Homeland Security

Daily Open Source Infrastructure Report for 29 March 2010

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- The Oregonian reports that police in Molalla, Oregon are looking for burglars who broke into the city's water-treatment plant and stole the system's computer. The city administrator said the computer, later found destroyed, contained all the programming that kept the water-treatment plant working on autopilot. (See item **30**)
- According to IDG News Service, a networking error has caused computers in Chile and the United States to come under the control of the Great Firewall of China, redirecting Facebook, Twitter, and YouTube users to Chinese servers. (See item **46**)

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. *March 26, Associated Press* – (Vermont) **Vt. electric utility offers reward in copper theft.** Vermont's largest electrical utility is offering a $1,000 reward to help find out who cut their way into a Bennington substation to steal copper ground wire. A Central Vermont Public Service Corp. spokesman says the theft was discovered Thursday morning by workers performing routine maintenance at the Lyons Street substation. He

says the value of the stolen copper was probably about $40, but the loss of the ground wire could have threatened anyone nearby with severe electrical shock or death. He says service to about 475 area customers was disrupted for about 20 minutes while workers repaired the damage. Repairs cost an estimated $2,000.
Source: http://www.rdmag.com/News/FeedsAP/2010/03/energy-vt-electric-utility-offers-reward-in-copper-theft/

[Return to top]

Chemical Industry Sector

Nothing to report

[Return to top]

Nuclear Reactors, Materials and Waste Sector

2. *March 26, Associated Press* – (National) **Commission begins 'daunting' task on nuclear waste.** A commission charged with coming up with recommendations on how to store the nation's nuclear waste has started what the co-chairman calls its "daunting task." The co-chairman, a former Democratic congressman from Indiana, is co-chairing the commission with a former National Security Adviser. The commission began its meetings Thursday as some in Congress criticize the Presidential administration for abandoning Yucca Mountain in Nevada as a permanent nuclear waste repository. A House resolution was introduced this week expressing disapproval of the move. The Energy Secretary told commission members to look to the future and not to review whether the Yucca decision was a good one. He said the panel is "not a siting commission."
Source: http://www.lasvegassun.com/news/2010/mar/26/commission-begins-daunting-task-on-nuclear-waste/

3. *March 26, San Diego Union-Tribune* – (California) **San Onofre plant managers say they are fixing problems.** Operators of the San Onofre nuclear power plant faced a skeptical public and hard questions by regulators this week about when the plant is going to fix long-standing weaknesses in its safety culture. Plant managers admitted the plant has problems but told Nuclear Regulatory Commission (NRC) officials that they have established new procedures to fix them. The NRC and representatives of Southern California Edison, the plant's operator, held a public meeting Wednesday at the Doubletree Guest Suites in Dana Point. About 175 people — many of them plant workers — attended. The NRC issued two letters this month, one citing a "chilling effect" at the plant that said plant workers feared retaliation if they raised concerns about nuclear safety issues.
Source: http://www.signonsandiego.com/news/2010/mar/26/san-onofre-plant-managers-say-they-are-fixing/

4. *March 26, Rutland Herald* – (Vermont) **Yankee says it stopped tritium leaks.** Entergy Nuclear said Thursday it is convinced it has found and stopped the source of multiple radioactive leaks at the Vermont Yankee nuclear reactor, which has been leaking tritium into the groundwater since last November. The company said it was starting cleanup efforts immediately, by pumping some groundwater out of the immediate contaminated area into holding tanks, with plans to filter and clean it and return it to the reactor for reuse. The Entergy Nuclear Executive vice president of operations said at a press conference the company was "embarrassed" by the leak, and labeled it "unacceptable." He vowed that Vermont Yankee officials planned on making the Vermont case a model to other Entergy Nuclear plants facing similar tritium leaks. The company said it still didn't know how long the pipes had been leaking or how much contaminated water escaped from the plant. But the company stressed that no drinking water sources had been contaminated, and that tritium was less of a threat to public health than other types of radioactivity. The vice president of operations said the company wanted to regain Vermonters' trust and hoped to convince state leaders to endorse another 20 years of operation for the Vermont reactor, whose current federal license expires in exactly two years.
   Source:
   http://www.rutlandherald.com/article/20100326/NEWS04/3260352/1003/NEWS02

5. *March 24, Star News* – (New Jersey) **Brunswick Nuclear Plant taking slow steps to contain radioactive isotope.** Progress Energy's plans to make sure tritium found at Brunswick Nuclear Plant stays on the power plant site are moving forward, about a year behind the schedule proposed two years ago. A radioactive isotope of hydrogen, tritium is produced naturally in the upper atmosphere when cosmic rays strike nitrogen molecules in the air. It is also produced during nuclear weapons explosions and as a byproduct in nuclear reactors. Leaks containing tritium have occurred at 27 of the 104 U.S. commercial reactors, a Nuclear Regulatory Commission (NRC) spokesman said. "In the grand scheme of radiation, (tritium's relative risk) is well down the scale. But in the area of public perception, it takes on great significance," the NRC Chairman said in mid-February speech.
   Source:
   http://www.starnewsonline.com/article/20100324/ARTICLES/100329857?Title=Brunswick-Nuclear-Plant-taking-slow-steps-to-contain-radioactive-isotope

[Return to top]

Critical Manufacturing Sector

6. *March 26, Port Huron Times Herald* – (Michigan) **Fire causes smoke damage at factory.** A piece of fiberglass caught fire at International Automotive Components Thursday night, the Port Huron Fired Department Captain said. He said the product did not load properly and caused a fire in the machine's heating element. The fire was put out quickly but the building sustained smoke damage, he said. He said the piece of equipment, worth about $1 million, needs repair and will not be in service.
   Source:

http://www.thetimesherald.com/article/20100326/NEWS05/100326002/Fire+causes+smoke+damage+at+factory

7. *March 26, USA TODAY* – (National) **Data analysis shows Toyota tops speed control complaints.** In a pattern almost unbroken since 2004, speed control problems are a higher proportion of Toyota's driver complaint filings than they are for other big automakers, a USA TODAY analysis of National Highway Traffic Safety Administration data from 2000 to mid-March of this year has found. The analysis showed 11.7 percent of the vehicle components named in driver complaints to NHTSA about Toyota-made vehicles in that period were in the safety agency's "vehicle speed control" category. That is the NHTSA complaint category that covers most incidents of unintended acceleration, the problem underlying Toyota's huge recalls in recent months. The five others among the top six automakers in the U.S. market ranged from General Motors' 2.2 percent to Ford's 4.8 percent over the decade. The analysis excluded the "cruise control" category that is one of several "speed control" classifications. Those weren't directly related to the current issue of stuck gas pedals. The analysis is similar to an approach used by safety officials to spot troubling trends. It suggests that Toyota's problems with sticking and jammed gas pedals could have been spotted earlier. Toyota said that it disputes USA TODAY's analysis, because the NHTSA data are polluted by what Toyota says would be "a variety of non-UA (unintended-acceleration) events" listed in NHTSA's "vehicle speed control" category. The automaker said it "disagrees with both the methodology and implications suggested by USA TODAY's analyses," and said, "Toyota has substantially superior performance in terms of complaints to NHTSA." Jammed and sticking gas pedals have forced Toyota to recall millions of vehicles and to appear before often-hostile committees of the U.S. House and Senate the past few weeks whose members questioned whether the recalls should have been sooner and should cover more vehicle models. The problems also have tarnished Toyota's quality image and led it to offer dramatic incentives to recapture sales lost over safety worries.
Source: http://www.usatoday.com/money/autos/2010-03-26-toyota26_CV_N.htm

[Return to top]

Defense Industrial Base Sector

8. *March 25, San Diego News Network* – (California) **120K in equipment stolen from defense contractor.** About $120,000 in equipment was stolen from a defense contractor in Logan Heights, police said Thursday. The theft from Surface Technologies Corporation was reported at 11 a.m. Wednesday, said a San Diego police Officer. The company specializes in the interior and exterior coating and non-skid surfacing of Navy ships, according to its Web site.
Source: http://www.sdnn.com/sandiego/2010-03-25/local-county-news/120k-in-equipment-stolen-from-defense-contractor

[Return to top]

Banking and Finance Sector

9. *March 26, Wall Street Journal* – (National) **More than a dozen banks suspected co-conspirators in Muni case.** More than a dozen banks and investment firms are suspected co-conspirators in a criminal probe by the Justice Department's Antitrust Division into alleged bid rigging and price fixing in the municipal derivatives market, according to a court filing. The list of banks was inadvertently filed earlier this week in U.S. District Court in Manhattan as part of a request for a bill of particulars in a criminal case against three former executives of CDR Financial Products Inc., a California municipal-bond broker. The executives, including the founder of CDR founder, were indicted in October on conspiracy and fraud charges. They have denied wrongdoing. In a letter on March 26, the lawyers asked a U.S. District Judge, who is hearing the criminal case, to strike the inadvertent filing. The banks and investment firms include units of J.P. Morgan Chase & Co., UBS AG, Citigroup Inc., Wells Fargo & Co., Bank of America Corp., General Electric Co. and Societe Generale. None of the alleged co-conspirators have been accused of criminal wrongdoing.
Source:
http://online.wsj.com/article/SB10001424052748704100604575145462475982000.html

10. *March 25, SCMagazine* – (National) **Hacker Albert Gonzalez receives 20 years in prison.** A notorious credit card hacker received, on March 25, the largest-ever U.S. prison sentence for a hacker. The 28 year old, of Miami, Florida, was sentenced to 20 years in prison for leading a group of cybercriminals that stole tens of millions of credit and debit card numbers from TJX and several other retailers. He pleaded guilty in September to multiple federal charges of conspiracy, computer fraud, access device fraud and identity theft for hacking into TJX, which owns T.J. Maxx, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble and Sports Authority. He was facing up to 25 years in prison for these charges. He also pleaded guilty last year in two other pending hacking cases for which he is scheduled to be sentenced on March 26. He faces up to 20 years in prison for his role in hacking into the network of Dave & Buster's restaurant chain and stealing credit and debit card numbers from at least 11 locations. As part of a third pending case, he faces between 17 and 25 years in prison for hacking into the payment card networks of Heartland, 7-Eleven and Hannaford Bros. supermarket chain to steal more than 130 million credit and debit card numbers. In a plea deal, his sentences will run concurrently to each other.
Source: http://www.scmagazineus.com/hacker-albert-gonzalez-receives-20-years-in-prison/article/166571/

11. *March 25, Reuters* – (National) **Dave and Buster's settles credit card security charges.** The entertainment and restaurant chain Dave and Buster's Holdings Inc has settled charges the company failed to adequately secure the credit and debit card information of customers, the Federal Trade Commission said on March 25. The company, which has 53 restaurants, was hacked in mid-2007 by an intruder who installed unauthorized software and intercepted data sent from the restaurants to credit card processing companies, the FTC said. About 130,000 credit and debit cards were

affected, with affected banks paying out "several hundred thousand dollars in fraudulent charges," the FTC said in its complaint. "After learning of the breach, respondent (Dave and Buster's) took steps to prevent further unauthorized access and to notify law enforcement and the credit card companies of affected consumers," the complaint said. The settlement requires Dave & Buster's to put in place a comprehensive security program.
Source: http://www.reuters.com/article/idUSN2522698920100325

12. *March 25, SC Magazine* – (International) **FSA investigation leads to insider trading arrests, as Oracle claims that IT systems can increase the levels of protection.** Employees of three major banks have been arrested on a charge of running an insider-dealing scheme. According to BBC News, the investigation is a joint venture between the Financial Services Authority and the Serious Organised Crime Agency (SOCA). It claimed that employees from Deutsche Bank, BNP Paribas and hedge fund Moore Capital are now known to have workers caught up in the investigation. The vice president of marketing at Oracle Financial Services global business unit, claimed that this incident shows that there is a need for IT security solutions that are suitable for use within the financial sector.
Source: http://www.scmagazineuk.com/fsa-investigation-leads-to-insider-trading-arrests-as-oracle-claims-that-it-systems-can-increase-the-levels-of-protection/article/166468/

13. *March 25, Fort Morgan Times* – (National) **Nationwide scam linked to Eben Ezer bank account.** Within the last several weeks, administrators at Eben Ezer Lutheran Care Center in Brush, Colorado have received dozens of calls from people who have received counterfeit checks linked to an Eben Ezer bank account as part of a nationwide scam. Those who received the fake checks for up to $29,000 were told that they won a sweepstakes, and that the checks were reimbursements for the taxes they were to pay on a larger sum of prize money that would be sent later. "All the paperwork that's coming with it doesn't say anything about Eben Ezer," said the facility chief finance officer. The people who received the phony checks were directed to send the tax payments directly to a bogus "personal receiving agent" to process the funds. Presumably, this would allow the scammers to pocket the real cash before the fake checks are rejected by Eben Ezer's bank, the Bank of Colorado in Brush. The phony checks have been sent to individuals in several states, including Texas, Ohio, Minnesota and Florida.
Source: http://www.fortmorgantimes.com/ci_14755700

14. *March 25, Courthouse News Service* – (Ohio) **Bank abetted $15M Ponzi, investors say.** Huntington National Bank aided and abetted a $15 million Ponzi scheme run by a felon who had already pleaded guilty to bank fraud, according to a complaint in Cuyahoga County Court, Cleveland. Seventeen investors say the bank put a hold on the suspect's accounts after finding out he had just been released from prison for bank fraud, then inexplicably released the money to him. The suspect promised about 250 investors 10 percent annual returns on Serengeti Diamonds USA and Lomas de la Barra Development, according to the complaint. The investors say the suspect used his

daughter, a teller, to open two bank accounts in 1998 that were "facially deficient." The only defendant in this complaint is the Huntington National Bank. The plaintiffs say the bank refused the suspect's requests to send money from his accounts offshore, in January 1999, but relented and went ahead with it after the suspect threatened it. The investors say the bank did it although it already knew the suspect was a felon.
Source: http://www.courthousenews.com/2010/03/25/25874.htm

15. *March 25, Bloomberg* – (National) **U.S. Treasury said to have plan for Citigroup shares.** The U.S. Treasury intends to unload its 27 percent stake in bailed-out bank Citigroup Inc. using a preset trading plan that will lock the government into a schedule for selling its shares, people with direct knowledge of the matter said. The program, which may be announced next month, is similar to those used by executives to protect themselves against accusations of insider trading, said the people, who asked not to be identified because the process isn't final. The Treasury would be able to issue instructions on how many shares to sell, when to sell them and at what price while eliminating concern that the sales are based on non-public information. A sale of the Treasury's shares, which could be completed this year, would bring Citigroup a step closer to exiting the government's Troubled Asset Relief Program. The firm had to get a $45 billion infusion of taxpayer money in late 2008 as withering confidence in the bank almost triggered a deposit run.
Source:
http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aqx4cZV8zhYM

16. *March 24, Reno Gazette Journal* – (National) **Utah police arrest suspected ATM skimmers; may be related to Reno-Sparks cases.** A Utah police department has arrested two men on charges they illegally hooked up devices to gas station pumps to collect ATM personal identification numbers from unsuspecting customers there. Authorities are trying to determine if the two men arrested in Richfield, Utah, are connected to ATM card skimming in Reno and Sparks in January and February. Local authorities received more than 100 complaints. Arrested on on March 19 by the Richfield Police Department were a 55 year old, of Burbank, California, and a 27 year old of Van Nuys, California. They were booked into the Sevier County jail in central Utah on $250,000 bail on 16 felony counts related to the alleged attempted ATM card skimming. A Reno Police Department lieutenant said there was a similar arrest in Benecia, California, about three weeks ago and the ATM skimming thefts stopped in Reno after that arrest. "I'm pretty certain that it was related to the one in this area," an investigator said of the Benecia case. "According to the information, it was the whole west coast group so I'm assuming it's the whole group involved."
Source: http://www.rgj.com/article/20100324/NEWS01/100324011/1321/news/Utah-police-arrest-suspected-ATM-skimmers-may-be-related-to-Reno-Sparks-cases

For another story, see item **31**

[Return to top]

Transportation Sector

17. *March 26, Associated Press* – (New Mexico) **Heart attack prompts jetliner's emergency landing.** A Boeing 737-800 carrying 167 people made a safe emergency landing in New Mexico after a passenger suffered a heart attack. A Continental Airlines spokeswoman says Continental Flight 602 from Newark, N.J., to Los Angeles landed at Four Corners Regional Airport in Farmington late Thursday afternoon to assist the stricken 70-year-old man. The Four Corners Airport Manager says that while the plane landed on 6,500-foot runway without any problems, it wasn't long enough for it to safely take off again. Officials say the aircraft loaded with luggage and cargo coupled with the airport's mile-high elevation and runway distance made the takeoff inadvisable. Luggage was put on a different plane and the Boeing and its passengers continued to Los Angeles after about a three hour delay. The Farmington Daily Times reported that authorities said the man had a heart attack. He was hospitalized but his name and condition weren't available.
Source: http://www.forbes.com/feeds/ap/2010/03/26/general-us-emergency-landing_7467180.html

18. *March 26, Associated Press* – (Hawaii) **Honolulu rail planners knew of airport issues in 2006, state says.** Honolulu's proposed rail-transit project needs to be conducted with "a higher level of transparency," the state Department of Transportation said yesterday as it made public all its correspondence on the issue. "There is a lot of misinformation out there about the Honolulu rail-transit project and the public deserves to know all the facts," said a state DOT director. The state's release of five letters to the city and two other documents was partially driven by statements from city officials that the rail line's encroachment on airspace at the Honolulu International Airport was not brought to the attention of the city until mid-2009, the director said. The airport encroachment issue must be resolved before the start of construction on the $5.3 billion, 20-mile elevated rail line from East Kapolei to Ala Moana. The issue with the airport could have been addressed by the city sooner, the director said. "In 2006, our first letter indicated that they should be aware of runway issues in the Lagoon Drive area, so we have continually offered our assistance and willingness to meet with the city on numerous occasions ," he said. "There has been more than ample time for these issues to be addressed in the timeframe that the city had hoped to go out to bid and start construction. To date, the (project's environmental impact statement) ... has not addressed those concerns." Under current plans, the elevated train track and a station near the intersection of Aolele Street and Lagoon Drive would be at least four stories tall and about 1,300 feet from airport runways. That encroaches on a runway airspace buffer designed to keep buildings and other obstructions from affecting airplane operations.
Source:
http://www.honoluluadvertiser.com/article/20100326/NEWS01/3260360/Honolulu+rail+planners+knew+of+airport+issues+in+2006++state+says

19. *March 26, WGMD 92.7 Rehoboth Beach* – (Virginia) **Coast Guard responds to train derailment in VA.** Coast Guard pollution responders along with local fire departments are responding to a train derailment off the A&C Canal Bridge on the intracoastal waterway between the Great Bridge bypass and Centerville turnpike in Chesapeake,

Va., this morning. Watchstanders at Sector Hampton Roads received a call at 5 a.m., from a representative of the Chesapeake-Albermarle train company stating their train had derailed and was leaking fuel into the waterway. Coast Guard pollution investigators, Chesapeake, Virginia Beach, and Newport News fire departments are currently on scene to help contain approximately 1,700 gallons of the diesel fuel spill. No injuries have been reported. The waterway remains closed until further notice.
Source: http://www.wgmd.com/?p=1781

[Return to top]

Postal and Shipping Sector

20. *March 25, Associated Press* – (Texas) **2nd apparent pipe bomb found in east Texas mailbox.** An object resembling a pipe bomb was found in a mailbox in front of a small east Texas post office Thursday, the second such incident in three days, authorities said. Federal officials have acknowledged that they are investigating a series of apparent incendiary devices placed in east Texas mailboxes in the past month. Authorities said the device found March 25 in Troup, about 100 miles east of Dallas, appeared similar one found March 23 in a collection box in front of a post office in Laird Hill, 20 miles to the northeast. A postal employee found the Troup device about 1 p.m. "The employee went to collect the mail and found the device," the police chief told the Tyler Morning Telegraph. "They then notified us. We secured a perimeter and called the ATF." Postal inspectors and ATF agents summoned a bomb-disposal team. Further details about the device were not available as of early evening. An ATF official and a U.S. Postal Inspector declined to estimate the number of apparent incendiary devices found in mail collection boxes around east Texas in the past month, but reports from various law enforcement agencies put the number at at least 11.
Source: http://news.yahoo.com/s/ap/20100326/ap_on_re_us/us_mailbox_explosives

21. *March 25, Metro International; Reuters* – (New York) **Rep. Weiner gets powder in the mail.** A New York democratic Representative was targeted for his support of the President's health care bill on Thursday afternoon when his Kew Gardens, Queens, office received a package of white powder and a "threatening letter." "My first priority is the safety of my staff and neighbors, and the authorities are currently taking steps to investigate and resolve the situation," he said in a statement. The substance was deemed nonhazardous in an NYPDâ ˆfield test. Nine people who were exposed to the package were decontaminated. The office was closed as local and federal law enforcement officials investigated the incident. At least 10 Democrats have been threatened over the health care bill. â ˆA democratic Representative from Buffalo received a phone threat of a sniper attack and a brick was thrown through the door of her Niagara Falls office.
Source: http://www.metro.us/us/article/2010/03/26/04/1132-82/index.xml

22. *March 23, Bio Prep Watch* – (Missouri) **Missouri man pleads guilty to anthrax hoax.** A St. Genevieve, Missouri, man has pleaded guilty to sending a letter to a U.S. Senior Judge of the Eighth Circuit of Appeals containing white powder and a

threatening letter. The suspect was sentenced eight years in federal prison for threatening to kill a U.S. Senior Judge in a threatening letter sent to the Judge's office at the federal courthouse in Lincoln, Missouri on July 13. The letter threatened to kill beam and said that enclosed white powder was anthrax. A subsequent investigation revealed that the powder was not anthrax. The suspect's name and return address were on the letter and an investigation by the FBI determined that he was the source of the letter. The suspect, at the time, was a convicted sex offender being held at the Ste. Genevieve County Detention Center. Investigators learned during an interview that the suspect was angry with the Judge over how cases involving some of the suspects' friends and associates were handled by the Judge. Authorities also believe, based on other correspondence, that the suspect's motivation for threatening the Judge was to be moved from the Missouri prison system to a federal facility. Sentencing for the suspect took place on Monday. He was returned to custody in Missouri for further proceedings, the U.S. Attorney's Office said. The eight year federal sentence will follow the completion of his state sentence currently being served in Missouri.
Source: http://www.bioprepwatch.com/news/212550-missouri-man-pleads-guilty-to-anthrax-hoax

[Return to top]

Agriculture and Food Sector

23. *March 26, Calgary Herald* – (International) **Grocery stores step up security after food tampering.** Calgary grocery stores are ramping up security and safety precautions amid this week's rash of new food tampering incidents at three Sobeys outlets. "This is a top priority now for all our stores," said a Canada Safeway spokeswoman. "And while we haven't had any incidents in Safeway, it makes us no less vigilant. When it comes to food safety, our industry is one and we all have to take precautions." Safeway managers held meetings Thursday, discussing ways to beef up security. Security staff rotations have been increased, while managers have been asked to spend more time on the floor, monitoring staff and customers. Staff working in produce and bakery departments have been asked to be vigilant, checking food often, looking for suspicious people and conversing with customers to ensure they are regular customers and food is safe. All local Sobeys stores held several "checkpoint" meetings throughout the day Wednesday with managers and staff, reminding them to increase their food-checking practices. A company spokesman said, "Visual inspections are really important...does food look like it's been tampered with, disrupted?" Police are investigating three new incidents of food tampering at Sobeys stores in the south one week after charges were filed in a similar case at the Oakridge Co-op. A 43-year-old mother of two, was charged with mischief in connection with the Co-op case. The three tampered items found this week were purchased at Sobeys in Cranston, McKenzie Towne and Millrise. This time, the objects inserted were a pin, a nail and a small metal spring, inserted into an avocado and kaiser buns, according to police. These incidents are especially worrisome, say police, since the objects were buried in the food, whereas at the Co-op, the pins were more obvious.
Source:

http://www.calgaryherald.com/health/Grocery+stores+step+security+after+food+tampering/2728436/story.html

24. *March 25, Columbus Dispatch* – (Ohio) **Egg farm fire accidental, investigators determine.** A fire that caused at least $2.5 million worth of damage this week at the Ohio Fresh Eggs farm in Wyandot County appears to have been accidental. The state fire marshal's office wrapped up its investigation today and did not find evidence of a crime. Investigators were unable to identify a cause but said electrical components might be to blame. "The fire is likely going to be ruled undetermined," a spokesman said. The blaze started in a warehouse at the chicken farm overnight Tuesday in an area used to store plastic and foam shipping containers and materials. When firefighters arrived, they cut power to the chicken barns and ventilation systems to keep the flames from spreading. The conditions inside two of the farm's 14 barns rapidly deteriorated. On Wednesday, an environmental inspector for the Agriculture Department and Ohio Environmental Protection Agency personnel visited the farm, about 70 miles north of Columbus, to ensure that the 1 million gallons of water used to fight the fire were contained. A culvert was plugged with clay soil to collect the runoff water in a ditch, the spokesman said. He said the contaminated water will be pumped out, stored in a lagoon and used to irrigate fields for growing crops. Business resumed today in the undamaged barns, which were operating at full power, an Ohio Fresh Eggs spokeswoman said. The company processes ingredients for pet food and animal feed.
Source: http://www.dispatch.com/live/content/local_news/stories/2010/03/25/egg-farm-fire-accidental.html?sid=101

For another story, see item **28**

[Return to top]

Water Sector

25. *March 26, Kansas City infoZine News* – (Missouri) **Wastewater spill near Walnut Lake.** The City of Kansas City, Missouri, Water Services Department and the Missouri Department of Natural Resources report that Pied Creek Pump Station discharged an estimated 50,000 gallons of partially treated wastewater into a tributary approximately three miles from Walnut Lake. The overflow occurred due to the equipment malfunction at the pump station. The City's drinking water supply is not affected by this break. The pumps at the station clogged causing the automatic controls at the pump station to malfunction. The overflow was discovered by Water Services Department staff at 8 a.m. on March 24 and ended at 8:30 a.m., returning the pump station to normal operation. The City has posted the affected area to inform residents of the discharge and is working cooperatively with the Missouri Department of Natural Resources to mitigate the impact of this discharge. Water samples have been collected from the affected area.
Source: http://www.infozine.com/news/stories/op/storiesView/sid/40525/

26. *March 26, Kennebec Journal* – (Maine) **Waste-water plant said to be breached.** Gardiner, Maine, city councilors are considering security improvements at the city's waste-water treatment plant. Councilors met in executive session Wednesday to discuss security at the treatment plant "per confidential records." "Due to acts of criminal trespassing, city staff are working with the council to install a more modern security system at our waste-water treatment facility," the town manager said. "As the investigation into these acts is ongoing, the city cannot provide further comment on the matter at this time." He said there is an ongoing investigation by Gardiner police. "The federal government considers [waste-water facilities] a possible terrorist target," he added. "We're just looking at several different security options while trying to stay within constraints of the budget."
Source: http://www.kjonline.com/news/gardinerwaste-water-plant-said-to-be-breached_2010-03-25.html

27. *March 26, WFTS 28 Tampa* – (Florida) **Port Richey residents asked to boil water.** Residents of Port Richey, Florida, are being advised by the city to boil their water after lighting hit the city's water plant over night. The precautionary boil water notice is being issued because the lightning strike knocked out the electronics at the water plant. Officials are working to fix the problems and will advise the residents when the boil water notice has been lifted.
Source: http://www.abcactionnews.com/content/news/local/pasco/story/Port-Richey-residents-asked-to-boil-water/OssFJS6d-E6GYt5I0y2Wyw.cspx

28. *March 26, EastBayRI.com* – (Rhode Island) **Rain overwhelms Bristol sewer system.** Bristol Harbor is closed to shellfishing and the Bristol Wastewater Treatment Facility was running at about three times its normal rate on Wednesday after two rainstorms in a week overwhelmed the town's sewer system. During three heavy days of rain last week, and in another power-packed day of rain on Tuesday, hundreds of thousands of gallons of rainwater and sewage spilled into the streets of Bristol, in some places bubbling through manhole covers. The water overflows occurred at several locations throughout town, the most noticeable at Hope Street and Gooding Avenue. The Wastewater Pollution Control superintendent said overflow occurred because the town's main treatment facility at the south end of Wood Street could not keep up with the volume of water. The water and sewage backed all the way up Hope Street to the area of Gooding Avenue. Other failures occurred at pump stations on Annawamscutt Road, Brookwood Road, Mt. Hope High School and Ferry Road. "We typically do 4, maybe 4 1/2 million gallons a day. This afternoon (Wednesday), we're still doing over 11 million," he said. It may take days for the impact of the latest storm to drain through the system. If the system has not returned to normal by the time another storm arrives, the system could face more stress.
Source: http://www.eastbayri.com/detail/134983.html

29. *March 25, Discovery News* – (National) **Taking showers could contaminate drinking water.** With every shower a person takes, they may be unwittingly polluting the environment. As they scrub off dirt, they also wipe off medicines from their skin and pharmaceuticals excreted in sweat, according to a new study. Those chemicals pass

through the sewage system and might even end up in drinking water. The director of the Institute for Environmental Medicine at the Touro University College of Osteopathic Medicine in Henderson presented her work this week at the American Chemical Society meeting in San Francisco. “If you think about other people exposed to these drugs that are intended for a particular population,” she said, “that could be a concern.” Their research revealed that human skin fails to absorb much of the medicine that is applied topically, such as antibiotic ointments and steroid creams. Showers, baths, and laundry wash those drugs directly into the sewage system. Chemically, these compounds often remain whole, unlike the broken-down versions in feces and urine. The scientists also found that a significant percentage of the medicine we swallow end up coming out in our sweat. Those chemicals go down the drain, too. It is not yet clear how pharmaceutical residues in the environment will affect the health of animals or people, especially because concentrations for now are low. Still, tiny doses can add up after years and years of exposure. It’s a phenomenon that scientists have become increasingly worried about.
Source: http://news.discovery.com/earth/showers-pollution-drinking-water.html

30. *March 25, Oregonian* – (Oregon) **Burglars steal, destroy Molalla water system computer.** Police in Molalla, Oregon, are looking for burglars who broke into the city’s water-treatment plant and stole the system’s computer. The city administrator said theft of the computer is a federal crime and has been reported to the U.S. Department of Homeland Security. He said the computer, later found destroyed, contained all the programming that kept the water-treatment plant working on autopilot. Water quality is unaffected, he said. The only difference is the plant is running in manual-control mode and must be monitored in-person. “And frankly, we can shut off the plant at night because we keep our reservoirs topped off. We have enough water stored that we’d be good for days.” He said he hired a security consultant to “harden” both the water-treatment plant and the sewage-treatment plant against future break-in attempts. On Saturday, an assistant plant operator was on standby duty when an intruder alarm alerted him to the break-in. When he arrived at the plant, he found the plant’s front door open and the computer gone. City staff members immediately began searching Internet sites such as Craigslist and eBay to see whether anyone had put the computer up for sale. The next day, however, the computer and monitor were discovered in the backwash pond at the plant site. The computer and monitor are destroyed. Atkins estimated cash value loss at “less than $1,000.” Computer experts are trying to recover the programming from the hard drive. Police said the burglar gained access to the plant by driving around a fenced and gated area through an adjacent tree farm.
Source:
http://www.oregonlive.com/clackamascounty/index.ssf/2010/03/burglars_steal_destroy_molalla.html

For another story, see item **55**

[Return to top]

Public Health and Healthcare Sector

31. *March 26, Chicago Post-Tribune* – (Illinois) **Private patient information stolen from Northwestern used in massive identity theft.** A group of thieves stole the identities of hundreds of patients at Northwestern Memorial Hospital in Chicago, Illinois, and then spent more than $300,000 on items charged from stores like Jared the Galleria of Jewelry, Victoria's Secret and Lowe's, Cook County's sheriff said Thursday. Some of the ill-gotten purchases were resold for cash, the sheriff said. Others were posted on Facebook, the perpetrators preening in new jewelry and clothing, he said. Charges for all the suspects — three of whom are sisters — range from felony theft to identity theft to organizing a continuing financial criminal enterprise. A number of those charged appeared in bond court Thursday. Working at night,one of the women charged jotted down private patient information from as many as 250 files left in unlocked file cabinets. That information was used to solicit credit reports or for applying to be added on to cardholder accounts. Once given access to the accounts, the shopping sprees began, often in suburban areas where those using the fraudulent account information would claim discrimination if their access to credit was questioned by cashiers, the sheriff said.
    Source: http://www.post-trib.com/news/2123042,identity-theft-ring-bust-women-032510.article

32. *March 26, Boston Globe* – (National) **FDA reviewing Boston Scientific data.** The Food and Drug Administration said it has not completed a review of paperwork the Natick, Massachusetts, company filed after recalling its cardiac defibrillator devices. The FDA expects to complete its review within 30 days, a spokeswoman said. Boston Scientific announced March 15 that it had stopped sales of implantable cardiac defibrillators and was voluntarily recalling the devices because two manufacturing changes had not been submitted for review to the FDA, as required. The FDA says doctors should not use the defibrillators until the changes are approved. A Boston Scientific spokesman had no comment.
    Source:
    http://www.boston.com/business/healthcare/articles/2010/03/26/fda_reviewing_boston_scientific_data/

33. *March 25, Nashville Tennessean* – (Tennessee) **Tennessee officials take control of Springfield-based insurance scam.** State insurance regulators today took control of two Robertson County companies that have been accused of selling illegal health insurance policies to thousands of consumers nationwide. The Tennessee Department of Commerce and Insurance appeared to be in control this morning of the Springfield offices of Smart Data Solutions LLC and American Trade Association. The companies have been accused by insurance regulators in at least 20 states of selling bogus health insurance policies to unspecting consumers nationwide. Court records show a third company, Serve America Assurance, is also linked to the Springfield businesses. Regulators believe it was shell company set up in Bermuda to receive the insurance premiums from Springfield businesses.
    Source: http://www.tennessean.com/article/20100325/NEWS03/100325033/2066

[Return to top]

Government Facilities Sector

34. *March 26, U.S. Army Corps of Engineers Baltimore District* – (Maryland) **Munitions disposal by U.S. Army Corps of Engineers.** In April, the U.S. Army Corps of Engineers (USACE), in partnership with the Environment Protection Agency and the D.C. Department of the Environment, will destroy recovered chemical and liquid filled munitions currently in storage at the federal property located on Little Falls Road using the Army's specially designed Explosive Destruction System (EDS). The EDS operation is expected to approximately two weeks. In accordance with the official decision document also know as the Action Memorandum, USACE started planning the mobilization efforts for the munitions destruction operation. The mobile EDS will be brought to the Spring Valley Project federal property to destroy the recovered chemical munitions and munitions filled with liquid, likely water. The safety measures, including a temporary structure that fully encloses teh EDS, ensure that the EDS operations have no impact on nearby community, Sibley hospital, or the reservoir. Also underway are the equipment mobilization plans for destroying the recovered conventional munitions (non-chemical, non-liquid) currently in storage. The conventional munitions will be destroyed at that location, using the Army's Contained Detonation Technologies later this Spring.
Source: http://www.nab.usace.army.mil/projects/WashingtonDC/springvalley.htm

35. *March 26, Salt Lake Tribune* – (Utah) **11 at Camp Williams seek treatment for possible hazmat exposure.** A reaction between a "weak acid" leaking from a heating system and drywall sickened 11 people at Camp Williams on Thursday morning, prompting a full-scale hazardous materials response and sending the group to a Riverton hospital. The group of civilians and Guardsmen, were working in the Utah Center for Domestic Preparedness Training Facility when they complained of burning throats and noses and watery eyes, said a Unified Fire Authority spokesman. All were released in good health by 2 p.m., said an Intermountain Health Care spokesman. The building has been under renovation recently, the fire authority spokesman said. The acid from the leaking heating system reacted with calcium carbonate in the drywall, creating the irritant, said a Major with the Guard's 85th Civil Support Team. Smith said the incident was reported about 9:30 a.m. UFA immediately dispatched its hazardous materials unit to set up a decontamination operation outside the hospital. Meanwhile, the Guard's Civil Support Team, which specializes in securing and investigating possible chemical exposure scenes, was dispatched to Camp Williams.
Source: http://www.mlive.com/newsflash/health/index.ssf?/base/national-114/1269598556216560.xml&storylist=health

36. *March 26, WHAM 13 Rochester* – (New York) **"Sniper" threats shine light on security.** Public anger over health care reform has not quieted. The FBI is investigating similarities between the brick thrown through Rochester Democratic Headquarters and the one that crashed through the Niagara Falls office of a Congresswoman two days earlier. "I think it's part of a pattern," the Congresswoman says. A voice message

threatening a sniper attack was also left on a campaign phone here. It was found in an office the Congresswoman rarely uses. Her main Rochester headquarters is at the Keating Federal Building. Visitors there must first pass through a metal detector. Other security measures there are slightly more subtle. Planters holding flowers are solid cement blockades which keep vehicles from barreling through the front door. Security guards now patrol 24 hours a day. The Congresswoman said she is comfortable with security in Rochester. "Niagara Falls is the one we're really worried about," she said.
Source: http://www.13wham.com/news/local/story/Sniper-Threats-Shine-Light-on-Security/XuqtsAIFx0OF2jCh1Ubeqw.cspx

37. *March 25, Standard Speaker* – (Pennsylvania) **Hazleton man cited after bomb scare in Scranton.** A Hazleton man left a small, black suitcase at the local Social Security Administration office and then walked away Tuesday, bringing the city's police bomb squad to investigate and prompting a partial evacuation of the Oppenheim Building. The suspect, 40, was taken into custody when he returned to retrieve his suitcase just after the bomb squad rolled a remote-controlled robot into the building at 409 Lackawanna Ave. to remove the suspicious bag. He was cited for disorderly conduct.
Source: http://standardspeaker.com/news/hazleton-man-cited-after-bomb-scare-in-scranton-1.697967

38. *March 25, DarkReading* – (National) **Ninth state department insider found guilty of illegal database access.** A State Department employee was sentenced yesterday to 12 months of probation for illegally accessing more than 60 confidential passport application files, according to the U.S. Department of Justice. The 47 year-old defendant, who hails from Oxon Hill, Maryland, was also ordered by the U.S. Magistrate Judge in the District of Columbia to perform 50 hours of community service. The defendant pleaded guilty on December 11, 2009, to a one-count criminal information charging her with unauthorized computer access. According to court documents, the defendant has worked full-time for the State Department since September 1995 as a file clerk and a file assistant in the Bureau of Consular Affairs. In pleading guilty, the defendant admitted she had access to official State Department computer databases in the regular course of her job, including the Passport Information Electronic Records System (PIERS), which contains all imaged passport applications dating back to 1994.
Source:
http://www.darkreading.com/database_security/security/government/showArticle.jhtml?articleID=224200410

39. *March 24, WVEC 13 Hampton Roads* – (Virginia) **Chesapeake teen charged with making hoax device.** An 18-year-old is charged with making a hoax explosive device. Fire investigators say the March 12 incident forced Western Branch High School to go on lockdown. The suspect, who goes to the school, was arrested Monday and is free on bond. "Someone on the school site found the device and called us. I would describe it as an electronic device with a threatening note attached to it," a spokesman with the Chesapeake Fire Dept. told WVEC.com. It was outside between the existing school building and the on-going construction. The spokesman said the Deputy Fire Marshal

and State Police bomb technicians determined the device was safe and it did not have to be blown up. The charge is a Class 6 felony with a possible penalty of up to 5 years in prison. He faces disciplinary action from suspension to expulsion, said a Chesapeake Schools spokesman.
Source: http://www.wvec.com/home/Teen-charged-with-making-hoax-device-89012717.html

For more stories, see items **21** and **22**

[Return to top]

Emergency Services Sector

40. *March 26, KSL 5 Salt Lake City* – (National) **AT&T mysteriously directs Salt Lake 911 calls to Seattle.** Many AT&T carriers had a big, and potentially life-threatening problem Thursday when emergency calls in Salt Lake City, Utah were redirected to Seattle, Washington. AT&T says the problem was fixed by 11:30 p.m. MDT, but they still do not know exactly what caused it. When KSL News contacted Salt Lake police, they said they thought one emergency caller had misdialed, or that the GPS on his phone was malfunctioning. But then the officers started trying to call from their phones, and they discovered nearly every AT&T phone they tried dialing 911 on was directed to the Seattle dispatch center. Seattle dispatchers said they received multiple calls from Salt Lake City all day. Before the problem was resolved, Salt Lake police were advising cell phone users to call the local dispatch number instead of 911 if they had an emergency.
Source: http://www.ksl.com/?nid=148&sid=10149938

41. *March 26, KLEW 3 Lewiston* – (Idaho) **Upgrade will improve emergency communications in Asotin County.** The Asotin County Fire District is working to safeguard emergency communication. Three years ago the district was awarded a grant through FEMA for $234,000 to create a system to make sure communication with emergency dispatch is always available. “Once it is all up and running there will be a redundant system in place, that connectivity will always be there and so we’re excited about that,” said Asotin County’s fire chief. “When we need to talk to dispatchers we need to be able to do that. It doesn’t necessarily affect the 911 system, those calls are always going to come in when you dial 911, this is primarily for our radio traffic with Whitcom.” The fire chief said other communication systems could be added to the tower, located behind the fire district. Currently the tower is used in partnership with Inland Cellular.
Source: http://www.klewtv.com/news/local/89074412.html

42. *March 25, Popular Mechanics* – (National) **Medical helicopters need better safety standards—now.** The medical helicopter industry has more than tripled in size over the last two decades, expanding from 200 helicopters in 1988 to 668 in 2008. While the pilots and crew endeavor to save lives, they also put their own at risk: flying to the scenes of accidents in often remote, dark locations, landing not on pads but in fields

and on streets. But though the industry is the most dangerous sector of commercial aviation, it operates with some of the least safety regulation. Officially, "â ¦the pilot is responsible for [the] safety of [the] aircraft and deciding whether to go forward or not," a spokeswoman for the Federal Aviation Administration, told CNN within hours of the crash. In other words, if he crashes, it's his fault. Helicopter ambulances have crashed 149 times since 1998, killing 140 people and seriously injuring dozens more. An industry created to save lives actually has the highest rate of fatal accidents in all of commercial aviation. In fact, working onboard a medical helicopter is the most dangerous profession in America, with a higher risk of death than fishermen, steel workers or loggers.
Source:
http://www.popularmechanics.com/science/air_space/4350249.html?nav=RSS20&src=syn&dom=yah_buzz&mag=pop

43. *March 25, CNN* – (Tennessee) **FAA: 3 dead in medical helicopter crash.** Three people died Thursday when a medical helicopter crashed in western Tennessee, the Federal Aviation Administration said. The helicopter had dropped off a patient in Jackson, Tennessee, and was returning to Brownsville, Tennessee, about 30 miles west of Jackson, when the crash was reported, said an FAA spokesman. The Tennessee Emergency Management Agency spokesman said the crash occurred shortly after 6 a.m. Three people were initially reported to be on board the helicopter. All three were believed to be fatalities, as the aircraft — a Eurocopter AS350 — was burned.
Source: http://www.cnn.com/2010/US/03/25/helicopter.crash/?hpt=Sbin

44. *March 25, Eureka Times-Standard* – (California) **Humboldt officials say few glitches in tsunami test.** Officials said Wednesday's tsunami warning communications test uncovered a few technical glitches, but was otherwise successful. The test — a collaboration between the California Emergency Management Agency (CalEMA), the National Weather Service (NWS) and Humboldt County — included a broadcast on the National Oceanic and Atmospheric Administration (NOAA) weather radio as well as local radio and television stations, the remote activation of four sirens, a reverse 911 telephone call test and an airplane flyover. "This was an excellent cooperative effort between the federal, state, and local government. We've been involved with preparations for this test for the last five months," a CalEMA official said at a media briefing about the drill, which has been held on the North Coast each of the last three years. Del Norte and Mendocino counties and several Northern California tribes also participated. The test was simulating a situation that would result from a long-distance tsunami source, an event which would give officials some time for preparation. In Crescent City, the county simulated a local earthquake emergency drill and had about 1,000 people participate in an evacuation.
Source: http://www.times-standard.com/localnews/ci_14754686

45. *March 24, Federal Computer Week* – (National) **ATF wants more functionality from mobile devices.** The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) is wrapping up a three-month pilot program to test mobile technology to give bureau officials more advanced capabilities on their personal digital assistants (PDAs), such as

letting officials securely monitor surveillance video for investigations, the bureau's chief information officer said today. The bureau's CIO detailed the pilot that involved deploying 150 devices to ATF field divisions around the country to test the ability to manage video on devices such as the HTC Touch Pro. Another pilot using iPhones that's focused on business intelligence is planned. The pilots are testing capabilities on and for an unclassified network. The pilot demonstrated several usability functions that need to be dealt with in the next phase of testing, the CIO said. Software for the first pilot cost a few hundred thousand dollars, he said, but a cost comparison the bureau did showed that over time costs for the pilot technology would be about the same as what ATF spends on BlackBerrys. Other agencies weren't formally involved in the pilot, but ATF officials have talked with the bureau's parent agency, the Justice Department, about the test. ATF is also comparing notes with the FBI (another Justice bureau) about such capabilities.
Source: http://fcw.com/articles/2010/03/24/web-fose-atf-pilot.aspx

[Return to top]

Information Technology Sector

46. *March 25, IDG News Service* – (International) **China's Great Firewall spreads overseas.** A networking error has caused computers in Chile and the U.S. to come under the control of the Great Firewall of China, redirecting Facebook, Twitter, and YouTube users to Chinese servers. Security experts are not sure exactly how this happened, but it appears that at least one ISP recently began fetching high-level DNS (domain name server) information from what's known as a root DNS server, based in China. That server, operated out of China by Swedish service provider Netnod, returned DNS information intended for Chinese users, effectively spreading China's network censorship overseas. China tightly controls access to a number of Web sites, using technology known colloquially as the Great Firewall of China. The issue was reported on March 24 by a DNS admin with NIC Chile, who found that an unnamed local ISP reported that DNS queries for sites such as Facebook.com, Twitter.com and YouTube.com — all of which have been blocked in China — were being redirected to bogus addresses. It is unclear how widespread the problem is.
Source:
http://www.computerworld.com/s/article/9174132/China_s_Great_Firewall_spreads_overseas

47. *March 25, The Register* – (International) **Hackers hit where they live.** The countries of hackers originating malware-laced spam runs have been exposed by new research, which confirms they are often located thousands of miles away from the compromised systems they use to send out junk mail. A third of targeted malware attacks sent so far in March came from the United States (36.6 percent), based on mail server location. However, after the sender's actual location is analyzed, more targeted attacks actually began in China (28.2 percent) and Romania (21.1 percent) than the US (13.8 percent), according to the March 2010 edition of the monthly MessageLabs security report. The MessageLabs intelligence senior analyst, explained the discrepancy: "A large

proportion of targeted attacks are sent from legitimate webmail accounts which are located in the US and therefore, the IP address of the sending mail server is not a useful indicator of the true origin of the attack. “Analysis of the sender’s IP address, rather than the IP address of the email server, reveals the true source of these targeted attacks.”
Source: http://www.theregister.co.uk/2010/03/25/spam_malware_trends/

48. *March 25, Help Net Security* – (International) **Rogue toolbars phish for Facebook credentials.** Two rogue toolbars have been spotted in the wild by Sunbelt researchers. At first glance, they look legitimate enough. Purportedly enabling the user to cheat at popular Zynga games on Facebook, they contain various links and other teature usual for this kind of tool. Upon closer inspection, the toolbar is revealed to be a tool used to steal login credentials. If the user clicks on the “Facebook” button in the left top corner, he is taken to a Facebook look-alike phishing page: The domain on which the phishing page is hosted is constantly changing because in time every domai gets reported, detected and blocked by the browsers. The problem is that the toolbars - when they are not pointing towards the phishing page - point to the real Facebook URL, and the switch can happen anytime. It is best to distrust “cheating” toolbars altogether, and access Facebook and other networks and services by typing in the URL yourself or following your own bookmark.
Source: http://www.net-security.org/secworld.php?id=9065

49. *March 25, IDG News Service* – (International) **New malware overwrites software updaters.** For the first time security researchers have spotted a type of malicious software that overwrites update functions for other applications, which could pose additional long-term risks for users. The malware, which infects Windows computers, masks itself as an updater for Adobe Systems’ products and other software such as Java, wrote an analyst with Bach Khoa Internetwork Security (BKIS), a Vietnamese security company, on its blog. BKIS showed screen shots of a variant of the malware that imitates Adobe Reader version 9 and overwrites the AdobeUpdater.exe, which regularly checks in with Adobe to see if a new version of the software is available. Users can inadvertently install malware on computers if they open malicious e-mail attachments or visit Web sites that target specific software vulnerabilities. Adobe’s products are one of the most targeted by hackers due to their wide installation base.
Source:
http://www.computerworld.com/s/article/9174126/New_malware_overwrites_software_updaters

50. *March 25, V3.co.uk* – (International) **China implicated in flood of email-borne attacks.** China is the number-one source of email-borne targeted attacks of the sort Google and at least 30 other companies are believed to have suffered, according to the latest monthly MessageLabs Intelligence report from Symantec Hosted Services. The firm analyzed the email headers of suspect messages intercepted last month to identify the true IP address of the senders, and found that around 28 percent of targeted attacks originated in China. The emails described by Symantec Hosted Services are targeted in low numbers at key figures in an organisation, and contain legitimate-looking but

malicious attachments. They are similar to those understood to have been used by Chinese hackers to infiltrate Google's systems. The findings chime with what many commentators have been saying about the Google hacks, in that they represent just the tip of the iceberg with respect to global attacks of this kind. "These targeted attacks are very low in number, individually targeted and the attackers have done their reconnaissance beforehand," explained Symantec hosted services senior analyst.
Source: http://www.v3.co.uk/v3/news/2260238/symantec-uncovers-google

51. *March 24, Reuters* – (International) **Inside a global cybercrime ring.** Innovative Marketing Ukraine, or IMU, was at the center of a complex underground corporate empire with operations stretching from Eastern Europe to Bahrain; from India and Singapore to the United States. A researcher with anti-virus software maker McAfee Inc who spent months studying the company's operations estimates that the business generated revenue of about $180 million in 2008, selling programs in at least two dozen countries. "They turned compromised machines into cash," said the researcher. The company built its wealth pioneering scareware — programs that pretend to scan a computer for viruses, and then tell the user that their machine is infected. The goal is to persuade the victim to voluntarily hand over their credit card information, paying $50 to $80 to "clean" their PC. Groups like Innovative Marketing build the viruses and collect the money but leave the work of distributing their merchandise to outside hackers. Once infected, the machines become virtually impossible to operate. The scareware also removes legitimate anti-virus software from vendors including Symantec Corp, McAfee and Trend Micro Inc, leaving PCs vulnerable to other attacks. When victims pay the fee, the virus appears to vanish, but in some cases the machine is then infiltrated by other malicious programs. Hackers often sell the victim's credit card credentials to the highest bidder. In a rare victory in the battle against cybercrime, the company closed down last year after the U.S. Federal Trade Commission filed a lawsuit seeking its disbandment in U.S. federal court.
Source: http://www.reuters.com/article/idUSTRE62N29T20100324

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

52. *March 25, South Oregon World* – (Oregon) **Cut fiber-optic line disrupts businesses.** Bank customers lined up outside Wells Fargo in Coos Bay on March 24, as tellers hand wrote transactions one by one inside the guarded doors. Elsewhere, shop workers processed credit cards manually, and people dialed phone numbers only to hear automated recordings. Phone and Internet service was cut off along the coast for

much of the day, after a construction crew working on a bridge six miles east of Myrtle Point struck a fiber optic cable. Communication lines were not restored until after 5 p.m., causing some businesses, including ACS in North Bend, to send employees home early. The crew knocked out the Verizon cable at 9:50 a.m., but the company did not locate the damage until around 1 p.m. Some users, such as emergency responders, were able to get service through a backup network. Service was affected in coastal communities all the way from Reedsport to Port Orford and possibly farther.
Source:
http://www.theworldlink.com/articles/2010/03/25/news/doc4babc0d6969ab864452706.txt

53. *March 25, ComputerWorld* – (National) **Public safety fee on wireless users a challenge for industry.** The FCC's proposed monthly public safety fee of up to $1 on every broadband user in the U.S. poses a political challenge for the private wireless industry. On one hand, the industry would like to see the FCC auction off radio spectrum in what is called the D block for private uses; the spectrum could then be shared with emergency groups, as the FCC has proposed in the National Broadband Plan. On the other hand, the wireless industry hates the idea of adding more user fees, with one industry-backed group, mywireless.org, noting that the average wireless consumer already pays 16 percent in taxes and fees — and the average wireless household pays $350 a year in wireless taxes. In a separate document not on the site, the group put the total of taxes and fees on the average wireless consumer at nearly $600 a year. The public safety fee, which would be used to support a $16 billion emergency wireless network, was proposed by the FCC in its National Broadband Plan. In that plan, it is described only as a "nominal" fee, although a spokesman recently said it would probably be less than $1 a month. Other officials this week pegged the fee at closer to 50 cents, although the matter is still under discussion and Congress must grant the FCC permission to impose the fee.
Source:
http://www.computerworld.com/s/article/9174135/Public_safety_fee_on_wireless_users_a_challenge_for_industry

54. *March 25, WOFL 35 Orlando* – (Florida) **Widespread cable outages reported.** Bright House Networks customers throughout Central Florida reported cable outages on March 25. Beginning around 10:30 p.m., cable customers around metropolitan Orlando experienced intermittent outages and frozen images on their television sets. The technical glitch appeared to be corrected by 11 p.m. It is still unclear exactly how many customers were affected. Some reported that certain channels were displaying properly while others remained frozen. Subscribers of high definition and select digital tier channels reported that most were displaying while standard cable tier channels were not. This is very similar to what Bright House Networks customers experienced on October 2 of last year, when the outage lasted approximately one hour. There were no reports of telephone or Internet outages on March 25.
Source:
http://www.myfoxorlando.com/dpp/news/lake_news/032510_Widespread_cable_outages

For more stories, see items **40** and **46**

[Return to top]

Commercial Facilities Sector

55. *March 25, Associated Press* – (California) **350,000-gallon sewage spill forces beach closures.** Orange County health officials say three miles of beaches between Dana Point and San Clemente could remain closed through the weekend after a ruptured pipe sent more than 350,000 gallons of raw sewage pouring into the ocean. A Santa Margarita Water District spokeswoman says a 24-inch iron wastewater pipe ruptured Tuesday afternoon. She says workers found the source of the spill on Thursday and began fixing the pipe. They are expected to work through the night and the pipe is expected to be operational again on Friday. A spokesman for the county's environmental health unit says the beach closures will be lifted once testing shows bacterial levels have fallen within state standards for two days in a row.
Source: http://www.mercurynews.com/breaking-news/ci_14761547?nclick_check=1

56. *March 25, Marin Independent Journal* – (California) **Bomb found in Corte Madera hotel room.** A woman under surveillance in an auto theft case was arrested after investigators found a homemade explosive in her Corte Madera motel room, the sheriff's department reported Thursday. The 29-year-old was booked on suspicion of vehicle theft, receiving stolen property, possession of explosives and drug possession. The arrest occurred Wednesday night, when she was under surveillance by the Marin County Auto Theft Task Force and the Marin County Major Crimes Task Force. She was being watched because investigators developed information that she could be involved in a recent spike of vehicle thefts in central and southern Marin, said a sergeant with the sheriff's office. Detectives contacted her after seeing her driving a stolen Honda, then conducted a search of her room at the Budget Inn on Meadowsweet Drive, the sergeant said. Investigators found suspected methamphetamine and what appeared to be makeshift pipe bomb in a dresser. The sergeant said the object was 5 inches long, 2 inches in diameter and wrapped in electrical tape, with a fuse-like device on one end. A bomb squad from the University of California at Berkeley was called to the motel, confirmed the device was an explosive and detonated it. The sergeant declined to comment on the suspected purpose of the device, citing the ongoing investigation.
Source: http://www.marinij.com/ci_14761810?source=most_viewed

57. *March 25, Associated Press* – (Kentucky) **Numerous reasons cited for crash of train at Louisville Zoo that injured 29.** A train ride at the Louisville Zoo was in poor condition and the driver was not adequately trained before a wreck last summer, the Kentucky Department of Agriculture concluded in levying a $37,000 fine against the zoo Thursday. The department released its findings in the June 1 wreck, which injured 22 of the 30 people aboard the ride. The Agriculture Department found six violations. Among them: The train derailed and flipped in a curve while traveling too fast. The fines issued by the department, including a pair $10,000 fines for the train's condition,

were the maximum allowed by law. The derailment happened about 90 minutes before the zoo's 6 p.m. closing and was not in a public area. Twenty-two people were injured in the wreck, some taken to Louisville hospitals for treatment. The 12-page report includes details on the half-dozen violations. It said multiple brake shoes should have been replaced, an improper replacement part had been used on the emergency air brake, the operator failed to follow the correct braking procedures and the train was running "in significant excess" of the recommended 12 mph. The driver, who was not identified in the report, told investigators in a deposition that June 1 was the first day she operated any of the train rides at the zoo by herself without an instructor or other zoo personnel. The driver also said she had never before operated the train that was involved in the accident and she did not receive any training on the emergency brake system on the train.
Source: http://www.lex18.com/news/numerous-reasons-cited-for-crash-of-train-at-louisville-zoo-that-injured-29

58. *March 25, Orange County Register* – (California) **Fair Board approves security system for CEO.** The Fair Board approved Thursday a security system to be installed at the Costa Mesa home of the CEO of the OC Fair and Event Center, who has reported acts of vandalism and distribution of defamatory fliers against him. A board member had suggested that the $3,000 security system be installed to provide the CEO and his family a sense of safety, officials said. The CEO also reported that a vial of noxious liquid was left on his front porch. The odor had permeated his and his neighbors' homes. Some Fair Board members' formation of a nonprofit organization late last year to purchase the fairgrounds was criticized by residents for its possible conflict of interest.
Source: http://www.ocregister.com/news/board-241048-fair-tickets.html

[Return to top]

National Monuments and Icons Sector

59. *March 26, National Parks Traveler* – (District of Columbia; Virginia) **Heavy flooding impacts C and O Canal National Historical Park, Great Falls Park, and other D.C. area parks.** National Park Service officials and volunteer crews near the nation's capital have their hands full these days, cleaning up after a flood. In mid-March, heavy rains and melt from the winter's record-breaking snowstorms combined to spill the Potomac River over its banks. While still considered a moderate flood, these waters were the highest the area had seen since 1996, said a deputy supervisor at Maryland's Chesapeake and Ohio Canal National Historical Park. "The thing about flooding on the Potomac is that it's guaranteed," said the acting site manager at Great Falls Park in McLean, Virginia. "It happens about every 11 years, so we were due." At the C&O Canal several campgrounds, boat ramps, and the popular Billy Goat Trail near Great Falls all were temporarily closed by the flooding. The Great Falls Tavern also was turned into an island amid the flooding. The resulting damage to the canal's towpath means the mule-drawn canal boat rides in Georgetown and Great Falls will be delayed this year, until May 1. One scare happened at the height of the flood when waters

punched through half of Lock 5, a few miles upstream from Washington, D.C. Quick-moving, muddy waters filled the canal, and park officials issued a hasty warning to businesses in Georgetown to prepare their buildings for flooding should the second half of the lock give way. Officials also closed the towpath through Georgetown. Luckily, the remaining section of the lock held, and repairs to the broken part were to start this week.
Source: http://www.nationalparkstraveler.com/2010/03/heavy-flooding-impacts-co-canal-national-historical-park-great-falls-park-and-other-dc-area-parks5580

[Return to top]

Dams Sector

60. *March 25, WDMA 7 Laurel-Hattiesburg* – (Mississippi) **Settlement reached in Big Bay dam break trial.** More than 100 property owners whose homes were destroyed by the 2004 Big Bay dam breach will split $1 million as a result of a settlement reached in the trial. The settlement was reached after three days of testimony on the Mississippi coast. The case was about to go to a jury when attorneys for both sides got together and hammered out the settlement. A jury could have found Big Bay developers liable for the dam break, which meant each property owner could sue individually for damages. The dam broke in March of 2004 — sending more than three billion gallons of water from the 1,100-acre Lamar County lake downstream. The breach flooded and destroyed more than 100 homes. No one was injured. Testimony varied during the three-day trial — whether it was negligence or an act of God. According to the settlement, the insurance company representing Big Bay development partners will pay the million-dollar sum, and the partners will add an additional $100,000 over the next 24 months. Property owners' share of the settlement will depend on the amount of damage each suffered, after attorney fees are paid.
Source: http://www.wdam.com/Global/story.asp?S=12204070

For another story, see item **59**

[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 NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
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