Top Stories

- The Minneapolis Star Tribune reports that about 250 people were evacuated from their homes, and students on a college campus were advised to stay indoors October 18, after anhydrous ammonia leaked from a farm tractor tank in Morris, Minnesota. (See item 28)
- According to CNN, at least five shots were fired at the Pentagon in Arlington, Virginia October 19, authorities said, striking a building window, causing a partial lockdown of parking lots, and forcing the temporary closure of a busy highway. (See item 42)

Fast Jump Menu

PRODUCTION INDUSTRIES
- Energy
- Chemical
- Nuclear Reactors, Materials and Waste
- Critical Manufacturing
- Defense Industrial Base
- Dams

SERVICE INDUSTRIES
- Banking and Finance
- Transportation
- Postal and Shipping
- Information Technology
- Communications
- Commercial Facilities

SUSTENANCE and HEALTH
- Agriculture and Food
- Water
- Public Health and Healthcare

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. October 19, Long Beach Press-Telegram – (California) Working to avoid a San Bruno tragedy. Five weeks after a natural gas pipeline explosion killed eight people in California’s bay area, a five-member panel has been named to study underground pipeline safety and regulatory changes. The group, which includes members from the legal, labor, engineering and education communities, are working under the auspices of the California Public Utilities Commission, which oversees gas and hazardous material
safety and transfer guidelines. Members include the chancellor emeritus of UC Davis; a member of the International Brotherhood of Electrical Workers; the chairman of the California Council on Science and Technology and former chancellor of UC Santa Cruz; a financial expert and former energy company executive; and the former president of the Sacramento Municipal Utility District. The group was organized as an “independent body” to investigate the causes, response, and liability arising from the September 9 explosion of a natural gas pipeline operated by Pacific Gas & Electric (PG&E) in San Bruno. Among the panel’s tasks are discerning “the public’s right to information concerning the location of natural gas transmission and distribution facilities in populated areas,” according to its mission statement. The panel will work with dozens of state and industry experts in coming weeks, with public hearings on their progress and findings scheduled each month.


2. *October 19, Sioux City Journal* – (Iowa) **Explosion rocks MidAmerican Energy plant.** An explosion at MidAmerican Energy plant on Southgate Drive in Sioux City, Iowa startled residents October 18. Several Sioux City fire and police units were dispatched to the scene, where heavy smoke and some flames rose from the side of a building shortly after the incident. A Sioux City Fire Rescue lieutenant said the approximately 30-by-90-foot building sustained major damage to its south side. Officials are still investigating, but do not suspect foul play, he said. A MidAmerican spokesman said the facility is part of a liquid natural gas, or LNG, plant. The explosion occurred while natural gas was being emptied from a line. The gas line was being emptied so employees of a third-party contractor could continue painting the holding tanks, which the MidAmerican spokesman said they had been doing for about 1 week. Sioux City police and troopers from the Iowa State Patrol temporarily blocked off some streets near the site of the blast due to danger posed by chemical holding tanks outside the building. However, they reopened the roads after determining the blast was confined to the building.


3. *October 19, Worcester Telegram and Gazette* – (Massachusetts) **Webster-Dudley power outage blamed on vandalism.** Vandalism to National Grid’s East Webster substation cut power to 6,700 customers in Webster, Massachusetts and 4,200 in Dudley, Massachusetts, about 8:30 a.m. October 19, according to a National Grid spokesman. Utility officials believe vandals got into the substation and cut ground wires. “Crews are there now working to restore the ground system to make it safe,” the spokesman said. Then the transformers at the substation will have to be powered up in stages. “We’re shooting for complete recovery this morning,” he said. “I ask people to be patient,” said the Webster police chief, especially at intersections. Area schools remained in session.


4. *October 18, Harrisburg Daily Register* – (Illinois) **Fire at natural gas plant causes substantial damage.** An October 18 explosion at the Compressed Energy Systems
natural gas plant in Raleigh, Illinois sent area fire departments scurrying. The rapid response helped limit damage at the gas plant on state Route 34 just beyond the Raleigh curve. “I think I got some belts hot,” the owner said. “I was out here at midnight changing some belts.” He said the most likely scenario is a belt slipped and caught fire, then spread through the building. Firefighters from Eldorado, Galatia, and Harrisburg responded at about 7:30 a.m. after a report of an explosion. The owner shut the gas after he discovered the fire. Firefighters started sending tankers back to the station about 8:30 a.m. The building is a total loss, but the tanks beside the building were not damaged. In all, about $300,000 to $500,000 damage is possible including the building and machinery, the owner said. Compressed Energy pulls methane gas out of the old mines in the area and puts it on a pipeline after processing. Traffic at state Route 34 and Raleigh Road was diverted for a while after the fire departments began arriving on the scene. Traffic was back to normal again by about 8:30 a.m. 

For more stories, see items 19, 20, and 34

Chemical Industry Sector

5. October 19, WVEC 13 Hampton Roads – (Virginia) Recent spill raises concerns at Chesapeake chemical storage site. After some 2,000 gallons of chemical fertilizer spilled at Allied Terminals October 18, the community in Chesapeake, Virginia, expressed concerned about letting the firm store other chemicals in the future. This is the second chemical spill at Allied Terminals in 2 years. The company plans to begin storing sulfuric acid, a highly corrosive acid, on the site in 2011. Although officials said the spill had no apparent impact to the nearby Elizabeth River and South Hill neighborhood, the city remains apprehensive. The City of Chesapeake has protested, stating a special permit would be required to store the sulfuric acid. Allied Terminals claims it needs no such permit. 

For more stories, see items 2, 28, and 33

Nuclear Reactors, Materials and Waste Sector

6. October 19, National Nuclear Security Administration – (National) NNSA office of emergency operations develops cutting-edge nuclear terrorism software. The National Nuclear Security Administration (NNSA) October 19 announced its office of emergency operations has developed and delivered a new X-ray image processing capability to U.S. emergency responders. X-Ray Toolkit (XTK) is an application used
by field responders and NNSA Laboratory experts to acquire, process and analyze X-ray images obtained during a potential nuclear terrorism incident. XTK development was sponsored by NNSA’s emergency operations technology integration program, and implemented by its stabilization program. “We have received overwhelmingly positive feedback about XTK software from our operational partners,” said NNSA’s Associate Administrator for Emergency Operations. XTK was designed for joint use by Explosive Ordnance Disposal (EOD) and NNSA Laboratory personnel during nuclear render safe operations, where specialized procedures, methods and tools prevent the detonation of a nuclear device. Previous software was converted for use from the medical diagnostic industry, not specifically designed for use by EOD experts.

Source: http://www.yournuclearnews.com/nnsa+office+of+emergency+operations+develops+cutting-edge+nuclear+terrorism+software_55411.html

7. October 19, Computer Weekly – (International) Investigation launched into Sellafield’s lost USB stick. United Kingdom nuclear processing company Sellafield has launched an investigation into the loss of a USB stick containing information about the company’s business operations. The unencrypted stick was found in a hotel room in Cumbria by a coach driver. It contained details of a proposed workforce transfer and data suggesting International Atomic Energy technicians visiting the site were not sufficiently briefed regarding health and safety regulations, said the Northwest Evening Mail. A Sellafield spokesman said no sensitive material was thought to be contained on the memory stick. “However, we take this issue very seriously and are investigating how this happened,” he said. Sellafield provides USB sticks to employees for transferring business-related information. All stick users receive guidance, the company said. However, the vice-president at data security firm Credant said corporate USB sticks should always include encryption. “Sellafield has done the right thing in launching an investigation, but this is a potentially serious breach of data security on several levels, with national security overtones,” he added.

Source: http://www.computerweekly.com/Articles/2010/10/19/243403/Investigation-launched-into-Sellafield39s-lost-USB.htm

8. October 19, Las Vegas Review Journal – (National) Dispatch center to coordinate radioactive waste transport. A company based in Washington state is establishing a trucking dispatch center in northwest Arizona to coordinate transportation of low-level radioactive waste throughout the country for disposal at the Nevada National Security Site (NSS) 65 miles northwest of Las Vegas. The company owner said Specialized Services Trucking has a contract with the Department of Energy to transport hazardous materials from 15 different states. The company is leasing a former Bureau of Land Management building in Kingman from a private owner to dispatch tractors to sites where materials are packaged in casks that are pre-loaded on trailers. The waste will be trucked into Nevada on Interstate 15. The CEO said the hauling could begin early next month with 24 big rigs. She said as many as 100 trucks could eventually be used in the operation. The CEO said the company will be hauling from former laboratories in Nevada, Utah, California, New Mexico, South Carolina, North Carolina, Tennessee, Kentucky, Indiana, Ohio, New York, Georgia, Virginia, Illinois, and Washington.
NNS spokesman confirmed the labs identified by the CEO are sites from which waste product would be transported to the Nevada facility.

9. **October 18, The Herald** – (International) **Laptop with classified info stolen at NMMU.** A laptop containing highly classified documents about the Koeberg nuclear power station in Cape Town, South Africa has been stolen from the engineering department at Nelson Mandela Metropolitan University (NMMU). The laptop contains secret documents about the plant and fears that the theft could jeopardize security have been raised. Police are creating a task team to investigate the case. According to police sources, a lecturer left the laptop on the table in the engineering department October 18 when he finished a lecture earlier in the day. “He was packing up in his office ... and he went back to the lecture room and noticed the laptop was missing,” the officer said. “He only reported it to police Tuesday afternoon.” A police spokesman confirmed the theft. A NMMU spokesman said last night: “All I can say is the incident was reported to our security department and it is receiving the highest priority investigation. We hope the information contained in the laptop doesn’t land up in the wrong hands.”
Source: http://www.theherald.co.za/article.aspx?id=615760

**Critical Manufacturing Sector**

10. **October 18, KFOX 14 El Paso** – (Texas) **Anthony worker killed in possible plant explosion.** The El Paso County Sheriff’s Office has confirmed the death of an employee at the Arcelor Mittal Plant formerly known as Border Steel in Vinton, Texas. The Anthony, Texas man was killed following reports of an explosion at about 2:40 a.m. October 18. Plant employees reported hearing a loud explosion and then saw heavy smoke. As workers were accounting for all personnel, they found one employee was missing. The workers entered the affected building and turned off the power to the furnaces, which is when they found the man on the ground. He was transported to the hospital with serious injuries and died a few hours later.

**Defense Industrial Base Sector**

Nothing to report

**Banking and Finance Sector**
11. **October 19, Softpedia – (International)** **Multi-bank phishing attack targets Indian taxpayers.** Security researchers warn of a new phishing attack exploiting the tax return filing period in India, which uses fake pages for a large number of banks. Floods in certain parts of India led the country’s Central Board of Direct Taxes to extend the due date for filing income tax returns from September 30 to October 15. According to a security researcher with Symantec, this decision attracted phishing attacks, which distributed links to a fake version of the Indian Income Tax Department Web site. The rogue page instructed visitors to select their bank from a list of over a dozen financial institutions to complete the refund request. “Once a bank was selected from the list, the customer was redirected to a phishing site spoofing the log-in page of the selected bank. “After the log-in credentials were entered into the phishing site, the customer was redirected back to the legitimate bank’s Web site,” the security researcher explained. Phishing e-mails claiming to originate from tax collection agencies are common during tax filing periods, especially in countries like the United States, U.K., Canada, or Australia. However, attacks targeting so many banks at once are relatively rare.


12. **October 19, Softpedia – (International)** **Phishers use mobile credit bait.** Security researchers from Symantec warn of a phishing campaign, which promises free mobile credits in order to trick online banking users into exposing their credentials and phone numbers. This particular attack targeted customers of an Italian bank, but it’s a good indication of the various methods used by phishers to lure victims. The phishing page was hosted on a domain that was a typo of the bank’s real Web address, a technique known as typosquatting. The site claimed that if the users recharged their mobile credit through the bank system with 10 euros, they would receive an additional 40 euros as a bonus. This attack is a double phishing attempt, because the users are first asked to log in to their accounts, which exposes online banking credentials, and then they must input mobile phone numbers.


13. **October 18, WIAT 42 Birmingham – (Alabama)** **Mountain Brook bank robbed; employees evacuated.** The chief of Mountain Brook Police tells CBS42 that employees of Wells Fargo, located at 100 Office Park Drive in Mountain Brook, Alabama, were evacuated due to a robbery October 18. A police spokesman said the suspect arrived at the location in a vehicle, passed a note to a teller claiming there was a bomb on the roof and then drove off. Officials think the man got away with some money. The suspect is a black male in a white Chevrolet; the police spokesman said he is still on the loose. Officials from the Hoover Police Department were called to the scene and determined there was no bomb at the bank.

Source: [http://www.cbs42.com/content/localnews/story/Mountain-Brook-Bank-Robbed-Employees-Evacuated/4_nLqVtOdUSScYhhply9hw.cspx](http://www.cbs42.com/content/localnews/story/Mountain-Brook-Bank-Robbed-Employees-Evacuated/4_nLqVtOdUSScYhhply9hw.cspx)

14. **October 18, Softpedia – (International)** **Number of fake electronic tax payment emails has spiked.** Security researchers warn that a ZeuS distribution campaign
producing e-mails about failed electronic tax payments, has significantly increased its aggressiveness the weekend of October 16-17. The rogue e-mails started hitting inboxes from October 11-15 and come with a subject of “Your Tax Payment ID ####### is failed. Update information.” The from field is spoofed to appear as if the e-mail is originating from “EFTPS Tax Payment,” and it tells users their tax payments submitted through the Electronic Federal Tax Payment System (EFTPS) has failed. Also, the messages claim the payment failed with an R21 error code and provide a link to obtain additional information. Clicking on the link takes recipients through a series of redirects until they land on a drive-by download page, where their computers are targeted with exploits for outdated versions of many popular applications. Successful exploitation results in a variant of the ZeuS banking Trojan being installed. This malware is commonly used by fraudsters to steal online banking credentials, credit card details and other sensitive data. According to researchers from e-mail security provider AppRiver, the number of these ZeuS distribution e-mails spiked October 16, with over 100 new domains being used in the attack. Source: http://news.softpedia.com/news/Number-of-Fake-Electronic-Tax-Payment-Emails-Has-Spiked-161368.shtml

15. **October 18, IDG News Service – (International)** U.K. arrests man accused of organizing money ‘mules’. United Kingdom police arrested a 34-year-old man October 18 on suspicion of creating counterfeit credit cards and organizing a network of people involved in money laundering, officials said. Authorities from the Metropolitan Police’s Central e-crime Unit also seized data and equipment believed to be used to created fraudulent payment cards, including blank dummy cards with magnetic strips, during a raid October 18 in London. The man is also accused of organizing money “mules” — people recruited to accept stolen funds and transfer them to other bank accounts for a small share of the amount. The latest action follows a spate of arrests in the United Kingdom, United States and Ukraine in one of the largest coordinated computer crime actions by law enforcement. Source: http://www.computerworld.com/s/article/9191618/U.K._arrests_man_accused_of_organizing_money_mules

16. **October 16, BankInfoSecurity.com – (National)** Three banks closed on Oct. 15. Federal and state banking regulators closed three banks October 15. These closures raise the total number of failed institutions to 152 so far in 2010. The latest failed banks include: Security Savings Bank, F.S.B, Olathe, Kansas was closed by the Office of Thrift Supervision, and the Federal Deposit Insurance Corporation (FDIC) was appointed receiver. FDIC arranged for Simmons First National Bank, Pine Bluff, Arkansas, to assume all deposits. The nine branches of Security Savings Bank will reopen as branches of Simmons. Security Savings had $508.4 million in assets. The estimated cost to the Deposit Insurance Fund (DIF) will be $82.2 million. WestBridge Bank and Trust Company, Chesterfield, Missouri was closed by the Missouri Division of Finance. FDIC was appointed receiver. FDIC arranged for Midland States Bank, Effingham, Illinois, to assume all deposits. The sole branch of WestBridge will reopen as a branch of Midland States. WestBridge had $91.5 million in total assets. The
estimated cost to the DIF will be $18.7 million. Premier Bank, Jefferson City, Missouri, was closed by the Missouri Division of Finance, and the FDIC was appointed receiver. FDIC arranged with Providence Bank, Columbia, Missouri, to assume all the deposits. The nine branches of Premier will reopen as branches of Providence. Premier had $1.18 billion in assets. The estimated cost to the DIF will be $406.9 million.


17. **October 15, DataBreaches.net** – (Illinois) **Illinois AG sues Payday Loan Store over improper disposal of customer data.** The Illinois attorney general filed a lawsuit in Cook County Circuit Court October 15 against The Payday Loan Store of Illinois, Inc. (PLS), for allegedly failing to safeguard customer data. The attorney general filed the suit after learning that documents containing customers’ personal information had turned up in trash bins outside four store locations. “Data security is absolutely critical to protecting consumers from identity theft,” the attorney general said. PLS, which sells high-cost, short-term loans throughout Illinois, provides customers with a privacy policy that promises the company will protect personal information by maintaining physical, electronic and procedural safeguards in compliance with federal regulations. The attorney general’s complaint alleges, however, that PLS did not maintain those safeguards and instead disposed of customers’ personal data in publicly accessible trash containers. The complaint alleges a concerned individual alerted Bolingbrook police that he had found documents containing sensitive information in a trash container behind the PLS location in Bolingbrook. The police retrieved approximately two boxes of documents containing nonpublic personal information, including Social Security numbers, driver’s license numbers, financial account numbers and PLS loan account numbers.

Source: [http://www.databreaches.net/?p=14735](http://www.databreaches.net/?p=14735)

For another story, see item 55

[Return to top]

**Transportation Sector**

18. **October 19, ABC 13 Roanoke** – (Virginia) **Diesel fuel spill closes Newport News harbor.** The Small Boat Harbor in Newport News, Virginia is closed following a diesel fuel spill. The Newport News Fire Department said in a news release that a large amount of fuel spilled into the harbor shortly after 7 a.m October 19. The source of the spill hasn’t been determined. Fire and hazardous materials crews put a retention boom across the harbor’s mouth and around all drains to contain the spill.


19. **October 19, Occupational Health and Safety** – (National) **New rules coming for onshore hazardous liquid pipelines.** An advance notice of proposed rulemaking published October 18 by the Pipeline and Hazardous Materials Safety Administration (PHMSA) outlines new safety rules it may put in place for onshore hazardous liquid pipelines. While PHMSA regulates about 173,000 miles of hazardous liquid pipelines,
only 76,000 of these miles are in areas that could affect a High Consequence Area (HCA), which is defined as a commercially navigable waterway, a high-population area, or another populated area. PHMSA said it may expand the definition of an HCA so more miles of pipeline are subject to the requirements. For example, it may change the phrase “commercially navigable waterways” to “navigable waters” or “waters of the United States,” as in the Clean Water Act. The publication also asked whether major road crossings and/or railway crossings should be included as HCAs. Pipelines affecting HCAs must have leak detection means installed, and the agency wants to improve leak detection for the remaining pipelines and increase their use of check values or remotely controlled valves to isolate sections of a pipeline. Current Pipeline Safety Regulations don’t apply to all onshore hazardous liquid pipeline facilities. The agency asks whether these exemptions should be revised or repealed.


20. October 19, Texas Tribune – (Texas) Heavy loads, some from wind and gas, damage Texas roads. Part of Farm to Market Road 97 in Floyd County, Texas, has been so heavily repaired that one lane is a gray, black, and sandy-colored patchwork. The cause: Convoys of trucks lugging materials to a nearby wind farm that was built several years ago. Heavy truck traffic, some of it related to the energy industry, has increased sharply across the state in recent years, and it has taken a heavy toll on rural roadways. The number of super-heavy vehicle permits — granted by the Texas Department of Transportation (TxDOT) to trucks over 254,300 pounds — rose from 208 in fiscal year 2005 to 1,525 in fiscal year 2009, due to increased economic activity, and improved processes for identifying heavy loads. In February, a record 1.7 million-pound load moved through Texas, a generator bound for a coal plant in Riesel from the Port of Houston. To TxDOT’s chagrin, trucking companies and the industries they serve rarely shoulder the cost of fixing the damage, which can run in the hundreds of thousands of dollars for a single state road. In 2007, when natural gas prices were high and drilling was booming, the agency spent more than $23 million in road rehabilitation funds in Johnson County alone — more than one-third of the available funds — plus an additional $11 million from other sources.


21. October 18, WRTV 6 Indianapolis – (Indiana) Police: Woman had 2 loaded guns at airport. An Indianapolis, Indiana woman was arrested after she tried to bring two loaded handguns into Indianapolis International Airport, police said. The 56-year-old woman was stopped at a security checkpoint just before 7 p.m. October 16 after an X-ray machine showed the outline of a gun in her carry-on luggage, police said. She was carrying two loaded handguns — a .25 caliber black Colt automatic and a 6mm black Browning — at the bottom of her bag, police said. She told officers she had forgotten the guns were in her purse when she came to catch a flight from Indianapolis to Baltimore-Washington International Airport. She also admitted to not having a license for the guns, police said. The woman was arrested and preliminarily charged with entering a controlled area of an airport with a weapon, and carrying a handgun without
22. **October 18, AOL News** – (International) **Cruise ship collides with cargo ship in Shanghai.** The Costa Classica cruise ship was damaged in a collision with a cargo ship during an Asia cruise, causing some minor injuries to passengers, the Italian cruise line said. The accident occurred in the Yangtze River as the cruise ship returned to Shanghai from Cheju, Korea, Seatrade Insider reported. After the 4:46 a.m. collision with the Belgian-flagged Lowlands Longevity, Classica passengers were summoned to their emergency muster stations. Several reported to the ship doctor with minor injuries, and three passengers were sent ashore for medical care. Seatrade said local news images show the ship docked in Shanghai with a 60-foot scrape or gash along its starboard side on Deck 5, a deck below the lowest level of cabins, but well above the water line. There were mostly Asian passengers, but also Americans and Canadians on the cruise ship.


23. **October 18, Moultrie Observer** – (Georgia) **Pilot reports plane shot at.** A Coolidge, Georgia man reported he was shot at as he flew his plane over a field October 17. A Colquitt County sheriff’s deputy was called to Moultrie Municipal Airport on Highway 319 South in Moultrie, Georgia about 6:50 p.m. about a plane being shot at. The deputy met with the pilot who stated he was flying over a field off of Smithwick Bridge Road and saw several vehicles in the field. Believing the vehicles were there for a quail hunt, the pilot stated he was trying to make a course correction and head away from the field. As he began making his turn, he saw several people appear, and they began to shoot at him and his plane. There was no reported damage to the plane.

Source: [http://moultrieobserver.com/local/x1416241661/Pilot-reports-plane-shot-at](http://moultrieobserver.com/local/x1416241661/Pilot-reports-plane-shot-at)

24. **October 18, WIVB 4 Buffalo** – (New York) **Officials train for NFTA terror attack.** Police agencies in Buffalo, New York spent the night practicing what to do in the event of a terror attack on Buffalo’s public transportation system October 18. Niagara Frontier Transportation Authority (NFTA) police teamed up with state police, Erie County Emergency Services, the FBI, as well as Buffalo and Cheektowaga Police for a training exercise at the Metro Rail LaSalle Station. They simulated defusing a suspected explosive device and a hostage situation. “It’s very important from a learning standpoint to keep up with this type of training, because all of these tactical skills are very perishable skills and if you don’t practice you’re not going to be as good when the time comes to use them for real,” said NFTA’s transit police chief. About 175 members from seven local agencies took part in the training.


25. **October 17, Buck’s County Courier Times** – (Pennsylvania) **Tanker cars vandalized.** Vandals ruptured several railroad tanker cars, dumping about 240,000 gallons of used cooking oil and 1,500 gallons of diesel into a rail yard in Falls, Pennsylvania October 14. The fire marshal said employees of Tyburn Railroad Co.
discovered pools of oil and fuel when they arrived at work. The company notified the state department of environmental protection, police, fire officials and the U.S. Coast Guard, due to the proximity to the Delaware River. The rail yard is designed to pool spills in designated areas. Tanker trucks used vacuum hoses to suck up the oil and diesel, then deposited the fluids back in the repaired tanker cars. The company hired to help clean the spill received assistance from Waste Management, which created sand berms between the oil and river in the event rainwater would cause oil to flow into the river or the river to flood to the oil.


For more stories, see items 1, 4, 5, 8, and 60

Postal and Shipping Sector

26. October 19, Daytona Beach News Journal – (Florida; Pennsylvania) Bomb threat leads to courthouse evacuation. A Pennsylvania prison inmate with a penchant for writing threatening letters prompted Volusia County sheriff’s deputies to evacuate the DeLand, Florida courthouse mailroom October 18 because of one of his letters, a sheriff’s spokesman said. The inmate is serving a long prison sentence in Pennsylvania, said a sheriff’s spokesman. “The letter alleged that bombs had been placed in several courthouses around the state, and DeLand was one of them,” the spokesman said. “I don’t know that he has any particular connection to DeLand.” Deputies with bomb detection dogs were sent to the courthouse at noon. A dog hit on a package but it turned out to be a delivery to the courthouse’s information technology office, which had a substance in it detected by the dog, the spokesman said. He said the mailroom and offices around it were evacuated in an “abundance of caution.”


27. October 16, Boston Herald – (Massachusetts) Mail scare empties Newton City Hall. A citizen’s gripe about a broken Newton, Massachusetts trash receptacle prompted the evacuation of Newton City Hall for more than 2 hours October 15 in a suspicious package scare. The alarm was called off after state police and a haz-mat team examined the suspicious envelope and determined it contained a harmless shard of plastic and a letter to the the mayor, the Newton fire chief said. Staff members were cleared to return to work in city hall at about noon.

Agriculture and Food Sector

28. October 19, Minneapolis Star Tribune – (Minnesota) Ammonia leak prompts evacuation in Morris. Part of Morris, Minnesota, was evacuated October 18 after anhydrous ammonia leaked from a tank attached to a farm tractor, a city official said. No one was reported injured. The director of emergency response in Morris said five or six blocks were evacuated on the north end of the city as a precaution. Stevens County sheriff’s officials said about 250 people were evacuated from their homes. At midnight, the leak had been stopped and officials were waiting for the cloud of gas to dissipate, but it was taking a long time because there was nearly no wind in the area, the emergency response director said. KSAX-TV reported residents were allowed to return to their homes about 1 a.m. October 19 after the gas dissipated. The University of Minnesota, Morris, sent an alert advising students not to go outside.

29. October 18, Food Poison Journal – (National) Wright County Egg receives warning letter; Hillandale Farms cleared to resume shipping. On October 18, the Food and Drug Administration (FDA) released its warning letter to Wright County Egg in the wake of the massive recall and outbreak that caused more than 1,600 confirmed Salmonella illnesses nationally. Hillandale Farms, which was also implicated in the outbreak and recall, was cleared to resume shipping shell eggs. According to a reporter of the Chicago Tribune’s Washington Bureau, the warning letter, dated October 15, followed weeks of negotiations between Wright County Egg and federal officials over how the company would correct a lengthy list of sanitation and biosecurity deficiencies identified by FDA inspectors in visits to the mammoth egg-laying facilities.

30. October 17, Medford Mail Tribune – (Oregon) ALF incident in Molalla does not concern ranchers here. Fallow deer ranchers in Jackson County, Oregon, said it would remain business as usual for them despite an act of sabotage against a Molalla deer ranch October 9 claimed by the Animal Liberation Front (ALF). The incident, in which a section of fencing was removed in an unsuccessful attempt to allow the deer to escape, joins a July firebombing at a former Astoria mink farm as two recent crimes claimed on behalf of the ALF, which had strong roots in southern Oregon more than a decade ago. “It never entered into my mind that someone would be interested in that,” said a woman, who has a state license to raise up to 63 fallow deer on her White City farm. The family has been raising and selling fallow deer and butchered deer meat for 10 years. They have suffered no vandalism nor worry about being targeted by animal-rights extremists, despite knowing deer-ranching licenses are public record, she said. In an anonymous e-mail posted by the North American Animal Liberation Press Office Web site labeled a “communique,” the ALF removed the fencing in Molalla so the captive deer could escape into the surrounding forest. An FBI spokeswoman in
Portland said agents are investigating.
Source:

For another story, see item 63

[Return to top]

Water Sector

31. October 19, Fulton County Expositor – (Ohio) Wauseon wastewater plant asks OEPA for variance on mercury. With the renewal of its permit more than a year ago, the Wauseon, Ohio wastewater treatment plant has requested more time from the Ohio Environmental Protection Agency (OEPA) to meet relatively new federal guidelines regarding mercury discharge. Should the variance be denied, the city could face a probable $10 million price tag to meet the requirement. The public service director told city council members the wastewater treatment plant asked for the variance to allow 5 additional years to meet lower mercury levels issued by the OEPA. In exchange, the plant pledges to lower mercury levels by identifying area sources of contamination and eradicating them. The wastewater treatment plant renewed its permit in August 2009. The federal regulation is effective November 1.
Source: http://www.expositornews.com/ful/mercury

32. October 18, KCBD 11 Lubbock – (Texas) City of New Deal fined, wastewater violations. Texas regulators have fined the City of New Deal for six wastewater violations including unauthorized discharge of wastewater from a holding pond to a playa lake. Public records said New Deal “Failed to prevent an unauthorized discharge of an unknown amount of wastewater.” The official record noted, “Specifically, a discharge of wastewater was noted from the northeast corner of the northern holding pond, running directly into a nearby playa lake bottom.” New Deal denied the charges but agreed to take corrective action and pay the fine of $6,578. The violations were discovered during a routine inspection March 16, and became public record as part of the week of October 11’s meeting agenda for the Texas Commission On Environmental Quality (TCEQ). TCEQ also claimed that New Deal failed to test equipment that prevents cross contamination between wastewater and drinking water.

33. October 18, Wicked Local Weymouth – (Massachusetts) Chlorine leak forces evacuation of Weymouth treatment plant. A chlorine leak in a new $35 million water treatment plant in Weymouth, Massachusetts, forced workers to evacuate the facility at Great Pond October 18, but did not disrupt service to customers. The leak sent high levels of the chemical into the air inside a treatment room shortly before 11 a.m. The water and sewer superintendent said a state hazardous materials team was called in. “All of our alarms and safeguards worked,” he said. “We don’t know what caused the issue. We won’t know until they get into the building.” The chlorine treatment for the water is provided in a building separate from the main facility. The
superintendent said water quality was being monitored in a former facility that had been in operation for 74 years. He explained that the safeguards for treating high levels of chlorine involve a scrubbing method that removes the chemical from the air and then replaces it with clean air.


34. *October 18, Waste & Recycling News* – (West Virginia) **EPA to stop W.Va. mine from dumping waste into streams.** The U.S. Environmental Protection Agency (EPA) has moved to stop a Logan County, West Virginia mine from dumping mining waste in streams. In a decision released October 15, the EPA regional office that oversees the implementation of the Clean Water Act in West Virginia recommended the agency prohibit the Spruce No. 1 mine from disposing mining waste and veto the mine’s permit from the Army Corps of Engineers. In March, EPA proposed to withdraw or restrict the use of a number of streams as waste dumps associated with the mountaintop removal mine and valley fills at the Spruce No. 1 site. The agency raised concerns about the scale, water quality and wildlife impacts, environmental justice implications, and cumulative impact of the Spruce mine combined with other mining activity in the area.


35. *October 17, Washington Post* – (District of Columbia) **Water main break affects activities in busy heart of District.** A large water main break near the National Mall in Washington D.C. occurred October 15. It shut down a sizable portion of Constitution Avenue NW October 16 and it closed the Smithsonian’s National Museum of Natural History. That meant postponing opening day at the museum of the “Hyperbolic Crochet Coral Reef” exhibit. Behind the disruption was the rupture of a 24-inch water main, which ripped up the roadbed near 10th Street and Constitution Avenue NW, according to a D.C. Water and Sewer Authority spokeswoman. The water main, installed in 1928, is “pretty large” for a system in which most pipes are 8 or 12 inches in diameter, she said. We had “a lot of water coming out,” she said, and road damage appeared substantial. Constitution Avenue was closed from Ninth Street to 12th, and part of 10th was also closed in that area. Traffic was still restricted October 16, and it was not clear when the roads would reopen completely. She said work might continue through October 17. She said workers expected to make a temporary street repair that would allow traffic to flow unimpeded the morning of October 18. Full repair would wait until the weekend of October 23 and 24, she said.

Source: [http://www.washingtonpost.com/wp-dyn/content/article/2010/10/16/AR2010101604143.html](http://www.washingtonpost.com/wp-dyn/content/article/2010/10/16/AR2010101604143.html)
36. **October 19, CNN** – (National) **Tylenol product recalled after complaints of moldy odor.** The maker of Benadryl and Tylenol has added another popular over-the-counter drug to its growing list of recalled products. The October 18 recall affects Tylenol 8-hour caplets 50 count, sold in the United States and Puerto Rico. The lot number is BCM155. Complaints of a musty or moldy odor led to the recall, McNeil Consumer Healthcare said. The company believes the odor is caused by the presence of trace amounts of a chemical called 2,4,6-tribromoanisole. McNeil, a subsidiary of Johnson and Johnson said the “risk of adverse medical events is remote.” Adverse event reports are consumer complaints of a serious side effect associated with the use of a medical product, according to the Food and Drug Administration. The company has issued several recalls this year of non-prescription cold and pain drugs such as Tylenol, Benadryl and Motrin — prompting a Congressional inquiry.


37. **October 18, Infosecurity** – (International) **ICO takes action on data losses against healthcare recruitment agency.** The Information Commissioner’s Office (ICO) of the United Kingdom (U.K.) has ruled that a specialist healthcare recruitment agency was in breach of the Data Protection Act after it lost personal data relating to doctors employed by the organization. The data breach at Healthcare Locums Plc, a specialist National Health Service and private health recruitment agency, took place when a hard drive was transferred between the firm’s offices in Skipton and Loughton, and subsequently sold on eBay. The ICO said the hard drive contained doctors’ security clearance and visa information. Infosecurity indicated the firm was unaware the drive had gone missing, because it had no inventory that included the unit. The drive was eventually returned to the agency and wiped in June 2010. Commenting on the case, the ICO’s enforcement group manager said the breach highlights the importance of making sure personal data is transported in a way that complies with the Data Protection Act. According to Cyber-Ark’s U.K. and Ireland director, the information was not encrypted and its transfer was not logged.


38. **October 18, WPRI 12 Providence** – (Rhode Island) **Ten hospitalized by fumes in Cranston.** Ten people were hospitalized after 40 people were exposed to hydrogen sulfide October 18 at the Eleanor Slater Hospital Complex in Cranston, Rhode Island according to the Rhode Island Department of Behavioral Health Care, Developmental Disabilities and Hospitals. Firefighters were called to the complex at about 8 a.m. after staff in the patient care unit at the Regan Building complained of a foul odor. The gas was released when foam insulation was disturbed as crews replaced roof tiles on the building. The renovations were stopped and the building was ventilated. One patient in the building was affected, but is doing fine, officials said.

Government Facilities Sector

39. October 19, Charlotte Observer – (North Carolina) Streets closed again as Charlotte bomb probe continues. Authorities have closed a portion of Mount Holly Road and several nearby streets October 19, while they continue their search of a northwest Charlotte, North Carolina, house linked to an explosion October 18 of a pen at a school. One student was injured at the school, and three firefighters were hurt in the explosion of materials at the Mount Holly Road home later in the day. Police, firefighters and the haz-mat team returned to the house about 8 a.m. October 19. Two teens who live at the house have been charged in the case. “Hazmat and other agencies continue to remove hazardous materials from the house,” a Charlotte-Mecklenburg Police Department spokeswoman said. Meanwhile, classes at Turning Point Academy resumed at 8 a.m. October 19.

40. October 19, Associated Press – (Virginia) Bullet holes found in Marine Corps museum windows. Police in Prince William County, Virginia, said bullet holes have been found in windows at the National Museum of the Marine Corps. A cleaning crew at the museum in Triangle called police when they noticed the bullet holes in windows high up in a part of the building that faces Interstate 95. Police believe the shots were fired late October 16 or early October 17, when no one was inside. Investigators used a crane to inspect the damage October 18. Because of the height of the holes, police suspect the bullets were likely fired from a rifle, but they are still working to determine what caliber of bullet was used. Several glass panels were hit, causing about $20,000 in damage. None of the museum’s artifacts — including a harrier jet hanging near the damaged windows — were hit.
Source: http://wtop.com/?sid=2084662&nid=730

41. October 19, North Carolina News Network – (North Carolina) State officials practice cyber attack response. Officials said North Carolina is well-prepared to handle a serious cyber attack. State and local computer technicians recently participated in a coordinated exercise with DHS. In the drill, technicians were able to restore state systems, which involved malware being sent from a presumably safe source.
Source: http://www.ncnn.com/content/view/6505/26/

42. October 19, CNN – (Virginia) Shots fired at the Pentagon, police say. Shots were fired at the Pentagon in Arlington, Virginia October 19, authorities said, striking a window of the building. A Pentagon police spokesman said it is not known who fired the shots. Pentagon police officers heard at least five shots around 4:50 a.m. According to another Pentagon Force Protection Agency spokesperson, two bullets hit the Pentagon on the south side of the building — one striking a window and the other hitting the building itself. This is an unoccupied part of the building that is being renovated. The spokesman said a fragment of one of the bullets is lodged in the window. The windows, which are bullet-proof, did not shatter. There was a partial lockdown of the Pentagon’s south parking lot and south entrance for about 1 hour after the shooting, and authorities
briefly shut down a portion of Interstate 395 going out of the capital — which runs along the south side of the Pentagon — to conduct a search in the investigation. 

43. October 18, Associated Press – (National) **N.C. teen pleads guilty to college bomb threats.** A North Carolina teenager has agreed to plead guilty to federal charges that he used the Internet to make fake bomb threats to Purdue University and other college campuses across the country. A judge has scheduled a hearing for October 20 in South Bend, Indiana, to consider whether to accept the plea agreement with the 17-year-old boy from Oxford. The teen admits in court documents that he made the threats in early 2009 to Purdue, Indiana University-Purdue University at Fort Wayne, UNC-Chapel Hill, Clemson University in South Carolina and Florida State University, along with FBI offices in Louisiana and Colorado. 
Source: [http://www.news-record.com/content/2010/10/18/article/nc_teens_pleads_guilty_to_college_bomb_threats](http://www.news-record.com/content/2010/10/18/article/nc_teens_pleads_guilty_to_college_bomb_threats)

44. October 17, Oklahoman – (Oklahoma) **Men wanted in connection with Langston shooting turn themselves in.** Two men wanted in connection with a shooting at Langston University in Langston, Oklahoma October 14 turned themselves into the Logan County Sheriff’s Office October 16, an Oklahoma State Bureau of Investigation spokeswoman said. A 22-year-old turned himself in along with his 19-year-old brother. The 19-year-old is a Langston student and was wanted as a “person of interest” by authorities. The 22-year-old is being held on a complaint of assault and battery with a deadly weapon. The 19-year-old suspect was released after being questioned, Logan County authorities said. Police were seeking both men in connection with a shooting at the Scholars’ Inn Complex dormitory. Shots were fired after a fight broke out and a bystander was wounded in the leg. 

45. October 16, Salisbury Daily Times – (Virginia) **Accomack laptop stolen in Las Vegas; residents’ information was on computer.** An Accomack, Virginia, employee had a county-owned laptop computer stolen while on a personal vacation to Las Vegas, and with it the names and Social Security numbers of roughly 35,000 county residents. In some cases, actual addresses of county residents also may have been included in computer files. “It was taken there without permission,” a county administrator said of the computer. The worker remains employed. The matter was discussed during a closed meeting of the Accomack Board of Supervisors October 13. The incident happened October 7. The county waited 7 days before issuing a prepared release about the event to the media. 
Source: [http://www.delmarvanow.com/article/20101016/ESN01/10160303](http://www.delmarvanow.com/article/20101016/ESN01/10160303)

For more stories, see items 26, 27, and 61
Emergency Services Sector

46. **October 18, Federal Bureau of Investigation** – (National) **FBI releases 2009 statistics on law enforcement officers killed and assaulted.** According to information released October 18 by the FBI, 48 law enforcement officers were feloniously killed in the line of duty last year; 47 officers died in accidents while performing their duties; and 57,268 officers were assaulted in the line of duty. The 2009 edition of Law Enforcement Officers Killed and Assaulted provides comprehensive tabular data about these incidents and brief narratives describing the fatal attacks. The number of officers feloniously killed in 2009 increased by seven compared with the 2008 figure (41 officers).


47. **October 16, Stockton Record** – (California) **Explosive material found in container.** Explosives and hazardous-materials technicians were called to the Stockton, California Police Department October 15 to handle a dangerous substance a man had turned in after finding it near the airport. The police department said the substance was in a container a man had found on a Highway 99 frontage road. On the exterior of the container was a warning that its contents would explode if exposed to water. Police said the man opened the container and saw that it was full, then he noticed it was warming. The man took the container to the police department, where members of the fire department’s hazardous-materials team and the police department’s bomb squad inspected and removed the container. It was to be destroyed at a remote location. A firefighter confirmed the substance was calcium carbide, which is potentially explosive and dangerous.


For another story, see item 6

Information Technology Sector

48. **October 19, Help Net Security** – (International) **Kaspersky download site hacked, redirecting users to fake AV.** For three and a half hours October 17, the Kaspersky’s USA download site provided download links that redirected users to a malicious Web page where windows telling them their computer was infected were popping up and they were encouraged to buy a fake AV solution. The fact was noted by various users on three separate forums. Among those was Kaspersky’s own forum, and judging by the comment left by someone with the username “Micha” — who appears to be an employee of the security firm stationed in Japan — the problem was solved. According to ITPro, the incident was first denied, then confirmed by Kaspersky. They said they
took the server offline as soon as they found out about the breach, that the compromise was caused by a vulnerability in a third party application for Web site administration, and that customer details contained on company servers were not compromised.
Source: http://www.net-security.org/malware_news.php?id=1499

49. October 19, V3.co.uk – (International) **RealPlayer receives critical security update.** Real Networks has issued a security update for RealPlayer, addressing flaws in versions 1.1.4 and earlier of the application. The company said RealPlayer 1.1.5 and later for Windows is not believed to be vulnerable to attack, neither is the Mac RealPlayer 12.0.0.144 and later release, or the latest RealPlayer Enterprise and RealPlayer for 11.0.2.1744 for Linux release. The update patches seven vulnerabilities ranging from buffer overflow and injection flaws to issues that could allow an attacker to remotely execute code on a targeted system. Real Networks advised administrators to upgrade RealPlayer installations to the most current stable version. No active exploitations of the flaw have been reported in the wild.

50. October 19, IDG News Service – (International) **Tests show consumer antivirus programs falling behind.** The latest tests of consumer of antivirus software released October 19 show the products are declining in performance as the number of malicious software programs increases. NSS Labs tested 11 consumer security suites and found that the products are less effective than 1 year ago as far as blocking the download and execution of malicious software programs. The company also tested if those programs detected and blocked malicious Web sites. The download and execution blocking rate for the top performing product, Trend Micro’s Titanium Maximum Security, fell from 96.4 percent to 90.1 percent from the third quarter of 2009 to the same period this year. All of the rates were lower except for two products: McAfee’s Internet Security and F-Secure’s Internet Security 2010, which upped their detection and blocking rates by 3.6 percent and .4 percent respectively. The biggest drop occurred for AVG’s Internet Security 9, which fell 18.5 percent, and Kaspersky’s Internet Security 2011, which fell 16.5 percent. The tested security products have not necessarily fallen in quality, but rather the threats are evolving at a rapid pace, said the president of NSS Labs.
Source: http://www.computerworld.com/s/article/9191718/Tests_show_consumer_antivirus_programs_falling_behind?taxonomyId=17&pageNumber=1

51. October 18, Softpedia – (International) **Scammers impersonate Adobe employees to sell fake Reader upgrade.** Security researchers warn of scam e-mails purporting to come from Adobe employees, who advise users to buy a fake upgrade for Adobe Reader. The e-mails bear a subject of “Action Required : Active Your New Adobe PDF Reader” and come from an “Adobe Support” address. A link is included and recipients are advised to open it in order to download the upgrade. The domain has been registered through a Russian registrar and redirects to a professionally looking Web site that advertises a program called PDF Pro 2010, which asks for registration and money. It appears this campaign has been running for weeks. There are reports about it on Adobe’s forum dating back to September 27, but an ESET blogger wrote about one
sent October 17. “Adobe doesn’t send out unsolicited stuff like this, even when it concerns security patches and the like. If you’re not subscribed to one of their lists, that’s red flag number one,” the researcher warned.

52. October 18, Softpedia – (International) Drive-by kit generates fake Twitter home pages. Security researchers warn of the increasing popularity of a drive-by kit, which allows attackers to create fake copies of the Twitter home page and use them to distribute malware. The real Twitter main page currently promotes a video about the site’s new design. The malware toolkit, which was discovered by researchers from Sunbelt Software (now part of GFI), allows attackers to edit the part of the page where the video is located and change it with whatever their wish. In some live examples, the malware pushers used a video thumbnail depicting a scantily-dressed woman. Clicking the image prompted the execution of a malicious Java applet. The applet tried to exploit a vulnerability in older versions of Java to install malware on the victim’s computer. The attackers upload these pages to free Web hosting accounts and then target users on Twitter via shortened URLs included in spam messages. They hope that when users open them, they will click on the intriguing picture without verifying the URL in the address bar.

53. October 18, Computerworld – (International) ‘Unprecedented wave’ of Java exploits hits users, says Microsoft. Microsoft said October 18 that an “unprecedented wave” of attacks are exploiting vulnerabilities in Oracle’s Java software. According to a manager at Microsoft’s Malware Protection Center, attempts to exploit Java bugs have skyrocketed in the past 9 months, climbing from less than half a million in the first quarter of 2010 to more than 6 million in the third quarter. She noted that the bulk of the attacks in the quarter that ended September 30 were exploiting just three Java vulnerabilities, all of which had been patched months or even years ago. “IDS/IPS vendors ... have challenges with parsing Java code,” she alleged. “Think about incorporating a Java interpreter into an IPS engine. ... [T]he performance impact on a network IPS could be crippling. [So] the people that we expect to notice increases in exploitation might have a hard time seeing this. Call it Java-blindness.”

54. October 18, Softpedia – (International) Exploit toolkit infects one in ten users via outdated Java. While analyzing a live drive-by download attack, researchers from M86 Security found that 1 in 10 users visiting the compromised pages were being infected because they had an outdated version of Java installed. The exploit toolkits used in drive-by download attacks target known arbitrary code execution vulnerabilities in older versions of popular applications, such as Adobe Flash Player, Adobe Reader, Java, or even the browsers themselves. The exploit pack used in this attack is called
Zombie Infection Kit and is neither the most popular, nor the most sophisticated. The toolkit exploits two Java vulnerabilities, four Adobe Reader ones (via a single PDF document), the Windows XP Help Center (HCP) flaw discovered earlier this year, an old one in IE6, and two in Adobe Flash Player. According to its control panel, the two Java vulnerabilities accounted for a bit over 60 percent of all successful infections. This is consistent with numbers seen in other exploit toolkits. Given that the overall infection rate achieved by this installation of Zombie Infection Kit was 15.39 percent, it can be concluded that 9 percent of users, who landed on the infected pages, were compromised through Java exploits.


55. *October 18, Computerworld* – (International) **Microsoft’s anti-Zeus tool cleans quarter-million PCs.** Microsoft said its free malware cleaning tool had scrubbed the money-stealing Zeus bot from nearly 275,000 Windows computers in under 1 week. On October 12, Microsoft added Zeus/Zbot detection to its Malicious Software Removal Tool (MSRT), a free malware-removal program that the company updates each month and distributes alongside its Patch Tuesday security fixes. MSRT does not prevent attack code from getting on a Windows machines. Instead, it detects infected machines and then deletes the malware. Since October 12, MSRT has removed 281,491 copies of Zeus from 274,873 PCs, Microsoft announced in a post to a company blog October 17. Those numbers put the Zeus bot into the top spot on MSRT’s hit list. Zeus infections accounted for 20.4 percent of all machine cleanings since October 12, said the director of Microsoft’s Malware Protection Center.

Source: [http://www.computerworld.com/s/article/9191599/Microsoft_s_anti_Zeus_tool_cleans_quarter_million_PCs](http://www.computerworld.com/s/article/9191599/Microsoft_s_anti_Zeus_tool_cleans_quarter_million_PCs)

56. *October 18, Commtouch* – (International) **Report: Malware delivery technique focus on HTML attachments.** Use of malicious HTML e-mail attachments increased significantly in the third quarter, Commtouch reported October 18 in its third quarter Internet Threats Trend Report. The HTML attachments displayed phishing pages on the user’s local computer or redirected users to sites hosting malware or spam products. The Q3 report examines the methodology within blended attacks, such as the “Here You Have” worm, which spread widely in September using Outlook contact lists from infected PCs. Both Here You Have and numerous fake LinkedIn invitations relied on a combination of social engineering and masked hyperlinks to lead users to Web sites with malware scripts. During Q3, the PayPal, LinkedIn, Craig’s List, Bell Canada, NewEgg, and Amazon brands were used by spammers to inspire action by consumers. The report also features the unusual bedfellows of a pharmacy spam campaign based on solidarity with several European politicians and celebrities. The increased use of HTML attachments shows how prominent the multi-stage attack vector has become, said a Commtouch vice president.

Communications Sector

57. October 19, TMCnet – (Pennsylvania) **AT&T helps Philadelphia businesses prepare for potential disasters.** AT&T announced the results of a new study conducted on how Pennsylvania businesses prepare to ensure business continuity and save their businesses from unforeseen natural or manmade disasters. According to the 2010 Business Continuity Study, businesses are proactively preparing to face these challenges and protect their operations and maintain communications in times of disruption. Many businesses in Philadelphia and Pittsburgh are preparing for potential disasters and investing in additional technology, according to AT&T. About 81 percent of AT&T survey participants in these metro areas said they have business continuity plans, and two-thirds of executives indicated their companies are investing in new technologies in 2010. The survey found business continuity is essential as these businesses allowed most employees to work from home or remote locations, and use communications facilities like automated calling systems to reach employees by telephone or cell phone outside of work. A majority (78 percent) of survey participants were concerned about the increasing use of mobile networks and devices and their impact on security threats. AT&T also announced it is working with officials and business leaders to conduct a full-scale disaster recovery simulation — a Network Disaster Recovery or “NDR” exercise — in King of Prussia, Pennsylvania, October 19 to 20. The company conducts NDR several times a year as part of its strategies to test, refine and strengthen the business continuity and disaster recovery services to minimize network downtime. Source: [http://mpls.tmcnet.com/topics/business-continuity/articles/109843-att-helps-philadelphia-businesses-prepare-potential-disasters.htm](http://mpls.tmcnet.com/topics/business-continuity/articles/109843-att-helps-philadelphia-businesses-prepare-potential-disasters.htm)

58. October 18, Network World – (International) **Gap between IPv4 depletion, IPv6 adoption widens.** With the Internet’s largest-ever upgrade looming, network operators are using up address space based on the current standard — known as IPv4 — much faster than they are adopting IPv6, the next-generation standard. The Internet’s regional registries, which dole out blocks of IPv4 and IPv6 address space to carriers, will announce October 18 that less than 5 percent of the world’s IPv4 address space remains unallocated. IPv4 is the Internet’s main communications protocol. It uses 32-bit addresses and can support 4.3 billion devices connected directly to the Internet. IPv6, on the other hand, uses 128-bit addresses and supports a virtually unlimited number of devices — 2 to the 128th power. Overall, more than 200 million IPv4 addresses have been allocated from the so-called free pool of available IPv4 addresses since January 2010, with most of the addresses being snapped up by Asian carriers. Allocation of the
remaining blocks of IPv4 addresses is “imminent,” according to the chairman of the Number Resource Organization (NRO), which represents the five regional registries. “It is critical that all Internet stakeholders take definitive action now to ensure the timely adoption of IPv6,” he said in a statement. The NRO warned the last IPv4 address blocks will be allocated from the free pool to the regional registries in early 2011. Experts predict the registries will hand out these addresses to network operators by the end of 2011, leading to full-fledged depletion of IPv4 addresses. Once IPv4 addresses are depleted, ISPs must give their new customers IPv6 addresses or use carrier-grade network address translation to share a single IPv4 address among multiple customers.


59. October 18, Wired.com – (International) Outage forces Peek to upgrade older devices. An unexpected glitch felled older models of Peek, the email-only device, and has forced the company to offer a free replacement upgrade to users. The outage, which started October 14, bricked Peek models — the Pronto and Classic. “Unfortunately, one of the connectivity providers we were using went down for good. That’s the bad news,” wrote the Peek CEO on the company blog. But Peek said its customers will gain because it is replacing existing bricked out devices with its latest model Peek 9. Peek 9 offers push e-mail, access to Facebook, Twitter, weather and maps for $69 and a monthly service plan of $20. However, the device does not require long term contracts with the wireless carrier.


60. October 18, McClatchy-Tribune Information Services – (International) Airline may let fliers use cellphones. Early next year, Singapore Airlines will begin to install technology in dozens of planes to let passengers surf the Internet and send e-mail from 35,000 feet in the air, the airline has announced. The circuitry it plans to install in at least 40 long-haul jets by 2013 would also allow passengers to make airborne cellphone calls. But Singapore Airlines remains undecided whether to allow cellphone calls. “As we get closer to the launch date, we will decide whether voice calling in the cabin will be activated,” said a Singapore Airlines spokesman. One consideration, he said, is whether passengers want to make calls in flight. The hesitation is not surprising. Although a handful of airlines in the Middle East and Europe allow cellphone calls, U.S. regulators prohibit the practice, saying the calls may interfere with navigation systems. But the problem may not be the technology. After all, Emirates airline has allowed cellphone calls since 2008. Cathay Pacific announced plans in July to let passengers use their cellphones in the plane by 2012. A bigger issue may be that passengers and airline crews hate the idea of turning a crowded, airborne cabin into a flying phone booth. The Federal Communications Commission considered lifting the ban in 2004, but it stopped looking into the idea after being inundated with letters, e-mails and calls in opposition. The pending reauthorization bill for the Federal Aviation Administration includes a proposal to ban all cellphone calls on U.S. commercial planes — except by airline crews and law enforcement. In a 2005 survey by the
National Consumers League and the Association of Flight Attendants, 63 percent of airline passengers said they opposed cellphone use on planes.
Source: http://voices.washingtonpost.com/dr-gridlock/2010/10/early_next_year_singapore_airl.html

Commercial Facilities Sector

61. October 18, CNN – (New York) 4 found guilty in NYC synagogue bomb plot case. Four men were found guilty October 18 of planning to bomb a synagogue and Jewish center in New York and plotting to shoot military planes with missiles. The four — all from Newburgh, New York — were charged with conspiring to blow up a synagogue and Jewish community center in the Riverdale section of Bronx, New York. They were also accused of planning to fire surface-to-air-missiles at the New York Air National Guard Base at Stewart Airport in Newburgh. The men, who could now face life in prison, were arrested in 2009 after planting what they thought were live explosives. They had unknowingly been working with an FBI informant, who supplied them with what they were told was military-grade explosive material and a Stinger surface-to-air guided missile. “Homegrown terrorism is a serious threat, and today’s convictions affirm our commitment to do everything we can to protect against it,” the U.S. attorney in Manhattan said in a statement soon after the verdict. The four men were found guilty on seven of the eights counts against them, including conspiracy and attempts to use and acquire weapons of mass destruction and anti-aircraft missiles.

62. October 18, KOSA 7 Odessa – (International) ‘All of Mexico’ travel warning could affect Texas tourism. A strong warning from the Texas Department of Homeland Security is advising people not to visit Mexico right now and that includes all cities. Concerns over travel to Mexico have been growing for years as violence in border cities claims more and more lives. After an American man turned up missing in September 2010 in a fatal shooting that some claim involved Mexican pirates on Lake Falcon, fears may have reached a fever pitch. On October 14, the Texas Homeland Security director said Americans should avoid Mexico altogether. He made the statement in testimony before a Senate committee, saying nobody should be going into Mexico, including tourist cities like Cancun and Cozumel. Wide scale travel warnings can affect tourism in the United States as well, according to the Marfa Chamber of Commerce. “It does have an effect. A person from California who hears that has no idea that we’re an hour away from the border. It may impact our tourism,” said a chamber spokesperson. A U.S. Department of State travel warning singles out various “no-visit zones” in Mexico, but also points out that millions of Americans travel to the country safely and without incident every year.

63. October 18, WAPT 16 Jackson – (Mississippi) Official: Crystal Springs fire started in restaurant. A massive fire that swept through downtown Crystal Springs,
Mississippi, started in a downtown restaurant and spread to other buildings, a fire 
official said. Fire officials said it started just before 1 a.m. at a business on Jackson 
Street. The October 18 fire spread and destroyed at least four buildings, including a 
framing shop, a restaurant, an alteration business, and the city’s Masonic lodge. There 
was an apartment on top of one the buildings, but firefighters said everyone got out 
safely and there were no injuries. 
Source: http://www.wapt.com/r/25426093/detail.html

National Monuments and Icons Sector

64. October 19, Alexandria Town Talk – (Louisiana) Kisatchie wildfire rages in 
Natchitoches Parish. Local and national firefighters October 18 continued to fight a 
Kisatchie National Forest wildfire in Louisiana that started October 14. The blaze 
began in southern Natchitoches Parish and had grown to more than 1,300 acres by 
October 18. The U.S. Forest Service reported more than 200 personnel were working 
on the fire, which was 30 percent contained. The Kisatchie Hills Wilderness Area 
remains closed. 
Source: http://www.thetowntalk.com/article/20101019/NEWS01/10190318

65. October 17, North Jersey Record – (New Jersey) Vandals hit veterans monuments in 
Paterson again. Veterans in Paterson, New Jersey discovered another wrecked 
monument October 17 at Hayden Heights Park. “Enough is enough,” said a Vietnam 
veteran and president of the Paterson Veterans Council who, for the second time in a 
week, surveyed the damage at the park, where monuments and military vehicles are on 
display. This time, a 4-foot tall Disabled American Veterans “Argonne Chapter 18” 
monument was knocked over, he said. The Argonne monument is next to an American 
Legion granite monument that was pulverized into four pieces October 11. 
son_again.html

Dams Sector

66. October 19, Ghana News – (International) Akosombo spillage: Residents asked to 
evacuate immediately. Communities along the banks of the Volta Lake in Ghana are 
being asked to evacuate to higher grounds as mangers of the Akosombo Dam prepare 
to open the spillways of the dam to save it from collapse. Officials of the Volta River 
Authority (VRA) said that for the first time in 20 years, the dam has exceeded its 
maximum capacity. Some communities along the lake in Northern, Ashanti, Volta and 
Greater Accra Regions are most likely to be affected. A public relations officer of VRA 
said the water level is alarming and increasing day by day. She said VRA would be 
forced to spill the water if the situation does not improve by October 21. “What has
exacerbated the situation is the direct rainfall into the lake, because of that, we can foresee the possibility of the communities along the river to be flooded both downstream and upstream. Right now we are at 274.80 feet.”


67. **October 19, Monroe News-Star** – (Louisiana) **Corps finds few faults with levees.** The U.S. Army Corps of Engineers October 18 presented the Tensas Basin Levee District Board in Louisiana preliminary inspection findings that will determine whether the Ouachita River levee system will receive certification. The findings reported only one major issue on the east bank of the Monroe side and that is a cave-in on the Ouachita River just south of the Buckhorn Bend area. The report only cited minor deficiencies in the West Monroe and Bawcomville area, most of which are in the process of being corrected or are scheduled to be repaired. Once the Corps finishes its report, it will be forwarded to the Federal Emergency Management Agency (FEMA). FEMA will make the final determination on whether or not the levees are accredited. If the levee system is not accredited, homeowners could see their flood insurance premiums skyrocket based on a flood map.

Source: http://www.thenewsstar.com/article/20101019/NEWS01/10190302

68. **October 19, Milford Daily News** – (Massachusetts) **Dam repairs to begin this week in Hopedale.** Repair work on the Freedom Street dam in Hopedale, Massachusetts is scheduled to begin October 21 or 22, and could be finished by the first week of November, the town coordinator told selectmen October 18. The town hired Franklin-based MAS Building & Bridge Inc. to repair the dam, while Pare Corp., a Foxborough engineering company, will oversee the project, which has been estimated to cost from $75,000 to $95,000. Damage to and deterioration of the dam led to historically low water levels in Hopedale Pond this summer. The repair work includes building a wall 1 foot in front of the dam’s apron using metal sheet piping, and plugging the space between the apron and the wall with fill through which water cannot flow.

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 cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at 703-872-2267

Subscribe to the Distribution List: Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.

Removal from Distribution List: Send mail to support@govdelivery.com.

Contact DHS
To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.
To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer
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.