Homeland Security

Daily Open Source Infrastructure Report for 19 March 2010

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- The Associated Press reports that Virginia Tech is urging calm as e-mails and Internet postings originating in Italy threaten another attack on campus. Though police do not believe the threats are credible, classes were held Thursday with additional security on campus. (See item **37**)
- According to Reuters, hackers have flooded the Internet with virus-tainted spam that targets Facebook's estimated 400 million users in an effort to steal banking passwords and gather other sensitive information. (See item **48**)

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 18, Standard Speaker* – (Pennsylvania) **Tanker spill closes store.** A tanker truck dumped between 350 and 500 gallons of gasoline while refilling underground tanks at the Turkey Hill Minit Market at Humboldt Station, just off Commerce Drive, on the morning of March 17, shutting down the store for hours. The Hazle Township Fire Chief said a nozzle popped off the tank during the refilling, allowing the gasoline

to spill onto the ground and get into the drains on the property. Vapor levels remained just under explosive levels, but emergency crews evacuated the store and parking lot, and asked the nearby Residence Inn to shut down its air systems and for guests to stay inside, he said. Firefighters from Hazle, West Hazleton, Harwood and Sheppton-Oneida responded, as did American Patient Transport Systems, Luzerne County Emergency Management Agency, the state Department of Environmental Protection, and the U.S. Environmental Protection Agency. The state Department of Agriculture was also notified to advise employees regarding the food inside the store, a county EMA director said. A DEP spokesman said the spill was contained and the gasoline did not leave the site, posing no environmental concern.
Source: http://standardspeaker.com/news/tanker-spill-closes-store-1.688111

2. *March 18, Associated Press* – (Wyoming) **Wyoming seeks $660,000 from Sinclair for spill.** Wyoming is seeking a settlement of $660,000 against Sinclair Wyoming Refining Company — a penalty that would be among the state's biggest in recent years — for failing to take measures to prevent a huge spills last year. Nearly 3 million gallons of a gasoline blend spilled from a storage tank at the Sinclair refinery in south-central Wyoming on May 3, 2009. The penalty is proposed in a draft settlement agreement the Wyoming Department of Environmental Quality has sent to the refinery owned by Salt Lake City-based Sinclair Oil Corp. The Associated Press obtained the document by filing a public records request. The spill released a fluid called light straight run, which is blended with gasoline. The fluid was contained to the refinery grounds but local officials expressed concern about the risk of explosion and lack of information from Sinclair about the situation. The spill happened when pontoons holding up the floating roof of a storage tank took on fluid, causing the roof to sink to the bottom of the tank. The roof punctured the tank bottom in several places. A December 30 state violation notice says Sinclair failed to address leakage into the pontoons. A contractor documented the leakage months before the spill but the refinery lost track of the report and didn't correct the problem.
Source: http://www.trib.com/news/state-and-regional/article_09f6d5ba-9d88-57d3-886a-2d0b8617dba3.html

3. *March 18, KNXV 15 Phoenix* – (Arizona) **Wrong gas sold at 17 Arizona Mobil gas stations?** Officials say the wrong gas was sold at 17 Mobil gas stations across Arizona over the past several months. The mistake is being blamed on an automated coding error that blends the gasoline at Kinder Morgan's Phoenix terminal from October 2009 through mid February 2010. The company discovered the program error on February 17. Since then, both Kinder Morgan and Mobil have notified state officials about the mix up. Signs have also been placed at the affected gas stations telling customers and offering to remedy the situation. Kinder Morgan says it supplied 643,257 barrels of premium gasoline to the market during the time frame, about 2 percent of it contained regular instead of premium. The Arizona Weights and Measures Department was made aware of the situation and is investigating and may fine the company, although that has not been determined yet. The affected Mobil gas stations include four in Flagstaff, two in Kingman, and one in each of the following: Ashfork, Winslow, Payson, Lake Havasu City, Quartzite, Williams, Mojave Valley, Tonopah, Wickenberg, Camp Verde,

and Snowflake.
Source:
http://www.abc15.com/content/news/investigators/consumeralerts/story/Wrong-gas-sold-at-17-Arizona-Mobil-gas-stations/4cnzBdhYLUK9konrQfQL6Q.cspx

4. *March 17, Associated Press* – (Nebraska) **7 coal cars spill loads in Nebraska rail yard.** Union Pacific (UP) officials are trying to find out what caused eight cars to jump off tracks in the company's vast Bailey Yard in North Platte. A UP spokesman said no one was injured in the accident. It occurred about 7:55 a.m. on March 17. Eight coal cars left the tracks, and seven tipped over completely. He says 2 of the many yard tracks were still blocked on March 17 afternoon, but cleanup work was continuing. He says the 24-car train was headed to Kentucky and had pulled into the yard for refueling and lubrication.
Source: http://www.nebraska.tv/Global/story.asp?S=12156639

[Return to top]

Chemical Industry Sector

5. *March 17, WFSB 3 Hartford* – (Connecticut) **DEP: Industrial cleaners spilled from truck.** The Connecticut Department of Environmental Protection (DEP) was called to a truck stop off Interstate 95 in Branford the evening of March 17 after officials said a truck began leaking hazardous fluid. DEP officials said a tractor-trailer was coming in from Pennsylvania with a mixed load of industrial cleaners and chemicals. The truck was fueling up and another driver noticed the truck was leaking. The tractor-trailer pulled over to the side of the truck stop at about 6:30 p.m. and called his company, which then contacted an environmental company out of South Windsor. DEP officials were also called to the scene. Officials said there was a 110-gallon tow in the middle of the truck that contained an industrial garage floor cleaner. They said the cap on the tow was cracked, causing the cleaner to leak out of the top. DEP officials said every time the truck moved, the fluid came splashing out of the truck. A DEP spokesman said the truck was improperly packaged. State police were notified and the truck was taken out of service. The environmental contractor is expected to return on March 18 to unload and repackage the truck. The spilled fluid was cleaned up by 10:15 p.m.
Source: http://www.wfsb.com/news/22873100/detail.html

[Return to top]

Nuclear Reactors, Materials and Waste Sector

6. *March 18, Reuters* – (Ohio) **NRC sends team to Ohio Davis-Besse reactor.** The U.S. Nuclear Regulatory Commission sent a special inspection team to FirstEnergy Corp's (FE.N) 879-megawatt Davis-Besse nuclear power plant to look into indications of cracks in multiple reactor vessel head nozzles. The NRC said there was no danger to the public from these cracks since the plant has been shut for scheduled refueling. Before the plant can resume operations, the NRC said it must be satisfied the problem

has been addressed. Earlier this week, FirstEnergy could not say whether the repairs would add to the length of the refueling outage.
Source: http://www.reuters.com/article/idUSN1821251620100318?type=marketsNews

7. *March 16, World Nuclear News* – (Illinois) **Illinois Senate votes to overturn nuclear ban.** The Illinois State Senate has voted overwhelmingly to remove a 23-year-old moratorium on the construction of new nuclear power plants in the state. However, the bill stills need to be approved by the House. The Senate voted 40-1 in favour of a bill (SB3388) amending Illinois' Public Utilities Act of 1987. The amendment would remove a clause stating that utilities cannot construct new nuclear power stations in the state. It would also remove a requirement that the US federal government "has identified and approved a demonstrable technology or means for the disposal of high-level nuclear waste" before any state approvals can be issued for nuclear new build.
Source: http://www.world-nuclear-news.org/NP-Illinois_Senate_votes_in_favour_of_nuclear_new_build-1603104.html

8. *March 16, Environmental Health News* – (National) **Depleted and enriched uranium affect DNA in different ways.** Meticulous research identifies for the first time how two main types of uranium – enriched and depleted – damage a cell's DNA by different methods. The manner – either by radiation or by its chemical properties as a metal – depends upon whether the uranium is processed or depleted. This study shows that both types of uranium may carry a health risk because they both affect DNA in ways that can lead to cancer. Why does it matter? Regulatory agencies determine safe uranium exposure based on the metal's radioactive effects. Currently, safe exposure levels for workers and military personnel are based on enriched uranium – which is the more radioactive form and is considered to have a higher cancer risk than depleted uranium. Uranium exposure has been shown to affect bone, kidney, liver, brain, lung, intestine and the reproductive system. Yet, many people are exposed at work or through military activities to the less radioactive, depleted form. They may not be adequately protected based on current methods that evaluate uranium's health risks. As a naturally-occurring element, most people are exposed to low levels of uranium through food, air and water. Additional exposure to uranium occurs when it is mined and altered for civilian or military purposes. Workers who process uranium into nuclear fuel for energy or weapons face additional exposure to enriched uranium. Depleted uranium – a by-product of the enriching process – is used in military armor and in armor-piercing ammunition.
Source: http://www.environmentalhealthnews.org/ehs/newscience/depleted-enriched-uranium-affect-dna-differently

[Return to top]

Critical Manufacturing Sector

9. *March 17, Worcester Telegram* – (Massachusetts) **Industrial oven explodes, blows out windows.** An industrial oven at the Walker Magnetics Group plant in Worchester, Massachusetts exploded and caught fire, blowing out windows and prompting a

hazardous materials response. The acting district fire chief said there were no employees inside. The damage was contained to the industrial oven in the rear of the building and several windows that had blown out. He said fire officials were trying to find out what kind of chemicals were being used near the machine; a hazardous materials team was later called to the building to make a determination. The chief said it was unclear whether an electrical problem or the oven itself caused the explosion; he said firefighters used fire extinguishers, and vented the building with fans. A worker at Walker Magnetics said the factory portion of the plant cleared out about 3 p.m.
Source: http://www.telegram.com/article/20100317/NEWS/100319747/1116

10. *March 17, First Coast News* – (National) **Toyota warns of engine stalling in 1.2M Corollas.** Just when Toyota thought it was getting hold of its recall nightmare, it is now trying to figure out how to fix computer flaws in up to 1.2 million Toyota Corolla and Matrix models that can cause engines to stall, the Detroit Free Press is reporting. But Toyota has told federal auto safety regulators it does not think the problem "an unreasonable risk" to safety. Drive On guesses that is because these ones have engines that will not stay running, rather than engines that run out of control, the subject of unwanted-acceleration recalls. So far, the Corolla problem in 2005 to 2007 models is not at the recall stage yet. But this is another tough break for the automaker. In a letter to NHTSA, Toyota said the problem was due to physical faults in the production of the vehicles' engine control units, which it blamed on mistakes at two suppliers, one of which was identified as Delphi, the Free Press said. "Toyota has been investigating this issue and is now considering how to address our customer concerns," the automaker said in a March 2 letter to NHTSA obtained by the Free Press. "Based upon its analysis, Toyota does not believe that the alleged defect creates an unreasonable risk to motor vehicle safety."
Source: http://www.firstcoastnews.com/news/usworld/news-article.aspx?storyid=153447&catid=6

[Return to top]

Defense Industrial Base Sector

11. *March 17, Associated Press* – (Colorado) **Colo. company accused of exporting military tech.** Federal prosecutors say a Colorado company illegally exported technology used by the U.S. military to South Korea, China, Russia and Turkey. The U.S. attorney's office in Denver announced the charge Wednesday against Rocky Mountain Instrument Co., and said the company will be forced to forfeit $1 million if convicted. A spokesman for the U.S. attorney declined to comment on whether the alleged crime compromised national security. Lafayette, Colo.-based RMI says it has been cooperating with the government's investigation and is working toward a plea agreement with prosecutors. The company manufactures optics components. Prosecutors say it exported prisms and technical data for optics used in military applications to the four countries from April 1, 2005 to Oct. 11, 2007.
Source: http://www.wlos.com/template/inews_wire/wires.national/319ccece-www.wlos.com.shtml

For another story, see item **8**

[Return to top]

Banking and Finance Sector

12. *March 18, Morristown Daily Record* – (New York) **FBI seeks gentlemen bank robbers in NY.** A polite bank robber who says "thank you" as he holds tellers at gunpoint is part of at least a two-man crew who have robbed six Westchester banks since January, federal agents say. The men are picking up their pace, robbing two banks since March 13 and frustrating law enforcement officers who have set up roadblocks to try and catch them. Westchester appears to be their primary target — with the exception of the March 15 robbery of a TD Bank in Mahopac — but investigators said they believe they have robbed banks before this recent spree. The robber has demonstrated calm under pressure and is likely an experienced stickup artist. The result has been one of the biggest Westchester bank robbery sprees in decades. It has led state Crime Stoppers to offer a $2,500 reward for information leading to an arrest, and the FBI's Westchester County Violent Crimes Task Force to coordinate several police agencies in the investigation. Investigators said they believe there are at least two men involved in the seven heists.
Source: http://www.dailyrecord.com/article/20100318/UPDATES01/100318022/-1/UPDATES01/FBI-seeks-gentlemen-bank-robbers-in-NY-

13. *March 18, The Register* – (International) **Madoff geeks charged for writing book-cooking code.** A federal grand jury has indicted two computer programmers on fraud and conspiracy charges for developing programs used by a renown Ponzi artist to cook the books in his billion-dollar Ponzi scheme. The two suspects knowingly created the programs that removed or altered key data contained in reports submitted to regulators in the United States and Europe, according to the indictment filed on March 17 in U.S. District Court in Manhattan. Among other things, their code contained algorithms to randomly generate times for purported orders that in fact were never made. The reports were generated on "House 17," an IBM AS/400 server kept on the 17th floor of the Ponzi artist's offices that had no link to the outside world, prosecutors allege. To ensure the reports appeared genuine, the server pulled partial information from a separate AS/400 that was linked to the Depository Trust Company and other third parties. The document goes on to claim that the programmers knew their programs were being used to falsify information being provided to the Securities and Exchange Commission and the European Accounting Firm, and sought to profit from their expertise.
Source: http://www.theregister.co.uk/2010/03/18/madoff_programmers_charged/

14. *March 18, Help Net Security* – (International) **Barclays under strong phishing shower.** A highly productive phishing scam, with more than 180 messages sent in three minutes, hits a big chunk of the online segment of Barclays members. Various people are wondering what to do now that their bank has been acquired in the wake of the lending crisis. Do not click the links in e-mails supposedly sent by the bank. Barclays' members will be amazed to find in their inboxes an apparently legitimate message

which requires them to check their account details by following a link allegedly directing them to the financial institution's Web site. The provided link redirects the gullible users towards a fake Barclays Web site, which employs several PHP scripts for pilfering the sensitive data they fill in. And the phisher gets greedier: after completing the name and membership number, Barclays users are taken to a page where they are supposed to provide very sensitive information, such as their five digit passcode. In this final step, a request for an apparently trivial piece of information slips in: the first two letters of their memorable word. Considering that this detail serves as a password recovery hint for online banking accounts, this last move should make the alarm bell ring quite loudly.
Source: http://www.net-security.org/secworld.php?id=9038

15. *March 18, SC Magazine* – (International) **Authentication and transaction sectors boosted with new solutions.** The banking and payment industries have been bolstered this week with new options in authentication and transaction checking. FireID launched the FireID Authentication platform for banks this week, which provides transaction verification, authentication for mobile and online banking, and internal VPN access for bank use. It explained that the platform eliminates the need for hardware tokens by generating secure one-time passwords (OTP) on users' mobile phones, with no network connectivity required, to provide strong security for sensitive financial transactions. Ethoca360 Signals — a free fraud detection service targeted at preventing chargebacks and card not present (CNP) fraud — has also been launched by Ethoca. The company claimed that this checks transactions in real-time against the Global Fraud Alliance (GFA) repository and identifies matches and patterns that indicate either fraud risk or a probable good order through intuitive color-coded "warning signals."
Source: http://www.scmagazineuk.com/authentication-and-transaction-sectors-boosted-with-new-solutions/article/166017/

16. *March 18, Tallahassee Democrat* – (Florida) **Robber uses bomb threat to hold up bank.** A man robbed Farmers and Merchants bank on the 4200 block of West Tennessee Street, according to a spokesperson for the Tallahassee Police Department. The man entered the bank and claimed to have a bomb. He left with an undisclosed amount of cash. The package he claimed to be a bomb was left at the scene. The Hazardous Devices Team in currently on scene investigating the package. No one was injured during the robbery.
Source:
http://www.tallahassee.com/article/20100318/BREAKINGNEWS/100318008/Robber-uses-bomb-threat-to-hold-up-bank

17. *March 18, Washington Post* – (National) **Small banks lag in repaying Treasury for bailout funds.** The Treasury Department invested in large and small banks during the financial crisis. So far, the big bets are paying off better than the smaller ones. While the largest banks have borne the brunt of criticism for their role in triggering the crisis, they were among the quickest to give back their federal bailout funds. Sales of the warrants that these firms were required to hand over to the federal government as a condition of the aid also proved lucrative for the Treasury. But hundreds of community

banks have yet to return their bailouts. More than 10 percent of the 700 banks that got federal bailouts and are still holding the money even failed to pay the government a quarterly dividend in February. The list of 82 delinquent banks is significantly longer than the 55 banks that failed to make payments in November, according to an analysis by a finance professor at the University of Louisiana at Lafayette. The professor calculated that the missed payments totaled $78.1 million in February and that banks now have missed a total of $205 million in dividend payments to the government. Many of the community banks still holding aid from the Troubled Assets Relief Program are struggling with losses on real estate development loans.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/03/17/AR2010031704046.html

18. *March 18, Altassets.com* – (National) **Blackstone considers $1bn fund for failed banks.** Blackstone Group, the largest private equity firm in the industry, has initiated talks over raising a $1bn fund to buy up failed banks, according to reports. The firm is talking to a former president of Bluebonnet Savings Bank about the proposal. Regulators are said to have seized at around 160 lenders since the start of 2009, with the FDIC's list of "problem" banks standing at just over 700 with more that $400bn in assets. In May last year, Blackstone and Carlyle invested $900m in BankUnited after winning an auction for the troubled Florida lender. Investors, which also included funds managed by Centerbridge Partners and WL Ross & Co, bought BankUnited's operations, deposits, and assets from its receiver, the Federal Deposit Insurance Corporation (FDIC). The struggling bank had assets of around $13bn.
Source: http://www.altassets.com/private-equity-news/by-region/north-america/unitedstates/article/nz18170.html

19. *March 17, Dallas Business Journal* – (Texas) **40 indicted in alleged North Texas mortgage scheme.** A Florida man and 39 other defendants who are accused of conspiring with him have been named in a 16-count indictment filed in the U.S. Attorney's Office of the Eastern District of Texas. The U.S. Attorney's Office alleges that a 41 year old suspect, of Windemere, Florida, solicited real estate agents, property finders, mortgage brokers, real estate agents, property finders, title company attorneys, property appraisers and straw buyers to run a scheme in which lending institutions were defrauded by approving mortgage loans on properties that had fraudulently inflated values. At least a dozen of the defendants live in North Texas, and all allegedly were recruited by the suspect to take part in the scheme. Many of the defendants are from North Texas. The charges vary, but include conspiracy to commit mail and wire fraud, wire fraud, and money laundering. According to the U.S. Attorney's Office, the man operated the scheme through Florida-based businesses TKI Group Inc. and JAB Consulting.
Source: http://dallas.bizjournals.com/dallas/stories/2010/03/15/daily21.html

[Return to top]

Transportation Sector

20. *March 18, Washington Post* – (International) **Scanners may not have detected alleged explosive in Detroit jet case, GAO reports.** The U.S. president's push to deploy body-imaging scanners at airports worldwide will cost U.S. taxpayers roughly $3 billion over eight years, congressional investigators report, but it is unclear that the controversial devices would have caught an alleged al-Qaeda terrorist who tried to blow up a Detroit-bound jetliner with explosives hidden in his underwear. The administration has cited the Christmas day attack in pushing to double its planned deployment, to 1,800 scanners, at U.S. airports by 2014, and to encourage foreign governments to use the same new technologies at airports that send flights to the United States. "While officials said [the scanners] performed as well as physical pat downs in operational tests, it remains unclear whether the AIT would have detected the weapon used in the December 2009 incident," the Government Accountability Office, Congress's audit arm, said in testimony prepared for the hearing. The bomber allegedly concealed 80 grams of explosive powder in a pouch sewn into his underwear. "While GAO recognizes that TSA is attempting to address a vulnerability exposed by the December 2009 attempted attack, a cost-benefit analysis is important as it would help inform TSA's judgment about the optimal deployment strategy for the AITs, and how best to address this vulnerability," the prepared testimony states. The audit agency said TSA estimates each unit costs about $170,000, meaning it would cost about $300 million to buy 1,800 units, enough to cover about 60 percent of screening checkpoint lanes at the highest-priority commercial airports. Each scanner requires three people to operate. Based on the administration's request for $219 million to hire 3,550 TSA staffers next year alone, GAO estimates it will cost $2.4 billion overall to staff the machines over eight years.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/03/17/AR2010031700649.html?hpid=topnews

21. *March 18, Delaware County Daily Times* – (Pennsylvania) **Cops: Teen rips through U.D. in stolen SEPTA bus.** A stolen SEPTA bus careened through a parking lot in White Tower Township, Pennsylvania on Wednesday. Behind the wheel of the bus was a mentally handicapped 16-year-old boy who had commandeered it from the Victory Avenue depot moments earlier, according to police. The bus slammed to a halt just in front of onlookers, separated only by a utility pole. Nineteen parked vehicles were damaged during the estimated half-mile joy ride along West Chester Pike, police said. The accused juvenile driver, believed to be from a group home in Philadelphia, was charged with aggravated assault, simple assault, reckless endangerment and theft. According to police, the teenager got into the bus at the transit depot and proceeded onto Victory Avenue and then onto West Chester Pike. The youth struck five cars in the SEPTA lot, one car at Keystone Avenue, and 13 in the township parking lot, which is primarily used by commuters, police said.
Source:
http://www.delcotimes.com/articles/2010/03/18/news/doc4ba19a16e4e32771212871.txt

22. *March 18, Honolulu Star-Bulletin* – (Hawaii) **Rail line route raises airport safety issue.** City, federal and state officials met on Oahu in an attempt to resolve a question

about whether the proposed rail transit line intrudes into a safety zone at the Honolulu Airport. The Honolulu City Managing Director said officials with the Federal Aviation Administration and Federal Transit Administration met yesterday to discuss the proximity of the rail line to the Diamond Head-mauka side of the airport. An FAA spokesman said his agency is providing an analysis about several rail alignments' potential effect on airport operations. Part of the proposed 20-mile rail line runs along Aolele Street and would stop at a four-story station at Lagoon Drive, less than 1,000 feet from the end of runways 22 right and left, and encroaching on the airspace buffer zone, government officials said. Officials said while there are other buildings such as warehouses in the area, the station would be as high as the freeway viaduct and closer to the runway. The FAA says the city's rail transit plan runs too close to an active runway.
Source:
http://www.starbulletin.com/news/20100318_rail_line_route_raises_airport_safety_issue.html

23. *March 18, Associated Press* – (Delaware) **Bomb experts investigate suspicious Del. package.** Authorities said a suspicious package caused police to close streets for a few hours Wednesday in Wilmington. The package was found by police Wednesday afternoon under the Washington Street Bridge. Streets in the area were closed while bomb experts investigated the package. Authorities said the package was found to be harmless after police sent a robot to open it.
Source: http://wjz.com/wireapnewsmd/Suspicious.package.under.2.1571483.html

24. *March 18, Seacoastonline.com* – (New Hampshire) **State officials monitor erosion near Winnicut River bridge.** A crew of engineers and representatives of the state Department of Environmental Services spent Wednesday night monitoring the Route 33 bridge over the Winnicut River in Greenland to ensure serious damage does not occur as the latest severe storm to hit the Seacoast winds down. Concern over the bridge is focused on erosion issues that came about due to the inability of DES to construct permanent stabilization during its dam removal project. The program manager with the DES Coastal Program said the main concern for the state Department of Transportation is not the structural integrity of the bridge but damage to the road leading up to it. The senior associate of environmental management for Stantec Consulting, said sloughing of the slope at the bridge's northeast approach could result in some sinkhole formation that could potentially compromise the integrity of the embankment. Route 33 at the Winnicut River near the Bayside and Winnicut roads intersection was shut down Monday morning as the bridge and road was inspected by the DOT and deemed safe for passage and re-opened.
Source: http://www.seacoastonline.com/articles/20100316-NEWS-3160391

25. *March 17, Associated Press* – (International) **Grenade-shaped lighter forces airport evacuation.** A grenade-shaped cigarette lighter in a boy's checked luggage has forced the evacuation of some 1,000 people from an airport in Poland and delayed four international flights. A spokesman for the airport in Katowice, Poland said passengers and workers were evacuated Wednesday from the airport after a grenade shape was

detected in a suitcase destined for Dortmund, Germany. Some 80 firefighters and antiterrorists were involved in the evacuation and in checking the object, which a 13-year-old German boy bought as a souvenir during a school trip to Poland. The lighter was confiscated because objects that appear like weapons are banned from airplanes.
Source: http://www.forbes.com/feeds/ap/2010/03/17/business-financial-impact-eu-poland-airport-evacuated_7443006.html

For more stories, see items **4**, **5**, and **29**

[Return to top]

Postal and Shipping Sector

26. *March 17, Baltimore Sun* – (Maryland) **Responsibility unclear on mail security.** The U.S. Postal Service, which is charged with screening mail for safety, failed to detect bullets that were sent with threatening letters to at least two Baltimore judges in the past week. And it is unclear if it could. There appears to be no technology in place to identify the ammunition sent in the mail. The oversight raises questions about mail security and who is responsible for ensuring recipients' safety in the wake of five suspicious mailings, some with a powdery substance inside, that were delivered to City Hall and Baltimore Circuit Court on Friday and Monday. The courts say it's not their job to screen packages, and the postal system says it can do only so much. A joint investigation into the letters, sent to four judges and City Hall, has been launched by Baltimore police and the U.S. Postal Inspection Service. "Even though the powder contained in the mailings is not harmful, the threatening mailings not only constitute a federal crime, but they caused alarm to victims and institutions," said a U.S. Postal Inspector who works in the Washington division. She said postal inspectors will aggressively investigate "anyone who mails these types of threats, real or hoax."
Source: http://www.baltimoresun.com/news/maryland/baltimore-city/bal-md.letters17mar17,0,6471202.story

27. *March 17, WJZ 13 Baltimore* – (Maryland) **Courthouse receives another suspicious package.** There were tense moments at the Mitchell Courthouse in downtown Baltimore Wednesday morning. There, employees found another suspicious package. That package, apparently quite similar to the ones sent to judges there on Monday, contained a bullet and powdery substance. Hazmat teams raced to the second floor of the Baltimore Circuit Courthouse where an employee called 911 after identifying a suspicious package. "The fire engines pulled up and said no one could come inside," said a witness. A large envelope containing a bullet and a powdery substance was found in one of the judge's chambers, though a spokesperson told WJZ the envelope was not addressed to any particular judge. Authorities did not evacuate the building. Instead they isolated the one room where the package was found while police secured courthouse entrances. The US Postal Inspection Service is investigating and the FBI stated that it is not involved in the case.
Source: http://wjz.com/local/Baltimore.police.investigate.2.1568548.html

[Return to top]

Agriculture and Food Sector

28. *March 18, Pork Magazine* – (National) **Animal ID charts new course.** USDA officials and animal agriculture representatives set priorities and discussed new strategies for animal identification and traceability at the National Institute for Animal Agriculture's annual meeting held Wednesday in Kansas City, Missouri. USDA announced in February that it was going to scrap the National Animal Identification System in favor of a new state-based system. Representatives from the beef, dairy, horse, sheep and pork industries expressed concerns and suggested priorities as a replacement for the defunct NAIS is shaped. In addition, representatives from American Meat Institute and a livestock marketing agency stated their views. Input from Wednesday's meeting will be key to reshaping and defining USDA's role in developing new national animal identification efforts. According to the industry representatives, priorities for a new state-led animal identification system include development of uniform ID standards that apply across all states, ability for the system to move at 'speed-of-commerce', as well as availability of USDA funding for the effort. Minimizing producer costs and confidentiality also are important, according to some.
Source: http://www.porkmag.com/directories.asp?pgID=675&ed_id=9034

29. *March 18, Chicago Sun Times* – (Illinois) **25,000 pounds of honey spill onto the Ike.** Troopers are still cleaning up a sticky situation after 25,000 pounds of jarred honey was lost early Thursday morning when the semi truck hauling it rolled over on the Eisenhower Expressway. The semi was on the eastbound exit ramp of the Eisenhower Expressway (I-290) heading towards southbound I-294 when it hit a right barrier wall Thursday at 4:35 a.m., Illinois State police sergeant said. The semi then rolled and landed on its right side. The driver was taken to Loyola University Medical Center in Maywood with minor injuries, the sergeant said. No other injuries were reported. About 25,000 pounds of jarred honey spilled onto the ramp, causing it to close for about an hour. Most of the debris landed on the median, and the roadway was cleared as of 9 a.m. The driver said the truck's brakes locked up, causing him to lose control. Drugs or alcohol were not suspected in the crash.
Source: http://www.suntimes.com/news/metro/2110134,honey-spills-onto-eisenhower-031810.article

30. *March 17, Oregonian* – (Oregon) **Kulongoski declares drought emergency in Klamath County.** Oregon's Governor has declared a drought emergency in Klamath County and asked the federal government for a disaster determination that would bring more federal aid to farmers and ranchers. With snowpack and precipitation down, water levels in Upper Klamath Lake are near historic lows. The governor is trying to avoid a repeat of the Klamath basin's farmers-versus-fish water wars in 2001 and 2002 that generated national controversy. A state drought declaration — in this case for Klamath County and five surrounding counties — is far from a cure-all. But it would allow farmers to apply for emergency drought permits to tap ground water instead of surface waters and to transfer water from one piece of land to the other. He also wrote Tuesday

to U.S. Secretary of Agriculture to request a federal natural resource disaster determination, which would trigger two additional federal assistance programs on top of three now available in the basin.
Source:
http://www.oregonlive.com/environment/index.ssf/2010/03/kulongoski_declares_drought_em.html

For another story, see item **1**

[Return to top]

Water Sector

31. *March 17, U.S. Environmental Protection Agency* – (Missouri) **Iron ore recovery business to pay $138,016 civil penalty for unpermitted discharges, dredging in Washington County, Mo.** An iron ore recovery business has agreed to pay a $138,016 civil penalty to the United States to settle a series of alleged violations of the federal Clean Water Act (CWA) related to unpermitted dredging and discharges of pollutants into a stream in Washington County, Missouri. Upland Wings, Inc., of Sullivan, Missouri, agreed to the penalty in an administrative consent agreement and final order placed on public notice today in Kansas City, Kansas, The company runs an iron ore recovery operation at the former Pea Ridge mining facility near Sullivan according to the filing. The agreement says that EPA Region 7 inspectors witnessed pollutant discharges from Upland Wings' operations into Mary's Creek in March 2007. Those discharges contained levels of oil and grease, copper, chromium, cadmium, iron, lead, and total suspended solids that were in excess of limits set forth in the company's National Pollutant Discharge Elimination System (NPDES) permit. Inspectors from EPA Region 7 and the U.S. Army Corps of Engineers learned in 2008 that Upland Wings, acting without proper permits, used earth-moving equipment to dredge iron ore tailings from settling ponds at the Sullivan facility and place the material into Mary's Creek and adjacent areas, affecting approximately 18 acres of wetlands. In January 2009, EPA officials discovered that Upland Wings used earth-moving equipment to channelize about 300 linear feet of Mary's Creek and place the dredged material into adjacent wetlands, also without a permit.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/0/676751CE3288BB23852576E90069F099

32. *March 17, KWGN 2 Denver* – (Colorado) **Denver Water workers expose 'toxic cemetery' at foothills treatment plant.** Retired Denver Water workers are coming clean about hazardous waste they say they buried near dozens of homes and schools 20 years ago. "It is a toxic burial ground. People are going to die," says one of a dozen former Denver Water employees who say they were ordered by a Denver Water Manager to bury cement asbestos, radiation asphalt, and other toxic chemicals at the "Foothills Water Treatment Facility" in Douglas County, near Titan Road and Santa Fe. "They had us bury these toxins. We broke them up with back hoes and all we were given were dust masks," he claims. Asbestos-cement pipe or sheet can emit airborne

fibers if the materials are cut or sawed, or if they are broken. Workers claim they "crushed the asbestos piping, spread it out on the land and covered it with dirt. It was never properly capped," the workers say. The workers suffer from a wide range of illnesses they believe were caused by asbestos exposure and they're concerned the constant digging at the site could be releasing asbestos particles in the air and contaminating the soil and groundwater. The workers say a drain flushes ground water from the site past dozens of homes and empties out at the bottom of the hill just below Roxborough Intermediate School. The former workers took their concerns to the Denver Water Board. The Board president said the board would investigate the allegations. Denver Water does not confirm or deny the workers' allegations. Denver Water sent KWGN a statement which says in part, "burying of CA (cement-asbestos) pipe may have occurred, but if it did, it was per standard practice at the time."
Source: http://www.kwgn.com/news/kdvr-water-toxic-cemetery-031710,0,5172784.story

33. *March 17, KMGH 7 Denver* – (Colorado) **DIA releases 1M gallons of sewage, storm water.** Denver International Airport (DIA) blamed a mechanical failure at its airport lift station for the release of up to 1 million gallons of contaminated water. "After the spill was discovered Wednesday morning, DIA notified the appropriate federal, state, and local environmental and health agencies; as well as a downstream farmer, Adams County, and the Farmers Reservoir Irrigation Co., owner of the canal," read a statement from DIA. Airport workers were conducting downstream water sampling and the airport contacted the state health department, as well as the Tri-County Health Department and officials at Barr Lake State Park. "We looked at the water in the creek; we saw it was clear, we could still see minnows and we did not have any odor issues," said the director of environmental health at Tri-County Health Department. "Those were the three quick and easy things to check for." The airport and environmental agencies are working to determine the severity of the spill. He said test results from samples taken Wednesday should be available Thursday. A DIA spokesman said the pump stopped working about 7 p.m. Tuesday, but workers did not realize it was not working until about 7 a.m. Wednesday. "We do have backup alarms to notify the airport when this is happening," said the DIA spokesman. "We have every indication that that alarm worked properly, but it went unnoticed. We are investigating how that happened." He said the alarm sounds in the maintenance facility which is manned 24 hours a day.
Source: http://www.thedenverchannel.com/news/22871065/detail.html

34. *March 16, WCVB 5 Boston* – (Massachusetts) **Chinese fluoride in Mass. water raises concern.** Team 5 Investigates found the Amesbury Water Department pulled fluoride from its system amid concerns about its supply from China. The Department of Public Works director said after he mixes the white powder with water, 40 percent of it will not dissolve. "I don't know what it is," he said. "It's not soluble, and it doesn't appear to be sodium fluoride. So we are not quite sure what it is." He said the residue clogs his machines and makes it difficult to get a consistent level of fluoride in the town's water. Since April, the fluoride pumps in Amesbury have been turned off and they will stay that way until the director can find out what is in the fluoride that is imported from

China. Both state and federal health officials told Team 5 Investigates that Chinese fluoride is safe. The Department of Public Health said it believes that more than 650,000 customers in 44 Massachusetts communities are getting the flouride in question and only Amesbury has temporarily stopped using it. However, they were unable to say with certainty which of the other 43 communities are actually using the sodium fluoride from China in its water. The fluoride from China is not used in communities getting water from the MWRA. The New York company that supplies the fluoride said it is certified by the National Sanitation Foundation which assures the quality of the product. But the NSF said the company has never been on its certification list. Testing continues to determine the precise composition of the residue.
Source: http://www.thebostonchannel.com/investigative/22814488/detail.html

[Return to top]

Public Health and Healthcare Sector

35. *March 17, DNAinfo* – (New York) **Helmsley Medical Center on the Upper East Side evacuated after fire breaks out.** A residential tower that houses employees and relatives of patients at nearby hospitals had to be partially evacuated Wednesday afternoon after a fire broke out. Dozens of firefighters battled the blaze for more than an hour after it broke out just before 3:30 p.m. at the Helmsley Medical Tower, 1320 York Ave., near E.70th Street. The 37-story building is used as a residence for family members of patients and employees of the nearby Memorial Sloan Kettering Cancer Center and New York Presbyterian Hospital. It houses a five-floor clinic, which was also evacuated. The fire originated in one of the electrical rooms in the subbasement, the FDNY said.
Source: http://www.dnainfo.com/20100317/upper-east-side/helmsley-medical-center-on-upper-east-side-evacuated-after-fire-breaks-out

36. *March 17, Jewish Daily Forward* – (New York; New Jersey) **CDC warns that mumps may spread.** Experts are warning that an outbreak of mumps that has already sickened thousands in the Orthodox community could spread further this Passover. The outbreak, which first appeared last June, has been largely confined to Hasidic populations in Brooklyn, Orange, and Rockland counties in New York, and parts of New Jersey. But the Centers for Disease Control and Prevention has mounted a campaign to warn community members and health-care providers that the virus could reach new geographic areas as families gather for holiday celebrations. “We’re concerned that with travel, there’s a potential for introduction into other Hasidic communities that aren’t currently experiencing outbreaks,” said an epidemiologist at the CDC. The MMR vaccine, which protects against mumps as well as measles and rubella, is given to most Americans in two doses before they begin kindergarten. A high percentage of those infected in the recent outbreak did receive two doses as children.
Source: http://www.forward.com/articles/126682/

[Return to top]

Government Facilities Sector

37. *March 18, Associated Press* – (Virginia) **Online postings warn of another Va. Tech attack.** Virginia Tech is urging calm as e-mails and Internet postings originating in Italy threaten another attack on campus. Though police do not believe the threats are credible, the school president said in an e-mail to faculty and students Wednesday that classes will be held Thursday with additional security on campus. Authorities investigated similar threats earlier this month and in October and believe the new posts are from the same person. Virginia Tech was the scene of the worst mass shooting in modern U.S. history in April 2007. Virginia State Police and the FBI are assisting in the investigation.
Source:
http://www.google.com/hostednews/ap/article/ALeqM5hbPZ5kOxWcJud57pc0M8DykE-SFgD9EH0I9O3

38. *March 17, WLTX 19 Columbia* – (South Carolina) **Deputies arrest man in bomb threat investigation.** Orangeburg County deputies arrested a 51-year-old man they say threatened to blow up the Orangeburg County Courthouse in a fit of anger. Investigators with the Orangeburg County Sheriff's Office said at about 8:30 a.m. Wednesday, the suspect called in the bomb threat because he was upset about a court date scheduled for Wednesday. As a precaution, deputies worked with building officials to evacuate the courthouse. After officials received the threat, deputies say they noticed the suspect, who they say appeared to be suspicious. After the questioning the man, deputies say he admitted to placing the threat. The suspect was charged with attempt to destruct a county building.
Source: http://www.wltx.com/news/story.aspx?storyid=85214&catid=2

39. *March 17, Associated Press* – (International) **FBI: No evidence Mexico hit men targeted Americans.** Confused hit men may have gone to the wrong party, the FBI said Tuesday as it cast doubt on fears that the slaying of three people with ties to the U.S. consulate shows that Mexican drug cartels have launched an offensive against U.S. government employees. Gunmen chased two white SUVs from the birthday party of a consulate employee's child on Saturday and opened fire as horrified relatives screamed. The two near-simultaneous attacks left three adults dead and at least two children wounded. The attack drives home just how dangerous Ciudad Juarez has become — and just how vulnerable those who live and work there can be, despite the Mexican government's claims that most victims are drug smugglers. According to one of several lines of investigation, the assailants — believed to be aligned with the Juarez drug cartel — may have been ordered to attack a white SUV leaving a party and mistakenly went to the "Barquito de Papel," which puts on children's parties and whose name means "Paper Boat." "We don't have any information that these folks were directly targeted because of their employment by the U.S. government or their U.S. citizenship," an FBI spokeswoman told The Associated Press by phone from El Paso, just across the Rio Grande from Ciudad Juarez. The FBI is still investigating the backgrounds of the victims.
Source:

http://www.google.com/hostednews/ap/article/ALeqM5gMi5B2USfJStXxfqgWWr2xjRYpOgD9EG2ER00

40. *March 17, Associated Press* – (International) **Pakistani court charges five Americans with terrorism.** A Pakistani court charged five young Americans on Wednesday with planning terrorist attacks in the South Asian country and conspiring to wage war against nations allied with Pakistan, their defense lawyer said. The men — all Muslims from the Washington, D.C., area — pleaded not guilty to a total of five charges, the most severe of which carries a maximum sentence of life in prison, defense lawyer told The Associated Press. "My clients were in good shape and high spirits," the defense lawyer said. The men, ages 19 to 25, were charged by an anti-terrorism court inside a prison in Sargodha, the city in Punjab province where they were arrested in December. They were reported missing by their families in November after one left behind a farewell video showing scenes of war and casualties and saying Muslims must be defended. Their lawyer has said they were heading to Afghanistan and had no plans to stage attacks inside Pakistan. The court also charged the men with planning attacks on Afghan and U.S. territory, said the defense lawyer. The charges did not specify what was meant by U.S. territory but could be a reference to American bases or diplomatic outposts in Afghanistan.
Source: http://www.usatoday.com/news/world/2010-03-17-pakistan-americans-terrorism_N.htm

41. *March 17, Washington Post* – (National) **Federal Protective Service says security improved at government facilities.** The government agency responsible for protecting more than 9,000 federal facilities said Tuesday it has taken several steps to address security gaps first exposed in a government audit last year. The Federal Protective Service has developed new training on X-ray machines and magnetometers for the almost 15,000 private security guards it employs, the agency director told lawmakers. FPS officers have also reviewed the certifications of contract guards and increased spot inspections at guard posts, he said. The changes come amid a recent wave of attacks at federal facilities across the country and follow a 2009 Government Accountability Office investigation that exposed serious security gaps at 10 major federal buildings. GAO investigators smuggled bomb-making materials into the buildings while photos and video showed private contract guards asleep at their posts and a young child passing through an X-ray machine in a baby carrier.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/03/16/AR2010031604252.html

42. *March 16, Augusta Chronicle* – (Georgia) **Employee blamed for radiation contamination.** A Savannah River National Laboratory technician's failure to adequately monitor her gloved hands was the cause of a January incident in which her clothing and skin were contaminated with radiation. The employee was testing vials of plutonium samples when a radiation control officer detected radiation on a hood where the employee was working, according to a Defense Nuclear Facilities Safety Board report. The officer then examined the technician and found alpha contamination on the abdomen, lapel and right arm of her lab coat. "When the technician was sent to the

decontamination room, additional contamination was found on her personal clothing and on her skin in the vicinity of the lapel," the report said. A lab spokeswoman said the levels were well below what could cause health impacts, but was nonetheless investigated because the lab's goal is to avoid all such incidents.
Source: http://chronicle.augusta.com/latest-news/2010-03-16/employee-blamed-radiation-contamination?v=1268755213

For more stories, see items **8** and **27**

[Return to top]

Emergency Services Sector

43. *March 18, Associated Press* – (Rhode Island) **RI health officials probe alleged unlicensed EMT.** Rhode Island public health authorities are investigating allegations that an unlicensed emergency medical technician worked with the Barrington Fire Department for a year and a half. A spokeswoman for the Public Health Department tells the Providence Journal the agency is investigating how the Barrington resident was allowed to work for nearly 18 months without proper certification. The man completed his training but never took or passed a test to get his EMT license. The man resigned earlier this month after his lack of proper licensing came to the attention of the fire chief and town officials. The chief said there were never problems with the man's performance.
Source: http://www2.wjtv.com/jtv/ap_exchange/special_-_medical/article/RiHealthOfficialsProbeAllegedUnlicensedEmtRi/116310/

[Return to top]

Information Technology Sector

44. *March 18, SC Magazine* – (International) **One in four children has attempted hacking with one fifth believing that they could generate an income from the activity.** A survey has found that one in four schoolchildren have attempted some level of hacking. Despite 78 percent agreeing that it is wrong, a quarter have tried to surreptitiously use a victims' password, with almost half saying that they were doing it 'for fun'. However 21 percent aimed to cause disruption and 20 percent thought they could generate an income from the activity. Five percent said that they would consider it as a career move. Of those who had tried hacking, a quarter had targeted Facebook accounts, 18 percent went for a friend's email, seven per cent for online shopping sites, six per cent for their parent's email and five per cent breached the school website. A bold three percent had honed their skills enough to aim much higher with corporate websites under their belts.
Source: http://www.scmagazineuk.com/one-in-four-children-has-attempted-hacking-with-one-fifth-believing-that-they-could-generate-an-income-from-the-activity/article/166025/

45. *March 18, The New New Internet* – (National) **MIT keeps system online during cyber attack.** Previously, when a system was under cyber attack, the only solution to mitigate the threat was to take the server offline. However, there may now be another option. MIT researchers have developed a system that allows servers and computers to continue to operate even while under cyber attack. The research, predominately funded by the U.S. Defense Department's Defense Advanced Research Projects Agency (DARPA), has stood up to outside testing. DARPA hired outside security experts to attempt to bring down the system. According to an electrical engineering and computer science professor who led the project, the system exceeded DARPA's performance criteria in each test. During normal operations, the system developed by the MIT team monitors any programs running on computers connected to the Internet. This allows the system to determine each computer's normal behavior range. When an attack occurs, the system does not allow the computers to operate outside of the previously determined range. "The idea is that you've got hundreds of machines out there," the professor says. "We're saying, 'Okay, fine, you can take out six or 10 of my 200 machines.'" But, he adds, "by observing what happens with the executions of those six or 10 machines, we'll be able to deploy patches out to protect the rest of the machines." An associate professor of computer science at Columbia University finds the MIT approach to be novel. However, he feels that most web developers might be reluctant to implement the new technology in the near future.
Source: http://www.thenewnewinternet.com/2010/03/18/mit-keeps-system-online-during-cyber-attack/

46. *March 17, Wired* – (Texas) **Hacker disables more than 100 cars remotely.** More than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control, after an intruder ran amok in a web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments. Police with Austin's High Tech Crime Unit on March 17 arrested a 20-year-old who was a former Texas Auto Center employee who was laid off last month, and allegedly sought revenge by bricking the cars sold from the dealership's four Austin-area lots. The dealership used a system called Webtech Plus as an alternative to repossessing vehicles that haven't been paid for. Operated by Cleveland-based Pay Technologies, the system lets car dealers install a small black box under vehicle dashboards that responds to commands issued through a central website, and relayed over a wireless pager network. The dealer can disable a car's ignition system, or trigger the horn to begin honking, as a reminder that a payment is due. The system will not stop a running vehicle. Texas Auto Center began fielding complaints from baffled customers the last week in February, many of whom wound up missing work, calling tow trucks or disconnecting their batteries to stop the honking. The troubles stopped five days later, when Texas Auto Center reset the Webtech Plus passwords for all its employee accounts, says the manager of Texas Auto Center. Then police obtained access logs from Pay Technologies, and traced the saboteur's IP address to the suspect's AT&T internet service, according to a police affidavit filed in the case.
Source: http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+wired/index+(Wired:+Index+3+(Top+Stories+2))

47. *March 17, IDG News Service* – (International) **Nvidia warns of graphics drivers with overheating risk.** Nvidia on March 17 asked customers to remove drivers that caused its GeForce graphics cards to overheat, which ultimately crashed some PCs. Nvidia acknowledged on its support site that customers had problems with the 196.75 package of GeForce drivers. Nvidia is asking customers to remove the faulty driver package and upgrade to the latest package, which is 197.13. "Nvidia is aware that some customers have reported fan speed issues after installing 196.75 drivers from Nvidia's website. Nvidia has removed these drivers and asked its partners to also remove the drivers," Nvidia wrote on another support site. As an alternative, customers could roll back to the older versions of graphics drivers, Nvidia said. "In almost every case reverting back to our 196.21 driver immediately resolved their issues," Nvidia wrote.
Source:
http://www.pcworld.com/article/191813/nvidia_warns_of_graphics_drivers_with_overheating_risk.html

48. *March 17, Reuters* – (International) **New password-stealing virus targets Facebook users.** Hackers have flooded the Internet with virus-tainted spam that targets Facebook's estimated 400 million users in an effort to steal banking passwords and gather other sensitive information. The emails tell recipients that the passwords on their Facebook accounts have been reset, urging them to click on an attachment to obtain new login credentials, according to anti-virus software maker McAfee Inc. If the attachment is opened, it downloads several types of malicious software, including a program that steals passwords, McAfee said on March 17. Hackers have long targeted Facebook users, sending them tainted messages via the social networking company's own internal email system. With this new attack, they are using regular Internet email to spread their malicious software. McAfee estimates that hackers sent out tens of millions of spam across Europe, the United States and Asia since the campaign began on March 16.
Source:
http://www.reuters.com/article/idUSTRE62G5A420100317?feedType=RSS&feedName=internetNews&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+Reuters/InternetNews+(News+/+US+/+Internet+News)

49. *March 17, The Register* – (International) **Vodafone Spain supplies pre-Mariposa'd smartphone (again).** Vodafone Spain has again supplied a HTC Magic smartphone that came pre-infected with the Mariposa botnet client and other malware crud. The second incident, involving an Android-based phone supplied to a researcher at S21Sec, comes a week after the mobile phone giant supplied the same type of infection on the identical model of phone to a worker at Spanish anti-virus firm Panda Security. The S21Sec pre-pwned smartphone kerfuffle undermines Vodafone's assurances at the time of the Panda flap that the incident was "isolated and local". Both smartphones were ordered at around the same time towards the beginning of March. The Register spoke to Vodafone on March 17, making it aware of the second HTC Magic/Mariposa infection in Iberia. Vodafone stuck by its original line that the problem was "isolated and local" but added that it hadn't experienced the problem outside of Spain. A spokesman added that its investigation is continuing. The S21Sec worker detected the malware after he

plugged it into his PC using a copy of AVG's scanner. Aware of Panda's previous work, he forwarded an infected microSD drive to a researcher at PandaLabs, who carried out an analysis.
Source: http://www.theregister.co.uk/2010/03/17/vodafone_mariposa_again/

50. *March 17, IDG News Service* – (International) **Law enforcement push for stricter domain name rules.** Law enforcement officials in the U.K. and U.S. are pushing the Internet Corporation for Assigned Names and Numbers to put in place measures that would help reduce abuse of the domain name system. Now it is "ridiculously easy" to register a domain name under false details, said the senior manager and head of e-crime operations for the U.K.'s Serious Organised Crime Agency (SOCA). Domain names can be used for all kinds of criminal activity, ranging from phishing to trademark abuse to facilitating botnets. Law enforcement often run into difficulty when investigating those domains, as criminals use false details and stolen credit cards. The FBI and SOCA have submitted a set of recommendations to ICANN for how it could strengthen Registration Accreditation Agreements (RAA). The agreement is a set of terms and conditions that a registrar — an entity that can accept domain name registrations — would be subject to in order to run their business. ICANN's RAA applies to registrars for generic top-level domains (gTLD), such as ".com." The ideas from the FBI and SOCA have not been publicly revealed but include stronger verification of registrants' name, address, phone number, e-mail address and stronger checks on how they pay for a domain name, the manager said.
Source: http://www.networkworld.com/news/2010/031710-law-enforcement-push-for-stricter.html?hpg1=bn

51. *March 17, V3.co.uk* – (International) **Sophos warns of Facebook fakers.** Security experts are warning of yet another scam to hit Facebook, pointing out that the site is full of fake Fan Pages which could open users up to another avenue of attack A Sophos senior technology consultant, himself the victim of a fake fan page, urged Facebook to tighten up its rules on the creation of such sites, as their existence threatens the security of other users. "Innocent people — friends, acquaintances, and anyone who might follow my blog — are joining the fan page in the belief that they are somehow following me. They have no way of telling that I didn't create this fan page," said the consultant in a blog posting. Although the social networking site has rules in place to deal with unauthorized fan pages, and actually should be prohibiting the creation of unofficial ones, the fake profile has not been removed, despite calls from the real thing for its removal.
Source: http://www.v3.co.uk/v3/news/2259680/sophos-warns-facebook-fakers

52. *March 16, PC World* – (International) **Attack samples show targeted sophistication.** If anyone would like to know what a targeted e-mail attack looks like, take a look at samples posted today by antivirus maker F-Secure. The screen shots, pulled from malware analysis blog contagio, clearly show a greater attention to detail and grammar than the usual clumsy attack e-mails that stand out like a sore thumb. The first two samples in F-Secure's post lack any clear clues, while the third has some capitalization errors but no laughable grammatical mistakes. These types of polished

attacks are typically sent to high-value targets, and are comparitively uncommon. For instance, last January Google said it was hit by targeted attacks. But while the contagio samples do no immediately stand out, they do share a common thread: All have a .pdf attachment. F-Secure warned last year that .pdf's have become the attack of choice for targeted attacks, and these samples support that warning.
Source:
http://www.pcworld.com/article/191663/attack_samples_show_targeted_sophistication.html

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

53. *March 17, ComputerWorld* – (National) **Broadband plan gives FCC wider cybersecurity role.** The National Broadband Plan released by the Federal Communications Commission (FCC) recently contains several recommendations that are designed to boost the preparedness of communications networks to deal with cyberthreats. The plan gives the FCC a greatly enhanced role in developing and promoting cybersecurity measures and calls for closer cooperation between the FCC and the U.S. Department of Homeland Security on security matters. The 360-page broadband plan is a blueprint for modernizing the country's aging communications networks and for delivering broadband services to a majority of U.S. homes over the next decade. It contains six long-term policy goals and other recommendations for ensuring the availability of affordable 100Mbit/sec. service to 100 million U.S. homes, and 1Gbit/sec. service to institutions such as hospitals and schools, by 2020. While a vast majority of the recommendations deal with building out the communications infrastructure, several touch on cybersecurity and communications networks' ability to survive a cyberattack.
Source:
http://www.computerworld.com/s/article/9172258/Broadband_plan_gives_FCC_wider_cybersecurity_role

[Return to top]

Commercial Facilities Sector

See item **1**

[Return to top]

National Monuments and Icons Sector

54. *March 17, Maine Public Broadcasting Network* – (Maine) **Dry conditions prompt "Red Flag" warning.** The Maine Forest Service says dry conditions are creating a wildfire hazard in parts of Maine, including all of Washington County. A "red flag" warning has been issued for parts of Maine as high winds and low humidity combine to create ideal conditions for wildfires. The Maine Forest Service and the National Weather Service say the area near Greenville and Millinocket south, to the coastal areas of Hancock County and all of Washington County are particularly vulnerable right now to wildlfires. Several wildfires have broken out over the last few days, including a 6-acre blaze in Orland, which threatened two structures. The Maine Forest Service is urging people to postpone any outdoor burning until after a significant rainfall.
Source: http://www.mpbn.net/News/MaineHeadlineNews/tabid/968/ctl/ViewItem/mid/3479/ItemId/11440/Default.aspx

55. *March 17, Reuters* – (International) **Canada, U.S. set new avalanche danger warning system.** Canada unveiled the new warning system just days after a big snow slide slammed into a snowmobile rally near Revelstoke, British Columbia, killing two people, although officials said the timing was only a coincidence. The danger scale, to be implemented next winter, modifies current systems advising people whether it is safe to be in mountain regions, by incorporating both the likelihood and consequences of an avalanche in an area. The current systems used in Canada and the U.S. warns people about the likelihood of a snow slide, but does not communicate other important information, said a mountain risk specialist with Parks Canada. "(The new system) considers factors such as both the likelihood of triggering an avalanche and how big it will be," the specialist said. "Its job is to make it easier to understand." He said the danger of several small slides being triggered may be considered less than the likelihood of one very large slide. Parks Canada, the Canadian Avalanche Center, U.S. Forest Service and Colorado Avalanche Center were among the agencies that spent five years developing and testing the new warning system. "It's a significant accomplishment," said the director of the U.S. Forest Service's avalanche center in Ketchum, Idaho.
Source: http://www.reuters.com/article/idUSTRE62G53S20100317

[Return to top]

Dams Sector

56. *March 18, Reuters* – (International) **Kazakhstan flood death toll rises to 40.** The death toll from last week's flood that destroyed a village near the Kazakh financial hub Almaty, Kazakhstan, has risen to 40, the emergencies ministry said on Thursday. "A total of 40 bodies have been discovered since the start of rescue works," it said in a statement, adding that nearly 300 people had been injured when a dam burst in the village of Kyzyl-Agash last Friday. Previously the death toll had been 37. Police have since detained the village mayor and several other officials as part of the probe into the

dam rupture. Spring flooding is a frequent occurrence in Central Asia but a sudden rise in temperatures following weeks of heavy snow storms has exacerbated the problem this year.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031800094.html

57. *March 17, Morgan County Herald* – (Ohio) **High water spills over dam.** Water rushes over the dam at McConnelsville, Ohio, Sunday evening. Despite the snow melt and rain, it appeared Tuesday that the Muskingum River would not be flooding. The water level crested at 9.9' at 5 a.m. Sunday. It was at 9.31' at 8 a.m. Tuesday and is expected to slowly go down the rest of the week, according to the National Weather Service in Charleston, West Virginia. Flood stage at McConnelsville is 11'.
Source:
http://www.mchnews.com/articles/2010/03/17/news/top_stories_and_breaking_news/doc4ba0ecbfbb454381766754.txt

58. *March 17, Tulsa World* – (Oklahoma) **Meth equipment found behind Arkansas River levee.** Authorities discovered a large dumping ground of meth-making equipment behind an Arkansas River levee Wednesday morning that included nearly 100 plastic bottles used to make the drug. Maintenance workers stumbled upon the discarded bottles north of the river near 49th West Avenue and called the Tulsa County Sheriff's Office. The dump was substantially larger than most, a police spokesperson said, and it appears that a group of suspected meth cooks who live nearby hid their used equipment behind the levee. "Usually when we find a dump lab, it's one reaction vessel and some of the chemicals," he said. "It's been piling up for a long time." Deputies found between 75 and 100 bottles that had been used to make the drug, he said. The isolated spot is just south of the levee and an adjoining residential neighborhood. A trail system for all-terrain-vehicles spans the other side.
Source:
http://www.tulsaworld.com/news/article.aspx?subjectid=11&articleid=20100317_11_0_hrimgs334051&archive=yes

[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