Homeland Security

Daily Open Source Infrastructure Report for 4 March 2010

Current Nationwide Threat Level

ELEVATED

Significant Risk of Terrorist Attacks

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

Top Stories

- ClickonDetroit.com reports that 540 students at Phoenix Multicultural School on Detroit's southwest side were evacuated Wednesday morning after a "Drano bomb" detonated inside the building. (See item **36**)
- According to Reuters, Spanish police have arrested three men accused of masterminding one of the biggest computer crimes to date — infecting more than 13 million PCs with a virus that stole credit card numbers and other data. The men were suspected of running the Mariposa botnet, Spain's Civil Guard said on Tuesday. (See item **47**)

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 3, BBC* – (International) **Somali pirates seize empty Saudi oil tanker and crew.** Somali pirates have captured a small Saudi tanker and its crew, the EU naval force in the Gulf of Aden says. The tanker, travelling from Japan to Jeddah, was empty when pirates hijacked the vessel and took its crew captive. The MT Nisir Al Saudi was outside the shipping lanes patrolled by naval warships, it was reported. Somali pirate

attacks usually increase in the months between March and May because calmer seas allow the pirates to operate more freely. The captain of the ship is Greek, but the nationalities of the rest of the crew are not known. In November 2008, Somali pirates hijacked the Sirius Star, a Saudi supertanker loaded with two million barrels of oil. They released it after two months in return for a ransom, believed to have been $3m, which was parachuted on to the deck of the ship by helicopter. The latest ship to be captured was taken to the Somali town of Garacad, a known pirate stronghold, said a commander of the EU Naval Force in the area.
Source: http://news.bbc.co.uk/2/hi/africa/8547140.stm

2. *March 3, Associated Press* – (International) **Shell reports attack on Nigeria oil flow station.** Planted explosives damaged a Royal Dutch Shell PLC oil flow station in the Niger Delta, a company spokesman said on March 3, marking the latest attack in a region supposedly brought under control by a government amnesty program. A previously unknown militant group claimed responsibility for the attack Tuesday on the Kokori oil flow station, operated by a Shell subsidiary in Nigeria. A Shell spokesman said the flow station was not in use and was unmanned at the time of the explosion, so there were no injuries. "It hadn't been producing for some time," he said. In a statement to Nigerian newspapers, a group calling itself the People's Patriotic Revolutionary Force of the Joint Revolutionary Council claimed it attacked the flow station early morning on March 2. It warned all foreign oil companies to leave the oil-rich Delta immediately or face further violence. "We hereby announce the resumption of fresh and final hostilities in the Niger Delta and beyond," the group said. The Joint Revolutionary Council is a smaller militant group that once claimed to be allied with the Movement for the Emancipation of the Niger Delta, the main militant force in the Delta.
Source:
http://www.google.com/hostednews/ap/article/ALeqM5gHJyop68FyJkZy4mhXIgmHhzZRvwD9E762RO1

3. *March 3, Bloomberg* – (New Mexico) **Navajo oil refinery tank fire kills two workers.** A fire late on March 2 at an asphalt tank at Holly Corp.'s Navajo oil refinery killed two workers, a local police spokesman said by telephone. Two contractors working at the tank died and two were transported to a hospital in Lubbock, Texas for treatment, said a sergeant of the Artesia, New Mexico police department, where the Navajo plant is located. Holly, the owner of refineries and pipelines in the U.S. Southwest, earlier said the fire at an asphalt storage tank under construction "likely" killed a worker, in a statement on PRNewswire. The blaze occurred at about 12:40 p.m. local time and was extinguished in about 90 minutes by the refinery's fire fighting units. There was no impact to the operations of the 100,000 barrel-a-day plant. The workers were employed by an independent contractor building the new tank, the statement said. The company earlier said two workers were taken to the hospital, according to a spokesman for the refinery. The refinery had a fire on Jan. 18 in the crude unit that caused "minimal damage" and resulted in scheduled maintenance being brought forward, Holly said in a statement then. The crude distillation unit was returned to service Feb. 16.

Source: http://www.businessweek.com/news/2010-03-03/navajo-oil-refinery-tank-fire-kills-two-workers-update2-.html

4. *March 3, Montgomery Herald* – (North Carolina) **Major fuel spill causes evacuation.** A fuel spill closed a section of highway and caused the evacuation of nearby residents on February 28. The spill leaked an extensive amount of gasoline on the ground and in a nearby creek. The accident occurred shortly before 5 a.m. at the intersection of N.C. Highway 73 and Zion Church Road in Montgomery County. According to State Highway Patrol Officer, the driver, 45 of Chesterfield, S.C., was operating a 2005 International tractor-semi trailer, traveling southeast on N.C. 73 when he ran off the road to the right, collided with a ditch and overturned causing the truck to separate from the tanker. The truck landed upright after colliding with a tree. The tanker landed on its top. It was filled with 9,000 gallons of gasoline. The truck had loaded in Charlotte and was on its way to C's in Mt. Gilead. Cleanup has been extensive according to the Emergency Management Director. Crews from the Department of Environment and Natural Resources and the Environmental Protection Agency have been on scene. Extensive ground cleanup is occurring and on February 28 an inverted dam was placed in a nearby stream. Additional stream cleanup was also under way. The EPA according to the director will conduct testing in the stream and a nearby pond. Fuel was being moved from the overturned tanker to another tanker but the director estimates that between 6,000 – 7,000 gallons of fuel did leak out. A regional hazmat team did respond to the fuel spill as well as local fire departments that helped with the spraying of foam. The truck also clipped a power line when it wrecked causing nearby power outages.
   Source:
   http://www.montgomeryherald.com/articles/2010/03/03/news/top_stories/doc4b8e4302848ea452224941.txt

5. *March 3, Middletown Press* – (Connecticut) **Little oversight in regards to power plant safety.** Speakers at a forum before the state legislature's Energy and Technology Committee Tuesday fell silent when asked by a state senator which agency had the responsibility of safety oversight for the construction and operation of power plants. A supervisor of the gas pipeline safety unit at the state Department of Public Utility Control said: "I'm not sure I can tell you who does," he said. "I can say our department does not." Representatives of DPUC, the state Department of Public Safety, the state Department of Emergency Management and Homeland Security, the Connecticut Siting Council and the U.S. Chemical Safety Board testified at the informational forum on power plant safety. The chair of the committee requested that general power plant safety be the topic of testimony and questions rather than the deadly explosion at the Kleen Energy Systems power plant on February 7, although the incident clearly prompted the hearing and was occasionally mentioned during the forum. The Connecticut Siting Council executive director said that power plant developers are required to notice a host of agencies when seeking approval from the council but that the state departments of public safety and homeland security are not on that list. A deputy commissioner for the state Department of Public Safety said the regulations concerning power plants that his agency could promulgate were limited: the state fire

marshal's office would regulate activities such as demolition and blasting and the state building inspector would oversee a plant's elevators and boilers. He said the state Department of Public Safety only has jurisdiction over construction of power plants "as it relates to risks to the public and structures." Lawmakers tested the waters on possible legislative changes to make in the wake of the explosion, asking speakers whether they had an opinion as to which state department should be charged with overseeing the safety of power plants in the future.
Source:
http://www.middletownpress.com/articles/2010/03/03/news/doc4b8dda56bb246434762218.txt

6. *March 2, Omaha World-Herald* – (Iowa) **UP tanker spills ethanol in Iowa.** A dislodged cap allowed thousands of gallons of ethanol gas to leak from a Union Pacific tanker car as it passed through parts of western Iowa early morning on March 2. The leak might have begun in Greene County, authorities said. But the worst of the spill is in Boone County, where several fire departments, as well as Haz Mat crews from Des Moines, are cleaning up. Boone County Emergency Management Coordinator said the problem began when the UP tanker began leaking ethanol from a single spout beneath the car. The spout normally is covered with a cap. Authorities said about 30,000 gallons of ethanol leaked from the tanker.The leak was reported just before 4:45 a.m. Sand has been spread at each crossing along the train's route, from Ogden to the east side of Boone, as a precaution against fire. Fire is not a real concern until the temperature reaches 45 degrees, he said, "so as long as we're under 45 degrees, we don't have to worry too much about an accidental fire. "By the time we get this all cleaned up and it warms up a little bit, it's probably going to be evaporated enough that we won't have to worry about it then."
Source: http://www.omaha.com/article/20100302/NEWS01/703029847

[Return to top]

Chemical Industry Sector

7. *March 2, Charleston Gazette* – (West Virginia) **DuPont lifts Belle plant 'safety stand-down'.** Officials from DuPont Co.'s Belle plant said on March 2 that they have lifted a "voluntary safety stand-down" instituted in January after a series of accidents, including a phosgene leak that killed a longtime DuPont worker. In a prepared statement, a DuPont spokesman said the company has restarted most of the units that were not involved in any of those incidents. "We are monitoring each unit closely to ensure continued safe operation," he said in the statement. "We will continue with the staged resumption of operations as we determine that we can do so safely." Various federal agencies, including the U.S. Chemical Safety Board, have launched investigations at the Belle plant following a series of accidents. DuPont did not provide a full list of units that are still not in operation, but did identify one unit that will not restart. The Belle plant's sulfuric acid recovery unit — where a sulfuric acid leak occurred the same day as the phosgene leak — was already scheduled to shut down by March 31 under the terms of a federal environmental enforcement settlement. DuPont

and a partner in the unit, Lucite, agreed to pay a $2 million fine for not upgrading pollution control equipment when they expanded the unit's production capacity. "In light of the current voluntary pause in production and the brief timeline to March 31, the SAR unit will not be restarted," DuPont said. "We do not anticipate any job losses as a result of these actions. We expect to place employees assigned to the SAR unit into existing openings at the Belle plant."
Source: http://wvgazette.com/News/201003020410

For another story, see item **30**

[Return to top]

Nuclear Reactors, Materials and Waste Sector

8. *March 3, Brockton Enterprise News* – (Massachusetts) **Authorities say Middleboro 'radioactive' canisters a hoax.** The FBI has joined the investigation into who left five canisters marked "radioactive" and "nuclear waste" at Oliver Mill Park in Middleboro. Park Department employees found the canisters sitting on a cement wall at the park Tuesday afternoon, prompting a hazmat response, said a fire chief. Authorities swept the area for radioactivity with Geiger counters and other devices. After a couple of hours the threat was determined to be a hoax, said the fire chief, and the Federal Bureau of Investigation took over the case. The canisters were labelled in magic marker bearing the descriptions Radio Active #1, Isotope #2, Nuclear Waste #13, Radio Active Isotope #9 and Thermo nuclear waste #13. The fire chief is seeking the public's help to find the perpetrator of the hoax. He said it is a serious crime and carries felony charges. The investigation will be a joint effort between the FBI and Bureau of Criminal Investigation.
Source: http://www.enterprisenews.com/news/x699612248/Authorities-say-Middleboro-radioactive-canisters-a-hoax

9. *March 2, Reuters* – (California) **SCE's San Onofre 2 reactor restart delayed.** Southern California Edison's SCE.N restart of the 1,070-megawatt Unit 2 at the San Onofre nuclear power plant in California has been delayed by problems with a pressure test in the containment building that occurred last week, a spokesman for the U.S. Nuclear Regulatory Commission said on Monday. The unit, which shut September 27 to refuel and to replace the unit's steam generators, is entering the sixth month of an outage that had been expected to return by late December.
Source: http://www.reuters.com/article/idUSN022563702010030?type=marketsNews

10. *March 2, Red Wing Republican Eagle* – (Minnesota) **Nuclear plant security stops trespasser.** A man who fled Treasure Island Resort & Casino security early Sunday morning was apprehended by nuclear plant security when he trespassed on Xcel Energy property in Red Wing. Plant security detected the individual at 1:45 a.m. near a wooded area several hundred yards from the plant, according to Xcel officials. He was intercepted by plant security at about the same time as Prairie Island Indian Community police arrived. Tribal police took the individual into custody. In a report filed with the

federal Nuclear Regulatory Commission, the plant said it was later determined that the individual had fled on foot from the nearby casino, where he had been detained on suspicion of underage drinking. The incident did not pose a threat to the plant or to the safety of the public and nuclear plant officials notified the NRC resident inspector.
Source: http://www.republican-eagle.com/event/article/id/65064/

[Return to top]

Critical Manufacturing Sector

11. *March 3, Associated Press* – (National) **Dept. of Transportation considers brake overrides.** The Department of Transportation may recommend that every new vehicle sold in the U.S. be equipped with brakes that can override the gas pedal. The U.S. Transportation Secretary said Tuesday his agency may recommend that every new vehicle sold in the U.S. be equipped with brakes that can override the gas pedal. The idea seemed to be gaining support among lawmakers as Toyota officials returned for a third congressional hearing on lethal safety defects. His testimony came as federal safety officials increased to 52 the number of reported deaths linked to sudden acceleration in Toyota vehicles, through the end of last month. Previously, 34 deaths were blamed on the problem. Multiple recalls have damaged Toyota's reputation and set the stage for large numbers of death and injury lawsuits amid a criminal investigation by federal prosecutors in New York, a probe by the Securities and Exchange Commission and more scrutiny from the Transportation Department. Since September, Toyota has recalled about 6 million vehicles in the U.S. Toyota has said it will put such a system into all future vehicles and will retrofit many recalled models. More than 8 million Toyota cars have been recalled in all because of sudden acceleration or braking defects.
Source: http://abclocal.go.com/wjrt/story?section=news/national_world&id=7308264

[Return to top]

Defense Industrial Base Sector

12. *March 3, Homeland Security NewsWire* – (National) **DARPA looking for military iPhone and Android apps.** DARPA has announced that it would like some apps written for the iPhone or for handsets running Google's Android OS — "with potential relevance to the military specifically and the national security community more generally." The Pentagon researchers note that in today's military, handheld systems are characterized by a tight integration of specialized hardware with a narrowly focused software suite. Most of the handheld devices are heavily optimized for a particular task and are ill-suited for general-purpose use. A soldier's radio, for example, has very limited data capability and essentially no multimedia capability. Current language translation devices support neither messaging nor collaboration of any form. A transformation in technical approaches and business processes is called for. Experts note that some military hardware, too, has already taken on many of the aspects of a smartphone — for instance, the Land Warrior wearable comlink/computer rig.

DARPA's preferences notwithstanding, at least one maker has produced a covert version of military belt-computer software to run on a Windows smartphone.
Source: http://homelandsecuritynewswire.com/darpa-looking-military-iphone-and-android-apps

13. *March 2, Daily Press* – (Virginia) **Shipyard drug probe continues.** As Northrop Grumman Corp. on Monday continued its investigation into dozens of employees at its Newport News shipyard on suspicion of illegal drug use and possession, the yard's general manager asked employees to stay focused and warned that "a lapse in judgment can be devastating." In an e-mail message sent Monday morning to all of Northrop's Newport News employees, the manager repeated the company's policy not to comment publicly on what it considers a "personnel matter," and said he "cannot address the information" contained in a Saturday Daily Press report detailing the investigation. "I'm asking you to stay focused — to remember the work we do directly contributes to the national security of our country," the letter from the manager said. Meanwhile Monday, several sources told the Daily Press that the company's investigation into as many as 40 workers continues. Several remain on administrative leave pending the results of drug tests, while others will remain off the job until the investigation concludes, said two sources with knowledge of the investigation. The probe was launched on February 23. As of February 26, company investigators had questioned several workers suspected of drug use and searched lockers, toolboxes, and employees' personal vehicles parked on shipyard property. At least 13 workers were required to submit to drug tests and inspectors found marijuana in at least two vehicles parked on shipyard property, sources said.
Source: http://articles.dailypress.com/2010-03-02/business/dp-biz_drug-folo_0302mar02_1_suspicion-of-illegal-drug-shipyard-drug-tests

[Return to top]

Banking and Finance Sector

14. *March 3, Bank Info Security* – (Colorado) **Heartland breach: Colorado bank reports new fraud.** A Colorado bank has come forward to reveal that as many as 5,000 of its customers were at risk because of new fraudulent transactions tied to the Heartland Payment Systems data breach. First National Bank of Durango, a $399 million institution, went public with the news on March 1, after several customers reported that their debit cards had fraudulent transactions on them. Additional staff was added by the bank to handle the front-end calls from customers. The bank's senior vice president says the first customers to come forward late last week reported strange charges on their bills. As First National bankers met to discuss the situation, they heard from several more customers and their credit card processor that several debit cards had been compromised. Fewer than 20 customers had reported fraudulent charges by March 1. First National says it has received a list of up to 5,000 card numbers, or one fourth of the debit cards it has issued, that may be compromised. No fraud amounts on the compromised cards were revealed.
Source: http://www.bankinfosecurity.com/articles.php?art_id=2259

15. *March 3, SearchFinancialSecurity.com* – (International) **RSA panel: No easy solution for Zeus Trojan, banking malware.** The Zeus Trojan, a sneaky, ever-changing malware comes in many variants and is constantly finding ways to evade detection, said the vice president of online security and enrollment at Bank of America. "The complexity of the Trojan is what makes it so scary," he said during a panel discussion on banking malware on March 2 at the RSA Conference. New solutions to fight the threat can quickly become outdated, he added. Bank of America does a lot of threat scoring; last year, phishing was the top threat facing its customers. But this year, in the wake of Zeus, "The customer endpoint has become the number one threat," he said. Cybercriminals have been using the Zeus Trojan to steal online banking credentials, and researchers say the highly customizable and easily obtainable malware kit has proven to be particularly successful. Small and midsize businesses have been especially hard hit by online banking fraud triggered by password-stealing malware.
Source:
http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1407907,00.html

16. *March 3, Free Internet Press* – (International) **Innovative bank scam: Criminals steal account numbers using one-cent transfers.** Criminals in Germany are exploiting a loophole in the banking system to get hold of customers' account details. They transfer one cent to random account numbers - if the transfer goes through, they know they can steal money from the account. According to German authorities, criminals attempt to transfer the sum of 1 euro cent to several accounts at a particular bank, using account numbers they have generated at random. If the payment gets rejected by the bank, then the account number does not exist - but if the transfer goes through successfully, then the crooks know they have stumbled upon a genuine account number. It's a similar approach to that sometimes used by the senders of e-mail spam, who may compile mailing lists by generating random email addresses and checking to see which of those accounts accept the messages. Armed with the account number, the crooks then start transferring sums of money out of that account, disguised as payments for supposed purchases or services. Often, they merely inform their own bank that they have the right to withdraw money from the account by direct debit, a procedure often used by utility companies, government institutions and associations. German banks generally do not check very closely to make sure the recipient has the right to make the direct debit. Instead, the onus is on bank customers to spot illicit withdrawals from their account - in cases of fraud, account holders have 13 months to cancel a transaction.
Source: http://freeinternetpress.com/story.php?sid=24774

17. *March 3, Washington Post* – (National) **Senators propose consumer-protection regulator within Fed.** Some lawmakers who set out to improve financial regulation by stripping the Fed of its powers are moving toward the grudging conclusion that the Fed should hold even more power. The central bank was responsible for the health of the nation's largest banks and the safety of American borrowers. Its failures in both roles have been well documented. Even so, key lawmakers on the Senate banking committee are seeking bipartisan support for a plan to house a new consumer-protection regulator inside the Fed. Separate efforts to strip the Fed of its responsibility for overseeing large

banks have lost momentum. Adding authority to the Fed has emerged as the only viable option, congressional aides said. Democrats wanted a free-standing consumer-protection agency. Republicans were willing only to tuck a new regulator inside another agency. Democrats suggested the Treasury Department. Republicans said no. The Fed, whose leaders had largely abandoned efforts to retain a role in consumer protection, was left as the last candidate.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/03/02/AR2010030204176.html?hpid=topnews

18. *March 2, SC Magazine* – (International) **Banks encouraged to implement decent multi-factor authentication to securely offer online banking.** Multi-factor authentication will solve the problems of online banking. In a blog posting on the threatpost website a senior anti-virus researcher in Kaspersky Lab's global research and analysis team claimed that banking Trojans reached a form of maximum sophistication in 2007. This specific subset of banker Trojans was - and still is - extremely sophisticated and will exploit per-bank specific vulnerabilities in the implementation of two-factor authentication. He said that a lot of banks do not employ two-factor authentication and when they do, it is a very weak form of it. He said, "In short: online banking requires multi-factor authentication. The authentication code needs to be received or generated on a device, which is not connected to the device that is doing the transaction. Ideally, not only the transaction authorisation code is generated dynamically but also the password for logging onto the banking site. One thing to keep in mind here is that the cryptographic response algorithm needs to be different for logging on and approving transactions." A solution inside this, suggested the researcher, is to make the receiving bank account number a part of the authentication process, either by sending along the number with the SMS or using it as an additional challenge when using a token.
Source: http://www.scmagazineuk.com/banks-encouraged-to-implement-decent-multi-factor-authentication-to-securely-offer-online-banking/article/164880/

19. *March 2, NACS Online* – (California) **California police nab two alleged in skimming scam.** Police announced the arrest of two men that they maintain ran an ID theft ring that used gas pumps to wipe-out bank accounts, KGO-TV reports. The suspects targeted at least 20 Bay Area cities, and police say that they are responsible for at least 400 identity thefts, all originating at gas stations. Martinez police said that the men used skimming devices to access people's bank accounts. A 7-Eleven clerk performing routine maintenance discovered the devices inside one of his store's pumps and notified police. Detectives installed a decoy device and apprehended the suspects when they came to retrieve it. Police estimated that skimming operations net $20,000 a day each. The PCI SSC Skimming Prevention paper can be downloaded online.
Source: http://www.nacsonline.com/NACS/News/Daily/Pages/ND0302102.aspx

For another story, see item **47**

[Return to top]

Transportation Sector

20. *March 3, Associated Press* – (New York) **FAA probes audio of child directing air traffic.** A child apparently directed pilots last month from the air-traffic control center at John F. Kennedy Airport, one of the nation's busiest airports, according to audio clips. The Federal Aviation Administration said Wednesday that it was investigating. "Pending the outcome of our investigation, the employees involved in this incident are not controlling air traffic," the FAA said in a statement. "This behavior is not acceptable and does not demonstrate the kind of professionalism expected from all FAA employees." The child can be heard on the tape making five transmissions to pilots preparing for takeoff. In one exchange, the child can be heard saying, "JetBlue 171 contact departure." The pilot responds: "Over to departure JetBlue 171, awesome job." The child appears to be under an adult's supervision, because a male voice then comes on and says with a laugh, "That's what you get, guys, when the kids are out of school." The FAA said the control tower is a highly secure area for air-traffic controllers, supervisory staff and airport employees with a need to be there. FAA spokesman said children of the tower's employees are allowed to visit but would need to get approval from the FAA first.
Source:
http://online.wsj.com/article/SB10001424052748703862704575099413770764770.html?mod=WSJ_latestheadlines

21. *March 3, Cincinnati Enquirer* – (Ohio) **Train derails in Hamilton.** A CSX train derailed Wednesday morning in the area of Martin Luther King Boulevard and Walnut Street, a Hamilton police dispatcher said. No injuries have been reported, but traffic is blocked until further notice, she said. "Four or five cars flew off the track. The wheels flew off and everything," said a spokesman for Hamilton police. The cars were empty, and no spills have been reported, he said. Traffic is expected to be blocked on Martin Luther King Boulevard most of the day because another train must be dispatched to tow the damaged one away and clear the cars. Motorists are advised to detour around the area by taking High Street instead of Martin Luther King Boulevard.
Source:
http://news.cincinnati.com/article/20100303/NEWS01/303030032/Train+derails+in+Hamilton

22. *March 1, Idaho Press-Tribune* – (Idaho) **Local airports say Austin crash would be difficult to prevent.** Directors of Nampa's and Caldwell's airports say little could be done at their facilities to prevent a tragedy like the one that took place last month in Austin, Texas. On February 18, a man crashed his small plane into an Austin office building that housed federal employees. The pilot and an office worker died. The directors said their airports would be hard pressed to prevent a similar action from happening there. "The guy owned the airplane, so that's pretty hard to catch," one director said. "How in the world can you police something like that?" The director said the Caldwell Airport keeps names of owners of hangars and people who have planes tied down there. But he said the airport does not keep track of takeoffs and landings, and pilots do not file flight plans unless they are traveling across the country. Both

airports urge pilots to follow an airport watch program to keep an eye out for suspicious behavior. But since the Austin pilot had not exhibited any unusual actions at the airport out of which he flew, even that program probably would not have stopped him.
Source: http://www.idahopress.com/news/article_0023a002-25c5-11df-8bf1-001cc4c03286.html

For more stories, see items **1**, **4**, **6**, and **29**

[Return to top]

Postal and Shipping Sector

23. *March 1, KRDO 13 Colorado Springs* – (Colorado) **Colo. man arrested in white powder mailings.** FBI agents have arrested a Denver area man suspected of sending white powder to multiple governmental offices including the offices of a U.S. Senator, an Eldorado Springs Democrat, a Denver Democrat; and the offices of two Representatives, one a Denver Democrat; and the other an Aurora Republican. The 41 year-old suspect, of Denver, Colorado, was charged by Criminal Complaint for mailing a threatening letter to a victim on February 15, 2008. The suspect was arrested by agents with the FBI Joint Terrorism Task Force and the U.S. Postal Inspection Service late Friday night, February 26.
Source: http://www.krdo.com/Global/story.asp?S=12065670

For more stories, see items **33** and **58**

[Return to top]

Agriculture and Food Sector

24. *March 3, Food Safety News* – (National) **Kroger recalls beef products for E. coli.** Between February 18 and 24, 2010, Kroger, the country's largest grocery store chain, recalled five separate beef products for potential E. coli O157:H7 contamination. The recall information is listed on the company's Web site, but in very limited detail. According to the Kroger Web site, burritos and tamales containing beef potentially contaminated with E. coli O157:H7 were distributed under the Little Juan, Tina's, Don Miguel, XLNT, and Deli names. Retailers distributing these brands are Smith's Food and Drug, Ralphs, Food 4 Less, King Soopers, QFC, and Fry's. The Food Safety and Inspection Service (FSIS), however, does not have these corresponding products or brands listed on their current recall list, which FSIS policy mandates. The current recalls listed on the Kroger site would fall under the Class I category.
Source: http://www.foodsafetynews.com/2010/03/kroger-recalls-beef-products/

25. *March 3, KMTV 3 Omaha* – (Nebraska) **Fire damages roof of Kellogg's plant in Omaha.** Emergency crews spent Tuesday night battling a fire on the roof of the Kellogg's plant in Omaha. The fire broke out just before nine o'clock at the cereal production plant near 96th and J Streets. Someone called 911, reporting flames on the

highest point of the roof. Once firefighters got to the top, they found a small fire. It did not take long for them to put the flames out, but they soon discovered that the fire may have spread into the roof of the building. They cut into the roof, to reach any extension of the fire and to make sure it had not damaged the structural integrity of the building. Within a couple of hours, firefighters had the fire knocked down and were watching to make sure no hot spots flared up. There are no reports of any injuries, and KMTV was told that many workers did not even have to evacuate the building.
Source: http://www.action3news.com/Global/story.asp?S=12074225

26. *March 2, U.S. Food Safety and Inspection Service* – (National) **North Carolina firm recalls beef products due to possible E. coli O157:H7 contamination.** Randolph Packing Co. Inc., an Asheboro, North Carolina establishment, is recalling approximately 96,000 pounds of beef products that may be contaminated with E. coli O157:H7, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced on March 2. Each package label bears the establishment number "EST. 6590" inside the USDA mark of inspection. The products were produced on February 25, 2010, and were distributed to federal establishments for further processing in Illinois, Missouri, New York, Ohio, and Virginia. None of these products are available directly to consumers. The problem was discovered through FSIS microbiological sampling.
Source:
http://www.fsis.usda.gov/News_&_Events/Recall_013_2010_Release/index.asp

27. *February 28, Associated Press* – (New York) **Cattle stuck in NY barn after snow collapses roof.** About 50 to 60 cattle were trapped inside a dairy barn in the upstate New York town of Fenner after the structure's roof partially collapsed under the weight of heavy snow. Volunteer firefighters and neighbors worked to shovel the snow off the collapsed part of the barn to free the animals on Saturday and to assess the damage. The Smithfield fire chief said some cattle died in the 4:45 p.m. collapse at the Stone Brothers Farm and Greenhouse. He said a 60- to 80-foot section of roof collapsed after being weighed down by an accumulation of heavy snow over the past two days. Fenner is about 8 miles south of Rochester, New York in Madison County.
Source: http://www.wcax.com/Global/story.asp?S=12059215

[Return to top]

Water Sector

28. *March 2, KHQA 7 Quincy* – (Missouri) **Water main break forces water shut off.** Clarence, Missouri, was without a water supply Tuesday. KHQA-TV got a phone call from the village hall saying that the main water supply line near the water tower in town gave way and the only way to fix the problem is to shut off the water supply. They expected the repair to last a few hours and are hoping to have the problem fixed sometime late Tuesday afternoon.
Source: http://www.connecttristates.com/news/story.aspx?id=423982

29. *March 2, WSVN 7 Miami* – (Florida) **Crews work to repair broken water main.** Crews have been working around the clock to make the necessary repairs to a water main that broke Tuesday in Hialeah, Florida. An estimated 10 million gallons of water flooded the streets, homes and cars in the neighborhood at around 1 a.m. The break also created a sinkhole 40-feet wide and about 10-feet deep at the intersection of West Fourth Avenue and 41st Place. Hialeah Police is diverting all traffic away from the area of West Fourth Avenue from West 37th Street to West 42nd Street, until further notice. Some residents also lost power. As of Wednesday morning, the majority of residents had power restored to their homes. Crews said it may take a week to repair the water main and fill the sink hole.
Source: http://www.wsvn.com/news/articles/local/MI145152/

30. *March 2, Bowling Green Daily News* – (Ohio) **Chlorine leak forces plant evacuation: No injuries reported; BGFD says leak did not present a public health hazard.** A chlorine leak at Bowling Green Municipal Utilities' wastewater treatment facility on Preston Avenue resulted in the evacuation of all employees the morning of March 1. No injuries were reported from the incident, which a BGMU spokesman said was discovered at about 10 a.m. on March 1 when two employees were changing a one-ton chlorine cylinder in the treatment plant's chlorine room. A siren indicating the leak sounded and employees were evacuated for slightly more than two hours, with several dozen standing at the intersection of Preston Avenue and Pearl Street. The Bowling Green Fire Department responded and the leak ultimately did not present a public health hazard. "They went in and evaluated the situation, and fortunately the leak was very small and they got everything under control," he said. An assistant chief for the Bowling Green Fire Department said the tank leak was able to be stopped and the tank will eventually be sent back to the company that manufactured it to fix the leak permanently.
Source: http://www.waterworld.com/index/display/news_display/141961673.html

[Return to top]

Public Health and Healthcare Sector

31. *March 3, WBRU 95.5 Providence* – (Connecticut) **Hospital patient shoots nurse.** Authorities in Connecticut say an eighty-five-year-old patient accused of shooting a nurse and himself remains hospitalized. Police say the man was being treated at Danbury Hospital when he shot a male nurse three times yesterday. He then shot himself after hospital staff restrained him. Neither man's injuries are life threatening. The man faces charges of first-degree assault and carrying a revolver without a permit.
Source: http://news.wbru.com/2010/03/hospital-patient-shoots-nurse/

32. *March 3, Network World* – (National) **Medical identity theft strikes 5.8% of U.S. adults.** Identity thieves are not only interested in tapping financial resources, but are also after your medical identification data and services. Medical identity theft typically involves stolen insurance card information, or costs related to medical care and

equipment given to others using the victim's name. Roughly 5.8% of American adults have been victimized, according to a new survey from The Ponemon Institute. The cost per victim, on average, is $20,160. "The National Study on Medical Identity Theft" is based on findings from 156,000 people who agreed to discuss identity theft in general. Among those surveyed, 5.8% provided specific details about how they had been hit by medical ID theft, in particular. Extrapolating to the general U.S. population, that means an estimated 1.42 million adults in this country may have experienced some type of fraud involving theft of their medical identification information, the report claims. According to the survey, 29% of victims of medical ID theft discovered the problem a year after the incident, and 21% said it took two or more years to learn about it. The average cost of sorting out the mess was $20,160, which might include making out-of-pocket payments to a health plan provider to restore coverage. Nearly half of the victims (48%) lost coverage due to medical ID theft. Roughly 75% found resolution difficult, and only about 25% said there were no consequences due to the theft.
Source: http://www.computerworld.com/s/article/9164979/Medical_identity_theft_strikes_5.8_of_U.S._adults

33. *March 3, Martinsburg Journal* – (Virginia) **Suspicious mail package closes facility.** Agents from the Federal Bureau of Investigation were investigating an incident at the Stephens City Community-Based Outpatient Clinic Tuesday in Winchester, Virginia, after a suspicious package led to the facility to being closed for safety precautions. The medical facility is one of six outpatient clinics operated for and by the Martinsburg Veterans Affairs Medical Center, which closed the facility located at 170 Prosperity Drive at 2:30 p.m. Tuesday to ensure the safety of both patients and staff after the suspicious package was discovered, according to a news release from the facility. No further information is available pending final investigation of the incident, the release stated.
Source: http://www.journal-news.net/page/content.detail/id/532668.html?nav=5006

34. *March 2, University of Rochester* – (New York) **U.S. agency selects Rochester for radiation research contract.** The University of Rochester Medical Center has received a $3.9 million one-year contract, with options to increase to a total of $42 million over the next four years, to develop a simple, quick blood test to measure radiation exposure after an act of terrorism or nuclear accident. The project is funded by the Biomedical Advanced Research and Development Authority (BARDA), within the Office of the Assistant Secretary for Preparedness and Response in the U.S. Department of Health and Human Services. http://www.hhs.gov/aspr/ The URMC was one of nine institutions to win BARDA awards, totaling $35 million for the first year and up to $400 million over five years.
Source: http://www.urmc.rochester.edu/news/story/index.cfm?id=2772

[Return to top]

Government Facilities Sector

35. *March 3, Daily Advance* – (North Carolina) **Student charged for false bomb threat.** A 16-year-old student was charged with making a false bomb report at Currituck County High School last month. The Currituck County Sheriff's Office investigated a report of a bomb threat on Feb. 9 about 1:35 p.m. The threat was that a bomb attack would take place, according to a news release by a law enforcement spokeswoman. A school resource officer from the sheriff's office and high school staff discovered who the caller was, a student, charged him with making a false bomb report on a public building and seized a computer at the student's home. He was given a first appearance on February 17.
Source: http://www.dailyadvance.com/news/student-arrested-bomb-threat-school-16878

36. *March 3, ClickonDetroit.com* – (Michigan) **Drano bomb goes off in Detroit school.** Students at Phoenix Multicultural School on Detroit's southwest side were evacuated Wednesday morning after a "Drano bomb" detonated inside the building, said authorities. The explosive device, made of household cleaning chemicals, went off in the hallway of the building at about 8:30 a.m., sending fumes into the air, said a school official. School officials said no students were injured because they were all inside classrooms. "The device itself could have caused a lot of damage if there were a lot of children around when the device actually went off. Those types of bombs are very, very unstable", said a police inspector with the DPD Bomb squad. Police said the 540 students at the K-8 school were immediately evacuated, and many were forced out into the cold without their coats. The students were bused to Roberto Clemente School in Detroit, which is located at 1551 Beard Street. Parents are asked to pick them up there at the end of the day. School is expected to resume at Phoenix Multicultural Thursday. A 14-year-old student is in police custody. Homeland security agents were at the scene with bomb-sniffing dogs, and have given the all clear. An investigation into how the student brought the device into the building is under way.
Source: http://www.clickondetroit.com/news/22726704/detail.html

37. *March 2, DNAinfo* – (New York) **Manhattan courthouse to stay closed Wednesday due to basement fire.** The main Manhattan criminal court building will remain closed again on Wednesday because of damage from a two-alarm fire that injured eight people and emptied the building for most of the day Tuesday, officials said. The 100 Centre Street courthouse may even be shut down for several days or an entire week, court sources said. Five firefighters, two civilians and one inmate sustained minor injuries. Only one was hospitalized and taken to Bellevue for treatment, a spokesperson for the FDNY said. One firefighter — who did not appear to be seriously injured — was carried out of the building on a stretcher. Fire marshals were still investigating the cause of the basement fire Tuesday evening, which sources said started inside a wooden storage shack in the basement of 100 Centre Street. Many of Wednesday's scheduled criminal court appearances will be held across the street at 111 Centre Street, said a spokesperson for the New York State court system. As court officers evacuated the building, hundreds of people filed out to surrounding streets, and inmates were all temporarily taken to the Manhattan Detention Center next door.

Source: http://www.dnainfo.com/20100302/manhattan/manhattan-courthouse-fire-leads-evacuation

38. *March 2, Los Angeles Times* – (New York) **Some voice support for terrorism trials in New York.** Though Manhattan officials and New York lawmakers have forced the Attorney General to reconsider, lawyers, federal marshals and security experts on other high-profile terrorism cases think that a trial can safely go forward. Others differ. The two top federal marshals who coordinated security in Denver for the 1997 trial of the Oklahoma City bomber said it seemed prudent to keep the September 11 suspects' trial out of a crowded hub like Manhattan. In the Senate, legislation has been introduced, with 28 co-sponsors so far, to deny all federal funding for trial security. That prompted the Attorney General and Defense Secretary to advise Congress last week that "it would be unwise and would set a dangerous precedent for Congress to restrict" terrorism prosecutions.
Source: http://www.latimes.com/news/nationworld/nation/la-na-terror-trial3-2010mar03,0,3150539.story?track=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+latimes/news/nationworld/nation+(L.A.+Times+-+National+News)

39. *March 2, Associated Press* – (Florida) **Suspicious bag in St. Pete building found harmless.** Officials say a suspicious package that led to the evacuation of a 10-story government building on Florida's Gulf coast turned out to be harmless. A brown bag with something inside was found propped against a door near the Pinellas County Supervisor of Elections office at about 11:30 a.m. Tuesday. The building also contains the courthouse and other government offices. Police said employees did not recognize the package. The Tampa Police Bomb Squad responded. It wasn't immediately clear what was found inside the bag. Roads around the building were sealed off but traffic is now flowing again.
Source: http://www.miamiherald.com/2010/03/02/1508403/suspicious-package-found-in-government.html

40. *March 2, Associated Press* – (Oregon) **Feds: Sergeant stole from Ore. Air National Guard.** Federal investigators say a member of the Oregon Air National Guard stole ATVs, motorcyles and electronics, then used Craigslist.com to resell many of the items. A search warrant affidavit unsealed in U.S. District Court on Tuesday says neighbors saw the Senior Master Sergeant bringing the items home in a U.S. Air Force truck, then resell them to people who showed up there. Investigators placed a hidden camera outside Senior Master Sergeant's house last November to monitor anyone coming and going. A special agent with the Department of Defense Criminal Investigative Service writes that he and FBI agents worked together to confirm that the three motorcycles, two ATVs and other items had vanished from the Senior Master Sergeant's unit, the 125th Special Tactics Squadron out of Portland. The Senior Master Sergeant has not been charged with any crime. He has an unlisted phone number and could not immediately be reached for comment Tuesday.
Source: http://www.seattlepi.com/local/6420ap_wa_national_guard_theft.html

41. *March 1, Greensboro News & Record* – (North Carolina) **Hacker broke into Bennett College office computer.** Police are investigating a computer breach at Bennett College, where a hacker accessed personal information of about 1,100 employees and students. The college's director of information technology said there was no indication the information had been used — just that it has been accessed. The breach at a payroll computer occurred the weekend of February 13 and involved names, Social Security numbers, birth dates, pay rates and bank transit numbers, the IT official said. He described it as "cybervandalism." The college posted an FAQ on its Web site and set up an automated number to call for updated information. The college reported the breach February 19, a Greensboro police detective said. At this point, it's hard to say what charges might be filed in the case because investigators are still determining what took place said the detective, who works for the computer forensics unit in the criminal investigation division. He would not comment on whether any money had been taken from victims' bank accounts or whether there were any suspects. "I really don't want to give out too much information," the detective said.
Source: http://www.news-record.com/content/2010/03/01/article/hacker_broke_into_bennett_college_office_computer

For another story, see item **23**

[Return to top]

Emergency Services Sector

42. *March 3, San Bernadino Press-Enterprise* – (California; National) **Hemet assassination plot follows national spike in police attacks.** Two recent assassination attempts on Hemet, California, gang task-force officers add to a national trend of more brazen and sophisticated attacks on police, often by gang members, law enforcement experts say. The attacks on the Hemet-San Jacinto Gang Task Force headquarters come amid an increase of violence against police nationwide this year that could reverse a trend of declining officer deaths. Both attempts in Hemet failed, but were characterized as unusually violent. Last week, a bullet fired by an altered gun narrowly missed an officer opening a parking lot gate at the task force's building, a block from the police station. On New Year's Eve, the same building was targeted when a gas line was rerouted to rig the building to explode when officers stepped inside. Experts say attacks on a police facility, such as the ones against the Hemet Gang Task Force building, are nearly unheard of. The FBI has joined the task force in the investigation of the attacks. While Hemet police have not identified any suspects, they believe the threat may involve area gang members now under investigation. Nationally last year, 125 officers were killed, the lowest number since 1959. Already this year, 34 officers have been killed in the line of duty in shootings and traffic fatalities, including three in California in the past week.
Source: http://www.pe.com/localnews/stories/PE_News_Local_W_attack03.4644056.html

43. *March 3, KING 5 Seattle* – (Washington) **Investigators: Radio system failing officers and public.** Across Pierce County, Washington, sheriff's deputies are encountering dead zones where their radios do not work. And even when they do work, transmissions are often scratchy, garbled or incoherent. That leaves dispatchers guessing about whether the deputies have run into trouble. That's exactly what happened when two officers were dispatched to a domestic violence call near Eatonville last December. Dispatchers at the law enforcement support agency, which handles police dispatch for Pierce County and area cities, heard an officer trying to radio in, but the call was inaudible. He had been shot and later died of his injuries. The department says a better radio system would not have saved his life, but it would have allowed dispatch to send help to the officers almost two-and-a-half minutes sooner, when the first inaudible radio call for help was made. That's because if that same call had been made over a newer, 800 megahertz system, which is what many surrounding jurisdictions use, the dispatchers at the law enforcement support agency would have known exactly who was calling in. Because with the newer system, as soon as the deputy keys the mic, a code is sent straight to the dispatcher's screen, identifying the unit. It's just like caller ID.
Source: http://www.king5.com/news/local/Investigators-Radio-system-failing-officers-and-public-85852077.html

44. *March 3, Albany Times Union* – (New York) **Firehouse has its own emergency.** The Castleton, New York, Volunteer Fire Department has been evacuated amid fear that a steep hill behind the fire station is about to collapse. The heavy rains last week caused a landslide that has buried a basketball court behind the firehouse. But officials say there are signs of a second, more severe slide threatening the already weakened hill. They fear it could give way at any time. ''It's not if the second slide will happen; it's just a matter of when,'' said the village building inspector. He said that because of the danger, there is nothing officials can do but wait for the hillside to come down. Meanwhile, the firehouse was evacuated and equipment, including three pumper tankers and an EMS/utility vehicle, was moved to the village public works garage and the Schodack Valley Fire Department. One piece of equipment was sent to East Greenbush. The department provides fire protection and EMS response for the village of Castleton and the Schodack Protective District and assists its neighbors with mutual aid, officials said.
Source: http://www.timesunion.com/AspStories/story.asp?storyID=906705

45. *March 2, HawaiiNewsNow* – (Hawaii) **Tsunami evacuation plan had glitches, state and county to examine.** The phone book was the first place many people turned to Saturday after a tsunami evacuation warning to find out if they live in an evacuation zone. There were many complaints the maps were not specific enough but a member of County Civil Defense says, changes are coming, " the maps in the phone book were put in place in 1990, we are looking to put new models in the next year." For most, the biggest issue with the phone books maps is that you cannot look up your exact street address, but you can online. But during this tsunami warning several websites with evacuation maps were bogged down and some even crashed because of so much traffic, "the site did get slowed down....I am wondering how many hundreds of thousands of

hit there were," he said. Some web pages like the Pacific Disaster Center are in the process of making their bandwidth more robust — saying this warning was a good test of their system. Online activity was at a peak, Hawaii News Now's website got 2 million views just on Saturday alone.
Source: http://www.hawaiinewsnow.com/Global/story.asp?S=12066943

46. *March 2, Hagerstown Herald-Mail* – (Maryland) **Maryland: Emergency personnel continue to probe 911 system outage.** Washington County, Maryland, emergency personnel on Tuesday were still investigating the cause of a 911 phone system outage, during which at least three people seeking emergency help were unable to get through on February 25, said the county's director of emergency communications. Emergency communications staff do not know how long the system was down, only that it was not working properly for at least 65 minutes, she said.
Source: http://www.herald-mail.com/?cmd=displaystory&story_id=240816&format=html

[Return to top]

Information Technology Sector

47. *March 3, Reuters* – (International) **Spain busts global botnet masterminds.** Spanish police have arrested three men accused of masterminding one of the biggest computer crimes to date — infecting more than 13 million PCs with a virus that stole credit card numbers and other data. The men were suspected of running the Mariposa botnet, named after the Spanish word for butterfly, Spain's Civil Guard said on March 2. A press conference to give more details is scheduled for March 3. Mariposa had infected machines in 190 countries in homes, government agencies, schools, more than half of the world's 1,000 largest companies and at least 40 big financial institutions, according to two Internet security firms that helped Spanish officials crack the ring. The security firms — Defense Intelligence Inc. of Canada and Panda Security S.L. of Spain — did not say how much money the hackers had stolen from their victims before the ring was shut down on December 23. Security experts said the cost of removing malicious program from 13 million machines could run into tens of millions of dollars. Mariposa was programed to secretly take control of infected machines, recruiting them as "slaves" in an army known as a "botnet." It would steal login credentials and record every key stroke on an infected computer and send the data to a "command and control center," where the ringleaders stored it.
Source: http://www.reuters.com/article/idUSTRE6214ST20100303

48. *March 2, Christian Science Monitor* – (National) **White House declassifies parts of US cybersecurity plan.** On March 2, the White House declassified cybersecurity somewhat when the cybersecurity czar pulled back the curtain, at least a bit, on the the previous U.S Presidential Administration's secretive plan to defend the nation's computer networks. At the RSA Conference, a security industry event, in San Francisco on March 2, the czar announced that the current Presidential Administration was partially declassifying the 2008 Comprehensive National Cybersecurity Initiative

(CNCI) in the name of transparency. The declassified portion of the CNCI includes descriptions of 12 broad initiatives of the CNCI, but few details. According to the Wired Threat Level blog, "the most most controversial part of the declassified plan is a discussion of a need for the government to define its role in protecting private critical infrastructure networks" such as telecoms, the electric grid, Internet providers, and banking networks. The document largely focuses on efforts to secure the federal government's vast computer networks with the use of its Einstein system to detect unauthorized attempts to access government computers.
Source: http://www.csmonitor.com/USA/2010/0302/White-House-declassifies-parts-of-US-cybersecurity-plan

49. *March 2, The Register* – (International) **Microsoft wants to put infected PCs in rubber room.** A top Microsoft executive is floating the idea of creating mandatory quarantines for computers with malware infections that pose a risk to internet users. The informal proposal, made on March 2 by Microsoft's vice president of trustworthy computing was short on specifics, such as who would be responsible for monitoring and isolating malware-riddled machines. But he laid out his case for keeping them away from the general populace, comparing such a move to laws that have gone into effect over the past 20 years banning cigarette smoking in public. The vice president is the latest to champion the idea that infected PC users should be put in their own rubber room, so the malware, spam, and other attacks they generate can't harm others. The logistics of such a plan remain woefully unformed. While many say ISPs should monitor subscribers for infections, there's considerable disagreement about how providers should carry out and pay for such a system.
Source: http://www.theregister.co.uk/2010/03/02/microsoft_charney_rsa/

50. *March 2, ComputerWorld* – (International) **Microsoft again pushes patch linked to Windows blue screens.** Microsoft on March 2 said it had restarted distribution of a security update that had crippled some Windows PCs last month with reboot problems and Blue Screen of Death error screens. The update, dubbed MS10-015, originally shipped on February 9, but was pulled from Windows Updates' automatic update two days later after complaints flooded Microsoft's support forum from users whose machines refused to restart after they had installed the patch. The affected PCs shuddered to a stop at the blue screen which indicates a serious software error and crash in Windows. Within a week, Microsoft announced that only PCs infected with the "Alureon" rootkit were incapacitated by MS10-015. It denied that there was any flaw in the security update itself. Users who have already installed MS10-015 without problems do not have to reinstall it, Microsoft said.
Source:
http://www.computerworld.com/s/article/9164518/Microsoft_again_pushes_patch_linked_to_Windows_blue_screens

51. *March 2, Help Net Security* – (International) **6 in 10 malicious URLs bypass AV scanners and URL filtering.** M86 Security released a new report revealing its Security Labs research results based on the primary attack vectors on the Web and how the common approaches used to fend off these attacks stand up in today's dynamic threat

landscape. The report titled "Closing the Vulnerability Window in Today's Web Environment," discloses both quantitative research on the percentage of Web threats correctly identified by URL filtering (3%) and Anti-virus scanning (39%) over the course of last month and three real-life studies of specific attacks, which are increasing in frequency: dynamic obfuscated code, hacking of legitimate Websites, and zero-day vulnerabilities. In February 2010, Security Labs collected and tested more than 30,000 live malicious URL samples against the typical tools of third-party URL lists and anti-virus scanners. The analysis found that in the best case scenario, 6 in 10 malicious URLs pass unnoticed through anti-virus scanners and URL filtering, even when these two approaches are used together. The test also looked at the growth rate of signatures behind anti-virus scanners, such as the popular AV-Test.org's malware collection, and found that despite the dramatic increase in signatures, organizations and end-users are less protected because of the evasive methods cyber criminals use as well as the real-time dynamic nature and sophistication of today's Web-based attacks.
Source: http://net-security.org/secworld.php?id=8956

52. *March 2, The Register* – (International) **Zombie tactics threaten to poison honeypots.** Innovations in botnet technology threaten the usefulness of honeypots, one of the main ways to study how bot herders control networks of zombie PCs. Computer scientists at the University of Central Florida warn that bot herders can now avoid honeypots - unprotected computers outfitted with monitoring software - set up by security firms. Ethical concerns mean that security firms do not allow their infrastructure to be used in sending spam or running attacks against victims. By monitoring such instructions it's therefore possible for cybercrooks to program command and control servers to disable or simply ignore these machines, thus depriving security firms of vital intelligence in how zombie botnets are operating in the real world. The scientists are working on techniques to make stealthier honeypot traps to trick bot herders. Preliminary findings from the Florida team's research were published in a recent edition of the International Journal of Information and Computer Security.
Source:
http://www.theregister.co.uk/2010/03/02/honeypot_anti_security_countermeasures/

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 3, Washington Post* – (National) **FCC Chairman Genachowski confident in authority over broadband, despite critics.** Internet service providers are stepping up

their campaign to prevent the Federal Communications Commission from regulating them like telephone companies and questioning the limits of the agency's power over the Internet. The commission chairman said in an interview on March 2 at The Washington Post that he's confident of the agency's authority, and that his focus is on moving ahead with the administration's campaign to bring high-speed Internet to all American homes. The FCC will present a national broadband plan to Congress in two weeks. The chairman said he plans to recommend unleashing 500 megahertz of spectrum for the next generation of smartphones, tablet computers and other portable devices that connect people wirelessly to the Web. But he wouldn't answer whether the FCC is considering a move, urged by some public interest groups, to reclassify broadband service providers — the companies that provide access to the Web — so they more clearly fall under the agency's jurisdiction.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2010/03/02/AR2010030203715.html

54. *March 3, DarkReading* – (International) **Ponemon study: Voice calls may be at risk.** A survey released today by the Ponemon Institute suggests that large and medium businesses are putting themselves at risk of cell phone voice call interception. According to a survey of seventy five companies and 107 senior executives in the United States, it costs U.S. corporations on average $1.3 million each time a corporate secret is revealed to unauthorized parties. Eighteen percent of respondents estimate such losses to occur weekly or more frequently; 61 percent say such leaks occur at least monthly. Ninety percent of companies say such leaks occur at least once a year. 67 percent of IT practitioners surveyed lack confidence that the proprietary and confidential information conveyed during cell phone conversations is adequately secured in their organizations. Eighty percent believe that their organizations would not discover the wrongful interception of a cell phone conversation that revealed valuable corporate secrets. Only 14 percent of organizations have deployed technological solutions to personnel travelling to high risk locations. Eighty-three percent of companies are not even training employees about the risks of using cell phones in high risk areas, Ponemon says.
Source: http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml?articleID=223101322&subSection=Vulnerabilities+and+threats

55. *March 3, Wall Street Journal* – (National) **Verizon Wireless fixes network outage.** Some Verizon Wireless customers in the eastern half of the U.S. were temporarily left without access to data services such as mobile Web and email early on March 3. The network outage, which was resolved by 8:15 a.m. Eastern Time, affected customers "east of the Mississippi," according to a spokesman. He cited "bad switch software" which resulted in a deterioration of service and lower wireless speeds. Not everyone in the area was affected, the spokesman said. Data access in New York, for instance, continued to work on March 3.
Source: http://online.wsj.com/article/SB10001424052748703862704575099402573651516.html?mod=WSJ_latestheadlines

56. *March 2, Homeland Security NewsWire* – (National) **FCC's new public safety proposal receives mixed response.** Ever since the 9/11 terrorist attacks, the United States has been trying to create a national, interoperable network for public safety. The plan encountered many hurdles, not least when the D Block of the 700 MHz band, earmarked for a public/private safety initiative, failed to reach its reserve price at auction in 2008. Now, the Federal Communication Commission (FCC) chief has announced new plans to relaunch the plan, putting up to $16 billion and more spectrum behind the proposals. A spokeswoman for Rethink Wireless's writes that some public safety groups are disappointed that the plan does not go further, while the wireless carrier community remains undecided on the plan. The FCC plans to re-auction the D Block, and will call on Congress to allocate $12 billion to $16 billion in funding over ten years to help build the network. The FCC also wants safety agencies to have access to the whole 700 MHz band, not only to the D Block. Verizon Wireless will soon start building its LTE network in the band, and AT&T has plans to do the same from 2011. Another major existing 700 MHz user is Qualcomm, for its MediaFLO mobile TV system.
Source: http://homelandsecuritynewswire.com/fccs-new-public-safety-proposal-receives-mixed-response

57. *March 2, MyCentralJersey.com* – (New Jersey) **Fire official: Welder hurt in explosion in Carteret.** A welder was sent to the hospital after a small explosion on Federal Boulevard in Carteret late Tuesday morning, according to a fire official. The fire captain said a worker was welding at a construction site at the Verizon Wireless data center on Federal Boulevard at 11:31 a.m. on March 2 when a blast made the doors of his nearby truck fly off and hit him. The captain said he did not know what the welder was working on, but said that the blast did not cause a fire. "Something touched off an explosion,'' he said. "I wouldn't say it was a big explosion, but it was enough to basically blow the compartment doors off of his truck, and the compartment door struck him.'' Authorities are investigating the cause of the blast.
Source: http://www.mycentraljersey.com/article/20100302/NEWS/100302051/-1/newsfront

[Return to top]

Commercial Facilities Sector

58. *March 2, WTOP.com and Associated Press* – (District of Columbia) **Powder found at D.C. office building not hazardous.** Authorities have given the all-clear after an office building near Union Station was evacuated Tuesday due to a suspicious envelope. There are no reports of injuries or illness. An envelope filled with white powder that was found at the American Psychological Association offices is not hazardous, a District of Columbia fire department spokesman tells WTOP. The powder was found in the first-floor mailroom of the building — located on First Street in Northeast D.C. — around 1:30 p.m. Tuesday. Crews have not identified any toxic or hazardous material, but they will take the substance to a lab for further testing. The FBI is also investigating, the spokesman says. Three people who were in the mailroom went to the

hospital on their own, before paramedics arrived, he added. They did not show symptoms of illness.
Source: http://www.wtop.com/?nid=596&sid=1901665

59. *March 2, Border Bureau, KENS 5 San Antonio, and Associated Press* – (International) **Feds: Gun battle along Rio Grande spills over into Nuevo Laredo zoo.** On Tuesday, the U.S. Consulate in Nuevo Laredo issued a warning that a gun battle had begun raging just yards from the Texas-Mexico border, spilling from the local streets into the municipal zoo. The consulate has advised all Americans in Nuevo Laredo to "take precautions until the fighting subsides." The battle comes just days after a state of unease settled over Nuevo Laredo. Border residents online and in the streets have been bracing for a clash between drug cartels. There have been several attacks in the Nuevo Laredo area, though KENS 5 has been unable confirm details of the fighting. The city's mayor said two attacks involved explosions at police stations, possibly from grenades. On February 24, the U.S. Consulate in Monterrey warned U.S. citizens to avoid the Mexican border state of Tamaulipas, home to Nuevo Laredo. The fighting will likely have an impact on the local economy. Merchants in downtown Nuevo Laredo say after years of staying away, tourists were just starting to return. Tuesday's violence will probably keep tourists away from the border town.
Source: http://www.kens5.com/news/Reports-Gunfights-along-Rio-Grande-spill-over-into-Nuevo-Laredo-zoo-86023272.html

For another story, see item **8**

[Return to top]

National Monuments and Icons Sector

Nothing to report

[Return to top]

Dams Sector

60. *March 3, Smithfield Times* – (North Carolina) **Erosion threatens town's dam on Waterworks Road.** Heavy rainfall in recent months weakened the Waterworks Road Dam, and consultants recommend immediate repairs — to the tune of about $300,000. Members of the Smithfield Town Council discussed the dam with two engineers from the consulting firm, Draper Aden, during a recent Public Works Committee meeting. "We strongly recommend that, if there is any way to treat this as an emergency project, that we do that," said an engineer. This will mean forgoing the regular procurement process in order to begin the job sooner, he said. The committee agreed with his recommendation. A motion to approve a sole-source emergency bid for the project was included in Town Council's Tuesday night meeting consent agenda. The engineer showed pictures of the dam, and explained that there has been "extensive erosion" on the structure's steep spillway bank. All the riprap and underlying fabric from that

section of the dam has been washed off the bank and is piled up downstream. The issue is a safety concern, because if left unfixed, the bank will continue to erode and Waterworks Road could be seriously compromised. “We’re about 18 inches from losing the guardrail.” He recommended that the town immediately commission a design/build project to stabilize the bank quickly. His plan included extending the existing spillway pipe by 20 feet to decrease the steepness of the bank and reduce erosion.
Source: http://www.smithfieldtimes.com/index.php/news/25-top-stories/140-waterworks-road-dam-

61. *March 3, Oregon Statesman Journal* – (Oregon) **Dam plans target early warning system.** Additional funding for the Silver Creek Dam early- warning monitoring system may allow the city to more easily notify residents of dam failure. The monitoring system, which has been discussed in variations for years, will visually monitor the dam and collect data that could alert Silverton officials to signs of a potential emergency situation. How officials will alert residents is another aspect of the project. Although an agreement has not yet been signed, the U.S. Army Corps of Engineers has notified the city about available funding for the project that exceeds the amount the city budgeted for the system. The Army Corps funding would total $539,000 with the agency assuming 65 percent of costs. The city would be responsible for the remaining 35 percent, which totals just more than $188,500. The city has a total of about $235,000 budgeted for the project. According to a spokesman for the U.S. Army Corps of Engineers Portland District, the project will be funded with the agency’s appropriated general construction funds. Silverton Public Works Director said the extra money will allow for additional components to the project. One such addition is downstream warning sirens that could warn residents to evacuate or move to higher ground. Instead of a loud, droning signal, however, the siren may actually take the form of a recorded voice that would instruct residents to evacuate.
Source: http://www.statesmanjournal.com/article/20100303/COMMUNITIES/3030392/1132/news

[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