



# Homeland Security

## Daily Open Source Infrastructure Report for 30 September 2009

**Current Nationwide Threat Level**

**ELEVATED**

*Significant Risk of Terrorist Attacks*

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

### Top Stories

- Reuters reports that a Singapore-flagged tanker carrying crude oil ran aground on Monday at mile marker 3 on the Lower Mississippi River, near Pilottown, Louisiana. At least eight large vessels are being held up due to the incident. (See item [3](#))
- Two U.S. sailors and a Filipino marine were killed Tuesday in a roadside bomb believed planted by al-Qaeda linked militants, the first American troops to die in an attack in the Philippines in seven years. (See item [39](#))

### Fast Jump Menu

#### PRODUCTION INDUSTRIES

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

#### SUSTENANCE AND HEALTH

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

#### SERVICE INDUSTRIES

- [Banking and Finance](#)
- [Transportation](#)
- [Postal and Shipping](#)
- [Information and 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. *September 29, Associated Press* – (North Carolina) **Power mostly restored in Greensboro.** A storm left more than 20,000 Greensboro, North Carolina, residential and business customers in the city’s northwest area without power early evening on September 28. The News and Record of Greensboro reported that 267 power outages were reported as of 5:30 a.m. A Duke Energy spokesman says a tree fell into a major power substation, causing the outage. Most of the power had been restored early on

September 29.

Source: <http://www.reflector.com/news/state/power-mostly-restored-in-greensboro-864176.html>

2. *September 28, Bloomberg* – (International) **TransCanada pipeline struck by blast, gas rerouted.** A section of a TransCanada Corp. natural-gas pipeline that exploded September 26 in Ontario has been isolated and gas is being transported around the area through other lines. The explosion and line break occurred on a 30-inch mainline about 37 miles northwest of North Bay, Ontario, a company spokesman, said in a telephone interview. There is “not expected to be any impact on service to customers” because the gas is being rerouted through another pipeline, he said. A 36-inch-diameter and a 42-inch-diameter pipeline run parallel in the region, according to the spokesman. In the area of the blast, one of those two lines remains out of service so that the line’s structural integrity can be checked, he said. The other line was returned to service late September 26. The pipeline with the line break is about 8,700 miles long and transports natural gas from Alberta to various points throughout Canada and other markets, according to the spokesman. The pipeline has a capacity of 7 billion cubic feet a day. The blast was the second pipeline rupture TransCanada has had this month. An explosion September 13 in northern Ontario forced nearby residents to evacuate. The incident did not interrupt the flow of natural gas, according to the company.  
Source: <http://www.bloomberg.com/apps/news?pid=20601082&sid=aBEdYAVFHyco>
  
3. *September 28, Reuters* – (Louisiana) **Mississippi River traffic blocked by grounded ship.** A tanker carrying crude oil ran aground and is blocking vessel traffic near the mouth of the Mississippi River, the most important U.S. commercial waterway, the Coast Guard said on Monday. No leak has been detected from the ship, the Singapore-flagged Eagle Tucson, which is owned by U.K.-based AET Inc. The vessel ran aground at 2:45 a.m. on Monday with 602,000 gallons of crude oil, according to a Coast Guard statement. At least eight large vessels are being held up due to the incident, a Coast Guard spokeswoman said. No information was available on what cargoes those vessels held. Four tug boats are on the scene, with another two en route, to help to refloat the Eagle Tucson, and a lightering vessel arrived to transfer its cargo if necessary. The grounding of the Eagle Tucson, an upriver-bound, 107,000-ton deadweight, double-hull oil carrier, occurred at mile marker 3 on the Lower Mississippi, near Pilottown, Louisiana, and around 85 miles downriver from New Orleans. Oil refiners in the Gulf Coast region should not have to make any cuts in production because of the incident, said a source at a major U.S. refiner. The channel may be cleared to outbound traffic later Monday, the source said. “Deep-draft vessels are currently unable to transit through the area,” the Coast Guard said. The Coast Guard said it was not immediately clear how long it would take to clear the Eagle Tucson. Small vessels were still able to transit in the area, which serves as a key U.S. shipping corridor, the spokeswoman said.  
Source:  
<http://www.reuters.com/article/domesticNews/idUSTRE58R55020090928?feedType=RSS&feedName=domesticNews>

4. *September 28, KHOU 11 Houston* – (Texas) **Officials: Houston Ship Channel back in business after fuel spill.** On Friday, a vessel called The Chemical Supplier collided with a barge near Brady Island and the East Loop Bridge. A 2-foot by 4-foot gash was torn in one of the vessel’s fuel tanks, and more than 10,500 gallons of diesel spilled into the water. No injuries were reported. Crews managed to contain the spill, but they were forced to close a three-mile stretch of the channel. “In this particular instance, the collision took place below the turning basin. The pilot is the individual that has the expertise to determine when and how to turn his or her vessel,” said the counsel for Buffalo Marina Service. “It did turn at the city docks,” said a Coast Guard Captain. “It will be part of our investigation to look at those aspects of it. Why did they turn there? Should they have turned there?” A spokesperson for the chemical supplier said that the incident is under investigation. Experts say that despite the damage, the spill could have been worse. According to the barge company, the barge that was hit was not loaded. “If the loaded barge had been hit you’re looking at a million gallons of fuel in the water,” said the spokesman. Officials said 130 people are involved in the cleanup effort. They also said they do not believe the spill will have an adverse affect on any wildlife in the area, but the Coast Guard has set up a safety zone. By Monday, about 4,200 gallons had been removed from the water, and the Houston Ship Channel was back in business.  
Source: [http://www.khou.com/news/local/galveston/stories/khou090928\\_tnt\\_houston-ship-channel-oil-spill.1c3d3c165.html](http://www.khou.com/news/local/galveston/stories/khou090928_tnt_houston-ship-channel-oil-spill.1c3d3c165.html)
  
5. *September 28, DarkReading* – (International) **New NIST report sheds some light on security of the smart grid.** A draft report published on September 28 by the task group heading up the security strategy and architecture for the nation’s smart power grid provided an initial peek at how the grid may be secured. The Cyber Security Coordination Task Group, led by the National Institute of Standards and Technology (NIST) and made up of members of the government, industry, academia, and regulatory bodies, plans to finalize the overall smart grid architecture and security requirements by March of 2010. The initial draft includes risk assessment, security priorities, as well as privacy issues. The task group will publish a second draft in December after addressing the round of comments from this first draft. The smart grid, which basically makes the electrical power grid a two-way flow of data and electricity, allows consumers to remotely monitor their power usage in real-time in order to help conserve energy and save money. But researchers have raised red flags about the security of the smart grid. Some have already poked holes in the grid, including an IOActive researcher, who was able to execute buffer overflow attacks and unleash rootkits on smart meters. The researcher found multiple vulnerabilities in smart meters, and pointed out that most of the devices do not use encryption nor do they authenticate users when updating customer software and other operations. A smart grid expert with FYRM Associates spoke at Black Hat USA about his worries over utilities “self-policing” their implementations of the security framework. “This is history repeating itself,” he said in an interview with Dark Reading in July. The new “Smart Grid Cyber Security Strategy and Requirements” draft, which is open for comment, covers various potential security issues with the grid, as well as privacy risks of the smart grid.  
Source:

<http://www.darkreading.com/insidertthreat/security/perimeter/showArticle.jhtml?articleID=220300142>

[[Return to top](#)]

## Chemical Industry Sector

6. *September 28, WALB 10 Albany* – (Georgia) **Chemical spill causes big problem in Thomas County.** Seven hundred gallons of hazardous chemicals leaked from transformers being hauled off as scrap metal. Monday’s cleanup is on highways, county roads, a parking lot and even a mobile home park. Officials say no one is in immediate danger because they covered most of the large chemical spills with sand, but they are still waiting on lab results that will tell them the chemical’s potency, and potential health hazard. Officials say Interstate Warehouse contracted two men to haul off three large transformers the company had for more than 20 years. But inside the transformers was a hazardous liquid called PCB or Polychlorinated Biphenyls — a liquid that covered more than four miles of Thomas County when the transformers started leaking. “The spill has been contained, precautionary measures have been taken there is no immediate danger,” said a code enforcement officer. County crews immediately called the Environmental Protection Division in Albany. They covered the spills with sand and sent off a sample of the chemical to test its potency and potential hazard to the community. “The sample will tell us the concentration of the PCBs in the fluid that’s been leaked in the soil and on the highways,” said the Thomas County fire chief. The man hauling the transformers on his trailer was cited by city and county law enforcement for an unsecure load. The warehouse company was cited by Code Enforcement’s environmental health division for illegal disposal of hazardous waste. Source: <http://www.walb.com/Global/story.asp?S=11213728>
  
7. *September 28, Omaha World-Herald* – (Nebraska) **I-680 reopens after spill.** The westbound portion of Interstate 680 near North 48th Street is now open, after authorities closed the thoroughfare for nearly four hours to clean up the remnants of a non-toxic fertilizer spill. A semi-trailer truck container carrying thousands of gallons of the substance ruptured shortly after 1 p.m. Monday, creating a large mess on the highway, authorities said. The Nebraska State Patrol said the closed portion of the highway was re-opened around 4:30. No crash was reported at the location, and no details were immediately available about what caused the tank to rupture. Omaha police are investigating the incident, the patrol said. The leak had been contained by mid-afternoon, after workers built dikes out of dirt and sand to contain the spill. Officials with the state’s department of environmental quality were dispatched to the scene, but said the situation would be handled by local authorities. Source: <http://www.omaha.com/article/20090928/NEWS01/909289988>
  
8. *September 28, Midland Daily News* – (Texas) **Small fire occurs at Dow Corning.** A small fire at Dow Corning’s Midland site Sunday evening caused no injuries and was extinguished quickly, a company spokesperson said. The fire started about 8:30 p.m. in a chemical containment area. Two buildings were evacuated, but no one was injured,

said a company spokesperson. Dow Corning and Midland firefighters responded, and the fire was extinguished quickly.

Source: [http://ourmidland.com/articles/2009/09/28/police\\_and\\_courts/2122512.txt](http://ourmidland.com/articles/2009/09/28/police_and_courts/2122512.txt)

9. *September 28, Riverside Press-Enterprise* – (California) **Acid spill prompts SigAlert, closes freeway lane.** A SigAlert traffic advisory has been issued until about 10 a.m. for a big-rig that has leaked acid, closing one westbound lane of Highway 210 in Rancho Cucamonga. “There’s about 65,000 pounds of acid on board. And some of it leaked onto the slow lane,” said an officer from the California Highway Patrol. “It’s a little difficult to clean up.” The problem was reported at 11:18 p.m. Sunday as a truck fire near Day Street. At 4:30 a.m., officials at the scene estimated that the cleanup and lane closure would continue for another five or six hours.

Source:

[http://www.pe.com/localnews/inland/stories/PE\\_News\\_Local\\_S\\_webacid28.dd865c.html](http://www.pe.com/localnews/inland/stories/PE_News_Local_S_webacid28.dd865c.html)

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

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

10. *September 29, Rutland Herald* – (Vermont) **Yankee protest ends in arrests.** Four elderly women living downwind of the Vermont Yankee nuclear reactor were arrested Monday afternoon when they walked through the first two security gates at the Vernon reactor and sat down on folding chairs, blocking entry to the plant. The four women, members of the Vermont Yankee Shut It Down Affinity Group, are no strangers to Vermont Yankee protests, and each said they had been arrested multiple times outside the Entergy Nuclear corporate headquarters in North Brattleboro but never prosecuted. Entergy Nuclear officials said that the response by the plant’s security forces Monday afternoon went well and denied that security had been breached. But the women, wearing tie-dye T-shirts and carrying folding stools and signs, ignored the entreaties of the armed guard at the guardhouse, marched right past him through the second chain-link gate and then sat down with their folding chairs and protest signs. In about a minute, the Vernon police chief showed up in his cruiser, and eventually three Vermont State Police cruisers showed up. The four women were put in the various cruisers and taken to the nearby Vernon Police Department, where they were processed and released.

Source:

<http://www.rutlandherald.com/article/20090929/NEWS04/909290330/1003/NEWS02>

11. *September 29, Nuclear Power Industry News* – (New Jersey) **NRC finalizes New Jersey agreement to regulate certain radioactive materials.** The Nuclear Regulatory Commission has completed an agreement with New Jersey, under which the state will assume NRC’s regulatory authority over certain radioactive materials. New Jersey becomes the 37th NRC Agreement State, effective September 30. Under the agreement, the NRC will transfer to New Jersey the responsibility for licensing, rulemaking, inspection and enforcement activities for: (1) radioactive materials produced as

byproducts from the production or utilization of special nuclear material (SNM – enriched uranium or plutonium); (2) naturally occurring or accelerator-produced byproduct material (NARM); (3) source material (uranium and thorium); (4) SNM in quantities not sufficient to support a nuclear chain reaction; and (5) the regulation of the land disposal of source, byproduct, and SNM received from other persons. The NRC will transfer an estimated 500 licenses for radioactive material to New Jersey’s jurisdiction. New Jersey will retain regulatory authority over approximately 500 NARM licensees, including 300 who also hold NRC licenses. These licensees would have their NRC and New Jersey licenses combined into a single state license. In total, New Jersey would then have jurisdiction over approximately 700 licenses.

Source: [http://nuclearstreet.com/blogs/nuclear\\_power\\_news/archive/2009/09/29/nrc-finalizes-new-jersey-agreement-to-regulate-certain-radioactive-materials-9296.aspx](http://nuclearstreet.com/blogs/nuclear_power_news/archive/2009/09/29/nrc-finalizes-new-jersey-agreement-to-regulate-certain-radioactive-materials-9296.aspx)

12. *September 29, Nuclear Engineering International* – (North Carolina) **NRC begins special inspection at Brunswick.** The Nuclear Regulatory Commission has dispatched a Special Inspection Team to the Brunswick nuclear power plant, operated by Progress Energy near Southport on the southeastern coast of North Carolina. The team will inspect and assess circumstances associated with a malfunction of one of the plant’s four emergency diesel generators. During return to service testing on September 19, Emergency Diesel Generator #4 shut down prematurely and would not restart. Since the problem could not be corrected within the time frame required by technical specifications, Progress was required to shut down both reactors on September 20. Progress officials believe the generator failure was caused by problems associated with the engine’s governor. The NRC’s three-person Special Inspection Team, which includes one region-based inspector, one resident inspector from another site and the senior resident inspector stationed at the Brunswick site, is developing a sequence of events related to the issue. The team will be reviewing the company’s actions following discovery; evaluating the adequacy of the company’s past post-maintenance testing; and identifying any generic issues for Brunswick or other nuclear plants. The special inspection began on September 25 and is expected to continue until early October. The NRC will issue a report within 45 days of the completion of the inspection.  
Source: <http://www.neimagazine.com/story.asp?sectioncode=132&storyCode=2054258>

13. *September 29, Nashville Tennessean and Associated Press* – (Alabama) **Whistle-blower wins TVA plant case.** A painter fired by a contractor at TVA’s Browns Ferry Nuclear Plant in Alabama after reporting safety concerns has won his whistle-blower case in a ruling by a U.S. Department of Labor appeals panel. The worker was fired by nuclear contractor Stone & Webster in 2004 after reporting what he said was a faulty paint job that could cause paint chips to clog emergency cooling pumps. The company had said he was fired for an angry outburst at a meeting in which he used inappropriate language. The panel overturned an administrative judge who ruled in the company’s favor. “It’s been difficult,” said the whistle-blower, 43, a lifelong painter now working on a project at NASA’s Marshall Space Flight Center in Huntsville, Alabama. “It’s good to see it hopefully coming to a close.” A spokeswoman for Stone & Webster said the company was disappointed the board opted “to overrule the decision of the arbitrator who conducted the hearing in this case, considered all of the evidence, and

ruled in the company's favor. "However, because this matter is still in litigation, we have no further comment at this time." Stone & Webster could appeal the case to the U.S. 11th Circuit Court of Appeals.

Source:

<http://www.tennessean.com/article/20090929/NEWS02/909290336/1009/NEWS02>

14. *September 28, U.S. Nuclear Regulatory Commission* – (National) **NRC chairman takes steps toward greater commission openness and transparency.** The Nuclear Regulatory Commission chairman announced Monday he plans to begin immediately releasing his votes to the public, moving away from the Commission's long-standing tradition of withholding that information until action on issues is completed. "I believe this will give the public a better understanding of how the Commission makes decisions. Public discussions of our deliberations are appropriate and beneficial," said the chairman adding, "I look forward to broadening this effort and taking the next logical step of convening public decision-making meetings of the Commission." To begin this new initiative, the chairman released his views on several items before the Commission, including a draft final rule on decommissioning planning and a draft policy statement on safety culture.

Source: <http://www.nrc.gov/reading-rm/doc-collections/news/2009/09-161.html>

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

## **Critical Manufacturing Sector**

15. *September 28, WYMT 57 Hazard* – (Kentucky) **Explosion at Special Metals, no serious injuries reported.** Emergency crews are responding to a reported explosion at the Special Metals Plant in Burnaugh, Kentucky. It happened at around 3 p.m. on September 28. A spokesperson for Special Metals says there were no serious injuries. Several employees are being treated for smoke inhalation. All workers have been accounted for. No word yet what caused the explosion. Earlier Monday, the spokesman said Special Metals laid off 30 hourly workers — 27 in the Huntington plant and 3 at the burnoff plant where the explosion happened. Several fire departments are on the scene.

Source: <http://www.wkyt.com/wymtnews/headlines/62417647.html>

16. *September 28, Bloomberg* – (International) **Singapore A380 engine failure forces flight return.** A Singapore Airlines Ltd. Airbus A380 bound for Asia returned to Paris after one of its four engines failed, the first time a mechanical malfunction forced an in-flight turnaround of the world's biggest passenger jet. Flight SQ333, with a crew of 27 and 444 passengers on board, left for Singapore at 12:35 p.m. on September 27. Two and a half hours into the flight, an engine message to the cockpit prompted a shutdown by the pilot, Singapore Airlines said. The airline did not reveal the cause of the malfunction. "While the aircraft is able to operate with three engines, the pilots decided to return to Paris as a precaution due to the long flight," the airline said. The A380 double-decker jet operated by Singapore is one of 19 in service. The craft is still in Paris. The jet is being fitted with a new engine on the ground, the airline said. The

A380 is certified as safe to fly with only three of its four engines, which led the pilot to return to Paris, where trained mechanics and other ground personnel could address the issue, said a spokesman for France's DGAC civil aviation authority. The Charles de Gaulle airport is equipped to accommodate the double-decker, wide-body A380. Rolls-Royce is working closely with the airline to investigate the reasons of the malfunction, a spokeswoman said. The company said the engine has proven highly reliable, with a dispatch rate, or number of times the aircraft has left at departure time, of 99.8 percent. Air France KLM Group's Air France is scheduled to take delivery of its first A380 by the end of October, and will fly the plane between Paris and New York's JFK airport. Deutsche Lufthansa AG's first delivery was pushed back from 2009 to 2010. Airbus delivered one A380 in 2007, 12 in 2008, and has committed to delivering 14 this year, after deferrals by several airlines forced it to drop down from 18 units. The company has a total order volume of 200 for the A380.

Source: [http://www.bloomberg.com/apps/news?pid=20601085&sid=aJzG6NMdJ\\_c](http://www.bloomberg.com/apps/news?pid=20601085&sid=aJzG6NMdJ_c)

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

## **Defense Industrial Base Sector**

17. *September 28, Marine Corps Times* – (National) **New Army tank could mean changes for M1A1 fleet.** With the Army developing a tank for the 21st century, the Corps faces tough decisions about its aging M1A1 Abrams fleet, the Corps' armor integration officer said. The Army intends to build prototypes of a high-tech M1A3 Abrams by 2014 and field new vehicles by 2017. The project will incorporate improvements made to the existing Abrams fleet in Iraq, such as underbelly armor and ballistic shields, and allow the new tanks to plug into modern computer networks, Army officials said. This puts the Corps at a crossroads. With far fewer tanks in its fleet and less money available for upgrades, Marine officials must decide between keeping the M1A1 in the field through 2050, moving to the M1A2 System Enhancement Package, or partnering with the Army on the M1A3, said the heavy armor capabilities integration officer with Marine Corps Combat Development Command. The Corps has about 400 tanks, which cost about \$4 million each. The Army has thousands, with an effort under way that converts older M1A1 models into newer M1A2 variants with upgraded equipment. The matter is complicated further by the Corps' decision to devote heavy funding through 2025 to the Expeditionary Fighting Vehicle, the Joint Light Tactical Vehicle and the Marine Personnel Carrier, the officer said. The Corps also is developing plans for active prevention systems that can stop rocket-propelled grenades and anti-tank rounds from destroying an Abrams, amphibious assault vehicles and armored trucks, he said. Several companies have developed devices that can destroy RPGs, but most work by shooting something at it, making the round explode before it hits the tank. While safety mechanisms can prevent nearby dismounted troops from getting hurt in the process, the Corps remains skeptical.

Source: [http://www.marinecorpstimes.com/news/2009/09/marine\\_abrams\\_092709w/](http://www.marinecorpstimes.com/news/2009/09/marine_abrams_092709w/)

18. *September 28, Asbury Park Press* – (National) **Employees of defense contractor in Red Bank plead guilty in conspiracy to accept kickbacks.** Two former employees of

a high-tech defense contractor in Red Bank, New Jersey have pleaded guilty in federal court to conspiracy to accept kickbacks in the awarding of subcontracts. The two men each entered a guilty plea to a conspiracy charge in separate appearances before a U.S. District Judge on September 28. The government information — a formal accusation in lieu of a grand jury indictment — that contains the charges does not disclose the name of the Red Bank company, referred to as Company-1 and described by authorities as a scientific, engineering, and technology applications company which contracts with the federal government, including the Department of Defense and its components. It also does not identify by name a second company involved, referred to as Company-2 in the document and described as a California-based communications infrastructure integration company. Officials at the Red Bank company were unaware of the illegal transactions, said a spokesman for the U.S. Attorney's Office. The defendants admitted that for about two years during their employment, they received approximately \$150,873 in kickback payments from representatives of Company-2, according to a prepared release from the U.S. Attorney's Office. The defendants admitted that their kickback fee was based on a percentage of Company-1 business that was referred to Company-2, the release said. To solicit, accept, and attempt to accept kickbacks to gain favorable treatment in connection with prime government contracts and subcontracts relating to prime government contracts is a violation of federal law, according to the formal charge.

Source: <http://www.app.com/article/20090928/NEWS05/909280345/1004/NEWS01>

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

## **Banking and Finance Sector**

19. *September 29, Los Angeles Times* – (California) **Riverside County man sentenced to 100 years for operating Ponzi scheme.** In what federal prosecutors described as the longest sentence ever imposed for a financial crime in Southern California, a Riverside County man was sentenced Monday to 100 years in prison for operating a Ponzi scheme that bilked investors of about \$35 million. The guilty party, who ran the operation from 2000 to 2003 through a company he called MX Factors, was sentenced by a U.S. district judge in federal court in Riverside. Dozens of the company's estimated 700 investors wrote the judge to demand a stiff sentence. Prosecutors said the guilty party, using a team of sales agents, told clients that he would invest their money in government-guaranteed construction loans and promised monthly returns as high as 14 percent every three months. Instead of investing in construction, the guilty party wired some of the money to foreign banks, paid high commissions to agents and launched a crab-fishing business in Ensenada, prosecutors said. Some early investors were paid dividends that came from later investors, a classic Ponzi scheme, said an assistant U.S. attorney.

Source: <http://www.latimes.com/business/la-fi-ponzi29-2009sep29,0,1441674.story>

20. *September 28, Associated Press* – (Pennsylvania) **Ex-CEO of Pa. drinks-maker charged in \$806M fraud.** A federal grand jury accused the former chief executive officer of a defunct soft-drink-maker and four others connected to the company of

perpetrating an \$806 million bank fraud, much of which went to the ex-CEO and his family. The suspect, of Ligonier, provided financial institutions and equipment suppliers “with dramatically false financial statements” to get equipment leases and loans for Latrobe-based Le-Nature’s Inc., said the U.S. Attorney. She called it the “largest fraud in the history of the Western District of Pennsylvania,” a 25-county area. According to the 29-count indictment unsealed on September 28, lenders and investors poured money into the company on the basis of the phony financial statements. The government wants the suspect to forfeit bank accounts worth more than \$7 million. Investigators have already seized tens of millions of dollars in jewelry and an 8,000-piece model train collection worth about \$1 million from the suspect. Authorities believe the suspect spent much of the money on himself or his family, as he once drove a Hummer and a high-end Mercedes, and was building a mansion in Ligonier, 45 miles southeast of Pittsburgh. The U.S. Attorney said the loss to the lenders and investors continues to exceed \$700 million. The criminal investigation grew out of Le-Nature’s forced bankruptcy in October 2006, when a judge determined it was likely the suspect and other company directors had engaged in criminal activity. The bankruptcy of Le-Nature has spawned a raft of litigation, including a racketeering suit brought by the bankruptcy trustee that accuses Charlotte, North Carolina-based Wachovia Corp. of aiding the scheme. Earlier this month, a federal judge ruled the trustee can continue to pursue Wachovia for allegedly continuing to lend money to Le-Nature’s despite red flags raised by Wachovia’s own analysts.

Source:

[http://www.google.com/hostednews/ap/article/ALeqM5iEbHtufksKXavPm47UEIkLLUn\\_sgD9B0IK001](http://www.google.com/hostednews/ap/article/ALeqM5iEbHtufksKXavPm47UEIkLLUn_sgD9B0IK001)

21. *September 28, Bloomberg* – (Michigan) **SEC sues Detroit broker for luring elderly to \$250 million scam.** The U.S. Securities and Exchange Commission sued a Detroit-area broker for allegedly defrauding elderly investors by selling interests in a firm that claimed it had telecommunications deals with hotels and truck stops. The suspect reaped at least \$3.8 million for himself and his company, Fast Frank Inc., by encouraging investors to refinance their homes to participate in a \$250 million Ponzi scheme run by the owner of the company E-M Management Co. LLC, the SEC said. The suspect raised \$74 million and the SEC said he was the most successful salesperson for the company owner, who was sued in 2007 for running the scam. The suspect falsely told investors he conducted due diligence in E-M, which claimed to have contracts to install and service telecommunications equipment with hotels and casinos in Las Vegas, the SEC said in a complaint filed at federal court in Michigan. Most, if not all, of the purported contracts did not exist, the agency said. The suspect did not know about the scam, has been cooperating for more than a year and provided documents to the agency, said his attorney. The regulator did not claim in its complaint that the suspect signed checks, received bank statements or that his name was mentioned in offering documents “that would show he had any actual knowledge that this was an alleged Ponzi scheme,” the attorney said. Several of the suspect’s 800 clients in Michigan and California used home-equity lines of credit to borrow \$100,000 or more, and he encouraged one investor to borrow \$1 million on her home to buy interests in the the company owner’s projects, the SEC said. The company owner had

1,200 clients.

Source:

[http://www.bloomberg.com/apps/news?pid=20601087&sid=a7Z1V\\_CXOKDw](http://www.bloomberg.com/apps/news?pid=20601087&sid=a7Z1V_CXOKDw)

22. *September 28, Canwest News Service* – (International) **Worm infecting banks' computers can steal passwords, company warns.** Computers at a majority of Canada's big banks are infected with a malicious computer worm capable of logging keystrokes and stealing passwords, an Ottawa security firm has warned. Defence Intelligence Inc. said on September 28 it has been monitoring the worm dubbed Mariposa for five months and has watched it spread to machines at more than 50 of the top 100 Fortune 500 companies as well as Canada's banks. The Canadian Bankers Association said it is aware of the worm, which it believes has done little if any damage. But the chief executive officer of Defence Intelligence called Mariposa "a highly sophisticated piece of malicious software" that appears to be very selective in its targets. "We've detected compromised behaviour from hundreds of government agencies, financial institutions, universities and corporate networks worldwide, but surprisingly few home users," he said. The chief executive officer said his team of 11 employees stumbled across the worm while monitoring routine Internet traffic in May. They noticed packets that seemed to be coming from a well known financial institution reporting back to servers in Israel and Germany. Further inspection revealed the packets were coming from a malicious software program designed to steal information from banks, government and other financial institutions. A spokesman for the Canadian Bankers Association, said Mariposa has not breached the sophisticated security systems in place to protect customers' personal and financial information. "Banks are aware of this malicious software and, based on discussions last week with a number of banks, there has been little-to-no-impact from it at all," he said. Still, banks are working to eliminate the worm, the spokesman said.

Source: <http://www.financialpost.com/news-sectors/story.html?id=2044247>

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

## **Transportation Sector**

23. *September 29, KRON 4 San Francisco* – (California) **Suspicious package in SF near Transbay Terminal deemed safe.** Police say they've determined that a suspicious package found on a Muni bus near San Francisco's Transbay Terminal was a backpack filled with clothing. Officials say the situation started after a Muni driver on a 5 Fulton bus discovered a large gym bag in the back of the bus during a routine sweep of the vehicle at the end of a trip Monday around 11 a.m. After streets were shut down and nearby businesses were either evacuated or told to shelter-in-place, the problem was cleared around 12:15 p.m. when the contents of the bag were deemed safe. During the situation, six Muni bus lines were rerouted and motor coaches shuttled passengers around. Transit officials say all Muni service has resumed. Though all has been resolved, officials are warning that traffic may be backed up for awhile.

Source:

<http://www.kron4.com/News/ArticleView/tabid/298/smId/1126/ArticleID/3281/reftab/>

24. *September 29, Los Angeles Times* – (California) **Jet halted at LAX; Two men are removed by police.** A plane was stopped from taking off from Los Angeles International Airport, and two men on board were taken into custody, according to the Los Angeles Police Department (LAPD). A police officer said the men, who appeared to be of Middle Eastern descent, were acting suspiciously. A law enforcement source said at least one of the men ran into a restroom on the plane and appeared to hide while the New York-bound jet was taxiing on the runway, according to the source, who spoke on the condition of anonymity because the case was ongoing. The flight crew confronted the two men and made the decision to stop the plane before it took off, the source said. The men were taken into custody by heavily armed law enforcement officials. The plane was taken to a remote area of the airport to be searched by a bomb squad, sources said. The Federal Bureau of Investigation (FBI) determined that the passenger removed from the United Airlines flight Tuesday morning posed no “identifiable threat” to the plane or passengers and that no criminal charges are anticipated. The passenger got up from his seat about 8:30 a.m. to use the restroom and would not comply with the flight crew’s instructions to return to his seat, an FBI source said. The captain of the plane then decided to return to the gate so that the incident could be investigated, she said. “The passenger is being interviewed in connection with the incident and is cooperative,” she said. “Out of an abundance of caution, the passengers and their carry-on luggage were rescreened and the LAPD bomb unit conducted a precautionary search of the aircraft. “No criminal charges are anticipated, and the passengers will proceed to their destination later today.”  
Source: <http://latimesblogs.latimes.com/lanow/2009/09/authorities-halted-a-plane-from-taking-off-from-los-angeles-international-airport-and-arrested-two-men-on-board-after-they-be.html>

For more stories, see items [3](#), [4](#), [6](#), [7](#), [9](#), [16](#), and [33](#)

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

## **Postal and Shipping Sector**

25. *September 29, WGGB 6 Springfield* – (Massachusetts) **Suspicious package at Springfield mail center prompts bomb squad response.** A suspicious package at a bulk mail center prompted a response from the Springfield Fire Department Arson and Bomb Squad Tuesday morning, but the object has been determined to be harmless. According to a Springfield fire department spokesman, a call for the package came in just after 8:30 a.m. Tuesday at the bulk mail center located at 190 Fiberloid St. Explosive experts used a suit made to protect against explosive blasts to inspect the package, he said, and it has been determined to be a microwave oven tightly wrapped in black plastic. The scene was cleared after the object was determined not to be explosive, according to the fire department spokesman.  
Source: <http://www.wggb.com/Global/story.asp?S=11222333>

26. *September 29, WHIO 7 Dayton* – (Ohio) **Bomb squad investigates package, finds porcelain pig.** The Dayton Bomb Squad called in when a suspicious package was found on property owned by the Mayor of Dayton. An aide to the mayor found a towel with something wrapped inside in a mailbox at the old McLin Funeral Home on Germantown. A robot was used to check out the package. The package contained a porcelain pig and was not detonated by authorities.  
Source: <http://newstalkradiowhio.com/localnews/2009/09/bomb-squad-investigates-packag.html>
27. *September 25, Yakima Herald-Republic* – (Washington) **Scare at courthouse in Ellensburg turns out to be a hoax.** Police will be investigating the source of three suspicious letters that were apparently intended to target the criminal justice system in Kittitas County. Police said Friday night that the county courthouse and two other government offices that received the letters had been cleared. “The incident has been declared a hoax,” the Ellensburg police captain said in an e-mail, adding that no further information would be released about the letters. The one received at the juvenile probation office on the second floor of the county courthouse contained a nontoxic white powder, officials said at the scene. The employee who opened the letter was decontaminated as a precaution at Kittitas Valley Community Hospital, but she did not suffer any symptoms, said a chief with Kittitas Valley Fire and Rescue. Dozens of courthouse employees were sent home for the day so that a hazardous materials team from the Washington State Patrol could secure the envelope there. The Health Department building at 507 Nanum St., which also houses the county probation division, reopened after a brief evacuation because the package there was still in a mailbox, officials said. At an afternoon news conference, the county commission chairman said he had not received any updates about possible suspects or motives. The police captain said police would be investigating, along with federal postal inspectors. The fire official said that even though the incident turned out to be a hoax, authorities still had to treat the letters as a real threat. He estimated that about 30 firefighters and police officers responded.  
Source: <http://www.yakima-herald.com/stories/2009/09/25/09-26-09-kittitas-courthouse>

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

## **Agriculture and Food Sector**

28. *September 29, Buenos Aires Herald* – (International) **Kraft union leaders barred from returning to work after agreement.** On Monday night, the owner of the U.S.-based Kraft plant signed an accord with workers to review the situation of 152 employees who were fired after they took over the company’s plant in General Pacheco, Buenos Aires province in Argentina. Five union leaders of Kraft-Foods were not allowed to enter the plant of the company in General Pacheco, a day after the company reached an agreement with a trade-union to rehire the workers who had been laid off as part of a labor dispute. However on Tuesday morning, the company refused to allow five union leaders, whom the company holds responsible for the violent

protests, back in the plant. The firm has reported that cameras had videotaped those employees smashing windows and breaking machines in the factory during protests. The labor action started in July, as workers pressed the company to suspend production due to a swine flu outbreak. Kraft employees later took over the company and suspended production for 38 days, until last Friday, when the police evicted the protesters amid violent clashes with the demonstrators. Twelve people, among them eight policemen, were injured during the eviction. Officers of the Buenos Aires police and anti-riot trucks remained inside the plant Tuesday to prevent further incidents from taking place.

Source: <http://www.buenosairesherald.com/BreakingNews/View/13202>

29. *September 29, Reliable Plant Magazine* – (Kansas) **Hiland Dairy Foods facing \$124,500 in OSHA penalties.** The U.S. Department of Labor’s Occupational Safety and Health Administration (OSHA) has cited Hiland Dairy Foods Company in Wichita, Kansas for alleged violations of the Occupational Safety and Health (OSH) Act and has proposed \$124,500 in penalties. OSHA’s inspection found 24 alleged serious violations of the OSH Act, the majority of which relate to deficiencies with the company’s process safety management program (PSM), an OSHA requirement for preventing the catastrophic release of hazardous chemicals. “There is no excuse for Hiland Dairy’s inattention to such a critical program aimed at preventing the catastrophic release of hazardous chemicals,” said OSHA’s regional administrator in Kansas City, Missouri. The serious violations stem from overall deficiencies in the company’s PSM program. Other issues included lack of hoist system inspections, unguarded floor holes, deficiencies in the facility’s lockout/tagout program, unguarded belts, pulleys and sprockets, and electrical hazards. OSHA issues a serious citation when death or serious physical harm is likely to result from a hazard about which an employer knew or should have known.

Source:

[http://www.reliableplant.com/article.aspx?articleid=20269&pagetitle=Hiland+Dairy+Foods+facing+\\$124,500+in+OSHA+penalties](http://www.reliableplant.com/article.aspx?articleid=20269&pagetitle=Hiland+Dairy+Foods+facing+$124,500+in+OSHA+penalties)

For another story, see item [31](#)

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

## Water Sector

30. *September 29, Associated Press* – (Missouri) **DNR: broken sewer line releases 3 million gallons of untreated waste into Blue River tributary.** A sewer line break in the Kansas City, Missouri area released more than 3 million gallons of untreated waste into a tributary of the Blue River. The state Department of Natural Resources (DNR) said the break occurred Friday and was repaired late Monday. The waste was going into a southeast Kansas City stream that drains into the Blue River. The DNR said in a release late Monday that it had issued a notice of violation to Kansas City because of the sewer line break. A DNR spokesman said Tuesday it was unclear what caused the break. DNR ordered the city to sample water in the tributary above and below the site

of the release, and to sample water in the Blue River near the tributary.

Source: <http://www.fox2now.com/news/sns-ap-mo--sewagedumped,0,1176232.story>

31. *September 28, U.S. Environmental Protection Agency* – (Idaho) **Idaho Department of Fish and Game fined \$14,000 for chemical spill at Grace Fish Hatchery.** Idaho Department of Fish and Game (IDFG) has agreed to pay \$14,000 to the U.S. Environmental Protection Agency (EPA) to settle alleged federal Clean Water Act violations at the Grace Fish Hatchery near Pocatello, Idaho. In December of 2007, IDFG informed EPA that spilled disinfectants at Grace killed all of its fish, many of which were washed downstream into Whiskey Creek. EPA reviewed Grace's history and found IDFG also exceeded the monthly limit for total suspended solids in early 2004. IDFG's response has included collecting dead fish along Whiskey Creek after the chemical spill, creating a staff manual explaining correct chemical use and educating all IDFG hatchery staff on the requirements of the NPDES permit.

Source:

<http://yosemite.epa.gov/opa/admpress.nsf/0/FE8E2B25C3F8E7938525763F006D3626>

32. *September 27, Philadelphia Inquirer* – (Pennsylvania) **Breaking ground with a \$1.6 billion plan to tame water.** Philadelphia has announced a \$1.6 billion plan to transform the city over the next 20 years by embracing its storm water — instead of hustling it down sewers and into rivers as fast as possible. The proposal, which several experts called the nation's most ambitious, reimagines the city as an oasis of rain gardens, green roofs, thousands of additional trees, porous pavement, and more. All would act as sponges to absorb — or at least stall — the billions of gallons of rainwater that overwhelm the city sewer system every year. The plan's complex funding formula would raise rates somewhat but also attract grants and encourage private investment. The plan is a radical departure from the highly engineered tunnels and sewage plant expansions cities have traditionally opted for. Whether the plan will work as the department intends is still being analyzed by regulators and environmental experts. Sixty percent of the city has a combined sewer system, which means both runoff from streets and wastewater from bathrooms and kitchens flow through the same pipes. In dry weather, the system works pretty well, considering that portions are more than a century old. But when it rains — even as little as a tenth of an inch — the system overflows. With no place to go, the water — now laced with road oil, litter, and raw sewage — gushes from 164 pipes directly into the Delaware, the Schuylkill, and Tacony, Pennypack, and Cobbs Creeks. Bacteria levels skyrocket. Like many cities, Philadelphia is under orders to come up with a plan to reduce the overflows, which amount to 14 billion gallons a year.

Source:

[http://www.philly.com/philly/news/homepage/20090927\\_Breaking\\_ground\\_with\\_a\\_1\\_6\\_billion\\_plan\\_to\\_tame\\_water.html?viewAll=y](http://www.philly.com/philly/news/homepage/20090927_Breaking_ground_with_a_1_6_billion_plan_to_tame_water.html?viewAll=y)

33. *September 27, Cleveland Plain Dealer* – (Ohio) **Bridge spills blocked from water supply.** An innovative dirt and clay basin along I-80 in Mahoning County, Ohio will keep hazardous spills out of a reservoir that supplies drinking water to more than 300,000 people. Containment systems, one at each end of the two newly built I-80

bridges that span the Meander Creek Reservoir in the county, are a first for the Ohio Department of Transportation (ODOT). And they represent a victory for a fire chief who battled with the state agency to have the systems included in the bridge project. Construction on the \$91 million bridge and road project began in 2006 and was completed this month. ODOT says the \$1.2 million containment project is a model of how to eliminate contamination of fresh-water areas and wetlands from hazardous liquids that spill onto bridges during accidents. Shutoff valves contain the spills and prevent the substances from flowing through a pipe into the 2,010-acre reservoir, which provides water to Youngstown, Austintown, Niles, and several other cities.

Source:

<http://www.cleveland.com/news/plaindealer/index.ssf?/base/news/1254040327222640.xml&coll=2>

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

## **Public Health and Healthcare Sector**

34. *September 28, Washington Post* – (National) **Cyber gangs hit healthcare providers.** Organized cyber thieves that have stolen millions from corporations and schools over the past few months recently defrauded several health care providers, including a number of non-profit organizations that cater to the disabled and the uninsured. The victims are the latest casualties of an online crime wave being perpetrated against U.S.-based organizations at the hands of cyber thieves thought to be based out of Eastern Europe. On September 9, crooks stole \$30,000 from the Evergreen Children’s Association (currently doing business as Kids Co.), a non-profit organization in Seattle. Then last week, criminals targeted Medlink Georgia Inc., a federally qualified, not-for-profit health center that serves the uninsured and under-insured. The thieves stole the user name and password to Medlink’s online banking account, and used that access to send more than \$44,000 to at least five different “money mules.” Also last week, unknown hackers stole nearly \$200,000 from Steuben ARC, a Bath, New York-based not-for-profit that provides care for developmentally disabled adults. The fraudulent transfers were sent in two batches to at least 20 different money mules around the nation. Steuben’s bank blocked the second batch, for a total of \$103,000, and a portion of the \$93,000 worth of bogus transfers from the second batch. The Trojan horse in question is Clampi, by many accounts one of the most sophisticated pieces of malware in distribution today.

Source:

[http://voices.washingtonpost.com/securityfix/2009/09/online\\_bank\\_robbers\\_target\\_health.html](http://voices.washingtonpost.com/securityfix/2009/09/online_bank_robbers_target_health.html)

See item [40](#)

35. *September 28, Nashville Tennessean* – (Tennessee) **Doctors mistakenly fax patients’ data to Indiana company.** Doctors’ offices in Tennessee have been accidentally sending patient information, including Social Security numbers and medical histories, to an Indiana businessman’s fax machine for the past three years. The sensitive medical information was supposed to be sent to the Tennessee Department of Human Services,

but the owner of SunRise Solar Inc. in Indiana says hundreds of confidential medical faxes have been coming to him. He said he has tried to correct the problem with the state and doctors' offices but to no avail. He even called the governor's office. State officials say they have contacted the doctors' offices and told them to be sure to use the correct fax number.

Source:

<http://www.tennessean.com/article/20090928/NEWS01/909280333/Doctors+mistakenly+fax+patients++data+to+Indiana+company>

36. *September 28, Government Health IT* – (National) **CDC funds health threat detection centers.** The Centers for Disease Control and Prevention (CDC) awarded \$4.4 million to fund four university-based “centers of excellence” to help improve detection of public health threats and test new public health informatics tools. The grants will fund Centers of Excellence in Public Health at Harvard Pilgrim Health Care, Indiana University, the University of Pittsburgh, and the University of Utah. “These centers will advance the study and practice of public health informatics through collaborative efforts among academic public health experts, local and state public health departments, developing regional health information organizations, and other health and informatics professionals,” said the acting director of CDC’s National Center for Public Health Informatics. The centers will emphasize measurement of the public health effects of their work, he added. Each center will conduct two projects that support national priorities in informatics and support real-time bio-surveillance for potential health threats through immediate access to data from hospitals and health care systems in major metropolitan areas.

Source: <http://www.govhealthit.com/newsitem.aspx?nid=72146>

37. *September 28, Reuters* – (National) **AIDS vaccine works, but back to the drawing board.** More than 25 years into the AIDS pandemic, scientists finally have a vaccine that protects some people — but instead of celebrating, they are going back to the drawing board. The vaccine, a combination of two older vaccines, only lowered the infection rate by about a third after three years among 16,000 ordinary Thai volunteers. Vaccines need to be at least 50 percent effective, and usually 70 to 80 percent effective, to be useful.

Source: <http://www.reuters.com/article/healthNews/idUSTRE58R4KE20090928>

38. *September 28, San Antonio Express-News* – (Texas) **Liquid swine flu medicine in short supply.** With children hit hardest by swine flu and a vaccine still weeks away, many pharmacies have run out of liquid Tamiflu, the antiviral medicine used to keep them out of the hospital. Instead, pharmacists are advised to empty regular Tamiflu capsules into an old-fashioned mortar and mix it with syrup using a pestle. Many pharmacists do not compound medications because of the extra time and expense. Those that have been using the procedure to increase their supply of liquid Tamiflu have gotten a lot of business this week. Roche, the manufacturer of Tamiflu, made the decision to focus on producing pills rather than the oral medicine in the face of the pandemic, a spokesman said. “The capsule requires 25-times less manufacturing capacity than the liquid,” he said. “And the capsules have a seven-year shelf life, while

the liquid has a two-year shelf life. That was our rationale for doing that. And knowing we had enough of the larger capsules that could be converted should there be a shortage of the (liquid).” The federal government revised its recommendations for Tamiflu on Tuesday. It recommends the use of the antiviral in sick children age 2 and younger, and says it might be advisable in healthy children 2 to 4 — as well as older children with asthma or other chronic medical conditions that put them at high risk of serious complications.

Source: [http://www.seattlepi.com/health/410592\\_swinemed0928.html](http://www.seattlepi.com/health/410592_swinemed0928.html)

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

## **Government Facilities Sector**

39. *September 29, Associated Press* – (International) **2 U.S. troops killed in Philippines blast.** Two U.S. sailors and a Filipino marine were killed Tuesday in a roadside bomb believed planted by al-Qaeda linked militants, the first American troops to die in an attack in the Philippines in seven years. The Philippine military suspected Abu Sayyaf militants were behind the attack against the U.S. Navy troopers on the southern island of Jolo. Jolo lies in a poor, predominantly Muslim region. The American forces have been providing combat training and weapons to Filipino troops battling the Abu Sayyaf. Philippine officials described the blast as being caused by a land mine, a description normally used for military-grade weapons. The U.S. Embassy said it was an improvised explosive device.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2009/09/29/AR2009092900171.html?hpid=moreheadlines>

40. *September 28, IDG News Service* – (Illinois) **School boards hit with cash-stealing trojan.** The U.S. Federal Bureau of Investigation is probing a rash of reported online computer intrusions that have resulted in hundreds of thousands of dollars being stolen from school districts in Illinois. FBI investigators are working on a computer intrusion case at the Crystal Lake School District in Crystal Lake, Illinois, said a spokesman with the FBI’s Chicago office. But several other school districts also believe that they have been hit by the same malicious software, the spokesman said. The FBI believes that the Clampi virus, already associated with a rash of banking thefts throughout the U.S., may be to blame, the spokesman said. The spokesman declined to provide more information on the case because it is still under investigation, but local reports say that as much as US\$350,000 may have been taken from the Crystal Lake District alone. The district’s superintendent did not return a call seeking comment for this story.

Source:

[http://www.pcworld.com/article/172769/school\\_boards\\_hit\\_with\\_cashstealing\\_trojan.html](http://www.pcworld.com/article/172769/school_boards_hit_with_cashstealing_trojan.html)

See item [34](#)

41. *September 25, U.S. Department of Justice* – (International) **Jury convicts Defense Department official of unlawful communication of classified information and making false statements.** A former Department of Defense worker was convicted by a

federal jury today on charges involving providing classified information to a man working with the People's Republic of China (PRC) and lying to the FBI about it. The defendant was convicted of one count of unlawfully communicating classified information to an agent of a foreign government and two counts of making false statements to the FBI. He was acquitted of two unlawful communication of classified information, one count of conspiracy to communicate classified information to an agent of a foreign government and act as an illegal foreign agent, and one count of aiding and abetting an agent of a foreign government. The defendant faces a maximum of 10 years in prison on the unlawful communication of classified information count and a maximum of five years in prison for each false statement count when he is sentenced on January 22, 2010. The defendant, age 62, worked at the Pentagon and, from August 2001 through February 11, 2008, was the Deputy Director, Washington Liaison Office, U.S. Pacific Command (PACOM). He held a Top Secret security clearance, worked in a Sensitive Compartmentalized Information Facility (SCIF) and had a classified and unclassified computer at his cubicle. He has been on administrative leave with pay since mid-February 2008 and has not performed any duties in or for PACOM since that time.

Source: <http://www.usdoj.gov/opa/pr/2009/September/09-nsd-1033.html>

For another story, see item [27](#)

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

## **Emergency Services Sector**

42. *September 28, KTUU 2 Anchorage* – (Alaska) **State gets mobile emergency response center.** The Alaska Division of Homeland Security, which is in charge of handling emergencies, has a new tool at its fingertips: a new mobile unified command center that can coordinate operations in the middle of a disaster area. The \$930,000 command center comes to the state through a federal grant designed to protect energy infrastructure — in Alaska's case, the pipeline. But the state says they will be using it for more than just that. The 45-foot-long unit is equipped with top-of-the-line technology and spaces. It contains a conference room, a dispatch center, and even a mast cam that, using the Internet, can feed a live stream of its broadcast to emergency crews, who can check it on their iPhones. Emergency officials say the center's most impressive parts lie behind what is seen, like a satellite dish-equipped Internet and phone capability that can handle temperatures of 60 below.

Source: <http://www.ktuu.com/Global/story.asp?S=11215198>

43. *September 28, WIBC 93.1 Indianapolis* – (Indiana) **81 inmates evacuated in jail fire.** Eighty-one inmates were evacuated from the Starke County, Indiana, Jail Sunday night following a fire in a cell block. The sheriff said inmates attempted to ignite a mattress, which caused heavy smoke damage. The inmates were transported to Marshall and Pulaski county jails. They will be returned to the Starke County Jail when the air is determined to be safe. No injuries were reported. The state fire marshal is

investigating.

Source: <http://www.wibc.com/news/Story.aspx?id=1144677>

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

## **Information Technology Sector**

44. *September 29, Digital Signage Expo* – (National) **ICSA Labs addresses security threat to network-connected devices, including digital signs.** Responding to an often overlooked security risk, ICSA Labs, an independent division of Verizon Business, recently introduced a new program to help enterprises safeguard against intrusions through network-connected devices such as printers, faxes and point-of-sale systems, as well as help device manufacturers ensure that their products are secure. The new capabilities offered by ICSA Labs, a vendor certification program and a comprehensive enterprise assessment, are designed to protect these typically stand-alone, unattended devices, which connect directly to a network but are not part of the network infrastructure itself, according to the company. Also included in this product class of network-attached devices are copiers, ATM machines, digital signs, proximity readers, security cameras and facility management systems for power, lighting and HVAC systems, said the company. ICSA Labs has found that these unprotected devices can allow hackers easy access to corporate networks. According to the Verizon Business 2009 Data Breach Investigations Report, many breaches occur through what is called “unknown, unknowns,” which can involve systems such as printers and faxes. The report also points out that attackers choose the path of least resistance, targeting vulnerable systems. ICSA Labs’ first new offering, Network Attached Peripheral Security (NAPS) certification, provides manufacturers an opportunity to work with ICSA Labs to help identify and remediate existing and potential vulnerabilities in the devices the manufacturers sell, said the company. The NAPS certification program service also applies to manufacturers whose products are still under development and are seeking recommendations to make their products safer.

Source:

<http://digitalsignageexpo.net/IndustryNews/tabid/317/smId/1236/ArticleID/1942/t/ICSA-Labs-Addresses-Security-Threat-to-Network-Connected-Devices-Including-Digital-Signs/Default.aspx>

45. *September 28, The Register* – (International) **Sunbelt buckles up for anti-bloatware drive.** The anti-virus bloatware problem is getting worse despite what some vendors may claim, according to figures from Sunbelt Software. The Florida based vendor’s marketing claims tap into a deep well of discontent about anti-virus products but are not supported by the latest results from independent testing labs, such as AV-Test.org, and therefore ought to be treated with caution. What is not in dispute is that slow, bloated anti-virus engines chew up system resources. The problem has been a continual source of frustration for Windows users for years, and something their Mac and Linux-using peers always cite in operating system arguments. Worse yet, each new version of the leading Windows anti-virus products from Symantec, Trend and McAfee et al can increase the demand on CPU and memory by a significant factor, Sunbelt claims. This

can effectively reduce the useful life of existing machines which, according to Sunbelt, need 20 per cent more grunt (extra CPU power and RAM) for each update.

Source: [http://www.theregister.co.uk/2009/09/28/bloatware\\_survey/](http://www.theregister.co.uk/2009/09/28/bloatware_survey/)

46. *September 28, IDG News Service* – (International) **Pressure on Microsoft, as Windows attack now public.** Hackers have publicly released new attack code that exploits a critical bug in the Windows operating system, putting pressure on Microsoft to fix the flaw before it leads to a worm outbreak. The vulnerability has been known since September 7, but until September 28 the publicly available programs that leverage it to attack PCs have not been able to do more than crash the operating system. A new attack, developed by a Harmony Security senior researcher, lets the attacker run unauthorized software on the computer, in theory making it a much more serious problem. The researcher's code was added to the open-source Metasploit penetration testing kit on September 28. Two weeks ago, a small software company called Immunity developed its own attack code for the bug, but that code is available only to the company's paying subscribers. Metasploit, by contrast, can be downloaded by anyone, meaning the attack code is now much more widely available. A Metasploit developer said on September 28 that the exploit works on Windows Vista Service Pack 1 and 2 as well as Windows 2008 SP1 server. It should also work on Windows 2008 Service Pack 2, he added in a Twitter message. But the code may not be completely reliable. The Immunity senior researcher said that he could get the Metasploit attack to work only on the Windows Vista operating system running within a VMware virtual machine session. When he ran it on native Windows systems, it simply caused the machines to crash. Either way, the public release of this code should put Windows users on alert. Security experts worry that this code could be adapting to create a self-copying worm attack, much like last year's Conficker outbreak.

Source:

[http://www.pcworld.com/businesscenter/article/172739/pressure\\_on\\_microsoft\\_as\\_windows\\_attack\\_now\\_public.html](http://www.pcworld.com/businesscenter/article/172739/pressure_on_microsoft_as_windows_attack_now_public.html)

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

### 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 Website: <http://www.us-cert.gov>.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

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

## Communications Sector

See item [5](#)

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

## Commercial Facilities Sector

47. *September 29, Associated Press* – (Michigan) **It’s just a drill: Comerica Park NOT under attack.** Federal and local law-enforcement personnel will descend from helicopters into Comerica Park on Septmeber 30 at 11 a.m. as part of an exercise preparing for the possibility of a World Series in Detroit. Officials say Detroit SWAT and U.S. Customs and Border Protection personnel will participate in the “fast-roping” exercise, in which agents descend into the ballpark on a thick rope from a helicopter. Agents will meet with the media following the mission, which was originally scheduled for Tuesday but was postponed because of a rainout at Comerica Park Monday night. Source: <http://www.detnews.com/article/20090929/METRO/909290375/1265/It-s-just-a-drill--Comerica-Park-NOT-under-attack>

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

## National Monuments and Icons Sector

48. *September 28, U.S. Government Accountability Office* – (National) **Homeland Security: Actions needed to improve security practices at national icons and parks.** On September 28, the Government Accountability Office (GAO) released the August 2009 report entitled “Homeland Security: Actions Needed to Improve Security Practices at National Icons and Parks.” In 2004, the GAO determined whether the Park Service’s security efforts for national icons and parks reflected key practices given the post-9/11 environment. The GAO found that the Park Service has implemented a range of security improvements since the terrorist attacks and has worked to integrate security into its primary mission to preserve national icons and parks for the public’s enjoyment. For example, it has established a senior-level security manager position and taken steps to strengthen security at the icons, and is developing a risk management program for small parks. These efforts exhibit some aspects of the key protection practices, but GAO found limitations in each of the areas. The Park Service does not allocate resources using risk management service-wide or cost-effectively leverage technology; has not advanced this risk management approach for icons to the rest of its national parks; icons and parks may use a variety of security technologies and other countermeasures, they do not have guidance for evaluating the cost-effectiveness of these investments; the Park Service faces limitations with sharing and coordinating information internally and lacks a service-wide approach for routine performance measurement and testing; it lacks comparable arrangements for internal security communications and, as a result, parks are not equipped to share information with one another on common security problems and solutions; the Park Service has not established security performance measures and lacks an analysis tool that could be used to evaluate program effectiveness and inform an overall risk management strategy; finally, strategic human capital management is an area of concern because of the Park Service’s lack of clearly defined security roles and a security training curriculum. Source: <http://www.gao.gov/htext/d09983.html>

49. *September 27, Associated Press* – (New Mexico) **Pipe bomb found at Elephant Butte Lake.** New Mexico state police said no one was hurt by a pipe bomb left at Elephant Butte Lake. Bomb technicians were able to destroy the pipe bomb Saturday night. Officials at Elephant Butte Lake got a call Saturday night about a suspicious package left along the shore. State police discovered the pipe bomb.  
Source: <http://www.koat.com/news/21132223/detail.html>

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

## **Dams Sector**

50. *September 29, KING 5 Seattle* – (Washington) **Flood insurers leaving Kent valley residents high and dry.** Homeowners and businesses along the Green River in Washington are being urged to prepare for flooding, and part of that preparedness includes buying flood insurance. But flood insurance may be harder to come by. Lawmakers have been very proactive about warning people about the great potential for flooding in the Kent valley this winter. The trouble is many insurance companies are hearing the warnings too and deciding it is not a risk they want to take. The Howard Hanson Dam is weak and could potentially fail this winter. The Army Corps of Engineers has said it may be forced to release water during heavy rains to prevent a total failure of the dam. The release of water could cause flooding, but a dam collapse would be far worse. In either case, the risk is high. There is government flood insurance available from the Federal Emergency Management Agency. That would probably provide enough coverage for renters and homeowners, but businesses might be in trouble. Government flood benefits are capped at \$500,000 for business structures and another \$500,000 for contents. That's not nearly enough to cover many businesses in the valley. The Seattle Times says many of the policies that remain have exclusions for actions taken by governments, meaning if flooding was technically decided by the Army Corps, businesses could be left high and dry by insurance companies. In the meantime, businesses and homeowners are still being urged to buy government flood insurance.  
Source: [http://www.nwcn.com/topstories/stories/NW\\_092909WAB-flood-insurance-LJ.1c9309f29.html](http://www.nwcn.com/topstories/stories/NW_092909WAB-flood-insurance-LJ.1c9309f29.html)

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

## **DHS Daily Open Source Infrastructure Report Contact Information**

**About the reports** - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

### **Contact Information**

Content and Suggestions:

Send mail to [NICCCReports@dhs.gov](mailto:NICCCReports@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.