Daily Highlights

- Federal Computer Week reports a year after a laptop computer was stolen from the home of a Veterans Affairs Department employee, federal systems are still vulnerable, according to a study released Monday, June 4. (See item 10)

- The Associated Press reports Abdel Nur, a Guyanese suspect in an alleged plot to attack New York's John F. Kennedy International Airport, surrendered to police Tuesday, June 5, in Trinidad. (See item 40)

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument & Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

1. June 05, Reuters — Advocates: Wind to make 20 percent of U.S. power by 2030. The U.S. wind power industry will see half a trillion dollars of investment by 2030 to take the renewable source up to 20 percent of U.S. electricity generation, an industry conference heard on Monday, June 4. This would be a lofty rise from wind's use for less than one percent of U.S. power today, but many advocates at the American Wind Energy Association's (AWEA) annual conference this week were bullish as the United States develops green energy alternatives. Many aim to catch money blowing in the air that Ric O'Connell of engineering and consulting firm Black & Veatch says will total $500 billion in wind energy development in the next 25
years. U.S. President George W. Bush said last year that 20 percent of the nation's power needs can be met by wind. Since Bush's remarks, the AWEA and other wind energy advocates have worked to map out how to get to that target. 


2. June 05, Cape Cod Online (MA) — NRC doubts terror risk from spent nuclear fuel. The Nuclear Regulatory Commission (NRC) says in a court−ordered report it continues to believe that storage sites for spent fuel at the nation's nuclear power plants are not at risk of terrorist attack. While the report doesn't specifically mention the Pilgrim Nuclear Power Station in Plymouth, MA, it could tip the regulatory agency's hand about an ongoing safety review of the plant. The Diablo Canyon report, filed last week, was ordered by the Ninth Circuit Court in California. In it, NRC officials determined that in the event of a terrorist attack there would be no "significant effect on the human environment," NRC spokesperson Neil Sheehan said. Massachusetts Attorney General Martha Coakley and Mary Lambert of Pilgrim Watch want NRC officials to consider terror threats — especially in light of the 9/11 attacks — in deciding whether to renew Entergy's license to operate Pilgrim for 20 additional years. But the two plants are different because officials at Diablo Canyon are requesting a dry cask storage facility, while Pilgrim stores its spent fuel in a pool on site. Coakley has also asked the NRC to consider other risks, such as a natural disaster. 


3. June 04, LiveScience — Energy recycled by using sound to convert heat into electricity. Physicists have developed a way to turn heat into sound and then electricity, suggesting a new way to effectively recycle waste energy. Orest Symko of the University of Utah has developed recycling devices which are cylinder−shaped “resonators” that fit in the palm of a hand. Each cylinder contains a stack of material with a large surface area placed between cold and hot heat exchangers. When heat is applied, the heat builds to a particular threshold where hot, moving air produces sound at a single frequency — like air blown into a flute. The sound waves then squeeze what is called a piezoelectric device. The pressure created produces an electric voltage. Symko plans to test the devices within a year at a military radar facility and the University of Utah’s hot−water−generating plant. The U.S. Army funded the study in hopes the technology can be used to create a portable source of energy. 

Source: http://www.msnbc.msn.com/id/19034341/

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. June 05, WFTV Orlando — McDonald's evacuated after workers create toxic fumes. A McDonald's restaurant in Brevard County, FL, was evacuated Monday night, June 4, after several workers were overcome by toxic fumes. Firefighters and Hazmat crews were called to the restaurant on US−1 in Port St. John after the workers started having trouble breathing. Firefighters quickly found the source of the fumes. "We poured kitty litter back behind the fry mat and, apparently, you're not supposed to do that because it makes toxic fumes when it gets
heated up. It gets toxic and a lot of people were going home sick," said Matt Hoff, an employee. The workers were using the kitty litter to clean up grease. One person went to the hospital. Four others got sick, but refused medical treatment.

5. **June 05, White Mountain Independent (AZ) — Gasoline spill forces traffic detour.** A gas spill south of the Woodruff turnoff on state Route 77 has closed the road between the Navajo County Complex and Snowflake, AZ. Sheriff Gary Butler said traffic was diverted to state Route 377 at the county complex. Sheriff Gary Butler said it was his understanding that a motor home was followed by a gasoline tanker, which was, in turn, followed by a truck loaded with Conix boxes. When the motor home stopped quickly, it caused a chain reaction and the truck at the back took a gouge out the side of the tanker, which was carrying 16,000 gallons of gasoline.

6. **June 04, News 10 Now (NY) — Chemical leak forces evacuation of water filtration plant.** A chemical leak forced an evacuation at the Binghamton, NY, Water Filtration Plant. Police said a truckload of a water purification chemical was accidentally dumped into the wrong tank. The chemical then mixed with chlorine, releasing chlorine gas into the air. The fire department and hazmat crew contained most of the gas inside the building. Everyone was evacuated from the plant, as well as a few people living across the street from the facility.
Source: http://www.news10now.com/content/all_news/?ArID=107744&SecID=83

**Defense Industrial Base Sector**

7. **June 05, Los Angeles Times — Three plead guilty in military data conspiracy.** The brother, sister-in-law and nephew of a Chinese-American engineer who was convicted last month of conspiring to pass information about U.S. naval technology to China pleaded guilty Monday, June 4, to charges stemming from the same case. Tai Mak, 57, pleaded guilty to violating export-control laws. His wife, Fuk Heung Li, 49, pleaded guilty to aiding and abetting the violation of those laws. Their son, Billy Yui Mak, 26, pleaded guilty Friday to the same charge as his mother. Chi Mak, a naturalized U.S. citizen, worked at Anaheim, CA–based Power Paragon Inc., a firm with many Navy contracts. The FBI kept him under surveillance for 18 months using cameras, wiretaps and microphones hidden in his car and work cubicle. He was accused of transferring unclassified data onto three encrypted disks, which prosecutors described as sensitive and embargoed from China.

**Banking and Finance Sector**

8.
June 05, New Zealand Herald — **Kiwibank hit by another round of scammers.** Kiwibank has been hit for the second time in two weeks by Internet scammers. The latest phishing scam happened Monday, June 4, when thousands of New Zealanders were sent e-mails asking them to register for a Kiwibank "Customer Appreciation Day" this Thursday. The e-mails came from a fake sender "Kiwibank [mailto:customers@kiwibank.co.nz]" and directed the bank's customers to a bogus site where they were asked to register their account details and pin numbers. The message also invited customers to drop in at any Kiwibank branch on Thursday for coffee and cake, saying the bank wanted to thank them for their loyalty. Claims that customers could win $30,000 and a Mercedes-Benz SLK by registering their account details for the Customer Appreciation Day were also untrue. Bank spokesperson Bruce Thompson said the bank did not know the source of the scam. However, a similar scam late last month had come from the United States and it was likely the same scammers had struck again. On both occasions, the bank was able to shut down the fake sites within hours with the help of Internet providers overseas.

Source: [http://www.nzherald.co.nz/section/1/story.cfm?c_id=1&objectid=10443635](http://www.nzherald.co.nz/section/1/story.cfm?c_id=1&objectid=10443635)

9. June 04, North Jersey.com — **North Jersey bank data stolen.** Banks in northern New Jersey have had their share of data security problems. In 2005, security breaches at northern New Jersey branches of Wachovia, Bank of America, PNC Bank and Commerce Bank came to light when Hackensack detectives were investigating a check-fraud case. They learned instead that customer data were being stolen by rogue bank workers, to be sold to collection agencies. Just last month, another bank data-security breach, at Fair Lawn-based Columbia Bank, came to light. The lender sent letters to all of its online banking customers to let them know there was an "intrusion" into its system, and that their names and Social Security numbers were accessed. Providing data security advice to bankers is a growing business at the accounting and advisory firm Grant Thornton. "A successful plan must not only consider the technical aspects of information security, but the financial institution's people processes, policies, procedures and physical environment," Matthew Thompson, a Grant Thornton senior manager, wrote in an e-mail. Bank data-security professionals often talk about "C–I–A" objectives. CIA in this sense stands for confidentiality, integrity and availability, the guiding principles in data security.

Source: [http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFIZUVFeXk4NDImZmdlZWw3Zjd2cWVlRUV5eTcxNDQ2OTQmeXJpcnk3ZjcxN2Y3dnFIZUVFeXky](http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFIZUVFeXk4NDImZmdlZWw3Zjd2cWVlRUV5eTcxNDQ2OTQmeXJpcnk3ZjcxN2Y3dnFIZUVFeXky)

10. June 04, Federal Computer Week — **Federal data still vulnerable a year after VA laptop theft.** A year after a laptop computer was stolen from the home of a Veterans Affairs Department (VA) employee, federal systems are still vulnerable, according to a study released Monday, June 4. A Telework Exchange survey of 258 federal employees found that 13 percent don’t have encryption on their newly issued laptop PCs, compared with 11 percent in June 2006. The survey also revealed that although those who telework and those who don’t have about the same awareness of their agencies’ security policies — 97 percent compared to 96 percent, respectively — teleworkers are more likely to have received training on data security, have encryption on their laptops and have antivirus protection on their work PCs. According to researchers, non-teleworkers are the Achilles heel of federal data security. Fifty-four percent of them said they carry files home and 41 percent reported that they log onto their agency’s network from home. These unofficial teleworkers are removing data from the office and
working remotely in unauthorized locations, and therefore constitute a major risk in data security, researchers concluded. 

**Transportation and Border Security Sector**

11. *June 05, Associated Press* — **Air travel tips from Arkansas official: No guns in carry–on.** A common oversight the Transportation Security Administration sees at airports in Arkansas is small firearms. Usually, the person inadvertently carrying a gun has a concealed weapons permit, said Federal Security Director Jerry Henderson, and the matter is handled administratively, although there could be civil fines up to $10,000 and criminal laws might apply. Regulations do permit transporting firearms in checked baggage, but not in carry–on, with limited exceptions for law enforcement officers. Checked firearms must be unloaded, in a locked hard–sided container, and must be declared at the check–in. "The big concern we have is that we end up with a lot of firearms coming through our checkpoint," Henderson said. 

12. *June 05, Newsday (NY)* — **Airport protection system on the way.** A virtual fence with state–of–the–art heat, movement, and video sensors to detect and deter terrorists is being installed around John F. Kennedy International Airport and three other New York–area airports modeled on systems at Israel's Ben–Gurion and Baghdad's airports. The 57–mile system, which is expected to be in operation early next year, is supposed to tip off police to a plot like the one unveiled Saturday, June 2, that aimed to blow up a fuel line inside Kennedy airport. The $138–million design, which is being built at Kennedy, LaGuardia, Newark, and Teterboro, NJ, airports, is the first of its kind to be installed in the U.S., according to Marc La Vorgna of the Port Authority. It was in the works before the alleged Kennedy Airport plot was known. It is composed of strategically placed sensors, including radar, video motion detectors, thermal imagers and closed–circuit television, which would send round–the–clock information to a central Port Authority Police station, as well as to a command post at each airport. Homeland security expert James Jay Carafano called the new system a valuable addition to a layered security approach. 
Source: [http://www.newsday.com/search/ny–usair055243304jun05,0,49127 00.story](http://www.newsday.com/search/ny–usair055243304jun05,0,49127 00.story)

13. *June 05, Local10 (FL)* — **Gun found in suitcase st MIA.** A man is facing charges after allegedly trying to bring a loaded gun onto a plane at Miami International Airport (MIA). Police said Henry Clay Woods Jr. checked two pieces of luggage while trying to board a flight from Miami to San Pedro Sula, Honduras Friday, June 1. During a route X–ray, Transportation Security Administration officials noticed something suspicious in Woods' bag, according to police. Investigators said it was a loaded Smith and Wesson revolver hidden in a box of laundry detergent. The revolver and a box of .38 ammunition, which was also located inside the suitcase, had been wrapped in aluminum foil. 

14. *June 05, Department of Transportation* — **More U.S. crews for LNG tankers.** U.S. seafarers
will be able to get more jobs in one of the fastest growing segments of the international shipping trade, as a result of an agreement signed on Tuesday, June 5, by Maritime Administrator Sean T. Connaughton. The agreement implements a universal set of training standards developed by an industry working group facilitated by the Maritime Administration, and will expand opportunities for U.S. mariners on Liquefied Natural Gas (LNG) tankers. “The worldwide demand for qualified mariners, plus the growth in the LNG industry, provides a unique growth opportunity for U.S. merchant mariners and the U.S. maritime industry,” said Connaughton. He also noted that the LNG fleet is expanding rapidly: in January 2006 there were 194 LNG tankers worldwide, and the expected number at the end of 2007 is 373. There have been few opportunities for U.S. mariners to sail on those ships. While several maritime academies offer training for LNG, their training was not standardized, and standardization of training and credentials in an internationally accepted set of competencies will make it easier for U.S. mariners to be employed on the worldwide LNG fleet.

The training standards and agreement may be seen on the Maritime Administration’s Website: http://www.marad.dot.gov

Source: http://www.dot.gov/affairs/marad0707.htm

15. June 05, Mid−Hudson News — TSA considering Stewart need for more screeners, updated equipment. Federal Transportation Security Administration (TSA) officials and management of Stewart Airport at Newburgh, NY, have begun discussions about the need for additional security screeners and updated baggage screening equipment. Because of the addition of AirTran and JetBlue, and more recently, flights by Delta Air Lines, passenger traffic at Stewart has tripled in recent months, resulting in long lines at the check in point. Stewart officials and public officials have been saying that they need additional TSA screeners and more up−to−date screening equipment for luggage. Newer machines to detect trace amounts of explosives would screen more bags at a more rapid rate.

Source: http://www.midhudsonnews.com/News/SWF_TSA−05Jun07.htm

16. June 02, Associated Press — Terror threat first for pipeline firm. A foiled plot on Saturday, June 2, to blow up a jet fuel pipeline under John F. Kennedy International Airport drew attention to what counterterrorism experts have warned could be a key target. It was the first threat against Buckeye Pipe Line Co., which operates petroleum conduits in 18 states, the company said. Its pumping facility in Linden, NJ, has 45 storage tanks pumps turbine fuel, gasoline, diesel, and other fuel and heating oils through two 12−inch pipes to customers in New York City, including Kennedy and LaGuardia airports. The network totals 35 miles within the city alone. Buckeye works closely with federal Department of Homeland Security officials, the FBI, New York fire and police, and the Port Authority of New York and New Jersey, which operates the area's three major airports. An explosion's force would depend on the amount of fuel under pressure and likely would be "restricted" and not travel up and down the line, said Richard Kuprewicz, a pipeline expert.

Source: http://hosted.ap.org/dynamic/stories/T/TERRORISM_PLOT_PIPELI NE?SITE=WUSA&SECTION=HOME&TEMPLATE=DEFAULT

[Return to top]
17. *June 04, Information Week* — **U.S. Postal Service cracks down on cyberscams.** In conjunction with other law enforcement agencies, the U.S. Postal Service's Postal Inspection Service is a crack team of globe-trotting agents who break up international Web fraud syndicates and bring cybercriminals to justice. Greg Crabb, U.S. postal inspector program manager for the organization's international affairs group, explained that the Postal Inspection Service gets involved in information security crimes when those crimes involve use of the U.S. Postal Service to commit fraud. Crabb outlined several different types of criminal schemes he's investigated as a member of the Postal Inspection Service, which was formed in 1909.

Source: [http://www.informationweek.com/security/showArticle.jhtml;jsessionid=YQWO1VIWT5YC4QNSDLPCKH0CJUNN2JVN?articleID=199900962](http://www.informationweek.com/security/showArticle.jhtml;jsessionid=YQWO1VIWT5YC4QNSDLPCKH0CJUNN2JVN?articleID=199900962)

---

### Agriculture Sector

18. *June 05, Advocate (LA)* — **Tests find diseased crawfish.** A disease that can kill off crawfish has been confirmed in commercial ponds across southwest Louisiana and in the Atchafalaya Basin, state officials said Monday, June 4. White spot disease was first detected last month at a crawfish farm near Arnaudville. Further testing has confirmed the disease in 20 ponds in six parishes and in at least two samples of wild crawfish from the Basin, according to information from Louisiana State University (LSU) Agricultural Center and the state Department of Agriculture and Forestry. State Agriculture and Forestry Commissioner Bob Odom said the 20 positive results for commercial ponds were out of 29 tested, raising fears the disease is widespread. Test results are pending on more than 70 other samples taken since the disease was first discovered. Mark Shirley, southwest regional aquaculture specialist for the LSU Agricultural Center, said samples of crawfish were collected last week from ponds within a mile radius of the first positive tests. Random sampling from ponds in all crawfish-producing parishes is expected this week. Shirley said infected crawfish show signs of weakness and lethargy and may die. White spot disease has never before been detected in Louisiana crawfish.


19. *June 04, Reuters* — **China reports 18,000 pig deaths from disease outbreak.** China said a contagious pig disease had killed 18,000 in the first five months of 2007, in Beijing's first report on the scale of an outbreak that has disrupted the pig industry and caused pork prices to soar. A report on the agriculture ministry Website said the blue ear disease outbreak had infected 45,000 pigs through May, with 18,000 having died. It was the first official assessment since an outbreak of the disease a year ago killed what feed industry officials estimate at as many as one million pigs. The ministry did not say how many pigs had died last year but noted the highly contagious disease had "caused heavy losses to the pig breeding industry." The disease, caused by a variation of Porcine Reproductive and Respiratory Syndrome (PRRS) virus, was still being found among pigs in some provinces, according to the ministry.

Source: [http://www.alertnet.org/thenews/newsdesk/PEK1586.htm](http://www.alertnet.org/thenews/newsdesk/PEK1586.htm)

20. *June 04, AgProfessional* — **Delta and Pine Land announces closing of acquisition by Monsanto.** Delta and Pine Land Company, a commercial breeder, producer and marketer of cotton planting seed, announced that Monsanto Company has completed its acquisition of D&PL for approximately $1.5 billion in cash. D&PL will operate independently of Monsanto's
other commercial operations until Monsanto has completed its proposed divestitures of the Stoneville and NexGen businesses. Headquartered in Scott, MS, with multiple offices in eight states and facilities in several foreign countries, D&PL also breeds, produces and markets soybean planting seed.


**Food Sector**

21. *June 04, Associated Press* — *Errors, unapproved firm blamed for Korea beef ban.* U.S. inspectors wrongly allowed an unauthorized company to ship beef to South Korea that now has triggered a wider ban on two major U.S. processors, the U.S. Department of Agriculture (USDA) said on Monday, June 4. The ban punctuated long-running efforts by USDA to restore sales to South Korea. USDA spokesperson Keith Williams said that while Seoul hasn't officially issued a ban on all U.S. beef shipments, the incident negatively impacted exports in the short term. "The mere fact is if you tried to get beef in there right now, it probably wouldn't get in," said Williams. At present, Seoul allows imports of boneless U.S. beef from cattle less than 30 months of age. It says it will return 66.4 metric tons of beef that violated the rules and wants an explanation from USDA. Williams said a company that deals mostly with Mexico, Am–Mex, assembled and shipped the beef products that were rejected by South Korea. "There were not any other companies involved," he said. He also said USDA inspectors "did not follow procedures that were established for verifying requirements and for the product certification of the export certificate. This comes down to human error."

Source: http://www.reuters.com/article/healthNews/idUSN0419657220070605

22. *June 01, U.S. Food and Drug Administration* — *Agriculture department warns consumers of tainted raw milk.* Consumers who have purchased raw milk from Green Acres Jersey Farm in Lebanon, PA, any time after May 8 should discard it immediately due to the risk of Listeria monocytogenes contamination. Pennsylvania Agriculture Secretary Dennis Wolff said Friday, June 1. "During routine inspection of the dairy, a preliminary test showed the presence of Listeria bacteria in some raw milk samples," said Wolff. There have been no illnesses reported as a result of the potential contamination. The Pennsylvania Department of Agriculture has suspended sales of raw milk at the dairy and is ensuring that corrective action is taken. Samples were taken from the farm during routine testing on May 29 and tested positive for Listeria on June 1. Multiple laboratory samples must test negative before sales can resume. Symptoms of Listeriosis include fever, muscle aches and, sometimes, gastrointestinal symptoms such as nausea or diarrhea. If infection spreads to the nervous system, symptoms such as headache, stiff neck, confusion, loss of balance or convulsions can occur. Infected pregnant women may experience only a mild, flu–like illness, but infections during pregnancy can lead to miscarriage or stillbirth.

Source: http://www.fda.gov/oc/po/firmrecalls/greenacres06_07.html

23. *May 31, U.S. Food and Drug Administration* — *Recall for pelleted and crumbled shrimp feeds.* In cooperation with the U.S. Food and Drug Administration (FDA), Zeigler Bros., Inc. is issuing a voluntary nationwide recall of its pelleted and crumbled shrimp feeds. The recalled products all include the feed ingredient "AquaBond," which has been found to contain the
chemical melamine and related compounds. AquaBond is a binding agent purchased in the U.S. by Zeigler and used in its production of pelleted and crumbled shrimp feeds. It is used in a much lower concentration than similar ingredients used in the recent U.S. pet food recall. Zeigler is not aware of any instances of ill health effects in shrimp fed with Zeigler pelleted and crumbled shrimp feeds.

Source: [http://www.fda.gov/oc/po/firmrecalls/ziegler06_07.html](http://www.fda.gov/oc/po/firmrecalls/ziegler06_07.html)

**Water Sector**

Nothing to report.

**Public Health Sector**

24. *June 04, Associated Press* — **U.S. purchases new smallpox vaccine.** The federal government will purchase 20 million doses of a smallpox vaccine that, in the event of an outbreak, would be used to treat people with compromised immune systems. The five-year contract with a Danish pharmaceutical company, is valued at more than $500 million. The smallpox vaccine is a completely new product that will be added to the Strategic National Stockpile. The current stockpile contains enough smallpox vaccine for every American. However, that vaccine was produced using a live, replicating virus, which can be potentially life-threatening in rare instances. Patients, such as those getting chemotherapy, should not get such vaccines in non-emergency cases. This smallpox vaccine contains a highly weakened form of the virus that cannot replicate in humans.


25. *June 04, U.S. Food and Drug Administration* — **FDA announces new committee to address risk communication.** The U.S. Food and Drug Administration (FDA) Monday, June 4, announced a new advisory committee designed to counsel the agency on how to strengthen the communication of risks and benefits of FDA-regulated products to the public. The Risk Communication Advisory Committee will; help FDA better understand the communication needs and priorities of the general public; advise FDA on the development of strategic plans to communicate product risks and benefits; and make recommendations to FDA on what current research suggests about crafting risk and benefit messages, as well as how to most effectively communicate specific product information to vulnerable audiences. The advisory committee will be made up of 15 voting members that include experts and public members who are not affiliated with the FDA. Experts will include authorities knowledgeable in the fields of risk communication, social marketing, health literacy, cultural competency, journalism, bioethics, and other relevant behavioral and social sciences. Public members will include those who can provide the perspective of users of FDA-regulated products, such as consumers, patients, caregivers and health professionals.


26.
June 01, Clinical Infectious Disease — Infection due to three avian influenza subtypes in U.S. veterinarians. Researchers examined veterinarians in the U.S. for evidence of previous avian influenza virus infection. Researchers performed a controlled, cross-sectional seroprevalence study among 42 veterinarians and 66 healthy control subjects using serum samples collected from 2002 through 2004. Serum samples were tested using a microneutralization assay against 9 influenza A virus strains. Using multivariable logistic regression modeling, veterinarians exposed to birds demonstrated statistically significant elevated titers against the H5, H6, and H7 avian influenza virus isolates, compared with control subjects. These data suggest that occupational exposure to avian species may increase veterinarians’ risk of avian influenza virus infection. Veterinarians should be considered for priority access to vaccines and antiviral drugs in pandemic planning. Source: http://www.journals.uchicago.edu/CID/journal/issues/v45n1/50338/brief/50338.abstract.html?erFrom=5632526908397177127Gues t

Government Sector

27. June 05, KBAK (CA) — Two teens arrested for explosion at California high school. Students at Bakersfield’s Frazier Mountain High School returned to school on Monday, June 4, and saw a destructive scene: about a dozen lockers ripped apart by a blast. "It's the last week of school here so there are various pranks the senior class is doing, which is tradition up here," explained Senior Deputy Vince Martinez of the Kern County Sheriff's Department. Two Lancaster area teens have been arrested on several felony charges, including terrorism. One of those is Frazier Mountain High School senior Alexander Timothy Hancock. The second is Hancock's friend and neighbor, 18-year-old Thomas John Tosh, a former student at the high school. Authorities believe they used an empty CO–2 cartridge from a paintball container and filled it with a type of explosive. The pair allegedly set the bomb off late Saturday night. Source: http://www.eyeoutforyou.com/home/7834992.html

28. June 05, Department of Homeland Security — Department of Homeland Security expands graduate education program for government officials. The Department of Homeland Security (DHS) announced on Tuesday, June 5, that it is increasing homeland security graduate education opportunities to government officials by establishing the “DHS Homeland Security Academy” within the National Capital Region. The first class for the academy will begin June 6 at the U.S. Office of Personnel Management’s Eastern Management Development Center in Shepherdstown, WV, and will include DHS, state, local, and military officials. “Establishing the Homeland Security Academy is a significant achievement in the implementation of a comprehensive DHS education and training system,” said George Tanner, the chief learning officer for DHS. “Investing in the leadership and management capability of our employees is a top priority of the department.” More than 150 government officials have earned master’s degrees through the NPS 18–month program, which is sponsored by FEMA’s National Preparedness directorate. The master’s program prepares leaders to develop the policies, strategies, programs and organizational arrangements to prevent and respond to terrorist attacks and other disasters and strengthen the interagency and intergovernmental relationships that homeland security requires. Source: http://www.dhs.gov/xnews/releases/pr_1181075311087.shtm
Emergency Services Sector

29. June 06, CNET News — FCC homing in on a plan for cellular 911. The Federal Communications Commission (FCC) wants to make emergency calls on cell phones more reliable. Cellular companies need to provide more accurate information to police and firefighters who are trying to locate people calling 911 from mobile phones, according to the FCC. But exactly how to measure compliance and achieve this goal is still up for debate. Last week, the FCC said it would seek public comment from the industry and public safety organizations on several issues that it believes could improve the accuracy of what's known as enhanced 911 service, or E911. One proposal, supported by the FCC, would require cell phone operators to measure the accuracy of their location technology in smaller geographic areas. The commission is also looking at requiring mobile operators to use a hybrid solution that combines both GPS (Global Positioning System) satellite receivers in handsets and network–based location technologies to help pinpoint the location of callers. The FCC said all accuracy requirements would also apply to voice over Internet Protocol services that allow people to move their service to new locations.

30. June 04, Government Health IT — Prescription information now available online in an emergency. Doctors and pharmacists caring for disaster victims can now obtain medication histories through a new Web service. The service is named ICERx.org, which is shorthand for In Case of Emergency Prescription Database, makes permanent the type of service cobbled together on short notice in 2005 after Hurricane Katrina wiped out thousands of personal medical records and many of the local drug stores that filled prescriptions. Using the Web service in an emergency, physicians, pharmacists, and other licensed health care professionals can access prescription records compiled from local drug stores, pharmacy benefit managers, state Medicaid programs and other sources. The service delivers specifics about the prescription, who wrote it, and where it was filled. In addition, ICERx.org can provide patient clinical alerts, drug interaction and therapeutic duplication warnings, and other reference information and alerts.
Source: http://govhealthit.com/article102890−06−04−07−Web

31. June 04, Washington Technology — DHS seeks feedback on first responder capability gaps. The Department of Homeland Security (DHS) is looking for better ways to obtain feedback from potentially tens of thousands of first responders about their most critical technology needs for emergency response. The Science and Technology Directorate published a notice and request for public comment for its TechSolutions program that aims to provide technology information and training to fire, police, emergency medical, and other response agencies. The first responders are encouraged to identify and submit their ideas on “capability gaps” in which there exists an urgent need for a technology that is not yet available. The goal of TechSolutions is to field technologies that meet 80 percent of the operational requirement, in a 12– to 15–month time frame, at a cost commensurate with the proposal but less than $1 million per project, according to the program’s Website.
32. **June 01, U.S. Department of Defense** — **Army helps prepare hurricane states for heavy season.** The Army is helping out U.S. states and territories that are in the paths of potentially deadly hurricanes by providing equipment to help fill shortages identified by National Guard commanders there, a senior Army official said Friday, June 1. The Army is either issuing or loaning 2,600 pieces of equipment to a handful of coastal states, Hawaii, Guam, Puerto Rico and the Virgin Islands, said Army Brigadier General David Halverson, director of operations, readiness and mobilization, for the deputy chief of staff for operations and plans. The equipment includes relief necessities, such as generators, trucks, Humvees and radios. Some of the equipment will be permanently assigned to fill shortages at the states, Halverson said. Equipment on loan is temporarily assigned and positioned within the state and will be returned at the end of hurricane season, in November. Overall, lines of communication between state and federal agencies are now better equipped to manage disaster relief, and agencies are more focused on how to provide aid and less on establishing lines of control, Halverson said.


---

33. **June 04, eWeek** — **Virus targets popular calculators.** A popular brand of calculators is being infected by a new virus that causes screens to read, "t89.GARRA." The virus, which attacks Texas Instruments TI89 and compatible calculators, doesn't do any permanent harm, but Texas Instruments engineers haven't found a way to disable it either. And while the author of the virus has been charitable enough to include code for disabling it, researchers have not been able to validate that fix. TIOS.Tiagra, as it has been dubbed by researchers at Symantec, cannot spread without use of a USB cable. The virus works by appending its code to any suitable file, and searches for a particular instruction sequence to replace and point towards the virus code. If the sequence is not found, the virus will remain but will not gain control, according to Symantec security researchers. The virus only runs on files with ASM extensions, so, in order to propagate itself, it has to run a check on the calculator for ASM-type files; moreover, it cannot infect previously infected files, Symantec officials said in an advisory.


Source: [http://www.eweek.com/article2/0,1895,2141590,00.asp](http://www.eweek.com/article2/0,1895,2141590,00.asp)

---

34. **June 04, eWeek** — **EMC acquires 'enhanced' security vendor Verid.** Officials at data storage giant EMC have claimed that the company is not planning to acquire any more companies and instead wants to focus on building its existing storage- and security-related businesses. Nonetheless, the company announced Monday, June 4, that it has bought its second company of 2007 in Verid, a small, privately held information security technology vendor in Sunrise, FL, that makes knowledge-based authentication software. Verid's software is used by about 130 large consumer-facing financial institutions, telecom providers and retailers.

Source: [http://www.eweek.com/article2/0,1895,2141611,00.asp](http://www.eweek.com/article2/0,1895,2141611,00.asp)
35. **June 04, eWeek** — **Microsoft eschews patch, gives exploit code for IIS 5.0 bug.** Saying that an Internet Information Server exploit is due to a feature, not a flaw, Microsoft has published exploit code for the flaw but no workaround or patch. The exploit, which was discovered on December 15, 2006, and made public at the end of May, works against IIS 5.x. By design, versions 5.x allow bypass of basic authentication by using the "hit highlight" feature. The hit-highlighting feature can be used by an unauthorized user to grab documents to which he or she has no privileges. At the very least, this leaves IIS 5.x users vulnerable to data interception. And while the exploit hasn't been used to take over systems to date, that could well change, according to Swa Frantzen of the Internet Storm Center. According to Microsoft, which has written up the issue in its Knowledge Base article 328832, hit-highlighting with Webhits.dll only relies on the Microsoft Windows NT ACL (Access Control List) configuration on 5.x versions.

Microsoft article: [http://support.microsoft.com/kb/328832](http://support.microsoft.com/kb/328832)

Source: [http://www.eweek.com/article2/0,1895,2141587,00.asp](http://www.eweek.com/article2/0,1895,2141587,00.asp)

36. **June 04, IDG News Service** — **Avaya to be sold for $8.2 billion.** Network equipment manufacturer Avaya Inc. late Monday, June 4, agreed to an $8.2 billion cash buyout by private equity firms TPG Capital LLP and Silver Lake Partners, the companies announced. This latest acquisition continues a recent trend of networking and telecommunications firms being bought by private equity firms.

Source: [http://www.infoworld.com/article/07/06/04/Avaya-to-be-sold_1.html](http://www.infoworld.com/article/07/06/04/Avaya-to-be-sold_1.html)

37. **June 04, ComputerWorld** — **New zero-day bugs crop up in IE, Firefox.** A noted security researcher on Monday, June 4, disclosed four new zero-day vulnerabilities in Microsoft Corp. and Mozilla Corp.'s browsers, including a critical flaw in Internet Explorer (IE) and a "major" bug in Firefox. Michael Zalewski, who regularly publishes browser flaw findings, posted details on the Full-disclosure mailing list for cookie-stealing, keystroke-snooping, malicious downloading and site-spoofing bugs. The most serious of the four, said Zalewski, is an IE6 and IE7 flaw he rated "critical." Dubbing it a "bait-and-switch" vulnerability, he said that the Microsoft browser gives hackers a window of opportunity to run malicious JavaScript to hijack the PC. "The entire security model of the browser collapses like a house of cards and renders you vulnerable to a plethora of nasty attacks," Zalewski claimed. But Mozilla's browser also suffered at Zalewski's hands. A new IFrame vulnerability in Firefox 2.0 can let attackers plant keyloggers or drop malicious content into a legitimate Website. Zalewski posted information about two other bugs, both rated "medium." A Firefox vulnerability could lead to unauthorized downloads, while IE6 is open to yet another address bar-spoofing flaw.


Source: [http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9023043&intsrc=hm_list](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9023043&intsrc=hm_list)

38. **June 01, eWeek** — **Mac coming into focus as attack target.** There haven't been mass Mac exploits to date, but interest is growing, as evidenced by the quick turnout of exploit code for a recently disclosed vulnerability. Compared with Windows, the Macintosh platform is still largely untouched by vulnerability exploits. But the prompt release of exploit code for a vulnerability detailed in a May 24 set of updates shows that it's catching up fast when it comes to grabbing the attention of exploit writers. Security research company Immunity released the
exploit code — which leveraged a buffer overflow vulnerability in the UPnP Internet Gateway Device Standardized Device Control code that's used to create port mappings on home NAT gateways in the OS X mDNSResponder implementation — less than 24 hours after Apple had released a patch for it. The release of the exploit code for this flaw shows that interest in Mac vulnerabilities is high, analysts say. That's not surprising; even though Macs aren't used as broadly in businesses as Windows machines, plenty of consumers use them, said Rob Enderle, principal analyst for the Enderle Group. Another factor that may be causing attackers to focus more on Macs is that Windows operating systems are getting "much [harder] to penetrate," he said.

Source: http://www.eweek.com/article2/0,1895,2140308,00.asp

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: 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/.

Commercial Facilities/Real Estate, Monument &Icons Sector

39. June 04, Detroit News — Bomb threat temporarily closes three Michigan libraries. Police said on Monday, June 4, that a bomb threat forced them to temporarily close three library buildings while they searched for explosives. The Clinton Township Police Department received a 911 call at about 3:30 p.m. CDT Monday from an unknown caller who said he had put two pipe bombs in undisclosed locations. The caller later said one of the locations was a library and demanded money in exchange for not detonating the bombs. Police evacuated three libraries: the Macomb County Library on Hall Road, the Clinton−Macomb Public Library on Romeo Plank and the Clinton−Macomb Public Library South Branch on Gratiot. Police said no suspicious devices were found

Source: http://www.detnews.com/apps/pbcs.dll/article?AID=/20070604/UPDATE/706040425/1003

General Sector

40. June 05, Associated Press — Suspect in Kennedy airport plot surrenders. A Guyanese suspect in an alleged plot to attack New York's John F. Kennedy International Airport surrendered to police Tuesday, June 5, in Trinidad, a police official said. Abdel Nur turned himself in at a police station outside the Trinidadian capital of Port−of−Spain, police spokesperson Wendy Campbell told the Associated Press. Nur is the fourth man in custody in the alleged plot to blow up fuel lines that feed the airport. Two other men are already in custody in Trinidad and the fourth is in the United States. Until a suspected terrorist plot was revealed, few people even knew there was a pipeline of highly combustible jet fuel snaking beneath the
nation's largest city. But authorities said Monday that it's one of countless lesser-known targets --- including waterway retaining walls, dingy rail yards, and tunnel ventilation systems --- that they struggle to protect from attacks. New York police spend "considerable time and resources protecting the landmarks nearly everyone would recognize as emblematic of New York and America," Police Commissioner Raymond Kelly said. "But we also protect the anonymous, unheralded elements of infrastructure that are essential to the life of the city."