



# Homeland Security

## Daily Open Source Infrastructure Report for 25 May 2010

**Current Nationwide Threat Level**

**ELEVATED**



*Significant Risk of Terrorist Attacks*

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

### Top Stories

- According to The Associated Press, Vermont Yankee officials said that while cleaning up after a leak of radioactive tritium at the nuclear power plant, they found another, more potent radioactive isotope in soil near where the leak occurred. Strontium-90 is a byproduct of nuclear fission that has been linked to cancer and leukemia. (See item [10](#))
- San Antonio Express-News reports that U.S. Department of Agriculture fever-tick inspectors have become the latest set of American workers pulled from northern Mexico amid ongoing drug cartel violence, a move some Texas ranchers fear will reintroduce a pest that nearly wiped out U.S. cattle a century ago. (See item [34](#))

### Fast Jump Menu

#### PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

#### SUSTENANCE and HEALTH

- [Agriculture and Food](#)
- [Water](#)
- [Public Health and Healthcare](#)

#### SERVICE INDUSTRIES

- [Banking and Finance](#)
- [Transportation](#)
- [Postal and Shipping](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

#### FEDERAL and STATE

- [Government Facilities](#)
- [Emergency Services](#)
- [National Monuments and Icons](#)

### 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. *May 24, Bloomberg* – (Louisiana) **BP prepares ‘Top Kill’ operation to halt Gulf of Mexico leak.** BP Plc may try in the next few days to plug an oil leak in the Gulf of Mexico off the coast of Louisiana by injecting heavy drilling fluids into an undersea well. The so-called “top kill” operation involves “significant uncertainties” and isn’t

guaranteed to succeed, the London-based oil company said Monday in a statement. It will be followed by cement to seal the well about 5,000 feet underwater. The total cost of the clean-up has reached \$760 million. “Most of the equipment is on site and preparations continue for this operation, with a view to deployment in a few days,” BP said. BP continues to capture a portion of the oil from the leaking well. The leak began after an April 20 explosion aboard the Deepwater Horizon drilling rig, which the oil producer leased from Transocean Ltd. The “top kill” method to halt the leak requires that mud twice the density of water be pumped into the well using a Helix Energy Solutions Group Inc. rig, BP’s chief operating officer for exploration and production said last week.

Source: <http://www.businessweek.com/news/2010-05-24/bp-prepares-top-kill-operation-to-halt-gulf-of-mexico-leak.html>

2. *May 23, Allentown Morning Call* – (Pennsylvania) **Easton man caught stealing copper from PPL, police say.** An Easton, Pennsylvania man is charged with trying to stealing more than \$5,000 worth of copper from a Schuylkill County electric station, said state police in Frackville. The man is charged with theft, criminal conspiracy, criminal mischief, criminal trespass and possessing instruments of crime. He was sent to Schuylkill County Prison under \$25,000 bail. According to court records, troopers came across the man and an unidentified man inside the station and said they were stealing items. Police said the man and his accomplice cut a hole in a fence to enter the station, and tried to steal tools and a large amount of copper cable valued at \$5,500. Source: [http://www.mcall.com/news/local/all-a21\\_mc-schuylkill-theft.7282317may23,0,2781361.story](http://www.mcall.com/news/local/all-a21_mc-schuylkill-theft.7282317may23,0,2781361.story)
3. *May 23, Reuters* – (California) **Tesoro L.A. refinery hit by power outage.** Tesoro Corp’s 100,000 barrel per day Los Angeles-area refinery in Wilmington, California, was hit by an electrical power outage Sunday, according to a notice filed with California pollution regulators. “All units are releasing to flare,” according to the notice filed with the California Emergency Management Agency. “Power has been restored and units are being stabilized.” The cause of the power outage was unknown, according to the notice. Source: <http://www.reuters.com/article/idUSWEN506820100523?type=marketsNews>
4. *May 23, Marketwatch* – (Louisiana) **BP: Oil captured from Gulf spill down to 1,360 bpd.** The amount of oil BP PLC is siphoning from a massive leak on the floor of the Gulf of Mexico off the coast of Louisiana has declined to 1,360 barrels per day, a company spokesman said Sunday. The updated figure is down from the 2,200 barrels of oil per day BP said it was collecting Saturday and Friday to a vessel on the surface, and much lower than the 5,000 barrels of oil per day the oil giant said it was collecting Thursday. Thursday’s figure, which was as much crude as was officially estimated to be gushing out of a damaged well 1 mile below the surface of the water, forced BP to admit that the leak is larger than previously thought. BP has been under fire for not being able to stop the spill and for not providing an accurate estimate of how much crude is leaking. The pressure intensified last week as heavy oil has started to make landfall in Louisiana. BP has been criticized for the uncertainty over how much oil is

leaking. The current presidential administration has said the company is not doing enough to keep the government and public informed about the spill. Some lawmakers have accused BP of a “cover-up” over the size of the spill.

Source: <http://www.marketwatch.com/story/bp-oil-captured-from-gulf-spill-down-to-1360-bpd-2010-05-23>

[\[Return to top\]](#)

## **Chemical Industry Sector**

5. *May 24, KTVT 11 Fort Worth* – (Texas) **Fort Worth Dannon plant evacuated after acid spill.** A hazardous material situation at the Dannon yogurt plant in Fort Worth, Texas forced the partial evacuation of the facility Monday morning. Around 7 a.m., the Fort Worth Fire Department was notified about a hazardous materials problem at the plant located in the 1200 block of W. Peter Smith, just south of Interstate-30. It was later determined that peracetic acid, a solution primarily used for cleaning and sanitizing, had been spilled. The spill was contained to the building. There was a Level Two haz-mat response that included the evacuation of the immediate area inside the plant, advising other employees to “shelter in place,” and cordoning off streets surrounding the plant. The neighborhood around the facility was not evacuated. “This product did not pose a threat because of the concentration it was in,” explained the Fort Worth Fire Department public information officer. Some vapors were released and the City of Fort Worth Environmental Office was called to monitor downwind of the plant for any levels of the product in the atmosphere. By 9:30 a.m., the situation was under control and the product was being diluted. In all, five people were injured. Two of the injured included Dannon employees; one was decontaminated and released at the scene, the other was decontaminated and transported to a local hospital. A Fort Worth police officer, complaining of breathing problems, was also among the injured. The officer was decontaminated and transported to the hospital for observation. None of the injuries are considered life threatening.

Source: <http://cbs11tv.com/local/Fort.Worth.hazmat.2.1711695.html>

6. *May 23, WTVC 9 Chattanooga* – (Tennessee) **Train derails near south Broad Street.** A CSX train derailed just after 4 p.m. Sunday in Chattanooga, Tennessee on south Broad Street near the old Wheland Foundry site. No one was injured. But Chattanooga police said four or five cars carrying hazardous materials turned over. There have been no leaks yet, but Haz-Mat crews are on the scene making sure that does not change.

Source: <http://www.newschannel9.com/news/broad-991467-street-traffic.html>

For another story, see item [12](#)

[\[Return to top\]](#)

## **Nuclear Reactors, Materials and Waste Sector**

7. *May 23, Buffalo News* – (New York) **Protesters call for cleanup at radioactive waste dump.** About 50 people gathered outside a World War II radioactive waste dump in the Town of Lewiston, New York, Saturday morning as part of an ongoing protest against the federal government’s failure to clean up the site. Organized by the Niagara Watershed Alliance, the protesters rallied at the Niagara Falls Storage site, which began as the Army’s 7,500-acre Lake Ontario Ordnance Works and was the site of Manhattan Project research during World War II. The idea was to call attention to the lack of action by the federal government and to call on authorities to seek local input on an eventual clean-up plan. The Niagara Falls Storage Site is a 191-acre parcel owned by the Department of Energy. It contains a 10-acre “interim waste containment structure” where some radioactive waste from the Manhattan Project are buried. The dispute between some members of the public and federal regulators over input into the investigation has been going on for several years. The volunteer Restoration Advisory Board for the site has questioned federal regulators about how they have handled the investigation and some of their results. The Army Corps of Engineers, which is in charge of the cleanup, said it believes the site is not leaking.  
Source: <http://www.buffalonews.com/2010/05/23/1059194/protesters-call-for-cleanup-at.html>
  
8. *May 22, Red Wing Republican Eagle* – (Minnesota) **Prairie Island nuclear plant ‘making progress’.** U.S. Nuclear Regulatory Commission (NRC) officials said they have seen improvements in performance at the Prairie Island nuclear plant in Red Wing, Minnesota, but that progress must be maintained to eliminate issues that could undermine safety. Agency officials met with plant managers at a public meeting Thursday in Red Wing to discuss their annual assessment of the nuclear facility. The agency flagged the plant owned by Xcel Energy with a number of issues tied to human performance in 2009. “They have been making progress. The question is whether the improvements made will be sustained,” the NRC Division of Reactor Projects director said. Issues in 2009 crossed a variety of areas, but generally involved a relative lack of clear processes to manage problems, and decisions among plant staff that were not based upon “conservative assumptions,” according to the NRC’s senior resident inspector at the Prairie Island plant. Over the past year, plant officials say they have instituted a recovery plan designed to improve overall performance. Xcel recovery plan manager said that includes the development of clearer ways to manage challenges with equipment, more rigid enforcement of plant rules, fostering peer-to-peer coaching and giving lead technicians more of a leadership role. None of the issues found by the NRC directly violated regulations, said a NRC public affairs officer, but taken together they present substantive cross-cutting issues that are cause for concern with the agency.  
Source: <http://www.republican-eagle.com/event/article/id/66786/>
  
9. *May 22, Associated Press* – (National) **Texas may get nuclear waste from dozens of states.** Commissioners who oversee a nuclear waste agreement between Texas and Vermont may make the Lone Star state a radioactive burial ground for dozens of other states. The panel of eight commissioners could vote to adopt proposed rules June 12, which would allow 36 other states to bring their low-level radioactive waste for disposal in West Texas near the New Mexico border. Opponents said the dumping

ground will pollute groundwater and otherwise wreak environmental havoc. The company that runs the site contends it will be safe, and says nearby residents will see more jobs. Low-level waste includes workers' clothing, metal and other materials used at nuclear power plants, hospitals, universities and research labs. Currently those facilities store the waste at their own sites.

Source:

[http://news.bostonherald.com/news/national/southwest/view/20100522texas\\_may\\_get\\_nuclear\\_waste\\_from\\_dozens\\_of\\_states/srvc=home&position=recent](http://news.bostonherald.com/news/national/southwest/view/20100522texas_may_get_nuclear_waste_from_dozens_of_states/srvc=home&position=recent)

10. *May 21, Associated Press* – (Vermont) **Strontium-90 found in soil at Vermont nuke plant.** Vermont Yankee officials said that while cleaning up after a leak of radioactive tritium at the nuclear power plant, they found another, more potent radioactive isotope in soil near where the leak occurred. Strontium-90 is a byproduct of nuclear fission that has been linked to cancer and leukemia. A Vermont Yankee spokesman said Friday that the substance has not been found in any groundwater and plant officials believe they have removed all the soil containing it. He said they believe it poses no threat to public safety or health.

Source: <http://www.businessweek.com/ap/financialnews/D9FRJ11O2.htm>

For another story, see item [14](#)

[\[Return to top\]](#)

## **Critical Manufacturing Sector**

11. *May 24, Reliable Plant Magazine* – (Ohio) **Elyria Foundry fined \$201,500 after worker sustains a crushing injury.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) has cited Elyria Foundry Company LLC in Elyria, Ohio, with 29 alleged serious, and three repeat safety and health violations after a worker sustained a crushing injury requiring a lower arm amputation. Proposed penalties total \$201,500 and are based on a November 2009 safety inspection. Some of the violations address the company's failure to provide adequate personal protective equipment to employees; failure to provide proper eye protection while working with a sulfur dioxide tank; a lack of emergency escape respirators for workers; a lack of proper guarding on power band saws; blocked exit doors; failure to provide safety latches on crane hooks; and failure to provide fall protection. An OSHA violation is serious if death or serious physical harm can result from a hazard an employer knew or should have known exists. OSHA issues repeat violations if the employer has been cited previously for the same or a substantially similar condition or hazard at any other facility in federal enforcement states. The company also received three other than serious violations, including one for not paying for workers personal protective equipment. The employer also has been cited with four serious health violations. These citations address the company's alleged failure to provide proper respiratory protection and engineering controls for workers exposed to dust containing silica; failure to ensure workers used proper hearing protection; and a lack of proper labeling on hazardous-

material storage containers.

Source: <http://www.reliableplant.com/Read/24702/Elyria-Foundry-crushing-injury>

12. *May 24, Reliable Plant Magazine* – (New Jersey) **N.J. manufacturer cited for 14 serious safety and health violations.** The U.S. Department of Labor’s Occupational Safety and Health Administration (OSHA) has cited Church & Dwight Company Inc. for 14 serious violations involving employee exposure to chemical hazards at its plant in North Brunswick, N.J. Proposed penalties total \$55,125. “The identified violations could potentially place workers at risk and could result in injury or possible death,” said the director of OSHA’s Avenel Area Office. “One way employers can prevent potential hazards is by establishing an effective comprehensive workplace safety and health program that engages employees to proactively evaluate, identify and eliminate hazards.” OSHA initiated an investigation on November 18, 2009, as part of its Site-Specific Targeting Inspection Program for industries with high injury and illness rates. As a result of the investigation, OSHA inspectors have cited the company for its failure to comply with a process safety-management standard containing requirements for the management of hazards associated with processes using highly hazardous chemicals. This failure includes not performing an initial process hazard analysis on certain processes, and not performing inspection and tests on process equipment to maintain its mechanical integrity. OSHA issues a serious citation when there is substantial probability that death or serious physical harm could result and the employer knew, or should have known, of the hazard.

Source: <http://www.reliableplant.com/Read/24701/NJ-manufacturer-serious-violations>

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

13. *May 24, Space-Travel.com* – (National) **Aerojet validates engine design for Orion crew exploration vehicle.** Aerojet has completed a second set of hot-fire test sequences of its R-1E 25-pound thrust, bipropellant engine. This second test included more than 17,250 seconds of total burn time, demonstrating engine flexibility to operate under a broad variety of conditions expected for NASA’s Orion service module. Initial test results indicate the engine performed successfully in simulated space-flight mission scenarios. Lockheed Martin is NASA’s prime contractor for developing the Orion crew exploration vehicle as the nation’s next generation spacecraft for future exploration throughout the solar system. Aerojet is providing all of the engines for the Orion spacecraft, which is comprised of a crew module for crew and cargo transport, and a service module for propulsion, electrical power and fluids storage. Risk reduction testing of critical subsystems has been ongoing throughout Orion’s development phase to maximize mission success and crew safety. This early demonstration of the engine’s performance at expected Orion operating conditions was conducted to retire risk to the Orion vehicle including sustained operation at severe conditions.

Source: <http://www.space->

[travel.com/reports/Aerojet\\_Validates\\_Engine\\_Design\\_For\\_Orion\\_Crew\\_Exploration\\_Vehicle\\_999.html](http://travel.com/reports/Aerojet_Validates_Engine_Design_For_Orion_Crew_Exploration_Vehicle_999.html)

14. *May 23, Knoxville News Sentinel* – (Tennessee) **Stretching the life of a Y-12 dinosaur.** Trying to make Cold War facilities safe to operate in the 21st century is a difficult task. But that’s what they are trying to do at the Y-12 nuclear weapons plant. The Nuclear Facility Risk Reduction Project is a major effort to upgrade and stabilize systems at the 60-year-old production complex until the proposed Uranium Processing Facility (UPF) comes online around 2021. The project is moving forward in the design phase and preparing for construction improvements, according to officials with the National Nuclear Security Administration (NNSA). The project is a top priority at Y-12 and has been a continuing point of emphasis from the Defense Nuclear Facilities Safety Board. B&W Y-12 is reportedly under pressure to make progress and make it quickly, with some of its sizable fee at stake, although the NNSA did not immediately make information on the fee available. A NNSA spokesman said the purpose of the project is to “reduce the risk of failure of infrastructure utility components by implementing practical utility modifications determined prudent and necessary to ensure continued safe operations of Buildings 9212 and 9204-2E. The project scope includes improving maintainability and reliability needed to address the risk of failure of selected, high priority, infrastructure utility systems, structures, and components through planned replacement and upgrades of critical electrical control centers, switchgear, stacks, casting furnace vacuum system, and cooling tower and steam system pipes.” The project has been tabbed as a \$100-million effort, but the NNSA spokesman placed the cost range between \$61 and \$90 million. There are a number of systems that need to be upgraded inside Y-12 to make do until the state-of-the-art UPF becomes available, said the NNSA site manager “There are some places where we are going to upgrade maybe electrical control systems or switchgears and ventilation stacks will be replaced,” he said. “Our vacuum systems to support our casting furnaces will be replaced and then we are looking at cooling towers as well. Some of the steam system pipes will be replaced.”  
Source: [http://blogs.knoxnews.com/munger/2010/05/stretching\\_the\\_life\\_of\\_a\\_y-12.html](http://blogs.knoxnews.com/munger/2010/05/stretching_the_life_of_a_y-12.html)

For another story, see item [54](#)

[\[Return to top\]](#)

## **Banking and Finance Sector**

15. *May 24, Washington Post* – (National) **District food servers charged in theft of patrons’ credit card numbers.** Three servers at the Cheesecake Factory restaurant on Wisconsin Avenue in Washington D.C. allegedly stole credit card numbers from patrons as part of a scheme that racked up more than \$117,000 in fraudulent charges between 2008 and last year, authorities said. Investigators with the U.S. Secret Service allege the servers were working for a larger fraud ring and were using electronic devices to “skim” the credit card numbers of customers they served at the restaurant.

The devices were handed off to others, and the stolen numbers were used to make fake credit cards and later used to buy gift cards and merchandise in the Washington area, according to court records in U.S. District Court in Alexandria. Federal officials became aware of the scheme in April 2009, when Citibank investigators reported numerous fraudulent charges on cards that had been used at the Cheesecake Factory at 5345 Wisconsin Ave. in Friendship Heights, just south of the Maryland line. Because servers at the restaurant have to swipe a server card unique to them before processing a credit card, investigators were able to narrow the transactions to three servers, according to court documents. Secret Service agents interviewed two servers, identified in court documents only by their initials because they are cooperating with the investigation. The servers said they were recruited by another server at the restaurant. The recruiter allegedly provided the servers with “skimmers” to capture the credit card numbers and would then hand off the devices to two men, known only as “Slim” and “G.”

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052302921.html>

16. *May 23, KXII 12 Sherman* – (Texas) **Text scam targets Chase bank customers.** Over the weekend, messages requesting Chase customer’s bank information were sent via text. The message informed customers to call an 800 number, and then type in their account numbers because their funds may have been tampered with. One Chase customer shared the message with KXII 12 saying he was skeptical, and called his bank to confirm if the message was true. Chase representatives said they will never ask for personal information via text.

Source: <http://www.kxii.com/home/headlines/94705644.html>

17. *May 23, KKTU 11* – (Colorado) **Phone scam asking for credit card number targets region.** A phone scam is making its way throughout the region, asking customers for their credit card numbers in order to protect against future fraud. The scam works by trying to make an individual think they are already a victim of fraud. The caller tells the potential victim that someone has made fraudulent charges on the victim’s card, and in order to stop it, they need the credit card number. Aventa, which was formerly Colorado Springs Credit Union, is sometimes referenced in these scam calls, and a company representative said it has already started receiving calls from concerned customers. Aventa’s representative said customers should never give out personal and account information; if one’s financial institution needs it, they probably already have it.

Source: <http://www.kktv.com/news/headlines/94711734.html?ref=734>

18. *May 23, Associated Press* – (Oregon) **Man arrested in Eugene accused as ‘Grandpa Bandit’.** A man arrested in Eugene, Oregon in connection with a bank robbery has been indicted by a federal grand jury on charges that he robbed seven Oregon banks in a spree attributed to the “Grandpa Bandit.” Eugene Police arrested the 60-year-old Drain resident after \$939 was taken from an Umpqua Bank branch in Eugene. This week, the suspect was indicted by a federal grand jury in connection with seven robberies. An affidavit filed in U.S. District Court by an FBI agent said the suspect told

police he was responsible for several bank robberies. The reason he gave Eugene Police for robbing the Eugene Bank was “stupidity.”

Source: <http://www.statesmanjournal.com/article/20100523/UPDATE/100523013>

19. *May 22, Bank Info Security* – (Minnesota) **1 bank closed on May 21.** State and federal regulators closed one bank May 21. This closing raises to 81 the number of failed institutions so far in 2010. Pinehurst Bank in St. Paul, Minnesota was closed by the Minnesota Department of Commerce, which appointed the Federal Deposit Insurance Corporation as receiver. Coulee Bank, La Crosse, Wisconsin, will buy all of the deposits of Pinehurst Bank. The sole branch of Pinehurst Bank will reopen as a branch of Coulee Bank. Pinehurst Bank had approximately \$61.2 million in total assets. The estimated cost to the Deposit Insurance Fund (DIF) will be \$6 million  
Source: [http://www.bankinfosecurity.com/articles.php?art\\_id=2566](http://www.bankinfosecurity.com/articles.php?art_id=2566)
20. *May 22, Kentucky Post* – (Ohio) **Bank robber takes money, leaves fake bomb.** Police said a man walked into a PNC bank branch in Sharonville, Ohio, placed a suspicious device on the counter, and demanded money from the tellers. It happened around 6:05 p.m., just as the bank was closing. The PNC branch is located on Reading Road near I-275. The first Sharonville officer on the scene followed procedure by evacuating the bank and nearby businesses. He set up a 250-yard perimeter, and called in the Hamilton County Bomb Squad. Bomb technicians suited up in protective gear before entering the bank, and X-ray imaged the suspicious device. The X-rays revealed the device was not a threat.  
Source: [http://www.kypost.com/content/wcposhared/story/Bank-Robber-Takes-Money-Leaves-Fake-Bomb/EigIw2uWWUqyx\\_fodHJ6A.csp](http://www.kypost.com/content/wcposhared/story/Bank-Robber-Takes-Money-Leaves-Fake-Bomb/EigIw2uWWUqyx_fodHJ6A.csp)
21. *May 22, KRQE 13 Albuquerque* – (New Mexico) **Bank evacuated for bomb threat.** A bomb threat sent Bank of America employees scattering May 22 in Rio Rancho, New Mexico. Dozens of employees of a Bank of America were evacuated after someone made a “non-specific” bomb threat around 12:45 p.m. As the workers waited outside, police went through the building looking for anything suspicious. Police said it could be hard to pinpoint exactly where the call came from. Nothing was found.  
Source: <http://www.krqe.com/dpp/news/crime/bank-evacuated-for-bomb-threat>
22. *May 21, Computerworld* – (National) **Walmart to support smartcard payments.** Retail giant Walmart Stores Inc. is reportedly planning on making all its payment terminals in the U.S. compliant with a smartcard-based credit card technology that is widely used around the world but is not common in the U.S. Walmart’s plans were disclosed at a smartcard conference being held this week, and were first reported by Storefront Backtalk. Storefront Backtalk quoted Walmart’s director of payment services as saying the retailer was working on making all payment terminals in its domestic stores chip-and-PIN-capable. The director was reported as having said that signature-based credit-card transactions had become a “waste of time” for Walmart. Such a move by Walmart would have widespread ripple effects. As the largest retailer in the world, a Walmart decision to support chip-and-PIN could finally nudge card issuers, payment processors and other merchants to adopt the technology.

Source:

[http://www.computerworld.com/s/article/9177056/Wal\\_Mart\\_to\\_support\\_smartcard\\_payments](http://www.computerworld.com/s/article/9177056/Wal_Mart_to_support_smartcard_payments)

23. *May 21, DarkReading* – (International) **ID theft victims spending less in cleanup aftermath.** Nearly one-third of all identity theft victims say they are unable to completely clear up damaged credit or criminal records in the aftermath of their identities being abused. But the good news is they are spending much less time and money cleaning up the fraud perpetrated against them in their names, according to a newly released report. The Identity Theft Resource Center (ITRC)'s "Identity Theft: The Aftermath 2009" report found that ID theft victims spent about \$527 dollars out of pocket for an existing account compromised by an attacker, down from \$741 in 2008. They also spent less time repairing the damage from a compromised account — an average of 68 hours versus 76 hours in 2008. It takes more time to clean up a newly opened financial account or a case involving criminal or governmental issues — 141 hours last year, which was an improvement over '08, when it took an average of 265 hours. The ITRC report (PDF) surveyed 183 victims nationwide. Nearly 24 percent say they believed they knew their identity thief, who was either a relative, friend, roommate, ex-spouse, or ex-significant other. And 10 percent say their cases were traced to an employee at a business who had their identity information.

Source:

<http://www.darkreading.com/insiderthreat/security/client/showArticle.jhtml?articleID=224900713>

[\[Return to top\]](#)

## **Transportation Sector**

24. *May 24, KPBS* – (California) **Protecting San Diego's port from terrorism.** The Department of Homeland Security said San Diego's port could be vulnerable to a terrorist attack. But the city has received \$1.3 million worth of detection equipment to counter any threats. San Diego is in the middle of a pilot program to use portable devices that detect nuclear and radiological material brought into the city on small vessels. A spokeswoman with the San Diego office of the Department of Homeland Security said lifeguards, harbor police and the military are also being trained on how to react to potential threats. "If you come across the border there is detection at the border. There is detection in the airports. But there is no detection coming waterside," she said. She said that is a big problem because there are 95,000 miles of coastline on the West Coast. She said small vessels present a large potential risk because there are so many of them and they can move around with few restrictions. San Diego was selected for the pilot program based on its commercial importance, military importance and its proximity to the international border among other reasons. She said local agencies are conducting training exercises and have created protocols for responding to alarms. The spokeswoman said the agencies can keep the equipment and will continue training after the pilot program ends in December.

Source: <http://www.kpbs.org/news/2010/may/24/protecting-san-diegos-port-terrorism/>

25. *May 23, Associated Press* – (California) **Small jet makes emergency landing in Calif.** A small jet carrying 24 passengers from San Francisco made an emergency landing at a Southern California airport after its front landing gear failed to deploy. An Ontario International Airport spokesman said nobody was hurt Sunday when the SkyWest Airlines aircraft was forced to land with its nose gear up. Three crew members were on board. The jet is a Bombardier-manufactured CL601R, which seats about 50 people.  
Source: <http://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303185.html>
26. *May 23, KXTV 10 Sacramento* – (California) **Southwest flights stopped at Sac. International over lost bag.** Southwest Airlines flights out of Sacramento International Airport in California were stopped for nearly two hours Sunday while Transportation Security Administration (TSA) personnel worked to find luggage that triggered a security alarm, then disappeared, according to a TSA spokesman. The incident started around 3:30 p.m. when a bag going through airport screening procedures triggered an inspection alarm, the spokesman said. However, an apparent glitch in the screening process allowed the bag to continue down the Southwest Airlines bag belt, he said. After a computer alerted inspectors to the missing bag, at least five Southwest flights out of Terminal A were held while TSA officials looked for the bag, a Sacramento International Airport spokeswoman said. Passengers with tickets for flights headed to Las Vegas, Orange County, San Diego, Ontario and Burbank were not allowed to board and flights were delayed during the search. A team using an explosives-sniffing dog rescreened all the baggage and nothing suspicious was found, the spokesman said. It was not immediately clear whether the bag that triggered the alarm was ever located. Passengers began boarding and all flights were allowed to continue to their destinations just before 5:30 p.m.  
Source: <http://www.news10.net/news/story.aspx?storyid=82020&catid=2>
27. *May 22, The Washington Post* – (Virginia) **2 fire extinguishers used to put out blaze in jet cockpit.** Two fire extinguishers were needed to fight a blaze in the cockpit of a jet airliner that was diverted to Dulles International Airport Sunday, the National Transportation Safety Board (NTSB) said Friday. The captain and first officer of the United Airlines Boeing 757 both donned oxygen masks and smoke goggles when they spotted the smoke and fire, about 30 minutes into a New York to Los Angeles flight, the NTSB said. The NTSB said the captain discharged a halon fire extinguisher, and the fire dissipated. But the smoke and fire reignited, and the captain got another extinguisher from a purser, the NTSB said. One of the 105 passengers said he saw a flight attendant run to the back of the plane, then to the front, apparently with the second extinguisher. On final approach the captain's windshield cracked, the NTSB said. The passenger said he later saw a web of cracks in the glass. "You couldn't see through it," he said. The NTSB said it would try to find out whether the incident was linked to two previous windshield fires on 757-200s.  
Source: [http://www.washingtonpost.com/wp-dyn/content/article/2010/05/21/AR2010052105258.html?wprss=rss\\_metro](http://www.washingtonpost.com/wp-dyn/content/article/2010/05/21/AR2010052105258.html?wprss=rss_metro)

28. *May 22, KPIX 5 San Francisco and Bay City News* – (California) **Mechanical failure stalls muni light rail in SF.** San Francisco Municipal Railway light rail service was disrupted between the Embarcadero and Castro stations Saturday due to a mechanical problem involving a vehicle on the N-Judah line, an agency spokeswoman said. The problem was reported at about 2:40 p.m. near Duboce Avenue, a Muni spokeswoman said. An inbound train was disabled after the poles that connect it to the overhead wires were struck and damaged, the spokeswoman said. She said crews were investigating what caused the damage, which was on the second car of the two-car train. Service was being disrupted between the Embarcadero and Castro stations. Bus shuttles were taking passengers between the two stations, and light-rail vehicles were being turned around at those stations, according to the spokeswoman.

Source: <http://cbs5.com/local/muni.power.outage.2.1710009.html>

For another story, see item [38](#)

[\[Return to top\]](#)

## **Postal and Shipping Sector**

Nothing to report

[\[Return to top\]](#)

## **Agriculture and Food Sector**

29. *May 24, Capital Times* – (Wisconsin) **Ginseng growers get OK to use fungicide to avert crop crisis.** Embattled ginseng farmers in Marathon County in north central Wisconsin have been granted an emergency exemption so they can use a fungicide on their crops to try to save plants not destroyed by snow and cold in early May. The Wisconsin Department of Agriculture, Trade and Consumer Protection issued a “crisis pesticide exemption” May 21, allowing ginseng growers to apply the Gavel 75DF Fungicide on ginseng plants to fend off stem and leaf blight. Without it, the plants could die, which could wipe out an entire crop for some ginseng farmers. On May 7, 4 inches of heavy, wet snow came down in Marathon County, collapsing many of the shade structures that protect the ginseng plants from direct sun. The next night, freezing temperatures damaged or killed many plants, prompting the governor to declare a disaster in Marathon County, so ginseng farmers could get emergency loans and insurance to recoup some of their losses. There are about 200 ginseng growers in Marathon County, producing 95 percent of the U.S. ginseng crop, most of which is shipped to China. While work intensive, ginseng can be lucrative, with the root fetching \$25 a pound, according to state statistics from 2007, which showed ginseng farmers harvested 400,000 pounds of the root that year, valued at \$10 million.

Source: [http://host.madison.com/ct/news/local/article\\_07f4dd4a-672f-11df-9050-001cc4c002e0.html](http://host.madison.com/ct/news/local/article_07f4dd4a-672f-11df-9050-001cc4c002e0.html)

30. *May 24, Associated Press* – (National) **Huge grasshopper outbreak projected in Northwest.** The Pacific Northwest must prepare for the worst grasshopper outbreak in 30 years, according to Washington State University and United States Department of Agriculture scientists. Researchers found a big increase in the number of grasshopper eggs last fall and said a relatively mild spring has set the stage for a major grasshopper infestation. Last summer, grasshoppers wiped out 7,000 acres of grassland in the high desert of southeastern Oregon. The areas considered at most risk in Washington are the high desert regions near Othello, Yakima and the Tri-Cities. The infestation was expected to hit its peak in late July and early August. Federal officials are looking into pesticide options. “In some areas there will indeed be masses,” said a WSU entomologist. “Not biblical proportions, but big masses of grasshoppers moving through areas.” Grasshoppers can travel from 30 to 50 miles a day looking for food. Scientists are also warning of a possible outbreak of the “Mormon Cricket,” an insect that doesn’t fly, but travels in tight packs and devours everything in its path. “There are massive numbers of them, and then when they exit that area, pretty much anything green is gone,” said the WSU entomologist.  
Source: <http://www.fosters.com/apps/pbcs.dll/article?AID=/20100524/GJLIFESTYLES/100529884/-1/SANNEWS>
31. *May 23, Associated Press* – (Massachusetts) **Man sucked into sausage machine.** Police said a cleaning man was taken to a hospital after being sucked into a machine at a sausage-making company in Danvers, Massachusetts. The accident happened May 20 as the man was cleaning the vacuum-type machine that is used to season the meat at DiLigui Sausage Co. Police said the man’s head and shoulders became stuck in the machine after it somehow activated while being cleaned. A police lieutenant told The Salem News that the man - whose name was not released - was freed from the machine and showed no obvious sign of trauma, but was taken to a hospital as a precaution. The Occupational Safety and Health Administration is investigating the mishap.  
Source: <http://www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052301794.html?hpid=nation>
32. *May 23, Top News* – (International) **Large amount of Ivermectin found in cans of corned beef.** Caribbean food products maker Grace Foods USA reported May 22 that canned corned beef distributed in the United States contains higher than acceptable levels of a Ivermectin, which is used to treat cattle for parasites. Ivermectin can make people sick if they consume it. The recall of two batches of corned beef is based on an advisory from Grace Foods’ Brazilian supplier. The supplier gave the warning after testing showed higher levels of Ivermectin than the U.S. Department of Agriculture allows. The 12-ounce cans of beef have codes 100204 or 100205 with “Brasil Inspeccionado 337 S. I. F.” stamped on the top.  
Source: <http://topnews.us/content/220399-large-amount-ivermectin-found-cans-corned-beef>

33. *May 23, Oklahoman* – (Oklahoma) **Oklahoma’s wheat crop damaged by recent hail storm.** Recent hailstorms cut an unpredictable path of destruction through Oklahoma’s wheat crop — which had been poised for a banner year. Hardest hit areas are a swath from Okeene to Oklahoma City; pockets around Medford, Pond Creek, Hunter and Cherokee experienced losses as well, said the executive director of the Oklahoma Wheat Commission. It’s too early to determine how much of the state’s wheat crop — just two weeks from harvest — will be lost, he said. A wheat farmer from Perry said he was looking at a good crop until the May 19 storm. Now, anywhere from 30 to 80 percent of the wheat will be lost from hail damage. In her 30 years of insuring farmers, an insurance agent from Goltry said she’s never seen so many widespread claims of hail damage. “I work about 25 counties in the state, and there are losses in almost every county,” she said. Some farmers are working quickly to finalize claims so they can plant a spring crop such as soybeans, sorghum or corn. In the crops not damaged by hail, Oklahoma is looking at an average wheat crop this year and an estimated 128.7 million bushels, according to the U.S. Department of Agriculture.  
Source: [http://www.newsok.com/oklahomas-wheat-crop-damaged-by-recent-hail-storm/article/3463210?custom\\_click=pod\\_headline\\_national-finance-news](http://www.newsok.com/oklahomas-wheat-crop-damaged-by-recent-hail-storm/article/3463210?custom_click=pod_headline_national-finance-news)
34. *May 22, San Antonio Express-News* – (National) **Ranchers now fear return of fever ticks.** U.S. Department of Agriculture (USDA) fever-tick inspectors have become the latest set of American workers pulled from northern Mexico amid ongoing drug cartel violence, a move some Texas ranchers fear will reintroduce a pest that nearly wiped out U.S. cattle a century ago. Citing safety concerns, the department’s Animal & Plant Health Inspection Service March 29 suspended its cattle inspections in Reynosa and Nuevo Laredo, Mexico. The agency last week diverted Reynosa inspections to nearby Pharr, Texas and this week opened a second U.S. facility in Laredo. A USDA spokeswoman said the agency is taking precautions to minimize the risk of a reinfestation. The non-native fever ticks transmit a blood parasite that causes bovine babesiosis, otherwise known as “Texas fever” or “cattle fever.” The disease in the early 1900s spread through herds and wiped out nearly 90 percent of the cattle in some areas, helping end the era of cattle drives to the north. In 2006, the USDA marked the 100-year anniversary of its successful Cattle Fever Tick Eradication Program, which by 1943 had eliminated the ticks in the United States except for a narrow quarantine zone along the border. The ticks in 2007 turned up beyond the quarantine zone, prompting a cry for more federal resources. There’s growing concern about deer and other animals, such as non-native nilgai kept as exotic game for hunters, spreading the tick as they jump fences between ranches. A large part of the program has been done in Mexico, where the USDA has had 43 employees at 11 Mexican cattle inspection ports examining about a million head a year. About 38,000 of these come through Laredo, another 39,000 through Pharr. While the Laredo facility is outside the quarantine zone, a USDA spokeswoman said precautions were being taken to ensure ticks don’t drop onto U.S. soil. Mexican agriculture inspectors are doing visual inspections before the cattle cross, she said, which makes for a “double inspection.” Trucks are sealed by Mexican authorities and not unsealed until they get to the inspection facilities in Texas.  
Source:

[http://www.mysanantonio.com/news/mexico/usda\\_cattle\\_inspectors\\_pulled\\_from\\_mexico\\_94624674.html?showFullArticle=y](http://www.mysanantonio.com/news/mexico/usda_cattle_inspectors_pulled_from_mexico_94624674.html?showFullArticle=y)

35. *May 22, Los Angeles Times* – (California) **Alfalfa sprouts recalled by L.A.-area firm after salmonella outbreak.** A Los Angeles County firm issued a nationwide recall of alfalfa sprouts May 21, after a salmonella outbreak that has sickened 23 people in 10 states and caused four people to be hospitalized. “We’re very sorry that this has happened,” said the general manager at Maywood, California-based Caldwell Fresh Foods. The alfalfa sprouts were grown in Maywood and sold at supermarkets, delicatessens, and restaurants around the country, including at Trader Joe’s and Wal-Mart. Consumers have been infected in many states, including California, Colorado, Idaho, Illinois, Missouri, New Mexico, Nevada, Oregon and Wisconsin. The recalled sprouts were packaged in four-ounce plastic cups and one-pound plastic bags under the Caldwell Fresh Foods brand; four-ounce plastic cups under the Nature’s Choice brand; five-ounce plastic clamshell containers under the California Exotics brand; and two-pound and five-pound plastic bags in cardboard boxes with a Caldwell sticker. Health officials said consumers should throw away the sprouts or take them back to the place of purchase for a refund. The Food and Drug Administration, Centers for Disease Control and Prevention, and many other state and local health agencies are investigating the outbreak. This is the 32nd outbreak of food poisoning linked to alfalfa sprouts since 1990, and the second time in two years that sprouts produced by Caldwell Fresh Foods have been implicated.  
Source: <http://articles.latimes.com/2010/may/22/business/la-fi-sprouts-20100522>

For another story, see item [5](#)

[\[Return to top\]](#)

## Water Sector

36. *May 24, UPI* – (National) **South American insects fight U.S. weeds.** U.S. scientists said they are using a South American insect in an effort to control an invasive weed, water hyacinth, that is common across the United States. U.S. Department of Agriculture scientists at the department’s Agricultural Research Service (ARS) said water hyacinth (*Eichhornia crassipes*) is a free-floating aquatic plant native to South America that has infested freshwater ecosystems across the nation, but which is especially problematic in the southeastern United States. “The plant is a real menace, affecting water traffic, water quality, infrastructure for pumping and hydroelectric operations, water use and biodiversity,” the ARS said. “Other problems include fish kills due to low oxygen levels and increases in populations of vectors of human and animal diseases.” The insects were released last week at the Edgefield Regional Stormwater Treatment Facility near Palatka, Florida.  
Source: [http://www.upi.com/Science\\_News/2010/05/24/South-American-insects-fight-US-weeds/UPI-44321274706940/](http://www.upi.com/Science_News/2010/05/24/South-American-insects-fight-US-weeds/UPI-44321274706940/)

37. *May 21, KHBS 40 Fort Smith* – (Arkansas) **Alma water plant contaminated by motor oil.** The Alma, Arkansas Public Works director said someone is dumping motor oil into the city’s sewer system. He said in recent weeks it has stopped, but it already has had a big impact on the the city’s water treatment plant. He does not know exactly how much oil made its way into the sewer system, but said it was a substantial amount that started showing up in the middle of December. “We started observing more oil and it became a routine to see this motor oil in the influent,” he said. Workers launched an investigation. The source of the oil is still unknown. The plant works to reduce pollutants before the water travels to the Arkansas River. Fixing the problem involved an expensive treatment process in order to absorb the oil and restore biological elements to the plant’s treatment ponds. “The first treatment cost about \$20,000, and unfortunately we were continuing to see oil so that first treatment wasn’t effective.” Two treatments have been performed at a cost of \$40,000. Right now there are no plans to pass the costs on to residents. “It will affect the ratepayers if it continues,” he said. “We have funds that can absorb small amounts of unexpected expenses.” A letter explaining the contamination was placed the latest water bills. The department’s investigation into the contamination is ongoing.  
Source: <http://www.4029tv.com/mostpopular/23640771/detail.html>
38. *May 21, United Press International* – (Michigan) **Detroit sinkhole blamed on water line.** Detroit officials said a break in a water line caused a sinkhole in a road next to the site of the former Lafayette Building. Officials said the sinkhole took a school bus-sized chunk out of the sidewalk and driving lanes of Lafayette Boulevard in the city’s downtown Wednesday night, the Detroit Free Press reported Friday. A spokesman for the Detroit Water and Sewerage Department, said a line ruptured above a damaged DTE Energy gas line, causing damage that will likely keep the road closed to motorists for at least two weeks, The Detroit News reported. He said it appears the lines were inadvertently damaged by contractors from Adamo Demolition Co., who have been working to demolish the Lafayette Building. “We believe the break is related to the demo work,” he said. “First, we do the repairs, then we look at who bears the cost. It is an issue to be determined.”  
Source: [http://www.upi.com/Top\\_News/US/2010/05/21/Detroit-sinkhole-blamed-on-water-line/UPI-86951274473090/](http://www.upi.com/Top_News/US/2010/05/21/Detroit-sinkhole-blamed-on-water-line/UPI-86951274473090/)

For another story, see item [43](#)

[\[Return to top\]](#)

## **Public Health and Healthcare Sector**

39. *May 24, Columbus Dispatch* – (Ohio) **Much of H1N1 vaccine wasted.** Flu-shot providers in Ohio face a growing stock of expired H1N1 vaccine and plenty of good vaccine they probably will never use. The Columbus Dispatch requested data from the Ohio Department of Health showing that almost 1.5 million doses statewide expired before they were used and almost 1 million unused doses are still good. Those numbers come with a caveat: The state hasn’t gathered complete data on vaccine use. Providers

were supposed to report timely information, but many did not, said a department spokeswoman. Of 2,322 providers, 787 reported that they gave no doses, and 1,012 reported having used less than 10 percent, she said. Regardless, there is no question that plenty of vaccine - both expired and not - is lingering here and across the country. Through February, the federal Centers for Disease Control and Prevention estimated that 91 million shots and doses of the nasal spray FluMist had been administered of the 162 million doses manufactured. The cost of the national vaccine effort was about \$1.6 billion.

Source: [http://www.dispatch.com/live/content/local\\_news/stories/2010/05/24/much-of-h1n1-vaccine-wasted.html?sid=101](http://www.dispatch.com/live/content/local_news/stories/2010/05/24/much-of-h1n1-vaccine-wasted.html?sid=101)

40. *May 23, Daytona Beach News-Journal* – (Florida) **Officials here heed kids' virus outbreak.** A chickenpox outbreak warning this month in Lee County in Southwest Florida is a cautionary tale for this area. More than three times the usual number of children — 55 of them — were feeling the itch of the varicella zoster virus sometime between February and May in Lee County. This happened to children of all ages despite a chickenpox vaccination rate among incoming kindergartners slightly higher than the state's goal of 95 percent. Lee County's rate is a good deal more than the 88.5 percent of Flagler's incoming kindergartners who came fully vaccinated against it this year. Volusia's rate is also at 95.9 percent vaccinated, but the county has seen more than 200 cases in the past three years. The Lee County outbreak — and Volusia's cases in recent years — are being attributed to confusion surrounding a relatively new standard in which one vaccine dose is not enough.

Source: <http://www.news-journalonline.com/news/local/east-volusia/2010/05/23/officials-here-heed-kids-virus-outbreak.html>

[\[Return to top\]](#)

## **Government Facilities Sector**

41. *May 22, Florida Today* – (Florida) **Test upcoming to determine the extent of mercury contamination at school.** The Florida Department of Environmental Protection will test the campus of Palm Bay Elementary School to determine how widespread any mercury contamination might be after a student brought the chemical to class. The school was closed May 21, a day ahead of the last day of school for other county students, after a 12-year-old fifth-grader brought vials of low-grade mercury to school. Five students handled the mercury and were decontaminated on site. It is believed the student obtained the mercury from a dentist office, where his mother is contracted as a cleaner. There are concerns that other classmates may have been contaminated. At least 20 people were initially thought to have been exposed or had limited exposure to the mercury, which authorities said may have been on the campus since May 18. Parents of those directly affected were advised to clean their homes and throw away or wash the clothes of students. No criminal charges have been filed against the 12-year-old student.

Source:

<http://www.floridatoday.com/article/20100522/NEWS01/5220319/1006/Test+upcoming+to+determine+the+extent+of+mercury+contamination+at+school>

42. *May 21, GateHouse News Service* – (Kansas) **Courthouse evacuated due to suspicious package.** The Leavenworth County Courthouse in Kansas was evacuated for about an hour May 21 as authorities investigated a suspicious bag. Employees were allowed back into the building after it was determined the bag contained only personal hygiene products, according to law enforcement officials. The incident was reported at about 11:15 a.m. when an employee saw someone put down the bag but then lost sight of the person. The bag had been left in the area of the county treasurer's office. The bomb squad X-rayed the bag and found nothing associated with a hazardous device; rather, it was described as a shaving kit.  
Source: <http://www.leavenworthtimes.com/homepage/x1560873936/Courthouse-evacuated-due-to-suspicious-package>

For another story, see item [56](#)

[\[Return to top\]](#)

## **Emergency Services Sector**

43. *May 24, San Francisco Examiner* – (California) **Fire Department loses control of emergency water system.** Despite concerns from the civilian commission overseeing the San Francisco Fire Department, the water-delivery system set to receive a major upgrade with a June bond measure will be turned over to the San Francisco Public Utilities Commission (SFPUC). The transfer will save the fire department money, but will put control of the system in the utility agency's hands. The mayor ordered the transfer last week. The SFPUC was going to start paying the costs of maintaining the water system that supplies most of the fire hydrants around the city, but it ran into resistance from the fire commission, which fought to keep control under the fire department. Commissioners worried that the pipes and cisterns that carry water intended for battling fires would end up being used for other purposes, such as for drinking water and cleaning out the sewer system. But with a \$412-million bond measure meant to fix the Auxiliary Water Supply System on the June 8 ballot, the debate suddenly ceased. The agreement will divert money to San Francisco's general fund and was approved during the budget season earlier this year. The deal will save the fire department about \$2.4 million a year and the SFPUC will pay the department \$500,000 for miscellaneous equipment, according to the mayor's order.  
Source: <http://www.sfexaminer.com/local/Fire-Department-loses-control-of-emergency-water-system-94716584.html>
44. *May 20, New York Daily News* – (New York) **NYPD sued over internal database of names collected from stop-and-frisk program.** The New York City Police Department (NYPD) was slapped with a lawsuit for keeping an internal database of names collected from the controversial stop-and-frisk program. The New York Civil Liberties Union (NYCLU) argues in the class-action lawsuit that all police records

should be sealed after someone is cleared of a crime or found guilty of only a violation. The NYPD stockpiles the names of all people they stop - whether they are charged with a crime or not. The NYCLU said an overwhelming majority of the 360,000 people arrested or issued summonses after being stopped by police since 2004 should have their names removed from the database. The police commissioner defended the database, calling it “extremely useful to our detectives in doing investigations.” Police said the database helped solve a murder in Bushwick two years ago. More than 575,000 people were stopped, questioned and often frisked by police last year. Under the current commissioner, the number of stops has increased five-fold, though only about 10 percent of those stopped are arrested or issued summonses.

Source: [http://www.nydailynews.com/news/ny\\_crime/2010/05/20/2010-05-20\\_nypd\\_sued\\_over\\_internal\\_database\\_of\\_names\\_collected\\_from\\_stopandfrisk\\_program.html](http://www.nydailynews.com/news/ny_crime/2010/05/20/2010-05-20_nypd_sued_over_internal_database_of_names_collected_from_stopandfrisk_program.html)

For another story, see item [56](#)

[\[Return to top\]](#)

## **Information Technology Sector**

45. *May 24, V3.co.uk* – (International) **Botnets for hire at Â£5.99 per hour.** Authentication firm VeriSign has warned that botnets could become more widespread and dangerous as the services become easier to find and cheaper to hire. VeriSign’s iDefence arm said that criminals are advertising botnet services on online forums for just Â£5.99 an hour, which could be used to launch hacking attacks. The company warned that this cheap and wide availability means that businesses are increasingly at risk of sophisticated attacks from the lowliest of sources. VeriSign studied 25 botnet herders across three forums, and found that the average cost of a 24-hour rental is just under Â£45, and includes a range of attack vectors including ICMP, SYN, UDP, HTTP and HTTPS. The firm said that it had seen many forums using traditional types of marketing to promote their wares, including banner advertising, in a sign of how sophisticated such businesses had become. VeriSign added that one forum even offered prices for taking down sites that were already prepared to defend against such attacks.

Source: <http://www.v3.co.uk/v3/news/2263558/verisign-finds-botnets-rent>

46. *May 24, SC Magazine* – (International) **Google introduces SSL encrypted search engine, as Hotmail moves to protect users further.** Google has added full SSL encryption to its search services to allow users to have a secure https connection when searching google.com. The page is accessed by specifically entering <https://www.google.com/> in the address bar. A Google software engineer claimed that by adding SSL encryption to products including Gmail to Google Docs, the session-wide encryption was “a significant privacy advantage over systems that only encrypt login pages and credit card information.” Google also clarified that the release is in beta to cover only the core Google Web search product, and not on Image Search and Maps. Since SSL connections require additional time to set up the encryption between the

browser and the remote Web server, a user experience with search over SSL may be slightly slower than a regular Google search experience. Google also claimed that it will still maintain search data “to improve your search quality and to provide better service.”

Source: <http://www.scmagazineuk.com/google-introduces-ssl-encrypted-search-engine-as-hotmail-moves-to-protect-users-further/article/170796/>

47. *May 24, V3.co.uk* – (International) **Facebook users suffer second ‘sexy’ malware attack.** Security experts have called on Facebook to set up an early warning system on its network to notify users of any threats and when they occur, after yet another malware attack hit the site over the weekend. The attack is the second in successive Saturdays to use a “sexy video” to lure the recipient into clicking on a fake FLV Player upgrade message, which then downloads adware onto the PC. Both files arrive as a thumbnail video in messages posted to users’ walls. Last week’s included the message: “This is without doubt the sexiest video ever!: P :P :P.,” while the new scam refers to “distracting beach babes.” Facebook is aware of the problem and is “actively removing both the wall posts and the malicious applications,” wrote a Websense senior research manager in a blog post.

Source: <http://www.v3.co.uk/v3/news/2263552/facebook-suffers-second-sexy>

48. *May 24, Computerworld* – (International) **Microsoft smacks patch-blocking rootkit second time.** For the second month in a row, Microsoft has tried to eradicate a mutating rootkit that has blocked some Windows users from installing security updates. According to the Microsoft Malware Prevention Center (MMPC), this month’s Malicious Software Removal Tool (MSRT) has scrubbed the Alureon rootkit from over 360,000 Windows PCs since its May 11 release. That represented 18.2 percent of all MSRT detections for the month, more than double the 8.3 percent the rootkit accounted for in April. The free MSRT is updated each month as part of Microsoft’s monthly Patch Tuesday, and pushed to users via the same Windows Update mechanism used to serve up security fixes. April’s edition of MSRT, which was released April 13, also included Alureon sniffing skills. Last month, MSRT removed the rootkit from more than 260,000 Windows systems. Although the Alureon rootkit is no malware newcomer — antivirus company Symantec identified it in October 2008 — it first made news last February when Microsoft confirmed that the rootkit caused infected PCs to crash when users applied a patch the company issued that month.

Source:

[http://www.computerworld.com/s/article/9177223/Microsoft\\_smacks\\_patch\\_blocking\\_rootkit\\_second\\_time](http://www.computerworld.com/s/article/9177223/Microsoft_smacks_patch_blocking_rootkit_second_time)

49. *May 23, PC World* – (International) **Bugnets could spy on you via mobile devices.** Imagine an individual sitting in a café discussing the details of a business proposal with a potential client. Neither the individual nor the client has a laptop; they are just two people having a conversation. But unbeknownst to either, someone half a world away is listening to every word they say. Later, as the individual leaves, they receive a text message referring to the proposal and demanding money in exchange for silence. Recent research from two universities suggests that such a remote-

eavesdropping scenario may soon be possible. According to two George Mason University researchers, cell phones make excellent surveillance devices for remote snoops. In a paper, both discuss a “modernized mic hijacker” that an attacker could control over what they call a “roving bugnet.” The eavesdropper would use a piece of malware called a “bugbot” to listen in on in-person interactions via a nearby smartphone or laptop. Such attacks would be more likely to target specific people (a wayward spouse, say) than to play a role in widespread attacks on the general public. Source: <http://www.networkworld.com/news/2010/052310-bugnets-could-spy-on-you.html?hpg1=bn>

50. *May 21, The Register* – (International) **Flaw lets hackers delete Facebook friends.** The Facebook security gaffes keep coming, with the latest being a bug that allows hackers to delete all of a users’ site friends without permission, according to IDG News. The flaw was reported May 26 by a college student, but some 48 hours later it could still be exploited to delete an IDG reporter’s Facebook friends. The student has written proof-of-concept code that uses publicly available data from Facebook to systematically delete all of a user’s friends. “A malicious hacker could combine an exploit for this bug with spam or even a self-copying worm code to wreak havoc on the social network,” IDG said. The CSRF, or cross-site request forgery, bug that makes all this possible is the same one reported earlier last week that exposed user birthdays and other sensitive data even when they were designated as private. Facebook representatives had said company engineers had closed the hole, but that pronouncement was premature. The flaw could still be exploited to control the site’s “like” feature, a button users click to endorse ads and other types of content. Source: [http://www.theregister.co.uk/2010/05/21/facebook\\_bug/](http://www.theregister.co.uk/2010/05/21/facebook_bug/)
51. *May 21, DarkReading* – (International) **New threat for wireless networks: Typhoid adware.** There is a potential threat lurking in your Internet cafe, say University of Calgary computer science researchers: Typhoid adware. Typhoid adware works in similar fashion to Typhoid Mary, the first identified healthy carrier of typhoid fever who spread the disease to dozens of people in the New York area in the early 1900s. “We’re looking at a different variant of adware — Typhoid adware — which we have not seen out there yet, but we believe could be a threat soon,” said an associate professor who co-authored a research paper with a assistant professor and two students. Typhoid adware could be spread via a wireless Internet cafe or other area where users share a nonencrypted wireless connection. Typically, adware authors install their software on as many machines as possible. But Typhoid adware hijacks the wireless access point and convinces other laptops to communicate with it instead. Then the Typhoid adware automatically inserts advertisements in videos and Web pages on hijacked computers, the researchers said. Meanwhile, the carrier sips her latte in peace — she sees no advertisements and doesn’t know she is infected, just like symptomless Typhoid Mary. Source: [http://www.darkreading.com/vulnerability\\_management/security/client/showArticle.jhtml?articleID=224900741&subSection=End+user/client+security](http://www.darkreading.com/vulnerability_management/security/client/showArticle.jhtml?articleID=224900741&subSection=End+user/client+security)

52. *May 21, The New New Internet* – (International) **Swedish online network cyber attacked.** IDG, a Swedish online network with more than 25 technology-, IT- and business-related Web sites, suffered a cyber attack May 19, according to ComputerSweden. All sites belonging to the network crashed as result of a botnet targeting the whole network, as well as the internal one. The first signs of the cyber attack emerged around 10 p.m. After hours of intense work, the sites were back up the following day. An IP-address originating in Taiwan was identified as a possible culprit for the attack. With that information handy, technicians were able to block traffic and reboot the systems. Even IDG’s own Internet connection was compromised by the attackers, but the problem was solved thanks to alternative connections, including 3G modems.  
Source: <http://www.thenewnewinternet.com/2010/05/21/swedish-online-network-cyber-attacked/>
53. *May 21, The New New Internet* – (International) **Iranian cyber army second largest in the world, claims Iranian commander.** After hacking Twitter and various Iranian Web sites and engaging in a cyber war with China, the Iranian Cyber Army is said to be looking at the Revolutionary Guards for direction, according to a senior Revolutionary Guards Corps commander. Fars news agency reports that the commander of the Ali Ebn-e Abi Taleb Guards in Qom, said May 20 that the Revolutionary Guards has been successful in establishing a cyber army and “today the cyber army of the Revolutionary Guards is the second largest cyber army in the world.” The commander also claimed the objective of the Iranian Cyber Army is “to prevent the destruction of Iran’s cultural and social system” and added the “cyber army of the Revolutionary Guards is a force to reckon with in this arena.” The Iranian Cyber Army has not been officially claimed by any group. Last year, Defense Tech, a U.S. military and security organization announced that the Iranian Cyber Army belongs to the Revolutionary Guards of Iran.  
Source: <http://www.thenewnewinternet.com/2010/05/21/iranian-cyber-army-second-largest-in-the-world-claims-iranian-commander/>

### Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [sos@us-cert.gov](mailto: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

54. *May 24, PC Advisor UK* – (International) **US begins \$8 billion upgrade of GPS satellites.** The U.S. is upgrading its 24 Global Positioning System (GPS) satellites in a bid to improve the accuracy of the technology and prevent outages. As part of the \$8 billion upgrade, 18 new satellites are being built by Boeing’s Space and Intelligence

Systems, while Lockheed Martin has been commissioned to build a further 12 satellites. Each of the existing 24 satellites will be replaced, the first of which was launched this weekend, while the remaining six that have been manufactured will be kept as spares. “We know that the world relies on GPS,” the upgrade’s chief engineer told the Los Angeles Times. It is thought the new satellites will mean a location can be pinpointed to “within an arm’s length, compared with a margin of error of 20 feet or more today.” The upgrade is expected to take 10 years to complete and will be handled by engineers at the Los Angeles Air Force Base in El Segundo.

Source: <http://www.networkworld.com/news/2010/052410-us-begins-8bn-upgrade-of.html>

55. *May 22, The Day* – (Connecticut) **State regulators: AT&T should pay for slow repairs.** Telecommunications giant AT&T should pay \$1.12 million for its slow repair service, Connecticut regulators said May 21 in a decision cheered by consumer advocates and union leaders. “AT&T Connecticut has consistently and repeatedly failed to meet the requirement that 90 percent of all service repairs ... be cleared within 24 hours,” the state Department of Public Utility Control (DPUC) said in its decision. AT&T said it would contest the civil penalty, which looked back to the phone company’s record of service since 2001. The fines, officially proposed against AT&T subsidiary Southern New England Telephone, amount to \$10,000 per month since the requirement for quick phone repair has been in effect. “The DPUC’s notice of violation sends a strong message to AT&T that the customer service regulations are going to be enforced,” said a statement from the office of consumer counsel approving of the decision.

Source: <http://www.theday.com/article/20100522/BIZ02/305229897/-1/BIZ>

[\[Return to top\]](#)

## **Commercial Facilities Sector**

56. *May 24, Florida Today* – (Florida) **Brevard bomb-threat suspect eludes police.** Phony bomb threats continue to paralyze Space Coast hospitals and businesses in Florida, and authorities are asking for the public’s help in locating a suspect. The Brevard County Sheriff’s Office is searching for a 48-year-old homeless man in connection with more than 30 false bomb alerts in recent weeks. Detectives have issued an arrest warrant charging the man with 12 counts of threats to discharge a destructive device. On May 23, a bomb hoax temporarily shut down the Suntree Square shopping center on Wickham Road, and Wuesthoff Medical Center-Rockledge was placed on lockdown after an unidentified male phoned the medical surgical unit and said, “there was a device.” On May 22, Parrish Medical Center also received a bomb threat. On May 19, investigators said a scratchy-voiced caller threatened to detonate a pipe bomb in front of the Moore Justice Center parking lot. That same day, shoppers were evacuated from the Viera Walmart and Toys “R” Us in West Melbourne. Cape Canaveral Hospital in Cocoa Beach also closed because of a bomb threat. And a similar threat was placed at Eau Gallie High. A judge set the suspect’s bond at \$1.2 million. Investigators do not know the man’s location and believe he travels via Space Coast

Area Transit buses.

Source:

<http://www.floridatoday.com/article/20100524/NEWS01/5240312/1006/Brevard+bomb-threat+suspect+eludes+police>

57. *May 23, St. Petersburg Times* – (Florida) **Fire that caused Oldsmar Flea Market evacuation put out.** A fire May 23 at a manufacturing plant that uses cyanide led authorities to evacuate the nearby Oldsmar, Florida Flea Market as a precaution. Hazardous materials crews were called to the fire at 369 Douglas Road E, in an industrial district north of Tampa Road and west of Race Track Road. A passing motorist noticed smoke coming from the building about 10:30 a.m. Firefighters quickly contained the blaze, and there was no contamination to the surrounding area. No one was injured. Authorities are investigating what caused the fire.  
Source: <http://www.tampabay.com/news/publicsafety/fire/fire-that-caused-oldsmar-flea-market-evacuation-put-out/1097084>
58. *May 22, St. Helena Star* – (California) **Bomb squad explodes grenade found in downtown Napa.** Law enforcement officials detonated what they believed was an explosive device found in bushes near Exertec Fitness Center in downtown Napa May 19. No one was hurt in the blast. At about 11 a.m., city workers trimming the bushes in a planter that lines the fitness center's Clay Street parking lot spotted what appeared to be an old military-style grenade. Police told people to stay in the fitness center and several other surrounding buildings. A few buildings were evacuated, and officials closed sections of Seminary, Clay and Franklin streets and other nearby roads for about three hours. A deputy from the Napa County Sheriff Office's Bomb Squad put on an 80-pound protective suit and entered the area where officials had set up sand bags in the middle of Clay Street. The deputy attempted to X-ray the suspected grenade, but he was unable to do so because of its position. Instead, he attached a rope to the device, then stood back and dragged it across the street into the sandbags. He then packed other explosives and sandbags around the device and left the area. From about a block away, other officers detonated the grenade at 12:47 p.m. The explosion blew sand 25 to 30 feet in the air. People were released from where they were advised to stay in at about 1:10 p.m., and all streets were open again at about 2 p.m.  
Source: [http://www.sthelenastar.com/articles/2010/05/22/news/saturday\\_update/doc4bf6c22439f84494594436.txt](http://www.sthelenastar.com/articles/2010/05/22/news/saturday_update/doc4bf6c22439f84494594436.txt)
59. *May 22, WSAZ 3 Huntington/Charleston* – (West Virginia) **One dead after explosive device detonated outside club.** A person detonated an explosive device outside of a Huntington, West Virginia nightclub early May 22, killing himself; but he clearly had the intentions of killing others. The co-owner of the nightclub said that the 45-year-old man responsible was banned from her bar, because he came there to stalk his ex-wife. The explosion, which happened around 3 a.m., shut down Route 60, and put the lives of dozens of families at risk. Homes in the area of the bar were also evacuated. The man was at the nightclub wearing a disguise and had a bomb in his pocket. Investigators said the death toll could have been much higher. They discovered several more live

suspicious devices outside the bar. The name of the man has not been released.  
Source: <http://www.wsaz.com/news/headlines/94645894.html?ref=894>

60. *May 21, BBC* – (International) **Pakistan arrests many over Times Square bomb plot.** Pakistan has arrested several suspects in connection with the failed bombing in New York City. Pakistani officials told news agencies one of the arrested is the co-owner of a prominent catering firm used by the U.S. embassy in Islamabad. It is not clear when the arrests were made. They follow a visit to Pakistan by two senior U.S. security officials.  
Source: [http://news.bbc.co.uk/2/hi/world/south\\_asia/10140288.stm](http://news.bbc.co.uk/2/hi/world/south_asia/10140288.stm)
61. *May 20, KENS 5 San Antonio* – (International) **Pirates terrorize boaters on Texas lake along Mexican border.** With machine guns in hand, Mexico's deadliest cartel is patrolling Mexican territory in the waters of a Texas border lake. The pirates already have hit several boats on Falcon Lake near Zapata, which is about an hour south of Laredo. At least three boats have been robbed so far, and authorities say they are investigating a possible fourth incident. The fear of what lurks beyond the boundary is keeping even local fisherman well within the U.S. side of the lake. U.S. authorities said there just is not a Mexican law presence on the other side of the lake, so boaters who do venture to that part of Falcon Lake are on their own.  
Source: <http://www.kens5.com/news/pirates-94535754.html>

[\[Return to top\]](#)

## **National Monuments and Icons Sector**

See item [63](#)

[\[Return to top\]](#)

## **Dams Sector**

62. *May 21, Charlottesville Tomorrow* – (Virginia) **Earthen dam proposed for water plan.** More than a year and a half after a consultant was dismissed from work on the design of a new dam for the Ragged Mountain Reservoir in Charlottesville, Virginia, the Rivanna Water & Sewer Authority (RWSA) has unveiled a new approach that is expected to cost tens of millions of dollars less. Schnabel Engineering, based in Glen Allen, has recommended that the RWSA build a massive earthen dam just downstream from the Lower Ragged Mountain dam. The new dam would raise the water level by 45 feet, allowing for storage of more than three times the amount of water held in the reservoir today. The RWSA executive director said the new dam would cost between \$28.5 million and \$36.6 million, which includes final design and engineering work, an environmental mitigation plan, and protection of the Interstate 64 embankment the larger reservoir would reach.  
Source:

[http://cvilletomorrow.typepad.com/charlottesville\\_tomorrow\\_/2010/05/earthen\\_dam\\_proposed.html](http://cvilletomorrow.typepad.com/charlottesville_tomorrow_/2010/05/earthen_dam_proposed.html)

63. *May 20, Eureka Times-Standard* – (California) **Benbow Dam removal to be studied; Orick creek gets funding.** California State Parks has been awarded a \$75,000 grant to study how Benbow Dam can be removed. The study is being funded by American Rivers and the National Oceanic and Atmospheric Administration's (NOAA) Restoration Center. The North Coast Redwoods State Parks Eel River Sector superintendent said that the design study will show how much concrete would have to be removed and how much sediment is trapped behind the dam foundation. The dam's foundation remains in place year round, and in the late spring, the parks have for years put in wooden flashboards that dam the Eel River and form Benbow Lake, a popular summertime attraction. Federal regulations aimed at protecting salmon and steelhead have in recent years placed restrictions on when the flashboards can be put in place. Rebuilding the dam foundation to standard could cost more than \$1 million — while California struggles under a huge deficit. The design study should also show whether the banks of the river would be stable after the removal of the dam and give the parks a picture of what the river would look like if the foundation were removed. American Rivers claimed the removal of the dam would restore access to some 60 miles of salmon habitat upstream of the dam, which is a partial barrier to juvenile salmon at certain times of the year. American Rivers and NOAA also awarded \$58,000 to the Pacific Coast Fish, Wildlife and Wetlands Restoration Association to remove a culvert and replace it with a bridge on Strawberry Creek outside Orick.  
Source: [http://www.times-standard.com/localnews/ci\\_15123788](http://www.times-standard.com/localnews/ci_15123788)

[[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 [NICCRports@dhs.gov](mailto:NICCRports@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](mailto: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](mailto: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](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

### **Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.