



**UNCLASSIFIED**



# **North Dakota Homeland Security Anti-Terrorism Summary**



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

**UNCLASSIFIED**

**NDSLIC DISCLAIMER**

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

**QUICK LINKS**

[North Dakota](#)

[Energy](#)

[Regional](#)

[Food and Agriculture](#)

[National](#)

[Government Sector \(including Schools and Universities\)](#)

[International](#)

[Information Technology and Telecommunications](#)

[Banking and Finance Industry](#)

[National Monuments and Icons](#)

[Chemical and Hazardous Materials Sector](#)

[Postal and Shipping](#)

[Commercial Facilities](#)

[Public Health](#)

[Communications Sector](#)

[Transportation](#)

[Critical Manufacturing](#)

[Water and Dams](#)

[Defense Industrial Base Sector](#)

[North Dakota Homeland Security Contacts](#)

[Emergency Services](#)

## **NORTH DAKOTA**

Nothing Significant to Report

## **REGIONAL**

**(Minnesota) Month of glitches preceded siren failure on night of tornado.** A corrupted computer-activation code is responsible for several northwest Rochester, Minnesota weather sirens failing to sound during a June 17 storm that included damaging winds and one or more tornadoes. Officials from Olmsted County Emergency Management July 1 described, in detail, to county commissioners a host of technical glitches that preceded the damaging storm by about a month. Officials apologized for the failure and for reactions to criticism in the days after the storm that sounded “flip” to some commissioners. “Up until the 17th, I thought we had the greatest system in the country,” said the county’s deputy director of the Emergency Operations Center. “Nobody is more embarrassed and ashamed that this system failed.” Problems began in the third week of May, when the county installed a new version of siren-controller software. However, the software caused the system to “lock up.” The county’s tech-support staff, together with the software vendor, thought they had corrected the problem, but the system “locked up” again June 12. Two days later, the county re-installed the previous version of the software. But when they did that, apparently the code controlling Zone 5, a group of sirens covering northwest Rochester, became corrupted. Source: [http://www.postbulletin.com/newsmanager/templates/localnews\\_story.asp?z=2&a=459369](http://www.postbulletin.com/newsmanager/templates/localnews_story.asp?z=2&a=459369)

**(South Dakota) Police investigate mailbox explosive.** Sioux Falls Police are trying to figure out who put an explosive inside a mailbox at 3509 South Pillsberry Avenue, Sioux Falls, South Dakota. Just before 2:00 a.m., police were called to the home after the mailbox exploded. They are still investigating exactly how the explosive got there and what it was. Source: <http://www.ksfy.com/Global/story.asp?S=12778826>

## **NATIONAL**

**(New York) Terror defendant scoffed at JFK security.** A former cargo handler on a reconnaissance mission in an alleged plot to blow up New York’s John F. Kennedy International Airport marveled at the lack of security for jet fuel storage tanks there, according to tapes played July 6 at his terror trial. “You can’t believe how a place like Kennedy can be so (lax),” the former cargo handler said in a videotape recorded in January 2007. “No soldier. Nothing at all. ... The tanks ain’t got one person.” The grainy videotape of cargo handler in a front passenger seat was played in federal court in Brooklyn, New York during the testimony by another person, who went undercover to make a series of secret tapes. Prosecutors say the 66-year-old cargo handler, a naturalized U.S. citizen from Guyana, and his accomplice wanted to kill thousands of people and cripple the American economy by using explosives to blow up the fuel tanks. Source:

# UNCLASSIFIED

[http://www.google.com/hostednews/ap/article/ALeqM5imyS6Rxxh0dCsz\\_QIXiqWrCjtdtEwD9GPPLD0](http://www.google.com/hostednews/ap/article/ALeqM5imyS6Rxxh0dCsz_QIXiqWrCjtdtEwD9GPPLD0)

**Central states not ready for big quake.** The implications of a destructive earthquake in the New Madrid seismic zone covering eight Midwestern and Southeastern states are far greater than even previous worst-case scenarios have predicted, according to a study released June 25 by the University of Illinois. The study, Impact of New Madrid Seismic Zone Earthquakes on the Central USA, commissioned by the Federal Emergency Management agency, found that a 7.7 magnitude earthquake could leave at least 3,500 people dead, more than 80,000 injured and render at least seven million people temporarily homeless. Particularly hard hit would be St. Louis and Memphis — the two largest cities near the fault. The report also projects that damage to critical infrastructure (essential facilities, transportation and utility lifelines) would be substantial in the 140 impacted counties near the rupture zone, including 3,500 damaged bridges and nearly 425,000 breaks and leaks to both local and interstate pipelines. Source:

<http://www.hstoday.us/content/view/13821/128/>

**(Louisiana) 'A Whale' skimmer brought in to clean water as Gulf oil spill reaches record.** The oil that has spewed for two and a half months from a blown-out well a mile under the sea in the Gulf of Mexico hit the 140.6-million-gallon mark, eclipsing the record-setting, 140-million-gallon Ixtoc I spill off Mexico's coast from 1979 to 1980. Even by the lower end of the government's estimates, at least 71.7 million gallons are in the Gulf. It is crucial to track the total in part because London-based BP PLC is likely to be fined per gallon spilled, said the director of Texas A&M University at Corpus Christi's Gulf of Mexico Research Institute. The oil calculation is based on the higher end of the government's range of barrels leaked per day, minus the amount BP said it has collected from the blown-out well using two containment systems. BP collected a smaller amount of oil than usual yesterday, about 969,000 gallons. The government has pinned its latest clean-up hopes on a huge, new piece of equipment: The world's largest oil-skimming vessel, which arrived June 30. Officials hope the ship can scoop up to 21 million gallons of oil-fouled water a day. Dubbed the "A Whale," the Taiwanese-flagged former tanker spans the length of 3½ football fields and is 10 stories high. It just emerged from an extensive retrofitting to prepare it specifically for the Gulf. Source:

[http://www.pennlive.com/midstate/index.ssf/2010/07/whale\\_skimmer\\_tries\\_to\\_scoop\\_u.html](http://www.pennlive.com/midstate/index.ssf/2010/07/whale_skimmer_tries_to_scoop_u.html)

## INTERNATIONAL

Nothing Significant to Report

## BANKING AND FINANCE INDUSTRY

**(Florida) Hidden credit card skimmer found in local gas pump.** An alert technician found a device on a gas pump apparently designed to capture credit card information. The device, known as a credit card skimmer, was seized by the Alachua County Sheriff's Office. It was not immediately clear whether any credit card information was stolen or used illicitly. The small device wrapped in black electrical tape was found July 5 inside a Shell station in Gainesville, Florida. The device would not have been visible to those using the credit card reader to pay for their gas and was wired between the card scanner and the computer board of the pump, according to a sheriff's spokesman. The device was similar to those found at other stations along Interstates 75 and 95 in Florida and that it

UNCLASSIFIED

## UNCLASSIFIED

could have been installed in less than two minutes by someone who knew what he or she was doing. It did not appear the pump had been damaged by someone opening it, so the device was likely installed by someone with a universal gas pump key. Source:

<http://www.gainesville.com/article/20100707/ARTICLES/100709681/1109/sports?Title=Hidden-credit-card-skimmer-found-in-local-gas-pump>

**(Arizona) New twist to ATM scams.** Latest reports indicate that clear plastic overlays are being placed on top of the PIN pad to capture personal identification numbers in addition to card-skimming devices, helping scammers to steal even more of your personal information at ATMs. Thieves are also attacking outside the ATM. "In the past, we've had some elaborate schemes where they've actually put them inside credit devices that you would use — whether it would be at the gas pump or something like that," said a Phoenix Police sergeant. Source: <http://ktar.com/?nid=6&sid=1312252>

**FDIC targeted by phishers - again.** On July 2, the Federal Deposit Insurance Corporation (FDIC) warned consumers and financial institutions that bogus emails claiming to be from the FDIC are arriving in inboxes. This is the fourth time within a year that the federal banking regulator has issued alerts about phishing emails using its brand. The FDIC says subject lines of the e-mails state: "you need to check your Bank Deposit Insurance Coverage" or "FDIC has officially named your bank a failed bank." The email states: "You have received this message because you are a holder of a FDIC-insured bank account. Recently FDIC has officially named the bank you have opened your account with as a failed bank, thus, taking control of its assets." The email then directs recipients to click on a link stating "You need to visit the official FDIC website and perform the following steps to check your Deposit Insurance Coverage." If individuals click on the link, they are sent to a non-FDIC webpage. One email link has a .eu destination, which means the web server is located somewhere in the European Union. The e-mails and associated web site are fraudulent. Anyone getting these emails should consider the intent of this e-mail as an attempt to collect personal or confidential information, or to load malicious software onto end users' computers, says the FDIC. Source:

[http://www.bankinfosecurity.com/articles.php?art\\_id=2717](http://www.bankinfosecurity.com/articles.php?art_id=2717)

**Bank Failures: 2010 Pace Exceeds 2009.** Although there were no bank failures to report on the Fourth of July, midway through 2010, there have been more than twice the number of failed banks and credit unions as was seen at this same point in 2009. There have been 96 failures — 86 banks and 10 credit unions — so far in 2010. At the end of June 2009, there were 45 failures en route to a total of 171 failed institutions for the year. With institutions continuing to feel the effects of the 2008 economic meltdown, experts say we may well see significantly more bank failures before year's end. Of the 86 banks to fail so far in 2010, the largest is Westernbank Puerto Rico, which closed in April and had approximately \$11.94 billion in total assets. Of 10 credit unions to be closed, acquired or placed into conservatorship, the largest is Arrowhead Central Credit Union of San Bernardino, California. This full service credit union was placed into conservatorship in June, with assets of \$876 million. Florida leads the nation with 14 failures. Next on the list are: 12 failures in Illinois, nine in Georgia and California, seven in Washington State, and six in Minnesota. Meanwhile, with slightly fewer than 800 financial institutions now on the Federal Deposit Insurance Corporation's "troubled banks" list — up from 90 in 2008 — the likelihood of further bank closings is very real. Source:

[http://www.bankinfosecurity.com/articles.php?art\\_id=2720](http://www.bankinfosecurity.com/articles.php?art_id=2720)

UNCLASSIFIED

## UNCLASSIFIED

**(Maryland) The Bank of Glen Burnie advises of online banking e-mail phishing scam.** The Bank of Glen Burnie, Maryland is alerting consumers about an e-mail phishing scam designed to look like an online expiration warning from the bank. The e-mail informs customers that their account will be deleted if they do not update it by July 2, 2010. Consumers are urged to click on a Web site link to update their online account. This is a scam. The link goes to a Web site login, which looks exactly like The Bank of Glen Burnie's log-in page, but is not associated with the bank. Customers are asked to provide their username and password and anyone who provides the data is at risk of identity theft. The Bank of Glen Burnie's Web site is at [www.thebankofglenburnie.com](http://www.thebankofglenburnie.com). The Bank of Glen Burnie has not, and does not, request personal information in an e-mail. Source: [http://www.marketwatch.com/story/the-bank-of-glen-burnie-advises-of-online-banking-e-mail-phishing-scam-2010-07-01?reflink=MW\\_news\\_stmp](http://www.marketwatch.com/story/the-bank-of-glen-burnie-advises-of-online-banking-e-mail-phishing-scam-2010-07-01?reflink=MW_news_stmp)

**(Oregon) Bomb threat made at Sandy bank.** A man who robbed a U.S. Bank branch in Sandy, Oregon threatened employees with a gun and made a bomb threat as he left the bank, police said. The man escaped with an unknown amount of money and told bank employees he was going to blow up the bank, according to a representative with the Sandy Police Department. He left behind a paper bag which he claimed was a bomb, police said. The bank was evacuated and the robbery was reported to police, who rushed to the scene. A Portland Police Bureau bomb squad was headed to the area to examine the bag. They determined it was not an explosive device. Source: <http://www.kptv.com/news/24115169/detail.html>

## **CHEMICAL AND HAZARDOUS MATERIALS SECTOR**

**China's nuclear reactors to use technology rejected by U.S., U.K. as unsafe.** Ten of China's proposed nuclear power reactors will use Westinghouse's AP1000 advanced technology. The United States rejected the AP100 design, saying key components of the reactor might not withstand events like earthquakes and tornadoes. The United Kingdom indicated it, too, would reject Westinghouse's new reactor because it could be vulnerable to terrorist attacks. Ten of China's proposed nuclear power reactors will use Westinghouse's AP1000 advanced technology considered safer, a Chinese energy official said. The U.S. company's technology, described as among the most advanced in the world, operates longer, a Xinhua-China Daily report said, adding that China is currently building the largest number of nuclear power stations worldwide. UPI reports that The AP1000, a third-generation technology, will be used on six reactors at three inland nuclear plants in Hunan, Hubei, and Jiangxi provinces, and on two pairs of reactors in coastal Zhejiang and Shandong provinces, said the official, who asked not to be identified citing security reasons. Source: <http://homelandsecuritynewswire.com/chinas-nuclear-reactors-use-technology-rejected-us-uk-unsafe>

**Feds seek a temp home for depleted uranium.** The U.S. Department of Energy (DOE) has started looking beyond Utah for temporary storage of nearly 10,000 drums of depleted uranium for up to seven years. The cleanup waste from the Savannah River Site in South Carolina was originally headed to Utah to be buried for good at the EnergySolutions Inc. disposal site. In fact, the first of three shipments had already arrived in Utah when the Utah governor and the DOE agreed to put the disposal and the remaining two shipments on hold. The Salt Lake City nuclear services company has estimated it will be the end of the year before it can update a report on the site's ability to contain large quantities of the unusual waste, which grows more hazardous over time. And it will probably

UNCLASSIFIED

## UNCLASSIFIED

take at least another year for state regulators to review that site assessment. In the meantime, the first shipment containing about 5,400 drums of the Savannah River waste has been placed in an EnergySolutions disposal cell but will not be buried until the state gives its approval. Potential bidders have until July 15 to submit their temporary storage proposals to the Energy Department. And, there is just one site that is licensed to offer interim storage, a new facility in western Texas near the New Mexico border. Source: <http://sltrib.com/sltrib/home/49885304-76/waste-site-storage-depleted.html.csp>

**Heart tests add to U.S. radiation dose concerns.** Heart imaging procedures can deliver a significant amount of radiation to patients, U.S. researchers said on Wednesday, urging patients and doctors to weigh the risks against the benefits. They said nearly one in 10 adults under the age of 64 had a heart procedure involving radiation over a three-year period in five major healthcare markets. “For many patients in the United States, there is a substantial cumulative radiation exposure from cardiac procedures,” said a professor at Yale University School of Medicine, whose study appears in the Journal of the American College of Radiology. An advanced type of heart stress test called myocardial perfusion imaging, in which doctors inject a radioactive tracer in patients to test blood flow, accounted for 74 percent of radiation exposure from heart scans. Heart catheterization and stenting — procedures in which thin tubes are fished through blood vessels to open blocked arteries — were the second biggest contributor to radiation exposure, the professor said. More than half of the heart procedures using radiation were done in the doctor’s own office, the team found. “Policymakers have been concerned that there is a rise in physician office imaging and a rise in total use of imaging,” the professor said in a telephone interview. “I think there is legitimate concern that easy availability — convenience — makes the threshold for testing lower. Whether it is inappropriate or not, our study can’t say.” While doctors disagree over how much, most agree that radiation can cause cancer, and researchers are growing concerned that an explosion in the use of medical imaging is making it more likely that patients may develop cancer. Source: <http://www.reuters.com/article/idUSTRE6665R920100707>

**(New York) Nuclear material removed at hospital.** Federal agents and NYPD detectives closed down West 12th Street the week of June 28. They entered a building and worked through the night as counterterrorism detectives stood watch. Their mission was to unbolt a 4,000-pound, lead-lined piece of equipment with enough radioactive material in it to make it a “dirty bomb” concern. Their location was at St. Vincent’s Hospital. The officials placed the cesium-137 blood irradiator inside an 8-foot-tall hazardous-materials cylinder and loaded it onto a tractor trailer. Then the semi, flanked by federal escort vehicles, set off on a secret cross-country trip. It was not until they reached the storage facility in the “southwestern part of the country” two days later that officials were given the OK to talk about the mission. The big concern, according to a National Nuclear Security Administration official, is that the cesium, in the wrong hands, could potentially be used to make a “radiological dispersal device,” or left in a place where a large number of people could be exposed to it. The efforts at St. Vincent’s were unique, according to agency officials, because unlike most of the facilities using radioactive materials in the city, the hospital’s forced closure meant that something had to be done to secure the radioactive cesium, about the size of a soda can, inside the machine. Source: <http://online.wsj.com/article/SB10001424052748704699604575343384175611848.html>

## COMMERCIAL FACILITIES

UNCLASSIFIED

## UNCLASSIFIED

**(Virginia) City police respond to third Walmart bomb threat.** For the third time three months, Waynesboro, Virginia, city police responded to a bomb threat written on a bathroom stall in the women's restroom in a local Walmart July 7. Store workers asked customers to leave at about noon. The call sent about a dozen Waynesboro police, two state troopers, and a bomb-sniffing dog to the store. As in the previous two incidents, police found nothing. The store reopened after officers cleared the scene at about 3 p.m. Police officials say Wal-Mart loses \$30,000 to \$40,000 for every hour the store is closed. Whether the prior threats are connected to the one July 7 is unclear. Police said Walmart uses two security cameras near the entrance of the store that should capture footage of people going into and out of the bathrooms. Source:

[http://www2.newsvirginian.com/wnv/news/local/waynesboro/article/city\\_police\\_respond\\_to\\_third\\_walmart\\_bomb\\_threat\\_since\\_april/57994/](http://www2.newsvirginian.com/wnv/news/local/waynesboro/article/city_police_respond_to_third_walmart_bomb_threat_since_april/57994/)

**(Oregon) Pipe bombs close streets, buildings in Hillsboro.** A bag containing two suspicious objects were discovered by a County facility custodian in a parking lot just north of a Washington County Facilities building at 169 N. First Avenue in Hillsboro, Oregon July 2. The objects, two pipes with tape on them, were brought to the northern entrance of the Facilities building and 9-1-1 was called. The Hillsboro Police with the assistance of Washington County Sheriff's Office closed surrounding streets and evacuated the building. The Portland Bomb Squad arrived and removed the suspicious objects from the scene. The objects were transported to a safe location where they will be examined. The buildings were reopened shortly after. There are no suspects at this time. Source:

<http://theportlander.com/2010/07/03/pipe-bombs-close-streets-buildings-in-hillsboro/>

**(Florida) After Gulf swimmers report illness, questions about opening a beach.** Santa Rosa Island officials flew the double-red, no swimming flag over Pensacola Beach in Florida after a swath of thick oil washed ashore from the Gulf of Mexico oil spill June 23. Two days later, against the warnings of federal health officials and based on a visual survey of the beach, the local island authority director reopened the beaches for swimming, urging residents and tourists to come back to the beach. Officials left the ultimate decision on whether it was safe to swim to beachgoers. This week, health officials in Escambia County, Florida reported that about 400 people claimed they felt sick after visiting the beach and swimming in the Gulf. Testing by the University of West Florida in recent days has indicated small amounts of dissolved petrochemicals in the water near Pensacola Beach. Federal officials have urged caution about swimming in areas not only near the spill, but also where oil actually came ashore, and where tides buried some of the oil smudges. Federally managed National Seashore beaches on both sides of Pensacola Beach remained closed to swimming. Source:

[http://www.minnpost.com/worldcsm/2010/07/02/19408/after\\_gulf\\_swimmers\\_report\\_illness\\_questions\\_about\\_opening\\_a\\_beach](http://www.minnpost.com/worldcsm/2010/07/02/19408/after_gulf_swimmers_report_illness_questions_about_opening_a_beach)

**(Michigan) Suspicious package found at Walmart lot.** Michigan State Police bomb specialists were called to a Cascade Township Walmart July 1 to deal with a suspicious package. Employees of the store called police around 5:30 p.m. when someone told them there was a package abandoned in the parking lot. They then put the package in a shopping cart and wheeled it out to a relatively empty part of the parking lot. The Michigan State Police Bomb Squad opened the package and cleared it from the scene without incident. A police spokesman described the nonexplosive device as a case with several tubes and wires connected to an electronic device. Police took the package in as evidence and will continue to investigate. Source:

[http://www.woodtv.com/dpp/news/local/kent\\_county/Suspicious-package-found-at-Walmart-lot](http://www.woodtv.com/dpp/news/local/kent_county/Suspicious-package-found-at-Walmart-lot)

UNCLASSIFIED

**Two Chinese men sentenced in UAE mall bomb plot.** A court in the United Arab Emirates (UAE) has sentenced two Chinese Uighurs to 10 years in prison after planning a bombing attack on Dubai's Dragon Mart. The men were arrested in July and recently convicted of planning the attack and being members of a terrorist group. According to a charge sheet, the men communicated with the Islamic East Turkestan movement regarding carrying out the attack. The mall is a large shopping center for Chinese-made goods in Dubai. The men planned to detonate an explosive device either in or on a statue outside the 4,000-shop complex. The Chinese Embassy tipped off UAE authorities. The suspects had been under close watch by Chinese officials because of their ethnic and religious backgrounds. Source: <http://www.allheadlinenews.com/articles/7019163445>

## **COMMUNICATIONS SECTOR**

**U.S. to announce \$795 million in new broadband subsidies.** The President's administration will announce nearly \$795 million in grants and loans for broadband deployment projects across the nation July 2, officials with two federal agencies said. The U.S. National Telecommunications and Information Administration (NTIA) and the U.S. Rural Utilities Service (RUS) will officially announce awards for 66 new broadband projects that will touch all 50 states, the officials said. The money, from the American Recovery and Reinvestment Act passed by the U.S. Congress in early 2009, is expected to create or save about 5,000 jobs, officials said. The top goal for the grants and loans is to immediately create American jobs, while another goal is to give an economic boost to some areas of the country by providing new broadband service said the secretary of the Department of Commerce, the parent agency of the NTIA. The new broadband subsidies will bring service to 685,000 businesses, 900 health-care facilities, and 2,400 schools, he said. Source: [http://www.computerworld.com/s/article/9178807/U.S. to announce 795 million in new broadband subsidies](http://www.computerworld.com/s/article/9178807/U.S._to_announce_795_million_in_new_broadband_subsidies)

## **DEFENSE INDUSTRIAL BASE SECTOR**

**Study says Aegis radar systems on the decline.** The advanced radar systems aboard cruisers and destroyers are in their worst shape ever, according to an independent probe into Navy readiness, raising questions about the surface fleet's ability to take on its high-profile new mission next year defending Europe from ballistic missiles. Poor training, impenetrable bureaucracy and cultural resignation have caused a spike in the number of technical problems and a dip in the operational performance of the Aegis system, considered the crown jewel of the U.S. surface force, according to members of a "fleet review panel" tasked with assessing the surface fleet. Source: [http://nosint.blogspot.com/2010/07/study-says-aegis-radar-systems-on.html?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed:+blogspot/fqzx+\(Naval+Open+Source+INTelligence\)](http://nosint.blogspot.com/2010/07/study-says-aegis-radar-systems-on.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+blogspot/fqzx+(Naval+Open+Source+INTelligence))

**Malware takes aim at defense contractors.** A sophisticated malware operation targeting defense contractors has been uncovered, according to experts. Researchers at Symantec Hosted Services said the operation involved compromising the site of one firm, and then using the hacked site to host a malware attack on another contractor. The attack began when the first company's site was compromised and embedded with a landing page and obfuscated exploit code. The attackers then sent a series of e-mails to employees of a second firm claiming the company's chief executive had

## UNCLASSIFIED

been arrested by U.S. authorities. When the targeted users clicked on an included link, they were directed to the compromised site of the first company, which then attempted to exploit a newly disclosed vulnerability in the Windows Help component and infect users with an assortment of malicious software. A Symantec senior malware analyst said the sophistication and complexity of the attack was particularly noteworthy. Source: <http://www.v3.co.uk/v3/news/2265825/malware-takes-aim-defence>

### **CRITICAL MANUFACTURING**

**FAA orders cockpit-door fixes on Boeing planes.** For the fourth time in as many years, federal aviation regulators have ordered U.S. airlines to fix unspecified defects that could cause fortified cockpit-doors on potentially thousands of jetliners to malfunction. A pair of directives issued July 1 by the Federal Aviation Administration (FAA) indicates that a certain “feature of the flight deck door is defective” on a wide range of Boeing Co. jetliner models. Without identifying the problem, the FAA documents say failure of this “feature” could jeopardize safety, and that elements of the doors must be quickly replaced or modified. The directives mention every Boeing jet, from narrow-body MD-80 and Boeing 737 models to long-range, wide-body Boeing 747, 767 and 777 jetliners. An FAA spokeswoman said she couldn’t provide details because the directives focus on security matters. Source: <http://online.wsj.com/article/SB10001424052748704898504575342721294043134.html>

### **EMERGENCY SERVICES**

**(California) Suspicious device found attached to Hemet police car.** A suspicious device attached to a police car was discovered July 6 in another possible attempt to harm law enforcement officers in Hemet, California. Authorities noted that the mechanism appeared to have been placed on the vehicle before the recent arrests of two suspects in the attacks that began earlier this year. The device was located about 11:40 a.m. during an inspection of patrol vehicles parked at the City Yard, 3077 Industrial Ave., according to a Hemet police lieutenant. The area was evacuated and Riverside County sheriff’s bomb technicians secured the instrument. “This device could have been attached to the vehicle at any time in the last 60 days,” the lieutenant said. “Investigators believe they have the suspects in these attacks in custody and that this device was simply not discovered until today.” Source: <http://www.mydesert.com/article/20100706/NEWS0801/100706030/Suspicious-device-found-attached-to-Hemet-police-car>

### **ENERGY**

Nothing Significant to Report

### **FOOD AND AGRICULTURE**

**(Ohio) Bovine TB found in Ohio.** The director of Ohio Department of Agriculture announced July 8 that preliminary tests performed by the department’s Animal Disease Diagnostic Laboratory revealed a positive result for bovine tuberculosis in a Paulding County dairy herd. There is no known human illness associated with this occurrence. The herd was found positive after routine tuberculosis testing by the department. The herd was depopulated, and the department is currently conducting a trace-in

UNCLASSIFIED

## UNCLASSIFIED

and trace-out investigation to determine if other livestock may be affected. Source:

[http://www.dairyherd.com/directories.asp?pgID=675&ed\\_id=11820](http://www.dairyherd.com/directories.asp?pgID=675&ed_id=11820)

**Honey bees in New Jersey dying at an alarming rate.** The honeybee population in New Jersey continues to decline at an alarming rate: 35 percent of managed colonies didn't survive the past winter, according to a survey by the New Jersey Beekeepers Association. That decline follows losses of 35 percent over the winter of 2008-09 and 17 percent in 2007-08, according to the association. The decline mirrors similar colony collapses across the country. Losses nationwide totaled 34 percent over the winter, according to a survey by the non-profit Apiary Inspectors of America and the U.S. Department of Agriculture. Similar national surveys documented a 29 percent decline in 2008-09 and 36 percent the prior winter. But while some of the bombus species – better known as bumblebees – are clearly declining, others appear to be doing fine, according to a Rutgers University entomologist who specializes in pollination ecology. Source:

[http://www.northjersey.com/news/98090584\\_Honey\\_bees\\_in\\_New\\_Jersey\\_dying\\_at\\_an\\_alarming\\_rate.html](http://www.northjersey.com/news/98090584_Honey_bees_in_New_Jersey_dying_at_an_alarming_rate.html)

**(Pennsylvania) Warning issued on hard cheddar made by Troy, Pennsylvania farm.** The Pennsylvania Department of Agriculture on July 7 advised consumers to discard aged hard cheddar cheese made with raw milk from Milky Way Farm in Troy, Pennsylvania because of potential bacterial contamination. A Department of Agriculture lab found *Staphylococcus aureus* and enterotoxin in an aged hard cheese sample on June 21. The presence of enterotoxin violates the Milk Sanitation Law and the Food Act as it can cause serious illness, the release says. Aged hard cheese may be legally manufactured in Pennsylvania from milk that has not been pasteurized, as long as it is aged more than 60 days in temperatures exceeding 35 degrees Fahrenheit, a news release says. Additional testing has determined that pasteurized cheeses that are produced and sold on the farm are suitable for human consumption. Source:

<http://www.stargazette.com/article/20100707/NEWS01/7070334/Warning+issued+on+hard+cheddar+made+by+Troy++Pa.++farm>

**(Pennsylvania) Upper Macungie company recalls possibly tainted turkey.** K. Heeps, an Upper Macungie Township, Pennsylvania food manufacturer and wholesaler, said July 7 it was recalling 171/2 pounds of turkey possibly contaminated with a bacteria that is particularly harmful to pregnant women, children and people with weakened immune systems. The company said the recalled product was sold as sliced turkey breast to an unnamed restaurant in Reading. The U.S. Department of Agriculture routinely does not identify the restaurant that served the potentially tainted meat. According to USDA, the turkey may be contaminated with *Listeria monocytogenes*, a bacteria that can cause listeriosis, which can produce fever, headache, nausea, vomiting and in severe cases, infection and death. Source: [http://articles.mcall.com/2010-07-07/news/mc-allentown-turkey-recall-20100707\\_1\\_turkey-recalls-food-inspectors](http://articles.mcall.com/2010-07-07/news/mc-allentown-turkey-recall-20100707_1_turkey-recalls-food-inspectors)

**(Michigan; Illinois) 8,000 lbs of beef jerky recalled for allergens.** M&K II Co. recalled approximately 8,000 pounds of beef jerky June 6 because the products contain wheat and soy, undeclared allergens, according to the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS). The Macomb, Michigan company said products subject to the recall include: jerky-labels.jpg-1-ounce and 3-ounce packages of "Firehouse Jerky Mild Beef Jerky Smoke Flavor Added." "Sell By" dates ranging between 06/16/11 and 11/14/11 are ink jetted on the back of each package; and -1-ounce and 3-ounce packages of "Firehouse Jerky Pepper Beef Jerky Smoke Flavor Added." "Sell By" dates ranging

UNCLASSIFIED

## UNCLASSIFIED

between 06/12/11 and 11/25/2011 are ink jetted on the back of each package. Each package bears the establishment number “EST. 6935” or “EST. 10002” inside the USDA mark of inspection. The code number “6935” is ink jetted on the back of each package. These products were produced on various dates from January 28, 2010, through May 21, 2010, and were sent to Firehouse Foods, Inc., an Alsip, IL distributor, for further Internet and retail sales. Source:

<http://www.foodsafetynews.com/2010/07/beef-jerky-recalled-for-allergens/>

**E. coli contaminated 66,000 pounds of bison meat recalled.** Colorado-based meat processing company Rocky Mountain Natural Meats has announced a recall of 66,000 pounds of bison meat over concerns that they're contaminated with the dangerous E.coli bacteria. The Henderson, Colorado-based company said it is worried that the meat could cause food poisoning. The recall is voluntary in nature. The US Department of Agriculture (USDA) said it has already received five complaints that people who have consumed the contaminated meat have contracted E.coli O157:H7 illnesses. The USDA said in a statement that the recall involved ground bison meat and tenderized bison steaks produced between May 21 and May 27 with “sell or freeze by” dates in June. The contaminated products are also marked with a “EST. 20247” inside the USDA mark of inspection. They were sold under the names Great Ranger, Nature’s Rancher, The Buffalo Guys and Rocky Mountain Natural Meats and came in 1 lb and 12oz packs. Source:

<http://www.ibtimes.com/articles/32688/20100705/e-coli-contaminated-66-000-lbs-of-bison-meat-recalled.htm>

**(Colorado) 24 ill in Colorado raw milk outbreak.** An E. coli O157:H7 and campylobacter outbreak linked to raw goat milk from a Colorado dairy is now tied to 24 illnesses, including two children who required hospitalization, according to the Boulder County Public Health Department. The outbreak has been linked to Billy Goat Dairy in Longmont, near Boulder, Colorado. Lab results found both Campylobacter and E. coli in victims. State and local health investigators visited the Longmont dairy last week to collect samples from the goats and are in the process of contacting the 43 households that participate in the dairy’s goat-share program. Colorado state does not allow the retail sale of raw milk. According to analysis by Food Poison Journal, in the last six months, raw milk caused 11 outbreaks of Campylobacter, Salmonella, and E. coli O157:H7 in 9 different states, including Washington, Utah, Minnesota, Nevada, Pennsylvania, New York, Michigan, Indiana, and Illinois. Source: <http://www.foodsafetynews.com/2010/07/24-ill-in-colorado-raw-milk-outbreak/>

**(Pennsylvania) Pennsylvania cattle quarantined over well water concern.** The state agriculture department has quarantined 28 head of cattle at a central Pennsylvania farm after officials say the animals potentially consumed wastewater that leaked from a holding pond for a natural gas well on the property. The Agriculture Secretary said June 1 that uncertainty over how much water the cows drank warranted the quarantine to protect the public from eating potentially contaminated beef. The quarantine covered the 28 cows, plus their unborn calves on the farm in Wellsboro. East Resources was drilling the well. An East spokesman said agriculture officials may have overreacted, and that tests done at the request of state environmental officials found no reason for adverse impact on the cattle, or on public health. Source:

[http://www.montgomerynews.com/articles/2010/07/06/montgomery\\_life/doc4c3318e2ef89a812253469.txt](http://www.montgomerynews.com/articles/2010/07/06/montgomery_life/doc4c3318e2ef89a812253469.txt)

**Oil found in Gulf crabs raises new food chain fears.** University scientists have spotted the first indications oil from a massive spill in the Gulf of Mexico is entering the seafood chain — in crab larvae

UNCLASSIFIED

## UNCLASSIFIED

— and one expert warns the effect on fisheries could last “years” and affect many species. Scientists with the University of Southern Mississippi and Tulane University in New Orleans have found droplets of oil in the larvae of blue crabs and fiddler crabs sampled from Louisiana to Pensacola, Florida. “Fish are going to feed on (crab larvae),” said the director of the Center for Fisheries Research and Development at the Gulf Coast Research Laboratory. “We have also just started seeing it on the fins of small, larval fish — their fins were encased in oil. That limits their mobility, so that makes them easy prey for other species,” he said. “The oil’s going to get into the food chain in a lot of ways.” Source: <http://www.miamiherald.com/2010/07/01/1711304/oil-found-in-gulf-crabs-raising.html>

**Tainted candy being recalled for possible lead contamination.** California health officials are warning people not to eat spicy mango candy from India because it may contain excessive levels of lead. The director of the California Department of Public Health warned against consuming “Food World Aam Papad Candy Spicy” (Dry Mango Candy Spicy) imported from India after tests by the department. The candy is imported and distributed by Quality Products, Inc. of San Jose. The state is working with the distributor to ensure that the contaminated candies are removed from store shelves. Food World Aam Papad Candy Spicy is sold in a 5.25-ounce clear, plastic container that has a red top. It has a white label with a red rectangle containing the words “FoodWorld.” Recent analysis determined the candy contained as much as 0.29 parts per million (ppm) of lead. California considers candies with lead levels in excess of 0.10 ppm to be contaminated. Pregnant women and parents of children who may have consumed this candy should consult a physician to determine if medical testing is needed. Consumers who find the tainted candy for sale at retail outlets are encouraged to call 1-800-495-3232. Source: [http://www.chicoer.com/news/ci\\_15426105](http://www.chicoer.com/news/ci_15426105)

**(Michigan) State warns restaurants of fake food inspectors.** Michigan agencies are warning restaurant operators to watch out for fake food inspectors. Word of the scam comes from the Michigan Agriculture and Community Health departments and the Michigan Restaurant Association. They say bogus food inspectors now are making the rounds in Michigan. Restaurants are getting calls from people claiming to be from a health department and requesting to schedule an inspection. The callers also ask for sensitive information and threaten enforcement action and fines if the restaurant fails to cooperate. The agencies said people should demand identification and not give sensitive information on the phone. Source: <http://www.vcstar.com/news/2010/jul/02/state-warns-restaurants-of-fake-food-inspectors/>

## **GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)**

**Loophole may have aided theft of classified data.** The soldier accused of downloading a huge trove of secret data from military computers in Iraq appears to have exploited a loophole in Defense Department security to copy thousands of files onto compact discs over a six-month period. In at least one instance, according to those familiar with the inquiry, the soldier smuggled highly classified data out of his intelligence unit on a disc disguised as a music CD by a popular female recording artist. The suspect is said to have smuggled data disguised as a music CD. A Defense Department directive from November 2008 prohibits the use of small thumb drives or larger external memory devices on any of the estimated seven million computers operated by the Pentagon and armed services. The order was issued to forestall the accidental infection of national security computer networks by viruses — and the intentional removal of classified information. But the Pentagon directive and the

UNCLASSIFIED

## UNCLASSIFIED

amendment did not ban the use of compact-disc devices, which are built into many computers and therefore not included in the prohibition against the use of external memory devices. Source:

[http://www.nytimes.com/2010/07/09/world/09breach.html?\\_r](http://www.nytimes.com/2010/07/09/world/09breach.html?_r)

**South Korean government websites, banks hit by suspected cyber attack.** Suspected cyber attacks paralyzed websites of major South Korean government agencies, banks and Internet sites in a barrage that appeared linked to similar attacks in the U.S., South Korean officials said July 6. The sites of the presidential Blue House, the Defence Ministry, the National Assembly, Shinhan Bank, Korea Exchange Bank and top Internet portal Naver went down or had access problems, said a spokeswoman at Korea Information Security Agency. The alleged attacks appeared to be linked to the knockout of service of websites of several government agencies in the United States. The U.S. sites were hit by a widespread and unusually resilient computer attack that began July 4. In the United States, the Treasury Department, Secret Service, Federal Trade Commission and Transportation Department Web sites were all down at varying points over the holiday weekend and into this week, according to officials inside and outside the government. Some of the sites were still experiencing problems late July 6. Some of the South Korea sites remained unstable or inaccessible on July 7. The spokeswoman said there have been no immediate reports of financial damage or leaking of confidential national information from the alleged cyber attack, which appeared aimed only at paralyzing websites.

Source: <http://www.theglobeandmail.com/news/technology/south-korean-government-websites-banks-hit-by-suspected-cyber-attack/article1210171/>

**(Iowa) Hackers pose as US senator in email fraud bid.** Fraudsters attempted to scam a US state senator's contacts after breaking into his webmail account. Contacts of the state senator from Iowa received a message from his Yahoo account claiming that the lawmaker was stranded in Scotland and in urgent need of financial help. The scam message claimed that the state senator needed £10,000 to pay hotel bills and, even more unlikely, was out of access by phone. The targeted individuals were invited to wire over money which would be collected by the hackers who broke into the state senator's Yahoo! email account. The senator told local news channel KCRG TV News that his Yahoo account was compromised as the result of a phishing scam. Source:

[http://www.theregister.co.uk/2010/07/08/us\\_politico\\_email\\_scam/](http://www.theregister.co.uk/2010/07/08/us_politico_email_scam/)

**(Washington) Three dead in Coast Guard helo crash.** Three members of a Coast Guard helicopter crew were killed in a crash off La Push, Washington on the morning of July 7 and a fourth crew member, who was pulled from the water soon after the aircraft went down, suffered a broken arm and a broken leg. The injured crewman was airlifted from Forks to Seattle's Harborview Medical Center. "He's awake and alert and very stable," a hospital spokeswoman said of the man, who arrived at 12:47 p.m. PDT. He was in satisfactory condition with what are believed to be non-life-threatening injuries. The MH-60 Jayhawk helicopter crashed around 9:30 a.m. off James Island near the mouth of the Quillayute River at the northwest tip of Washington state. Two crew members were quickly rescued by five members of the Quileute Nation, who jumped into fishing boats and raced to the crash scene. One of the rescued men died after being taken ashore. Source:

<http://www.military.com/news/article/two-missing-in-coast-guard-helo-crash.html?ESRC=topstories.RSS>

**(Hawaii) UH breach affects 53,000.** University of Hawaii (UH) officials said July 6 that a hacker breached the security of a parking office computer server that contained personal information of

UNCLASSIFIED

## UNCLASSIFIED

53,000 people. There were 40,870 Social Security numbers and 200 credit cards that were possibly compromised. So far, "there is no indication that any information was misused, downloaded or viewed by the hacker," who planted a virus on the computer server. Although officials do not know how it happened, they believe a site in China was involved. The matter was turned over to the Honolulu police, the FBI, and UH's forensics investigator. As a safety precaution, the spokesman said letters were mailed July 3 to affected people. In addition, an e-mail notice will be sent to people for whom the university does not have a mailing address. A routine audit June 15 discovered that someone gained unauthorized access May 30 to a computer server used by the UH parking office. Source:

[http://www.staradvertiser.com/news/hawaii/news/20100707\\_UH\\_breach\\_affects\\_53000.html](http://www.staradvertiser.com/news/hawaii/news/20100707_UH_breach_affects_53000.html)

**(North Carolina) Bomb scare empties Revenue building.** Suspicious packages were found in front of the North Carolina Department of Revenue service center and behind a residence July 6. Bomb squad officers were called to inspect a bag. The building was evacuated, but officers determined that the bag held dental equipment. Moments after the first call, a landscaper found a mortar round behind a home. Surrounding residences were cleared. Police found that the round was not live. Source:

<http://www.newsobserver.com/2010/07/07/568614/bomb-scare-empties-revenue-building.html>

**(Texas) Bullets strike El Paso, Texas city hall.** City officials in El Paso, Texa, said they were still in shock June 30, the day after bullets, possible fired across the U.S-Mexico border, struck the El Paso City Hall. Seven bullets struck the ninth-floor office of the assistant city manager on the west side of the building, the El Paso Times reported. The gunfire may have been stray shots from Juarez, Mexico, on the other side of the border, police said. There were about five people in the office having a meeting late June 29, the city manager said. She said when they realized it was a bullet, they hit the floor and vacated the office. One of the bullets came through the wall and knocked over a picture frame, the El Paso Times reported. The city manager said safety procedures would be put in place.

Source: [http://www.upi.com/Top\\_News/US/2010/06/30/Bullets-strike-El-Paso-Texas-city-hall/UPI-70401277948500/](http://www.upi.com/Top_News/US/2010/06/30/Bullets-strike-El-Paso-Texas-city-hall/UPI-70401277948500/)

**(Texas) DPS investigates bomb threat at Texas Capitol.** The Texas Department of Public Safety has reopened the Capitol to visitors and workers, many hours after a bomb threat was called in. The call was made around 7 a.m. July 2, according to state troopers. They say a man made the call from a payphone. He said bombs were in the east and west wings of the building and they were set to go off at 9 a.m. The building was evacuated and put on lock-down with no one allowed inside until after a complete search was conducted. This is the second bomb threat in less than a month on the Capitol. DPS troopers evacuated and searched the Capitol June 18 after someone called 911 to report a bomb threat. Nothing was found after an extensive search that closed the Capitol for several hours. Source: [http://www.myfoxtampabay.com/dpps/news/national/DPS-Investigates-Bomb-Threat-at-Texas-Capitol-20100702-ktbcw\\_8451072](http://www.myfoxtampabay.com/dpps/news/national/DPS-Investigates-Bomb-Threat-at-Texas-Capitol-20100702-ktbcw_8451072)

**Social Security Numbers of 3,500-Plus Guard Members at Risk** The Oregon National Guard continues to deal with the aftermath of a stolen laptop computer that contained the names and Social Security numbers of more than 3,500 soldiers. The last of the notification letters were mailed today to individuals whose personal information was on the laptop, which was reported stolen from a Guard member's vehicle June 21 in the Portland area. The Guard member was using the laptop to conduct work from home. Maj. Gen. Raymond F. Rees, adjutant general Oregon, has asked for a review of

UNCLASSIFIED

laptop procedures and policies as a result of the incident. Full Article:

<http://www.statesmanjournal.com/article/20100701/UPDATE/100701064/Social-Security-numbers-of-3-500-plus-Guard-members-at-risk>

## **INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**GAO slams White House for failing to lead on cybersecurity.** The Government Accountability Office (GAO) said in a report released this week the U.S risks falling behind other countries on cybersecurity matters. The report highlighted the U.S. being unable to adequately protect its interests in cyberspace, and that the White House Office of Science and Technology Policy has so far failed to live up to its responsibility to coordinate a national cybersecurity R&D agenda. The GAO report was prepared at the behest of the House Committee on Homeland Security, and called on the OSTP to show more leadership in pulling together a focused and prioritized short, medium- and long-term R&D strategy for cybersecurity. Source:

[http://www.computerworld.com/s/article/9178959/GAO\\_slams\\_White\\_House\\_for\\_failing\\_to\\_lead\\_on\\_cybersecurity](http://www.computerworld.com/s/article/9178959/GAO_slams_White_House_for_failing_to_lead_on_cybersecurity)

**Germany may fine Facebook over privacy issues.** Facebook faces a fine from the Hamburg, Germany, Commissioner for Data Protection and Freedom of Information for failing to obtain the consent of the people whose contact details it stores. At issue are the site's invitation and address-book synchronization functions, through which it uploads and stores contact information from the e-mail and mobile phone address books of its users. The problem is that some of that personal information relates to people who are not Facebook users, and who have not given their permission for the site to store their personal information, nor use it for marketing purposes. Many citizens of the German state of Hamburg have complained in recent months of Facebook passing their contact information to third parties and storing information about their relationships in this way. Such storage of data by third parties is "inadmissible" because of its implications for data protection, said the head of the state's data protection service. Facebook did not immediately respond to a request for comment. Facebook has until August 11 to make its case to the data protection commissioner if it wishes to avoid a fine. Source:

[http://www.computerworld.com/s/article/9178984/Germany\\_may\\_fine\\_Facebook\\_over\\_privacy\\_issues](http://www.computerworld.com/s/article/9178984/Germany_may_fine_Facebook_over_privacy_issues)

**Apple: 400 iTunes accounts hacked.** Apple now admits 400 iTunes accounts were hacked and used by a Vietnamese developer to push his iPhone apps to best seller status over the weekend by purchasing his own apps using hacked iTunes accounts. At one point, the developer's apps occupied 42 of the top 50 apps sold in the Books section, and users reported purchases of up to \$500 with their accounts. Apple downplayed the attack, however, pointing out that 400 accounts equals 0.0003 percent of the over 150 million iTunes account holders. The downplaying of the hack comes as little consolation to many who believed Apple's walled garden would offer protection from rogue developers and hackers. The hacker's apps had been removed from the App Store because he "violat[ed] the developer Program License Agreement, including fraudulent purchase patterns," Apple said. The company also claims that its iTunes servers were not compromised in any way. Source:

[http://www.pcworld.com/article/200618/apple\\_400\\_itunes\\_accounts\\_hacked.html](http://www.pcworld.com/article/200618/apple_400_itunes_accounts_hacked.html)

## UNCLASSIFIED

**Google confirms attack on YouTube.** Malicious hackers attacked Google's YouTube July 4, exploiting a cross-site scripting (XSS) vulnerability on the ultra-popular video sharing site, hitting primarily sections where users post comments. The attack potentially put at risk YouTube cookies of users who visited a compromised page, but it could not be used to access their Google account. The attackers apparently targeted a teen singing sensation, incorporating code into YouTube pages devoted to him so that visitors saw tasteless messages pop up about the teen star, and were also redirected to external sites with adult content. An industry source familiar with the situation said that while the attack itself didn't involve malware infections, such a risk is inherent whenever users visit any Web page, such as the ones attackers redirected users to. It is not clear if those landing pages contained malware, but most up-to-date anti-virus software is designed to protect against those threats.

Source: [http://www.computerworld.com/s/article/9178861/Google\\_confirms\\_attack\\_on\\_YouTube](http://www.computerworld.com/s/article/9178861/Google_confirms_attack_on_YouTube)

**Tabnapping on the increase.** The use of Tabnapping, a recently-identified phishing technique, is on the rise, says Panda Labs. Tabnapping exploits tabbed browser system in modern Web browsers such as Firefox and Internet Explorer, making users believe they are viewing a familiar Web page such as Gmail, Hotmail or Facebook. Cybercriminals can then steal the logins and passwords when users enter them on the hoax pages. According to Panda's latest Quarterly Report on IT Threats, the technique is likely to be employed by more and more cybercriminals, and users should close all tabs they are not actively using. Panda also revealed the number of Trojans being used on the Web has surged, and they now account for about 52 percent of all malware. The number of viruses has also increased. Viruses account for 24 percent of all Web malware. The security firm said Taiwan had the most number of infections, with just over 50 percent of all global infections happening in the country, while Russia and Turkey were close behind. Panda also noted that attacks on social networks, fake-antivirus software and poisoned links in search engines continued to be popular techniques used by cyber criminals. Source: <http://www.networkworld.com/news/2010/070110-tabnapping-on-the.html?hpg1=bn>

**Microsoft Office 2010 security flaw reportedly found.** Researchers at Vupen Security say they have uncovered a security vulnerability in Microsoft Office 2010. However, their discovery has been met with criticism from Microsoft, which complains that it has not received technical details of the bug. Microsoft officials are upset researchers chose not to notify the company of their findings. The Vupen researchers said they discovered a memory-corruption flaw that could be used by an attacker to execute code. The company June 22 said it "created a code execution exploit which works with Office 2010 and bypasses DEP (Data Execution Prevention) and Office File Validation features." The bug, the Vupen CEO told eWeek, is caused by a heap-corruption error when processing malformed data within an Excel document. While technical details of the bug have not been disclosed, Vupen said, "our [government] customers who are members of the Vupen Threat Protection Program have access to the full binary analysis of the vulnerability" as well as detection guidance. But Vupen has not given the vulnerability details to Microsoft. Source: <http://www.eweek.com/c/a/Security/Microsoft-Office-2010-Security-Bug-Reportedly-Found-323576/>

**Spam now a vehicle for heavy malware distribution.** AppRiver released a detailed summary and analysis of spam and malware trends traced between January and June 2010. During this timeframe, they quarantined more than 26 billion spam messages to protect its customer base of 45,000 corporations and six million mailboxes. "Spam today is much more than just a nuisance, it is a vehicle for heavy malware distribution and other serious security threats," said the senior security analyst at

UNCLASSIFIED

## UNCLASSIFIED

AppRiver. “For example, more than 1-in-10 junk messages contained a virus during the past six months, making malware distribution a serious cause for concern. With many countries now on board with the cap and trade system, scammers have found a lucrative opportunity to exploit the global quest to go green. Source: [http://www.net-security.org/malware\\_news.php?id=1393](http://www.net-security.org/malware_news.php?id=1393)

**Phishing under the name of Wikipedia.** A new HTML phishing scam has seen a large number of spam e-mails prompting recipients to verify an alleged Wikipedia account by clicking on a link that appears to point to the official Wikipedia site. The e-mails contain such texts as “Someone from the IP address 112.135.3.205 has registered the account ‘iamjustsendingthisleter’ with this e-mail address on the English Wikipedia”, where the IP address corresponds to that of the spamming computer (bot), and the alleged Wikipedia account is the spam recipient’s e-mail account. While the included links appear to lead to the trusted service, when clicked, they take users to infected Web sites that the perpetrators may have injected with all sorts of dubious content, for example pill advertisements, malicious JavaScript code, or both. Source: <http://www.h-online.com/security/news/item/Phishing-under-the-name-of-Wikipedia-1032341.html>

## **NATIONAL MONUMENTS AND ICONS**

**(California) California Park closed after plague-infected squirrel found.** The Los Alamos Campground in the Angeles National Forest in California will be closed for the next eight days as officials investigate a case of a squirrel testing positive for the plague. The animal was captured two weeks ago. While the park is closed, squirrel burrows will be dusted for fleas, which can spread the bacterial disease. The public health director for Los Angeles County said that although wild rodents can pass the infection on to humans through fleas, there have been only four cases of humans coming down with the plague in the county since 1984. None of those cases were fatal, he said. County and National Park officials are warning visitors to stay clear of animal burrows and to avoid rodents, including chipmunks and squirrels. Visitors should also use an insect repellent while in the park. Source: <http://www.allheadlinenews.com/articles/7019199044>

## **POSTAL AND SHIPPING**

**Anthrax hoax cases pile up across the U.S., arrests lag.** Mailing a white powdery substance to scare people can land one in prison — even if the enclosed substance is non-toxic. Police and the FBI have responded to at least a dozen “white powder” cases in Boise, Idaho since 2003, with the most recent occurring at the U.S. attorney’s office June 14. Neither Boise police nor the FBI could say last week how many arrests have been made in connection with these crimes, though they did confirm there had been no arrests in the past two years. There have been some hoax case convictions this year in other parts of the country. Reports nationwide tapered off significantly after 2002 and have been dropping every month — until the past few months, an FBI spokesman in Washington, DC said. There were about 500 reports in 2008. Investigators have found there is a flurry of these cases after “key events,” such as the blackout in the Northeast, the Enron scandal and Hurricane Katrina. The oil spill in the Gulf of Mexico could be another key event. Typical targets include elected officials, government organizations and the media. Law enforcement officials treat every case as a serious threat. The hoaxes sap local and federal law enforcement, diverting them from investigations and other real emergencies. Source: <http://www.idahostatesman.com/2010/07/05/1256479/anthrax-hoax-cases-pile-up-arrests.html#ixzz0suJMipGy>

UNCLASSIFIED

## UNCLASSIFIED

**(Georgia) Teens hospitalized after pipe bomb explosion now face charges.** Two Augusta, Georgia teens sent to the hospital after a pipe-bomb explosion now face charges in Richmond County, Georgia. The two 17-year-olds have been charged with manufacturing explosive devices. The teens, who were rushed to Doctors Hospital with respiratory problems after a chlorine-filled pipe bomb exploded in front of them July 1 in McCormick County, may have been planning to blow up a mailbox, the Columbia County fire chief said. The teens stopped at a Wife Saver restaurant on their drive from McCormick County back to Augusta to wash the chemicals from the explosion off them, and employees found them struggling to breathe in the bathroom. The WifeSaver on Belair Road in Martinez was evacuated for about two hours while a hazardous-materials team checked the area. Source: <http://www.nbcaugusta.com/news/georgia/97642929.html>

## **PUBLIC HEALTH**

**J&J recalls more Tylenol, over-the-counter drugs.** Johnson & Johnson (JNJ.N) recalled more Tylenol and other over-the-counter drugs on July 8 after they were linked to a musty or moldy odor, expanding a recall the company started in January. J&J's Consumer Healthcare unit said the latest recall involved 21 lots of medications, including Tylenol for children and adults, several forms of Benadryl allergy tablets and Motrin painkiller. But it did not say how many pieces were in each lot or give a total number of items involved. The lots were sold in the United States, Fiji, Guatemala, the Dominican Republic, Puerto Rico, Trinidad and Tobago and Jamaica, J&J said. On June 15, J&J recalled four lots of Benadryl and one lot of Extra Strength Tylenol gels. Consumer complaints of odors traced to a chemical called TBA present in wooden pallets used to ship and store the medications led to the January recall. Source: <http://www.reuters.com/article/idUSN0823008420100708>

**HHS proposes new privacy, security rules.** The Department of Health and Human Services (HHS) secretary announced July 8 new proposed privacy and security rules and resources. The secretary said they would strengthen the privacy of health information and help all Americans understand their rights and the resources available to safeguard their personal health data. The rules are part of an effort led by the Office of the National Coordinator for Health Information Technology (ONC) and the HHS Office for Civil Rights (OCR) to ensure Americans trust personal health data exchange. The proposed rules come as part of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to ensure broader individual rights and stronger protections when third parties handle individually identifiable health information. Source: <http://www.healthcareitnews.com/news/hhs-proposes-new-privacy-and-security-rules>

**Advance in Quest for HIV Vaccine.** HIV research is undergoing a renaissance that could lead to new ways to develop vaccines against the AIDS virus and other viral diseases. In the latest development, U.S. government scientists say they have discovered three powerful antibodies, the strongest of which neutralizes 91% of HIV strains, more than any AIDS antibody yet discovered. They are now deploying the technique used to find those antibodies to identify antibodies to influenza viruses. The HIV antibodies were discovered in the cells of a 60-year-old African-American gay man, known in the scientific literature as Donor 45, whose body made the antibodies naturally. The trick for scientists now is to develop a vaccine or other method to make anyone's body produce them as well. Vaccines, which are believed to work by activating the body's ability to produce antibodies, eliminated or

UNCLASSIFIED

## UNCLASSIFIED

curtailed smallpox, polio and other feared viral diseases, so they have been the holy grail of AIDS research. Source:

[http://online.wsj.com/article/SB10001424052748703609004575355072271264394.html?mod=WSJ\\_hpp\\_LEFTTopStories](http://online.wsj.com/article/SB10001424052748703609004575355072271264394.html?mod=WSJ_hpp_LEFTTopStories)

**(Arizona) Dirty fungus threatens Arizonan's health.** Desert dwellers are at high risk of becoming infected with a fungus which thrives in the hot and arid southwest. The fungus *Coccidioidomycosis* causes valley fever. According to the Department of Health Services, valley fever represents 59 percent of the total infectious diseases reported in Arizona this year. The fungus is found in soil and lives just inches to a few feet beneath the surface, which means it can be easily stirred into the air by things like construction and even just wind. University of Arizona Valley Fever specialist said about 100,000 Valley Fever infections occur in Arizona. About two thirds of people who get infected have either no illness or an illness so mild that they don't bother to go to a doctor. The other third have an illness that is typically described as a pneumonia. Symptoms of Valley fever include fever, cough, chest pain that can range from mild constriction to intense pressure, chills, night sweats, headache, fatigue, shortness of breath, joint aches and a red, spotty rash. That rash is made up of painful red bumps and is usually on the lower legs, although it can show up on the chest, arms and back. Source: <http://www.azfamily.com/news/health/Dirty-fungus-threatens-Arizonans-health-97848129.html>

**White House orders pathogen policy changes.** The White House says the President has ordered fundamental changes in the way hazardous pathogens and toxins in the United States are secured against misuse. Research on Biological Select Agents and Toxins is critical for the development of tools to detect, diagnose, recognize and respond to outbreaks of infectious disease of both natural and deliberate origin, the White House said July 2. The expansion in the last 10 years of the infrastructure and resources dedicated to BSAT work, coupled with the discovery that the perpetrator of the 2001 anthrax attacks may have been a U.S. government employee, underlines the need to ensure BSAT are properly secured against possible misuse or attempts to harm people, animals, plants, or the environment, administration officials said. Source: [http://www.upi.com/Science\\_News/2010/07/02/White-House-orders-pathogen-policy-changes/UPI-65131278109924/](http://www.upi.com/Science_News/2010/07/02/White-House-orders-pathogen-policy-changes/UPI-65131278109924/)

**Media reports influence the severity of pandemics.** The widespread fear that various pandemics are set to devastate the human race has led to another kind of outbreak: a rash of models predicting how various diseases will spread through society. These models are valuable. They allow governments to estimate how badly their society will be influenced and to make emergency plans accordingly. Now students at Marshall University and Howard Weiss at Georgia Tech examine the effectiveness of another tool: the media. To test their hypothesis, they simulated the effect of an outbreak of Ebola fever in the West Virginia town of Huntington which has a population of 50,000. They used a standard model which counts the number of susceptible and infected individuals and the number of "removed" individuals, those that either die or recover and become immune, and models the rate at which people jump from one pool to another. They also add one additional assumption to this model: that the number of individuals who self-isolate increases with the number of infections reported by the media. So the idea is that public health agencies constantly update the media about the number of infections, which then immediately pass on the information to the general population. When that happens, the result is a dramatic decrease in the severity of the outbreak. The more up-to-date the

UNCLASSIFIED

## UNCLASSIFIED

information, the greater this effect. Source: <http://homelandsecuritynewswire.com/media-reports-influence-severity-pandemics>

**U.S. lacks unified bioterrorism detection framework, auditors find.** The U.S. Administration should pursue a national plan to develop a monitoring system for bioterrorism incidents and other disease threats, the U.S. Government Accountability Office said in a report released July 1. The United States lacks an overarching strategy for developing a “national biosurveillance capability,” says the report, which examines federal biological threat detection initiatives, policies and tactics, as well as official testimony from 12 federal departments overseeing the programs. “Efforts to develop a national biosurveillance capability could benefit from a national biosurveillance strategy that guides federal agencies and other stakeholders to systematically identify risks, resources needed to address those risks and investment priorities,” congressional auditors stated. Source: [http://www.globalsecuritynewswire.org/gsn/nw\\_20100702\\_7700.php](http://www.globalsecuritynewswire.org/gsn/nw_20100702_7700.php)

## **TRANSPORTATION**

**Feds: Subway bomb plot linked to British cell.** A failed plot to set off bombs in the New York subway system last year was part of a larger al-Qaida terrorist conspiracy that planned a similar attack in England, U.S. prosecutors said Wednesday. In an indictment unsealed Wednesday, prosecutors added several al-Qaida figures to the case, including an FBI most-wanted terrorist. One of the al-Qaida leaders in charge of plotting attacks worldwide was directly involved in recruiting and plotting the New York attack, prosecutors said. The U.S. attorney general has called that plot one of the most dangerous since the terrorists attacks of September 11, 2001. Two of the men indicted Wednesday were linked to a previously undisclosed companion plot in England. Three U.S. citizens were arrested in September 2009 before, prosecutors said, they could carry out a trio of suicide bombings in Manhattan. The men have pleaded guilty and admitted planning to detonate homemade bombs on the subway during rush hour. Source: <http://www.crainsnewyork.com/article/20100707/FREE/100709908/0/WB01#>

**(Texas; International) Texas-Mexico bridges close as Rio Grande rises.** Laredo officials are closing a second international bridge as the Rio Grande swells from the remnants of Hurricane Alex and releases from reservoirs upstream. The Colombia Bridge, which connects the city’s northwestern edge to Nuevo Leon, will close at 6 p.m. Wednesday evening. The city has already shut down the bridge that connects its downtown to that of Nuevo Laredo, Mexico. No buildings in Laredo were immediately in danger, but a city spokeswoman says officials could order some low-lying houses evacuated. Damage on the Mexican side of the river has been more severe. Tens of thousands have been forced to evacuate, and the mayor of Piedras Negras — across from Eagle Pass — and four others died when their plane crashed as they inspected flooded areas. Source: <http://www.kxii.com/txnews/headlines/97995229.html>

**(Pennsylvania) Barge hits Philadelphia ‘duck boat’ carrying 37; 2 people missing.** Authorities halted an hours-long search for two people missing Wednesday after a barge hit a tourist boat carrying 37 people on the Delaware River, authorities said. The search resumed Thursday morning for the 20-year-old man and 16-year-old girl, both from Hungary, officials said. They were among 35 passengers and two crew members aboard the amphibious “duck boat,” which gives tourists a water-and-land

## UNCLASSIFIED

## UNCLASSIFIED

view of Philadelphia, a Coast Guard senior chief said. The duck boat had driven into the water just after 2:30 p.m. and suffered a mechanical problem and a small fire, officials said. It was struck about 10 minutes later by a barge used to transport sludge, then sank. Source:

<http://www.washingtonpost.com/wp-dyn/content/article/2010/07/07/AR2010070705250.html>

**TSA to U.S. soldiers: Don't pack grenades.** The U.S. Transportation Security Administration (TSA) offered a reminder Tuesday to military members: When flying commercial, don not pack explosives — live or inert. “Prohibited items include blasting caps, dynamite, fireworks, flares, hand grenades, and explosives, either real or replicated,” the TSA said in a statement released by the Defense Department. A TSA spokesman said agency workers sometimes find inert grenades or other items packed by service members on commercial flights “as a keepsake from the battlefield.” “The problem is, when you're looking at that through an X-ray machine, you can't tell the difference” whether it's a live or inert grenade, the spokesman said. When TSA officers discover explosives, she said, they sometimes have to close checkpoints or baggage areas or call in bomb squads.

Source: [http://www.upi.com/Odd\\_News/2010/07/06/TSA-to-US-soldiers-Dont-pack-grenades/UPI-32641278469333/](http://www.upi.com/Odd_News/2010/07/06/TSA-to-US-soldiers-Dont-pack-grenades/UPI-32641278469333/)

**(New York) JFK terminal evacuated due to bomb scare.** A terminal was evacuated at the John F. Kennedy International Airport July 4 due to a bomb scare. “Only Terminal 1 was evacuated from 6:00 p.m. till 8:30 p.m. due to a bomb threat,” reported the airport's website during the scare. An unidentified caller tipped off the authorities, reported AFP, and an unattended piece of luggage was found during the search, leading to the evacuation of the terminal. The search of the bag revealed no bomb inside, officials said. The airport and the terminal are operating under normal conditions, an official subsequently told AFP. The incident proved problematic for travelers, as well as the airport, as the July 4 weekend is one of the busiest travel periods of the year. Airports across the United States placed increased security measures over the Independence Day holiday, noted AFP. Source:

<http://www.theepochtimes.com/n2/content/view/38600/>

**Cruise ship security bill clears Congress.** A bill that requires cruise ships to tighten security measures and report alleged crimes is awaiting the President's approval. The Senate June 30 passed the Cruise Vessel Security and Safety Act. The legislation received broad bipartisan support in the House with a vote of 416-4 last year. Peepholes on cabin doors, rails no lower than 42 inches and information packets on how to report crimes are some of the changes commercial cruise passengers can expect to see after the law takes effect. Ships built after the bill's passage must be equipped with security latched and time-sensitive key technology. The bill applies to all ships that dock in U.S. ports. Those ships will also be required to immediately report incidents to the FBI or the U.S. Coast Guard, whether the incident occurs on the high seas or at port. Source:

<http://www.cnn.com/2010/TRAVEL/07/01/cruise.ship.bill/>

**U.S. aircraft portable-missile defense may cost \$43 billion.** Arming U.S. passenger aircraft to deter shoulder-fired missiles may cost \$43.3 billion over 20 years, the Homeland Security Department says in an unpublished report that may reignite debate about the vulnerability of planes to terrorists. Airlines said the expense exceeds the risk, and oppose installing the systems. The missiles “could easily be smuggled into an airport in a western country,” said the manager of the arms-sales project of the Federation of American Scientists, which calls the portable weapons “an imminent and acute

UNCLASSIFIED

## UNCLASSIFIED

threat” to airliners. The Washington group disclosed the report after obtaining it through a Freedom of Information Act request. The systems foil attacks by using lasers to deflect heat-seeking missiles. The \$43.3 billion estimate is based on installing, operating and maintaining the defense systems on all large passenger planes, which the report defines as wide-body aircraft, and narrow-body planes the size of the Boeing 737 and Airbus A318 and larger. The cost equals almost \$12 million over 20 years for each plane, based on 3,636 aircraft as of 2008. An attack on a U.S. passenger plane by a shoulder-fired missile would have an economic cost of more than \$15 billion, assuming it led to a week-long shutdown of airspace, according to a 2005 report by the Rand Corporation. Source: <http://www.businessweek.com/news/2010-07-02/u-s-aircraft-portable-missile-defense-may-cost-43-billion.html>

## **WATER AND DAMS**

**(Texas; International) Mexico, Texas evacuate homes as Rio Grande floods.** Reservoirs along the U.S.-Mexico border have reached their highest levels in decades following days of drenching rain. That has forced officials to dump water into flooded rivers, with yet another storm on the way. Mexican officials evacuated nearly 18,000 people from houses in Ciudad Anahuac for fear that water would overflow the Venustiano Carranza dam and threaten lives. Water behind the binational Amistad Dam on the Rio Grande was at its highest level since 1974, according to the International Boundary and Water Commission, forcing officials to release water from it at the fastest rate in a quarter century. The Commission said the downstream Falcon dam would probably reach capacity within the next few days, suggesting future releases there will raise water levels along the river’s lower reaches. Much of that downstream area is protected against flooding by levees, but Mexico’s National Water Commission said it was worried about low-lying settlements, most built by poor people without official permission. Twenty floodgates had been opened by late Tuesday at the Venustiano Carranza Dam, which was releasing 600 cubic meters per second into the Salado River, a tributary of the Rio Grande. Officials were also evacuating 2,000 people near the swollen Rio Escondido. In Texas, authorities evacuated the Vega Verde neighborhood of Del Rio as more water was being released from the Amistad Lake, just upstream. One of three international bridges connecting Laredo, Texas and Nuevo Laredo, Mexico, was ordered closed as the Rio Grande rose dramatically. The water is expected to rise to 38.5 feet — high enough to touch but not run over the bridge. Source: [http://www.google.com/hostednews/ap/article/ALeqM5iJtis-T41gWr2Rm65LgE\\_HTKE3GgD9GQCAP80](http://www.google.com/hostednews/ap/article/ALeqM5iJtis-T41gWr2Rm65LgE_HTKE3GgD9GQCAP80)

**African, Asian nations top latest Water Security Risk Index.** Somalia has the least secure water supply while Iceland has the most stable in the world, according to a survey of 165 nations released last week by Maplecroft, a Britain-based consultancy company. The study, the Water Security Risk Index, featured three other African nations, including Mauritania, Sudan and Niger, as well as Iraq, Uzbekistan, Pakistan, Egypt, Turkmenistan and Syria. Population growth and climate change will further exacerbate water supplies and negatively impact industrial and agricultural sectors, according to the report. The index measured four inputs: access to improved drinking water and sanitation, availability of supplies and dependence on external sources, balance between supply and demand, and the dependence of each nation’s economy of water availability. These findings echo previous reports that areas with transboundary water sources have an elevated risk of conflict. “When water becomes scarce it turns into a commodity that people fight for. It also generates corruption due to its dwindling supply that is often controlled by businesses, governments, or criminals and insurgents,”

UNCLASSIFIED

# UNCLASSIFIED

the deputy director and senior fellow of the Transnational Threats Project at the Center for Strategic and International Studies, told Circle of Blue. The report also emphasizes that insecurity stems largely from uncertain and inconsistent supplies. Source:

<http://www.circleofblue.org/waternews/2010/world/african-asian-nations-top-latest-water-security-risk-index/>

## **NORTH DAKOTA HOMELAND SECURITY CONTACTS**

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **Fusion Center (24/7):** 866-885-8295(IN ND ONLY); Email: [ndslic@nd.gov](mailto:ndslic@nd.gov) ; Fax: 701-328-8175

**State Radio:** 800-472-2121 **Bureau of Criminal Investigation:** 701-328-5500 **Highway Patrol:** 701-328-2455

**US Attorney's Office Intel Analyst:** 701-297-7400 **Bismarck FBI:** 701-223-4875 **Fargo FBI:** 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security [kihagel@nd.gov](mailto:kihagel@nd.gov), 701-328-8168



UNCLASSIFIED

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**