Pennsylvania) **Police: Cop shooting suspect posed as FBI agent.** A man charged with critically wounding a Pittsburgh, Pennsylvania-area police officer who responded to a home invasion had pretended to be an FBI agent to gain entrance to the residence, according to a criminal complaint. Police were still trying to identify a second suspect they believe was with the first suspect when he forced his way into a home about 10:45 p.m. April 4. One of the robbery victims, a 45-year-old man, told police he opened the door after someone outside claimed to be an FBI agent. That is when the two suspects burst into the home brandishing handguns while ordering the man, a 26-year-old woman, an 8-year-old girl and 4-year-old boy "through the house at gunpoint, demanding money and narcotics," the complaint said. Three Clairton police officers arrived while the robbery was in progress. The two suspects fired at a police officer moments after he knocked on the back door and announced the police presence, an Allegheny County police superintendent said. Police believe both suspects fired, but ballistics tests have yet to confirm that or determine who fired the shots that wounded the police officer: one grazing his left side; one hitting his right forearm — which caused the officer to drop his weapon before it could be fired; and the third hitting him near his left armpit, which then ranged downward inside his body, the superintendent said. Police were on the trail of the second suspect but had not arrested him by the morning of April 6.
    Source: http://dailyitem.com/0100_news/x930492243/Police-Cop-shooting-suspect-posed-as-FBI-agent

42. *April 5, Associated Press* – (New York; New Jersey; Connecticut) **NYPD leads tri-state 5-day 'dirty bomb' exercise.** A vehicle carrying a "radioactive source" was stopped by law enforcement 12 times on an interstate parkway April 5 and never made it into New York City during a tri-state training drill to prepare for a "dirty bomb" attack, police said. The drill, which is scheduled to run through April 9, involves hundreds of personnel from 150 law enforcement, and other first responder agencies. It is being conducted on land, including rail hubs and highways, and on the waterways. A New York City Police Department (NYPD) police spokesman said his department and other agencies from New York City, New Jersey, Connecticut, and Rockland County successfully located all 17 sources of radioactivity. An NYPD spokesman said the April 5 exercises also included the identification and apprehension of people carrying radiological materials at Pennsylvania Station, at a subway station near Macy's, and at a subway transit booth at Columbus Circle. A Connecticut state trooper who was not involved in the drill stopped a participant in the exercise using a radiation detection device. The police commissioner said more than 400 checkpoints throughout the region would be manned by law enforcement agencies during the drill.
    Source: http://online.wsj.com/article/AP4da935e87e8b4cb1a8c2d3be7df8bc64.html

For another story, see item **51**

[Return to top]

Information Technology Sector

43. *April 6, Bloomberg* – (International) **Freescale won't reopen plant in Japan damaged by earthquake.** Freescale Semiconductor Inc., the chipmaker partly owned by Blackstone Group LP, will not reopen a factory in Sendai, Japan, that was damaged by the March 11 earthquake and tsunami. Safety concerns and damage to infrastructure mean the plant, which had already been scheduled to close in December of 2011, will not return to full operation, Austin, Texas-based Freescale said in a statement. Freescale will concentrate on transferring work to alternative facilities, it said in the statement. The Sendai plant, which makes chips used in cars, was being closed as part of a company-wide effort to cut costs.
Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2011/04/06/bloomberg1376-LJ7PYP6S972C01-01ESG9MSU7MJB3E50EOI421BDE.DTL

44. *April 6, H Security* – (International) **DHCP client allows shell command injection.** The Internet System Consortium's (ISC) open source DHCP client (dhclient) allows DHCP servers to inject commands that could allow an attacker to obtain root privileges, according to a new ISC advisory. The problem is caused by incorrect filtering of metadata in server response fields. By using crafted host names, and depending on the operating system and what further processing is performed by dhclient-script, it can allow commands to be passed to the shell and executed. A successful attack does, however, require there to be an unauthorised or compromised DHCP server on the local network. Dhclient versions 3.0.x to 4.2.x are affected. The ISC has released an update.
Source: http://www.h-online.com/security/news/item/DHCP-client-allows-shell-command-injection-1222805.html

45. *April 6, Softpedia* – (International) **Several vulnerabilities patched in WordPress 3.1.1.** The WordPress development team has released version 3.1.1 of the blog publishing platform in order to address multiple stability and security issues. In total, the new WordPress 3.1.1 fixes almost 30 bugs including 3 vulnerabilities discovered by core developers. One flaw was located in the media uploader component and allowed bypassing the cross-site request forgery (CSRF) protection. It was resolved by adding nonce checks to the code. This type of vulnerabilities allows attackers to hijack sessions of authenticated users by forcing their browser to perform unauthorized actions when visiting a maliciously crafted Web page. Such an attack abuses the inherent trust between Web sites and browsers and is resolved by associating unique codes (nonces) to requests. The second vulnerability was a minor cross-site scripting (XSS) issue located on the database upgrade screens. This type of flaw is the result of insufficient input validation and can be used, in the worst case scenario, to generate pages with rogue code inserted into them. The CSRF and XSS vulnerabilities were discovered and reported by a member of the WordPress security team. The vulnerability identified by one of the WordPress core developers concerns handling of certain links and can lead to a denial of service condition where the PHP process crashes. It can be exploited by inserting malformed links into comments.
Source: http://news.softpedia.com/news/Several-Vulnerabilities-Patched-in-WordPress-3-1-1-193434.shtml

46. *April 5, The Register* – (International) **Google Chrome to warn of malicious Windows executables.** Google said it is expanding its blacklist of malicious Web sites to include those that use deceptive claims to push harmful Windows programs. The addition to Google's Safe Browsing API will warn people when they are about to visit Web sites that offer Windows-based trojans disguised as screen savers or other innocuous applications. The company introduced the service 5 years ago to alert users when they try to browse sites that perform drive-by downloads that exploit security vulnerabilities in the operating system or browsing software. The underlying programming interface is already being used by browsers, including Google Chrome, Mozilla Firefox, and Apple Safari. It is also available to any Web master who wants to use the data available from Google to prevent malicious links from being posted to their sites. The new feature will initially be available only for Chrome users who subscribe to the browser's development release channel. The company plans to integrate it into the next stable release of Chrome. There is no mention of it being made available to browser providers outside of Google. The warning will be displayed whenever users encounter a download from a URL that matches the latest list of malicious Web sites published by the Google API.
Source:
http://www.theregister.co.uk/2011/04/05/google_malicious_executables_warning/

47. *April 5, Softpedia* – (International) **New DHL-themed malware distribution campaign in the wild.** Security researchers warn of a new malware distribution campaign that produces e-mails with malicious attachments that pose as delivery notifications from DHL. The rogue e-mails have a subject "DHL Express Services" and their headers have been forged to appear as originating from a @dhl.com address. They inform recipients their package is on its way, and ask them to read the attached document for more information and to obtain the tracking number. The attached document is called dhl(dot)zip and contains an executable file of the same name which is a trojan downloader. This threat is responsible for downloading additional malware including a fake antivirus called XP Home Security, according to Vietnamese security vendor Bkis. Judging from dates of scans and comments on Virus Total for the malicious files involved in this attack, the campaign began sometime the weekend of April 2 and 3. It also appears to have different variations, one using FedEx as cover, probably using similar fake package delivery notifications. Currently, the fake antivirus program installed by this infection has a very low detection count on Virus Total with only 4 in 40 antivirus engines detecting it based on signatures and heuristics.
Source: http://news.softpedia.com/news/New-DHL-Themed-Malware-Distribution-Campaign-in-the-Wild-193187.shtml

48. *April 5, Softpedia* – (International) **Fired Gucci network engineer charged for taking revenge on company.** A computer network engineer who worked for Gucci America has been indicted after hacking into his former employer's computer systems and damaging data, Softpedia reported April 5. According to prosecutors, while working at Gucci, the 34-year-old Jersey City, New Jersey man created a VPN USB token in the name of a fictional employee. After being fired in May 2010, the man contacted the company's IT department posing as that employee and asked for his token to be

activated. In the months that followed, the man used his knowledge to repeatedly cause damage to Gucci's operations by disabling servers, locking documents, and deleting e-mails. In one instance November 12, 2010, during the course of 2 hours, he deleted several virtual servers, shut down a storage area, and wiped clean an entire disk from the company's e-mail server. These actions have resulted in severe disruptions to daily activities, not only for Gucci's staff at the company's Manhattan, New York headquarters, but also store managers across the country who were unable to access their e-mails. The damages sustained by Gucci as a result of loss productivity, attack mitigation, and data restoration is estimated at $200,000. The man has been indicted on 50 counts of computer tampering, identity theft, falsifying business records, computer trespass, criminal possession of computer related material, unlawful duplication of computer related material, and unauthorized use of a computer.
Source: http://news.softpedia.com/news/Fired-Gucci-Network-Engineer-Charged-for-Taking-Revenge-on-Company-193321.shtml

49. *April 4, IDG News Service* – (International) **About 50 clients hit by Epsilon e-mail marketing breach.** About 50 companies were affected by a major security breach at e-mail service provider Epsilon Interactive that caused many U.S. corporations to warn their customers of online attacks April 4. Epsilon first warned of the incident April 1, saying that someone infiltrated company systems and obtained e-mail addresses and names belonging to some of its customers. However, it was not immediately clear how many of its 2,500 clients were at risk. Epsilon still has not disclosed much information about the problem, but it has now given a clearer picture of how many companies are affected. In a brief statement posted to Epsilon's Web site April 4, the company said that "approximately 2 percent of total clients" — about 50 businesses — were hit. Customers of many of these businesses received e-mail warnings April 4, telling them that their e-mail addresses had been stolen, and that spam or malicious messages could be coming their way. So far, Epsilon has refused to provide a detailed list of all companies that were affected. Companies hire Epsilon to send out a total of more than 40 billion messages on their behalf each year. With millions of addresses thought to have been stolen, the problem may be worse than many people realize, security experts said April 4, because once scammers know their victims' names and e-mail addresses, along with the companies that they do business with, they can craft very targeted "spear-phishing" e-mail attacks that try to trick victims into revealing more sensitive information such as passwords or account numbers.
Source:
http://www.computerworld.com/s/article/9215488/About_50_clients_hit_by_Epsilon_e_mail_marketing_breach

For another story, see item **2**

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

50. *April 6, Reuters* – (National) **Verizon customers exposed in massive epsilon data breach.** Customers of Verizon Communications had their e-mail addresses exposed in a massive online data breach the week of March 28, according to an e-mail to customers obtained by Reuters. In what could be one of the biggest such attacks in U.S. history, a computer hacker penetrated the online marketer Epsilon, which controls the customer e-mail databases for a broad swath of companies. Customers of about 50 companies, from banks to retailers and hotels, had their names or e-mail addresses exposed in the attack. Verizon, the largest U.S. mobile phone carrier, informed customers April 5 that it was part of the Epsilon data breach. "Epsilon has assured us that the information exposed was limited to email addresses, and that no other information about you or your account was exposed," Verizon said in an e-mail to a customer sent April 5.
Source: http://www.huffingtonpost.com/2011/04/06/verizon-epsilon-data-breach_n_845379.html

51. *April 5, IDG NEWS Service* – (National) **Verizon simulates disaster near operations center.** It was only a drill, but Verizon Communications' emergency response team brought in its serious equipment for a hazardous materials test in Cockeysville, Maryland, April 4 and April 5. In the scenario, a truck carrying chlorine collided with a light-rail train within a few hundred yards of Verizon's Cockeysville operations center, which provides nationwide customer support for the company's enterprise and federal government customers, dispatches field technicians to Verizon customers in the Baltimore area, and houses support staff. In a real disaster, all 791 employees of the Verizon facility would have to evacuate their building, with the Verizon Major Emergency Response Incident Team's mobile command center, a 51-foot truck trailer, restoring communications at the site. The trailer is a "completely autonomous unit," said the disaster recovery team lead for Verizon. When Verizon arrives at a disaster site, it wants to avoid taxing the local infrastructure, said the chief business continuity officer at Verizon. While the mission of the command center trailer is primarily to restore Verizon networks, it also can provide Internet and radio communications for local emergency response agencies.
Source: http://www.itworld.com/networking/152863/verizon-simulates-disaster-near-operations-center

[Return to top]

Commercial Facilities Sector

52. *April 6, Louisville Courier-Journal* – (Kentucky) **Man dies in French Lick apartment fire.** A man died in a fire at Camelot Courts apartments in French Lick, Kentucky, April 6. The man was a resident of the apartments, located on Maple Street, and occupied the second-floor residence where firefighters believe the fire started shortly after 7 a.m. About 35 other residents of the 3-story complex for the elderly and disabled had to be evacuated. The occupants of the apartments were taken to a nearby senior citizens center and were expected to need emergency housing because of the severity of the smoke and water damage. The fire was reported by a resident at 7:38 a.m. Fire crews from French Lick, West Baden, and three other departments were are on the scene, an Orange County dispatcher said.
Source: http://www.courier-journal.com/article/20110406/NEWS02/304060086/0/NEWS01/35-elderly-disabled-evacuated-from-French-Lick-apartment-fire?odyssey=nav|head

53. *April 6, Orlando Sentinel* – (Florida) **Felon wields sword, guitar in bloody tattoo-shop attack, cops say.** A man is accused of wielding a sword in one hand and a guitar in another when he allegedly attacked a tattoo artist and his customer in Orlando, Florida, April 4. The customer who was attacked in Ace's Tattoo Shop on South Orange Avenue retaliated by slamming a glass tabletop over the head of the assailant, leaving him in a wheelchair with a bloody face and in the Orange County Jail on two counts of attempted second-degree murder. The perpetrator, a 37-year-old homeless felon, also faces two counts of aggravated battery with a deadly weapon and two counts of battery. Corrections records show the man was released from prison in August 2010 after serving a 10-year sentence for a variety of violent crimes.
Source: http://www.orlandosentinel.com/news/local/crime/os-orlando-sword-attack-20110406,0,1078583.story

54. *April 5, Knoxsville News Sentinel* – (Kentucky) **Man's threat of planting dynamite forces evacuation of Knoxville church.** Police evacuated Saint Demetrios Antiochian Catholic Church in Mechanicsville, Kentucky, and blocked off surrounding streets for about an hour April 4 after a homeless man claimed to have planted a stick of dynamite inside. The 48-year-old man now is being held at the Knox County Detention Facility in lieu of $21,000 bond on charges of making a false report and disrupting a meeting or procession, according to jail logs. Knoxville, Tennessee, Police Department officers were called to the church at 2100 Middlebrook Pike at about 6:30 p.m. after the man made the explosive claim to police and EMS workers already called to the scene. The church was hosting its weekly Monday night dinner for about 35 to 40 homeless people when the man approached the parish priest. The man, who appeared intoxicated, then asked him to call an ambulance, the priest said. The man told responding police and emergency medical workers he had placed dynamite in the church attic in an attempt to kill himself, according to a court affidavit. He later claimed he had not left the explosive inside, but that someone else had. The small church was evacuated and all

lanes of Middlebrook Pike, along with several nearby side streets, were shut down until officers had searched and verified that the building was clear.
Source: http://www.knoxnews.com/news/2011/apr/05/mans-threat-planting-dynamite-forces-evacuation-kn/

55. *April 4, WPDE 15 Florence* – (South Carolina) **Device found in Bennettsville apartment building.** Police have charged a Bennettsville, South Carolina man with manufacturing an improvised explosive device after a device was found in the basement of an apartment complex, WPDE reported April 4. Bennettsville police called in the State Law Enforcement Division's (SLED) bomb squad to investigate a possible explosive device at an apartment complex on Market street. Police told WPDE that around noon, someone moving into the apartment found a suspicious device in the basement of the building. SLED used a robot to retrieve the device. The robot took the device to a safe location, put it in a hole in the ground, and used a small explosive charge on the device to detonate and destroy it. Police said the suspect was once a resident at the apartment but had been evicted.
Source: http://www.carolinalive.com/news/story.aspx?id=600983

For more stories, see items **1**, **3**, and **30**

[Return to top]

National Monuments and Icons Sector

56. *April 6, Associated Press* – (Texas) **Critical wildfire danger in Texas through Sunday.** Bulldozers and airplanes are on alert as Texas faces an increased threat for wildfires. The Texas Forest Service said hot weather, extremely dry vegetation, and widespread drought are combining to create dangerous fire conditions through April 10. The agency said the threat is high for wildfires west of Interstate 35, including the Western and Southern Plains, the Trans Pecos, and the Hill Country. Agency firefighters have battled more than 600 fires burning 70,000 acres in 2011. That compares to less than 150 fires burning about 5,200 acres in 2010. On April 4, crews contained a 27-acre wildfire in a small border town near Laredo, but not before it destroyed four homes and damaged several others. No injuries were reported in the fire in El Cenizo.
Source: http://www.chron.com/disp/story.mpl/ap/tx/7509150.html

57. *April 6, Fort Collins Coloradoan* – (Colorado) **Residents evacuated again because of Crystal Fire.** Authorities ordered a new round of evacuations late April 5 as the 3,200-acre Crystal Fire west of Fort Collins, Colorado, flared up in the day's warm temperatures and high winds. About 21 residences south of the main burn area and an unspecified number of homes north of the burn area were ordered to be vacated overnight. Residents who left were barred from returning. Cooler, calmer weather forecast for April 6 might give firefighters a chance to gain the upper hand with help from water-dropping helicopters, officials said. Evacuations were ordered for residents of Moondance Way, Stringtown Gulch, Redtail Way, Ohana Way, Lightning Ridge

Way, Deep Path Way, and lower Wildsong Roads at about 6:30 p.m. due to increased fire activity driven by high winds. The fire, which began April 1 or 2, is still estimated at 3,200 acres and 15 percent containment. Authorities April 3 ordered about 330 homes evacuated, then permitted residents to return later that evening but warned they might have to evacuate again. About 300 firefighters and 25 fire engines were working on the Crystal Fire April 5, but helicopters that could have doused the flames with retardant were grounded because of the winds in the afternoon, the incident commander of the Rocky Mountain Incident Management Team said.
Source: http://www.coloradoan.com/article/20110406/LOVELAND01/110405029

[Return to top]

Dams Sector

58. *April 6, KPAX 8 Missoula* – (Montana) **Repairs almost done on dam damaged by bus-sized boulder.** Repairs to the Madison River dam just below Ennis Lake in Ennis, Montana are nearly complete, according to PPL Montana. New gates and the structure supporting them can be seen at the far end of the dam. Last October a bus-sized boulder split off of the nearby cliff and fell on the dam. While the accident did not endanger any people or homes downstream, it caused water levels in Ennis Lake to drop quickly. A PPL spokesman said just removing the huge boulder was a large part of the project. "We drilled holes in the rock and put this pasty grout mixture in these holes and as it dries, it expands and that literally cracks the rock into smaller pieces," the PPL Montana director of external affairs said. Those smaller pieces were then placed in the river downstream of the dam. To make sure more boulders will not fall, PPL drilled holes and installed rods to hold the cliff face steady. The director said there is a good snowpack this year so he expects Ennis Lake to return to normal levels this spring, and for flow on the Madison River to be strong all season.
Source: http://www.kpax.com/news/repairs-almost-done-on-dam-damaged-by-bus-sized-boulder/

59. *April 5, Modesto Bee* – (California) **Flood emergency declared over Stanislaus County weakened levee.** Alarmed at a weakened levee on the San Joaquin River, Stanislaus County, California supervisors declared a state of flood emergency April 5. Damages "could run into millions of dollars," the county chief executive officer said, and the declaration could clear the way for state and federal financial relief if the governor agrees. The levee was not identified in a nonagendized item that supervisors agreed to hear because of its urgent nature, but the supervisor said it is near Gomes Lake. The area north of Crows Landing Road and west of Carpenter Road normally is dry-to-marshy, but swells into a larger body of water during wet seasons. Rising water has eroded 8 feet into the levee; with 30 feet of earth remaining, it's probably not an "imminent threat" but must be closely watched, he said. A breach would threaten 7,000 acres of farmland and 10,000 head of dairy cattle. Officers with Reclamation District 2063, which is responsible for the levee, proclaimed an emergency March 31, but notice of the declaration did not arrive until April 4. Flooding has forced evacuation of trailer parks and could damage county parks, roads and bridges, and the water may not

recede before July, officials said. Beautiful spring weather could actually increase flooding threats because extraordinary snowpack in the mountains could thaw, sending more water into the already saturated valley.
Source: http://www.modbee.com/2011/04/05/1631003/stanislaus-county-flood-emergency.html

[Return to top]

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/iaipdailyreport

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