

UNCLASSIFIED



# NORTH DAKOTA HOMELAND SECURITY ANIT-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

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](#)

[Regional](#)

[National](#)

[International](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous Materials  
Sector](#)

[Commercial Facilities](#)

[Communications Sector](#)

[Critical Manufacturing](#)

[Defense Industrial Base Sector](#)

[Emergency Services](#)

[Energy](#)

[Food and Agriculture](#)

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

[Information Technology and  
Telecommunications](#)

[National Monuments and Icons](#)

[Postal and Shipping](#)

[Public Health](#)

[Transportation](#)

[Water and Dams](#)

[North Dakota Homeland Security  
Contacts](#)

UNCLASSIFIED

## UNCLASSIFIED

### **NORTH DAKOTA**

**Driver rolls semi near Hurdsfield, ND.** The driver of a semi-tractor trailer has been hospitalized following a June 13 accident on Highway 200 near Hurdsfield, North Dakota. The highway patrol said the driver failed to negotiate a curve about 2 miles west of Hurdsfield. The man began to enter the north ditch and over-corrected by turning to the left. The tractor and trailer then rolled a half turn, coming to rest facing south with part of the tractor on the roadway obstructing some of the westbound traffic. The trailer came to rest in the north ditch. It leaked a majority of its haul of liquid fertilizer, but the leak was contained by responding firefighters. The fertilizer is not considered to be hazardous, but a patrol sergeant did not immediately have details on the type of fertilizer or how much spilled. The crash is still under investigation.

Source: [http://www.wday.com/event/article/id/9052/group/News/publisher\\_ID/30/](http://www.wday.com/event/article/id/9052/group/News/publisher_ID/30/)

### **REGIONAL**

**(Minnesota) Plymouth broker is third to be charged in Cook's Ponzi scheme.** A Plymouth, Minnesota, securities broker was charged June 13 in a Minneapolis federal court with securities fraud, wire fraud conspiracy, and money laundering in connection with another man's \$194 million Ponzi scheme. The 54-year-old man is the third person to be criminally charged in connection with the scheme but may not be the last. The charges were filed by way of "criminal information" rather than indictment, and search warrant documents filed in May suggest that the securities broker is helping the government investigate his former associates. According to the charges filed against the man, for 6 months in 2008 he conspired with others to pitch a fraudulent foreign currency investment program, which led to losses of more than \$150 million for nearly 1,000 investors, mostly retirees. He used his position as a licensed securities broker to lend credibility to the program, the U.S. attorney's office said in a statement June 13. He faces up to 10 years in prison on the money-laundering charge, and 5 years each on the securities fraud and conspiracy charges. Source:

<http://www.startribune.com/business/123787849.html>

**(Minnesota) Juveniles arrested in Roseau school fire.** Two juveniles appeared in court the week of June 6 in Roseau, Minnesota, on charges related to a fire set at the Roseau High School June 6. According to a news release from the Roseau Police chief, the two juveniles were arrested June 7 after an investigation into the fire, which damaged rubber roofing and insulation at the school. Officials at the school reported the damage June 7. The fire, thought to have been set June 6, was out by the time the damage was reported. Source:

<http://www.grandforksherald.com/event/article/id/206214/group/homepage/>

**(Montana) Montana halts search for militia member.** Montana authorities June 14 scaled down a search for a militia member accused of firing on two sheriff's deputies, saying the practiced survivalist and ex-convict could easily have traveled dozens of miles through the

UNCLASSIFIED

## UNCLASSIFIED

state's jagged western mountains. Missoula County sheriff's deputies saw a Jeep Cherokee run a stop sign June 12 and gave chase once it refused to pull over. The 47-year-old man led his pursuers off-road into the mountains, jumped out when he got stuck, and opened fire on the deputies with a handgun, authorities said. He then fled into the thick forest near Lolo, just southwest of Missoula. The man was convicted of weapons violations in 2002 as part of a federal investigation into a militia group called Project 7, which targeted law enforcement, according to an FBI report on domestic terrorism. He served 8 years in federal prison before his release in March 2010. Among the terms of his release was a prohibition on carrying firearms. Source: <http://www.latimes.com/news/nationworld/nation/la-na-militia-fugitive-20110615,0,7994391.story>

**(Montana) Increased water release from Fort Peck Dam continues.** The recent storms have forced the U.S. Army Corps of Engineers to continue to increase the amount of water released from the Fort Peck Dam in Fort Peck, Montana. On June 12, the dam was releasing 65,000 cubic feet per second (cfs). That is an increase from 60,000 cfs June 11. The Fort Peck reservoir met the water level record at 2,251.6 feet mean sea level, previously set in 1975. A Corps Fort Peck spokeswoman said, "we've just been getting so much rain and coupled with the snow melt forecasted levels are high, so we need to be releasing water to keep it in better balance between Fort Peck and Garrison Dam." There is still 80 percent snow pack above Fort Peck waiting to melt. Plus officials said more rain is on the way, so it does not look like the water levels will drop anytime soon. Source: <http://www.kfbb.com/news/local/Increased-Water-Release-from-Fort-Peck-Dam-Continues-123722184.html>

**(Iowa; South Dakota) Gavins Point Dam opens to maximum planned release (video).** The Gavins Point Dam in South Dakota began releasing 150,000 cubic feet per second of water through its spillways June 14 — the maximum release, according to the U.S. Army Corps of Engineers — feeding the swollen Missouri River and dumping a record amount of water on riverside communities downstream. The river at Yankton, South Dakota was 5 feet above flood stage the evening of June 14, according to the U.S. Geological Service. Overall, the Corps is anticipating that it will have to move twice as much water in 2011 through the river system above Sioux City, Iowa, as it normally does: 52 million acre-feet compared with an annual average of about 25 million acre-feet, said the Corps' operations director for the dam. Source: <http://www.argusleader.com/article/20110615/NEWS/106150318/Water-pushes-Gavins-Point-Dam-limit-video-?odysey=nav|head>

**(South Dakota) Levees protecting S.D. from the Missouri River holding, but gov. urges people to remain cautious.** Emergency earthen levees built to protect southeast South Dakota from the rising Missouri River were holding back the floodwaters as increased water releases from Gavin's Point Dam west of Yankton, South Dakota began reaching the area, officials said June 15. South Dakota's governor said levees also were holding strong in the Pierre and Fort Pierre areas, where earlier releases were increased to record levels on Oahe Dam a few miles upstream near Pierre. But the governor urged residents to remain cautious, pointing to recent levee ruptures in northwest Missouri, which show the situation can change quickly. The U.S.

UNCLASSIFIED

## UNCLASSIFIED

Army Corps of Engineers is pushing 150,000 cubic feet of water per second through both the Oahe and Gavin's Point dams. The goal is to get rid of unexpectedly heavy rains that fell upstream in May in eastern Montana and Wyoming, and western North Dakota and South Dakota. Source:

<http://www.therepublic.com/view/story/4be57da7d6ef474096a89ba114fb5e46/SD--Missouri-River-Flooding-South-Dakota/>

**(South Dakota) Dakota Dunes levees are near complete as flood waters rise.** Hundreds of people followed a non-mandatory evacuation order the week of June 6 in Dakota Dunes, South Dakota. The interstate exit to the Dunes has been closed ever since. South Dakota's governor said June 11 that as the levee work is completed, road access will open up again. He also said the real test of the levee's hold has not come yet, and noted officials do not want to let people back in until they know the levee will not breach. "Even as it's being finished in the next couple of days, it'll feel the full force of the 150 cfs (cubic feet per second) flow Tuesday and Wednesday of this week." the governor said June 11. Source:

<http://www.ktiv.com/story/14888305/the-test-of-dakota-dunes>

## **NATIONAL**

Nothing Significant to Report

## **INTERNATIONAL**

**New dam breach eyed in Manitoba.** The Hoop and Holler dam in the Canadian province of Manitoba might be intentionally breached again within days because of heavy Assiniboine River flows, partly due to another expected severe rainfall and a saturated ground. The Provincial Emergency Measures Minister said June 10 a decision will be made once the rain — up to 30 millimeter forecast for the already swollen Souris and Assiniboine river basins — falls June 12 and June 13. "What that translates into is our ability to flow those waters through the Assiniboine River and the Portage Diversion," he said at the legislature, predicting a flow of about 53,000 cubic feet per second or more into an area where an outlet runs north from near Portage la Prairie to Lake Manitoba. Meanwhile, an evacuation alert has been issued to 45 residents near the Portage Diversion. The provincial government intentionally broke the dike at the Hoop and Holler Bend May 14 to do what it claimed was needed to relieve the Assiniboine's pressure on its banks, and avert a possibly catastrophic flood downstream toward Headingley. That breach, just west of the village of Newton, along an Assiniboine River oxbow, remained for several days before it was closed. Source: <http://www.torontosun.com/2011/06/11/new-dam-breach-eyed-in-manitoba>

**Woman hurt in blast at Ikea store in Germany.** An explosive device went off in an Ikea furniture store in the German city of Dresden June 10, slightly injuring one person, a police

UNCLASSIFIED

## UNCLASSIFIED

spokesman told Agence France-Presse June 11. At the end of May, several small booby-trapped packages exploded in Ikea stores in France, Belgium, and The Netherlands, with no claim of responsibility. At least one woman suffered damage to her eardrum in the June 10 blast in the kitchen showroom part of the store, a police spokesman said. The explosion went off during the store's opening hours, a spokeswoman for Ikea in Germany said. But the police official said it was too early to say whether the latest blast had any connection with the May 30 explosions in the Belgian city of Ghent, Eindhoven in The Netherlands, and Lille, in France. No one was hurt in any of the blasts, which caused no damage. An Ikea spokeswoman in Sweden said those explosions had been caused by small fireworks devices. Source:

<http://www.google.com/hostednews/afp/article/ALeqM5jOUXEUStf9S3wVTfnWGXmRqmFWfA?docid=CNG.a8cea2d57046b5a32d61242ebc0ad8cc.5e1>

**Killing of embassy bombings mastermind deprives al Qaeda of key figure.** At 12 a.m. June 7, two men were traveling in a black four-wheel drive vehicle through the Somali capital, Mogadishu. One was the most wanted terrorist in Africa. He had survived more than a decade on the run, at least one attempt on his life, and a \$5 million price on his head for planning the 1998 attacks on the U.S. embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania that killed hundreds of people, including 12 Americans. The suspect was killed but to begin with the Somali security forces had no idea who he was. Only when they discovered cell phones, a South African passport, a substantial amount of cash, and a laptop did they realize this was someone of significance. A sample of his DNA was sent to Nairobi, Kenya, where U.S. officials confirmed his identity. Source: <http://edition.cnn.com/2011/WORLD/africa/06/13/somalia.mastermind/>

**IMF suffers major sophisticated data breach.** The International Monetary Fund (IMF) has become the latest well-known organization to suffer a major breach of its IT systems, in what some reports have suggested was a spear phishing attack orchestrated by a foreign government. The IMF, which oversees the global financial system and was instrumental in the economic bailout of countries such as Greece, Ireland, and Portugal, said it had suffered "an incident," but maintained that its fund is "fully functional." Reports suggested the IMF was forced to cut its network connection to the IT systems of the World Bank, located nearby, after finding that a compromised desktop had been used to access confidential files. Security experts warned that the security of the world's critical infrastructures is at risk unless large organizations better prepare themselves for such sophisticated attacks. The IMF breach comes as hacking attacks on major businesses and governmental organizations are snowballing, with Chinese perpetrators often suspected. Source: <http://www.v3.co.uk/v3-uk/news/2078440/imf-suffers-major-sophisticated-breach>

**Fears for patients' data after hackers hit NHS.** Patients of the National Health Service (NHS) of the United Kingdom face a potential security breach after computer hackers gained access to health service passwords. The group, which calls itself LulzSec, said June 8 it had accessed a system that handles sensitive patient data. The week of May 30, the group stole 1 million data records from a Sony Web site. It published an e-mail showing it had informed the NHS of the security breach, saying "we mean you no harm and only want to help you fix your tech issues." The group took master "admin" passwords from the system "months ago" while searching the

UNCLASSIFIED

## UNCLASSIFIED

Internet for other materials, but had not exploited them. LulzSec reported the security vulnerability on its Twitter account. The message said: "Greetings â€¦ we're a somewhat known band of pirate-ninjas that go by LulzSec. Some time ago, we were traversing the internet for signs of enemy fleets. While you aren't considered an enemy -- your work is of course brilliant -- we did stumble upon several of your admin passwords." The department of health admitted the system had been breached, but said it was only on a local level. It has reported the incident to police. "This is a local issue affecting a small number of Web site administrators," a spokesman said. "No patient information has been compromised. No national NHS information systems have been affected." Source:

<http://www.telegraph.co.uk/technology/news/8567008/Fears-for-patients-data-after-hackers-hit-NHS.html>

### **BANKING AND FINANCE INDUSTRY**

Nothing Significant to Report

### **CHEMICAL AND HAZARDOUS MATERIALS SECTOR**

**Nuclear plant safety rules understate risk, U.S. says.** Nuclear safety rules in the United States do not adequately weigh the risk that a single event would knock out electricity from both the grid and from emergency generators, as an earthquake and tsunami recently did at a nuclear plant in Japan, officials of the Nuclear Regulatory Commission said June 15. A task force created after the accident at the nuclear plant, Fukushima Daiichi, delivered an oral progress report June 15 to the five-member commission. In that session, commission officials said they had learned that some of the safety equipment installed at American nuclear plants over the years, including hardware added after the September 11, 2001, terrorist attacks, is not maintained or inspected as diligently as the original components are. A crucial reason for the extensive damage to the Fukushima plant's reactors was the loss of electricity needed to run water pumps and to reposition valves. The American nuclear industry has argued in recent months that its reactors are better prepared to cope with that kind of emergency. But the chairman of the task force said that studies by safety experts in the United States had analyzed the risk of losing electricity from the grid or from on-site emergency generators, but not both at the same time. The task force, appointed in April, is supposed to complete its investigation in August, but is periodically updating the commission. Source:

[http://www.nytimes.com/2011/06/16/business/energy-environment/16nrc.html?\\_r=1](http://www.nytimes.com/2011/06/16/business/energy-environment/16nrc.html?_r=1)

**75 percent of nuke sites have leaked tritium.** Radioactive tritium has leaked from three-quarters of U.S. commercial nuclear power sites, often into groundwater from corroded, buried piping, an Associated Press (AP) investigation shows. The number and severity of the leaks has been escalating, even as federal regulators extend the licenses of more and more reactors across the nation. Tritium, a radioactive form of hydrogen, has leaked from at least 48 of 65

UNCLASSIFIED

## UNCLASSIFIED

sites, according to U.S. Nuclear Regulatory Commission (NRC) records reviewed as part of the AP's year-long examination of safety issues at aging nuclear power plants. Leaks from at least 37 of those facilities contained concentrations exceeding the federal drinking water standard — sometimes at hundreds of times the limit. While most leaks have been found within plant boundaries, some have migrated offsite. But none is known to have reached public water supplies. At three sites — two in Illinois and one in Minnesota — leaks have contaminated drinking wells of nearby homes, the records show, but not at levels violating the drinking water standard. At a fourth site, in New Jersey, tritium has leaked into an aquifer and a discharge canal feeding Barnegat Bay off of the Atlantic Ocean. Any exposure to radioactivity, no matter how slight, boosts cancer risk, according to the National Academy of Sciences. Federal regulators set a limit for how much tritium is allowed in drinking water, where this contaminant poses its main health risk. Source:

<http://www.burlingtonfreepress.com/article/20110616/NEWS04/110616010/75-percent-nuke-sites-leaked-tritium-?odyssey=mod|newswell|text|FRONTPAGE|s>

### **COMMERCIAL FACILITIES**

**(Arizona) ATF: Greer Lodge fire was arson.** The Bureau of Alcohol, Tobacco and Firearms (ATF) was called in by the chief of the Greer Fire Department in Greer, Arizona to investigate the May 10 fire at Greer Lodge. The fire broke at about 4 a.m. and destroyed the 3-story, 11,000-square-foot historic building within a few hours. The lodge contained 10 rooms and a restaurant. It is the main building in a 50-cabin resort that covers 25 acres. At the time of the fire, only one couple was staying in the building. They were able to escape and no one was injured in the fire. The loss was estimated to be in excess of \$2 million. After ruling out all causes of accidental ignition, ATF investigators reached the arson ruling with conclusive evidence, an ATF public information officer said. He stated the fire was caused by an incendiary device, but he would not give out details of the location of the device. Source:

[http://www.wmicentral.com/police/atf-greer-lodge-fire-was-arson/article\\_228b5afe-92e3-11e0-a8d9-001cc4c002e0.html](http://www.wmicentral.com/police/atf-greer-lodge-fire-was-arson/article_228b5afe-92e3-11e0-a8d9-001cc4c002e0.html)

### **COMMUNICATIONS SECTOR**

**NSA allies with Internet carriers to thwart cyber attacks against defense firms.** The Washington Post reported June 16 the National Security Agency (NSA) was working with Internet service providers to deploy a new generation of tools to scan e-mail and other digital traffic with the goal of thwarting cyberattacks against defense firms by foreign adversaries, according to senior defense and industry officials. The novel program, which began in May on a voluntary, trial basis, relies on sophisticated NSA data sets to identify malicious programs slipped into the vast stream of Internet data flowing to the nation's largest defense firms. Such attacks, including in May against Lockheed Martin, are nearly constant as rival nations and terrorist groups seek access to U.S. military secrets. Officials said the pilot program does not

UNCLASSIFIED

## UNCLASSIFIED

involve direct monitoring of the contractors' networks by the government. The program uses NSA-developed "signatures," or fingerprints of malicious code, and sequences of suspicious network behavior to filter the Internet traffic flowing to major defense contractors. That allows the Internet providers to disable the threats before an attack can penetrate a contractor's servers. The trial is testing two particular sets of signatures and behavior patterns that the NSA has detected as threats. The Internet carriers are AT&T, Verizon, and CenturyLink. Together they are seeking to filter the traffic of 15 defense contractors, including Lockheed Martin, Computer Science Corporation (CSC), Science Applications International Corporation (SAIC), and Northrop Grumman. Source: [http://www.washingtonpost.com/national/major-internet-service-providers-cooperating-with-nsa-on-monitoring-traffic/2011/06/07/AG2dukXH\\_story.html](http://www.washingtonpost.com/national/major-internet-service-providers-cooperating-with-nsa-on-monitoring-traffic/2011/06/07/AG2dukXH_story.html)

**(Iowa) New attacks on cellphone towers impacting service.** According to police in Des Moines, Iowa, two cellphone towers were hit by vandals June 16 in the 3500 block of East Douglas. Police said the towers service Sprint, AT&T, T-Mobile, and U.S. Cellular. In the middle of the night, the phone companies were alerted of a power failure by alarms going off. They found the power meters pulled off and taken, the ground wires cut, and all the copper gone. The same night, another AT&T tower was stripped on Indiana Street, according to police. About 2 weeks ago, thieves using the same method struck a different AT&T and Erikson service tower on the 1800 block of County Line Road. Police said at one tower alone, they took at least 150 feet of thick copper wire. Scrap dealers said copper is now selling for between \$3 and \$4 per pound, and they pay cash. They said there is no way to tell if something is stolen because so many demolition and construction crews bring in scrap metal. Police said they have never seen theft from these targets before in Des Moines, but copper thieves are targeting these towers in other parts of the country. Workers who are making repairs to the towers said the thieves were not amateurs, and that they knew what they were doing. Des Moines police are now searching for the suspect(s). Source: <http://www.kcci.com/r/28262667/detail.html>

### **LightSquared cellular network interferes with all GPS applications, latest tests show.**

Transmissions from the nationwide cellular network planned by LightSquared knocked out GPS receivers operating at distances of 600 feet to 185 miles from the company's base station, according to the latest test report on interference caused by the company's system. The Federal Aviation Administration co-chairman of the National Position, Navigation and Timing Engineering (PNT) Forum, a multiagency group chartered to assess GPS technical issues, told a meeting of the National Space-Based PNT Advisory Board June 9 that tests in April showed "all GPS receiver applications [are] impacted by [the] proposed LightSquared network." The Federal Communications Commission approved LightSquared's hybrid satellite-terrestrial network January 26, which will include 40,000 base stations. The agency directed the company to work with the GPS industry to determine the potential effect its terrestrial transmitters, which operate in the 1525-1559 MHz and 1626.5-1660.5 MHz bands, would have on GPS systems that operate in the nearby 1559-1610 MHz band. The PNT co-chairman said simulation of the planned LightSquared network showed it would "degrade or result in loss of GPS function ... at standoff distances ranging from a few kilometers and extending to space operations." Source: [http://www.nextgov.com/nextgov/ng\\_20110610\\_6517.php](http://www.nextgov.com/nextgov/ng_20110610_6517.php)

UNCLASSIFIED

## UNCLASSIFIED

**FEMA, FCC announce nationwide test of the emergency alert system.** The U.S. DHS's Federal Emergency Management Agency (FEMA) and the Federal Communications Commission (FCC) will conduct the first nationwide test of the Emergency Alert System (EAS). The nationwide test will occur November 9 at 2 p.m. Eastern Standard Time and may last up to three and a half minutes. Similar to local EAS tests that are already conducted frequently, the nationwide test will involve broadcast radio and television stations, cable television, satellite radio, and television services, and wireline video service providers across all states and the territories of Puerto Rico, the U.S. Virgin Islands, and American Samoa. Source:

[http://www.thecyprsstimes.com/article/News/National\\_News/FEMA\\_FCC\\_ANNOUNCE\\_NATIONWIDE\\_TEST\\_OF\\_THE\\_EMERGENCY\\_ALERT\\_SYSTEM/46515](http://www.thecyprsstimes.com/article/News/National_News/FEMA_FCC_ANNOUNCE_NATIONWIDE_TEST_OF_THE_EMERGENCY_ALERT_SYSTEM/46515)

## **CRITICAL MANUFACTURING**

**Chrysler recalls 11,000 vehicles for steering issue.** Chrysler Group LLC has recalled 11,351 vehicles for a possible missing or incorrectly installed part that could result in loss of steering capability and increase the risk of a crash, Reuters reported June 16. Some of the 2011 model-year vehicles were built with a missing or incorrectly installed pivot rivet on the steering column, according to documents filed with the National Highway Traffic Safety Administration (NHTSA). A Chrysler spokesman said the company was cooperating with the NHTSA, and that there had been no reports of accidents or injuries related to the issue. Affected vehicles include the Chrysler 200 and 200 convertible cars; Town and Country minivan; Dodge Avenger, Caliber, Caravan, Journey and Nitro vehicles; and Jeep Compass, Liberty, Patriot, and Wrangler SUVs, according to the NHTSA documents. Dealers will inspect for the presence of the rivet and repair the steering column pivot as required. Plans call for the recall to begin in June. Source:

<http://www.reuters.com/article/2011/06/16/us-chrysler-recall-idUSTRE75F3M820110616>

**General Electric, Sharp recalls GE air conditioning and heating units due to fire hazard.** GE Appliances and Lighting, of Louisville, Kentucky, issued a recall June 14 for about 90,600 GE Zoneline air conditioners and heaters. The manufacturer of the equipment was Sharp Corp., of Osaka, Japan. An electrical component in the heating system can fail, posing a fire hazard to consumers. General Electric and Sharp have received four reports of incidents involving smoke and/or fire with the air conditioning and heating units. In two of the reported incidents, fire extended beyond the air conditioning and heating unit, resulting in property damage. No injuries have been reported. This recall involves GE Packaged Terminal Air Conditioners (PTAC) and packaged terminal heat pumps manufactured between January 2010 and March 2011, and are most often used in apartment buildings and commercial space. The items were sold by General Electric authorized representatives and HVAC distributors nationwide from March 2010 through March 2011. Source: <http://www.cpsc.gov/cpsc/pub/prerel/prhtml11/11247.html>

**GM recalls 50,500 Cadillac SRXs in North America.** General Motors (GM) recalled 50,500 Cadillac SRX luxury crossover vehicles because the performance of the front passenger airbag differs from the owner's manual. The recall, announced by GM June 10, affects 47,401 vehicles

UNCLASSIFIED

## UNCLASSIFIED

in the United States, and the rest in Canada and Mexico from the 2011 model year. The U.S. automaker said it knew of no crashes, injuries, or complaints related to the issue. The SRX and the CTS sedan are the top-selling Cadillac models in the United States in 2011, both with more than 22,000 sales. GM said the SRX air bags are programmed to turn off the right side roof-rail airbag if someone sits in the front passenger seat, but the owner's manual says that airbag will deploy whether or not the seat is occupied. Because the action of the airbag and the manual do not match, that violates federal safety standards. Source:

<http://www.reuters.com/article/2011/06/10/us-gm-recall-idUSTRE7592QH20110610>

## **DEFENSE/ INDUSTRY BASE SECTOR**

**F-22 grounding continues as oxygen safety probe widens.** More than 6 weeks after the US Air Force indefinitely grounded all Lockheed Martin F-22A Raptors, the scope of the safety investigation has widened beyond the Honeywell-supplied onboard oxygen generating system (OBOGS), Flight International reported June 16. Although internally described as the "OBOGS safety investigation," the probe launched after the May 3 safety stand-down of the F-22A fleet is "not limited" to that particular system, Air Combat Command (ACC) said. The stand-down was originally linked to five reports by F-22 pilots of potential oxygen system malfunctions, including one reported instance when an F-22 scraped treetops on final approach. The pilot could not remember the incident after landing, exhibiting a classic symptom of hypoxia. Source: <http://www.flightglobal.com/articles/2011/06/16/358103/f-22-grounding-continues-as-oxygen-safety-probe-widens.html>

**China urged to help in Senate counterfeit probe.** The U.S. Senate Armed Services Committee urged China to allow investigators to travel to the Chinese mainland to probe reports that Chinese-made counterfeit parts are making their way into U.S. weapons systems, and other electronics, Reuters reported June 14. So far, China has declined to grant visas to committee staff investigators. They are now in Hong Kong and seeking to conduct unfettered interviews in nearby Shenzhen, the suspected epicenter for substandard knock-off parts, the committee chairman, a Democrat, and the panel's top Republican told a news conference. A range of U.S. companies interviewed by the committee, from military contractors to consumer electronics makers, have pointed "almost totally and exclusively" to China, and more specifically to Shenzhen, in Guangdong province, as a source of counterfeit electronic parts, the committee chairman said. The chair said he and the ranking Republican had sought for more than 2 months to persuade the Chinese authorities to allow 1 or 2 days of interviews on the ground as part of an official Senate investigation. The chair said Beijing had asked that the investigators delay their proposed trip or, if eventually granted visas, agree to be accompanied by a China official during interviews. Source: <http://www.reuters.com/article/2011/06/14/us-china-usa-military-counterfeit-idUSTRE75D40Q20110614>

**(Tennessee) Y-12 resists cyber attack.** The Y-12 nuclear weapons plant in Oak Ridge, Tennessee was the target of a cyberattack, the Knoxville News Sentinel reported June 14. The plant's external Web site was shut down after a database associated with the site was attacked June

UNCLASSIFIED

## UNCLASSIFIED

12 “by an outside source,” a Y-12 spokesman confirmed. “The database did not contain any sensitive information and no Y-12-related activities were compromised,” a spokesman for the National Nuclear Security Administration said. “The database was immediately taken out of service and is being analyzed by Y-12 cyber security staff. For this reason, Y-12’s external Web site has been replaced with a temporary information page. At this point, there is no evidence that any plant-wide email or internal computing services have been affected, nor has any classified or sensitive information been accessed or affected by this incident.” The plant is part of the U.S. nuclear weapons complex, producing refurbished parts for aging nuclear warheads, recycling old weapons components, and storing most of the nation’s inventory of bomb-grade uranium. Source: <http://www.knoxnews.com/news/2011/jun/14/y-12-repulses-cyber-attack/>

**Feds accuse man of stealing, selling military ammo.** A former employee of a Nevada-based defense contractor has been indicted on charges that he conspired with others to steal U.S. military ammunition in Iraq and then sell it back to Iraqis and U.S. forces. The man was released on his own recognizance after being arrested at his Carson City home and making an initial appearance June 9 in U.S. district court in Reno on charges of conspiracy to defraud the U.S. government and money laundering. A federal grand jury indictment alleges the man was a manager in Baghdad with defense contractor Security Operations Consulting (SOC) in 2007 when he conspired with others to steal and sell the ammo and send cash shipments to the United States via Federal Express or couriers. The man — whose job was to ensure that all bases of operation in Iraq under contract with SOC had ammunition and other supplies — at times sold the ammunition back to the U.S. and coalition forces effectively requiring the government to pay for the ammunition twice, federal prosecutors contend. Source: [http://www.journaltimes.com/news/national/article\\_6669aa49-f9c5-5d7e-a96f-4f44e050c680.html](http://www.journaltimes.com/news/national/article_6669aa49-f9c5-5d7e-a96f-4f44e050c680.html)

## **EMERGENCY SERVICES**

**Coast Guard: Missing NJ boat case is possible hoax.** The U.S. Coast Guard (USCG) launched an investigation June 14 into a possible hoax after a 10-hour search turned up no sign of four boaters who sent distress calls saying they were abandoning ship. Boats, planes, and helicopters were dispatched before sunrise in a rescue operation that joined together military, state, and local agencies and cost the USCG almost \$88,000. The rescue was called off in the afternoon after a search of a 600-square-mile area failed to turn up a boat, debris or the sailors. Authorities are searching for whoever made two false distress calls — a federal felony — and are offering a reward of up to \$1,000 for information leading to arrest and prosecution. A USCG boat searched for 5 hours, while local police agencies searched from land. A USCG airplane from Massachusetts flew three rescue flights over the search area, while the USCG and New Jersey State Police searched by helicopter. Source: <http://www.aic.com/news/nation-world/coast-guard-missing-nj-976332.html>

UNCLASSIFIED

## **ENERGY**

**U.S. warns of problems in Chinese SCADA software.** Two vulnerabilities found in industrial control system software made in China but used worldwide could be remotely exploited by attackers, according to a warning issued June 16 by the U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The vulnerabilities were found in two products from Sunway ForceControl Technology, a Beijing-based company that develops supervisory control and data acquisition (SCADA) software for many industries, including defense, petrochemical, energy, water, and manufacturing, the agency said. Sunway's products are mostly used in China but also in Europe, the Americas, Asia and Africa, according to the agency's advisory. The problems could cause a denial of service issue or remote code exploitation in Sunway's ForceControl 6.1 WebServer and its pNetPower AngelServer products. Both issues were found by a researcher from security testing company NSS Labs. Sunway issued patches for the vulnerabilities May 20. ICS-CERT said there are no known exploits for the vulnerabilities, but computer security experts generally recommend patching software as soon as possible. ICS-CERT added that its unlikely someone could create consistent exploit code for the two vulnerabilities, and that an attacker would need to have "intermediate" skills to exploit the problems. Source:

[http://www.computerworld.com/s/article/9217722/U.S. warns of problems in Chinese SCA DA software](http://www.computerworld.com/s/article/9217722/U.S._warns_of_problems_in_Chinese_SCA_DA_software)

**U.S. unveils plans to invest in smart grid technology, security.** White House officials unveiled a series of initiatives designed to help implement information technology to the national power grid to make it smarter, more efficient, and secure. The National Science Technology Council outlined its plans to modernize the grid in rural areas and to create a "smart grid innovation hub" in a report titled "Building the 21st Century Grid" released June 13. The hub will be a collaboration of federal researchers, companies, and utility executives and will support research, development, and deployments of smart grid technology. The modernization of the grid will allow operators to have access to information about threats, help companies deliver new security tools, and create security standards. The project announcements are timely, considering the latest report on cyber-threats facing utilities and power generation companies from PwC, also released June 13. Several multinational energy companies recently suffered security breaches long before the victims became aware their systems were compromised, the report found. It said energy companies are vulnerable because they have valuable proprietary data on discoveries and financial information relating to existing power and fuel reserves. State-sponsored foreign attackers have used "highly sophisticated methods" to compromise these targets, the authors wrote. "Had digital evidence and breach indicators been recognized at the time of an event, victims of cyber-crime could have taken positive action and minimized their risk," the report said. Source: <http://www.eweek.com/c/a/Security/US-Unveils-Plans-to-Invest-in-Smart-Grid-Technology-Security-164442/>

**(California) U.S. leads criminal investigation into explosion of PG&E pipeline.** The U.S. Department of Justice (DOJ) is leading a criminal investigation into the fatal explosion in 2010 of a natural-gas pipeline owned by Pacific Gas & Electric (PG&E), the company said June 13. The

## UNCLASSIFIED

Justice Department told PG&E's utility June 9 that the agency had formed a task force with the San Mateo County District Attorney's Office to investigate the accident, PG&E wrote in a filing with the U.S. Securities and Exchange Commission. The September 9 pipeline explosion in San Bruno, California, killed nine people, injured several others and destroyed 38 homes. The DOJ probe is the latest in a string of investigations into the San Bruno pipeline explosion and PG&E's conduct before the incident. The National Transportation Safety Board (NTSB) has been investigating the cause of the explosion and has issued several pipeline-safety recommendations based on problems it found. While the NTSB's final report is pending, the agency has suggested in interim reports that poor record-keeping and a lack of safety tests by PG&E likely masked manufacturing defects in the 55-year-old pipeline. The agency also suggested that the local fire department may not have had the information it needed to react properly to the pipeline rupture. Source:

<http://www.foxbusiness.com/industries/2011/06/13/us-leads-criminal-investigation-into-explosion-pge-pipeline/>

**This week's solar flare illuminates the grid's vulnerability.** A massive burst of solar wind that erupted from the sun June 7 is expected to deliver only a "glancing blow" to the Earth's vulnerable magnetic field, NASA officials said June 8. But it will preview what some experts call a potentially existential threat to the power grids of the United States and other nations, and the populations that depend on them. A spokeswoman, who leads NASA's "Solar Shield" satellite-based detection system at the Goddard Space Flight Center, said the cloud of ionized particles from the June 7 violent "coronal mass ejection" will largely miss Earth, giving some North American residents a glimpse of the aurora borealis, or northern lights, the weekend of June 11 and 12. The next peak cycle of sunspot activity is predicted for 2012-2014, bringing with it a greater risk of large geomagnetic storms that can generate powerful rogue currents in transmission lines, potentially damaging or destroying the large transformers that manage power flow over high-voltage networks. "Geomagnetically-induced currents on system infrastructure have the potential to result in widespread tripping of key transmission lines and irreversible physical damage to large transformers," a 2009 report by the North American Electric Reliability Corp and the Energy Department said. Source:

<http://www.nytimes.com/cwire/2011/06/09/09climatewire-this-weeks-solar-flare-illuminates-the-grids-63979.html>

## **FOOD AND AGRICULTURE**

**(New York) Warning in New York for staph in Fresh Cheese.** Long Island consumers in New York have been warned not to eat a certain Queso Fresco "Fresh Cheese" because it may be contaminated with *Staphylococcus aureus*. Quesos CentroAmericano Corp. of Freeport, New York, recalled the fresh cheese after a routine sample, taken June 7 by an inspector from the New York Agriculture Department's Division of Milk Control and Dairy Services, was found to be contaminated with high levels of *Staphylococcus aureus*. The manufacturer was notified of the positive test result on June 13 and voluntarily recalled the product. The recalled fresh Spanish-style cheese is sold in 5-pound foil tray packages. The package label identifies the plant number

UNCLASSIFIED

## UNCLASSIFIED

36-9845 and the product lot code 05/31/11. The cheese was distributed to stores, delis, and restaurants on Long Island. Source: <http://www.foodsafetynews.com/2011/06/warning-in-ny-for-staph-in-fresh-cheese/>

**(California) Listeria found inside vegan food plant.** Gloria's Pantry in Soquel, California, received a warning letter earlier in June after the U.S. Food and Drug Administration (FDA) found *Listeria monocytogenes* on food contact surfaces inside the plant. The food manufacturer makes "grab and go" vegetarian and vegan foods sold in grocery store dairy cases. It underwent an FDA inspection from January 13 through February 2. Inspectors said lab tests returned positive samples for *Listeria* on food contact surfaces, including a bowl used to hold lettuce. In a June 3 warning letter released the week of June 13, the FDA said a cracked plastic bowl repaired with tape was found to be contaminated with *L. monocytogenes*, a known pathogenic micro-organism. Gloria's product line includes flour tortilla sambosas and burritos, wraps, and spring rolls. The products are sold through Lite for Life, Whole Food Markets, Piazzas Fine Foods, Roberts Market, Country Sun Natural, New Leaf Markets, Food Bin, Staff of Life, Shoppers Corner, Aptos Natural, and Cornacopia Market. Source: <http://www.foodsafetynews.com/2011/06/listeria-found-inside-vegan-food-maker/>

**(Alaska) Wild cranes caused 2008 Campylobacter outbreak.** A *Campylobacter jejuni* outbreak that sickened close to 100 people in Alaska in 2008 had a surprising cause: fresh peas contaminated by sandhill cranes, according to a report in *Clinical Infectious Diseases*. "This is the first reported outbreak of campylobacteriosis linked to produce contaminated with bird feces," read the report by researchers from the U.S. Centers for Disease Control and Prevention, and several Alaska state agencies. *C. jejuni* is one of the most common bacterial causes of diarrheal illness, with an estimated 2.4 million cases annually, but few cases are part of recognized outbreaks, the report said. Though the illness is usually linked to contaminated food or water, it is hard to trace the organism to a particular vehicle, because it does not survive long outside an animal host. But in the Alaska outbreak, investigators managed to confirm the pathogen in pea samples and sandhill crane feces, and to match those isolates to some of the isolates from sick patients. The outbreak began in August 2008 with 10 lab-confirmed cases in Anchorage residents. Three of the isolates were matched by pulsed-field gel electrophoresis. The cases triggered an alert to the public, and a multi-pronged investigation. A case-control study involving 45 patients with confirmed campylobacteriosis and 90 healthy controls pointed to consumption of raw peas as the only significant risk factor. Overall, 98 people had illnesses that met the case definition, and 63 cases were lab-confirmed, the report said. Source: <http://www.cidrap.umn.edu/cidrap/content/fs/food-disease/news/jun1411campy.html>

**(New Jersey) Listeria prompts another Stilton cheese recall.** Atlanta Corp., an Elizabeth, New Jersey food distributor recalled an 8-9 pound wheel of Royal Blue Stilton" cheese imported from England because it may be contaminated with *Listeria monocytogenes*. In a news release, the company said it decided to test its cheese after another importer in May recalled cheese made by the same English dairy. Testing revealed the presence of *Listeria*, which can cause serious and sometimes fatal infections. The company's inventory of affected product was

UNCLASSIFIED

## UNCLASSIFIED

quarantined and will be destroyed under U.S. Food and Drug Administration supervision. No illnesses have been reported. The recall involves just one 8-9 lb wheel of cheese contained in a master case with batch code B038. However, this cheese is routinely cut at retail from the bulk wheel and sold in random weight cuts. The cheese was manufactured in England by Quenby Hall Dairy and exported by Coombe Castle, but not all cheese exported by Coombe Castle International is manufactured by Quenby Hall Dairy. The affected lot is marked B038 on the original case cartons. There are no specific expiration dates. Source:

<http://www.foodsafetynews.com/2011/06/listeria-prompts-another-stilton-cheese-recall/>

**(Arizona) Another two horses test positive for virus.** Two more Arizona horses tested positive for equine herpes virus, or EHV-1, one with the EHM or neurological variant, according to a local equine veterinarian. The veterinarian, whose practice is Southern Arizona Equine, sent an e-mail to clients June 11 advising them of the latest two cases. The virus was first reported at a cutting horse competition in Ogden, Utah, in late April and has spread to other states from a few horses that contracted it. The spread of the virus has been somewhat contained through coordinated quarantine efforts and event cancellations throughout western states. The National Cutting Horse Association notified state animal health officials of horses that were entered in the event and may have been exposed to the virus. In turn, state animal health officials contacted owners of potentially exposed horses. While the outbreak is on the decline, intermittent cases across the western United States continue to be reported, she said. The following information is the most current EHV-1 incidence update provided by the U.S. Department of Agriculture. Primary exposed horses — exposed at the Ogden, Utah, event: 32 EHV-1 cases; 26 EHM or neurologic cases; and 10 dead or euthanized cases. Secondary and tertiary exposed horses: 23 EHV-1 cases; 7 EHM cases; and 2 dead or euthanized cases. To date, 19 states are reporting horses with primary exposure to EHV-1 after participating in the Utah event, for a total of 421 exposed animals. Source:

<http://www.svherald.com/content/news/2011/06/12/another-two-horses-test-positive-virus>

**(Ohio) State of Ohio investigating outbreak of infections caused by Salmonella.** State officials report that eight separate Salmonella illnesses in Ohio are part of a multistate outbreak associated with chicks and/or ducklings purchased in 2011 at agricultural supply stores sourced from Mt. Healthy Hatchery, an Ohio hatchery. The birds were sold at numerous agricultural outlets across the state and with these confirmed reports of Salmonella infections, health officials are encouraging any purchaser of baby chicks to use caution in their handling and care. The eight ill individuals range in age from 3 months to 76 years and live in Ashtabula, Columbiana, Franklin, Hamilton, Jefferson, Licking, Medina, and Wood counties. Specimens obtained from chicks belonging to one of the Ohio cases yielded the outbreak strain of Salmonella Altona. The Ohio departments of health and agriculture are working with the Centers for Disease Control and Prevention (CDC), the U.S. Department of Agriculture's (USDA) National Poultry Improvement Plan, and Ohio health departments in responding to the outbreak. Source: <http://www.woio.com/Global/story.asp?S=14875785>

UNCLASSIFIED

## UNCLASSIFIED

**(Missouri) US Department of Labor's OSHA cites Liquid Feed Commodities in Fremont, Neb., for serious health and safety violations.** The U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) has cited Liquid Feed Commodities Inc. in Fremont, Nebraska, for 20 serious and 1 other-than-serious violation of OSHA's safety and health standards. Proposed fines total \$79,200. OSHA's inspection of Liquid Feed was initiated in March under a local emphasis program that targets grain-handling establishments. The program is designed to reduce injury, illness, and death rates in the industry by increasing employers' knowledge of safety and health programs through outreach and enforcement activities. The serious violations stem from a lack of or inadequate fall protection, respiratory hazards, confined space hazards, energy source lockout/tagout hazards, a lack of eyewash facilities, a lack of powered industrial truck training, machine guarding hazards, electrical hazards, and chemical hazards. A serious violation occurs when there is substantial probability that death or serious physical harm could result from a hazard about which the employer knew or should have known. The other-than-serious violation is related to deficient powered industrial truck inspections. An other-than-serious violation is one that has a direct relationship to job safety and health, but probably would not cause death or serious physical harm. Source: [http://www.osha.gov/pls/oshaweb/owadisp.show\\_document?p\\_table=NEWS\\_RELEASES&p\\_id=19983](http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=19983)

**E.coli found in bean sprout package-German officials.** German authorities said June 10 they detected the deadly E.coli strain in a bean sprout package from the organic farm in Lower Saxony, which had already been under investigation. "According to our knowledge to date, the bean sprouts originated from the farm in Bienenbuettel," said the consumer protection agency from North Rhine Westphalia state, where the package was discovered. "The discovery confirms our current warning against the consumption of bean sprouts. It is therefore becoming increasingly more likely that bean sprouts are the source of the E.coli infections," the consumer protection minister in North Rhine-Westphalia said. Source: <http://www.fox13now.com/news/nationworld/sns-rt-us-ecolitre7591hw-20110610,0,4918652.story>

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

**(Virginia) Pentagon scare suspect ID'd as Marine reservist.** A source told CBS News that the man detained in the discovery of a suspicious vehicle outside the Pentagon in Arlington, Virginia June 17 has been identified as a lance corporal in the U.S. Marine Corps Reserve. The man told authorities during questioning June 17 that he was carrying explosive materials, the source told CBS News. Previously, an FBI Special Agent who heads the bureau's counterterrorism division in its Washington, D.C. field office, told reporters a non-explosive material was found in a backpack the suspect was carrying at the time of his arrest. A law enforcement official speaking on the condition of anonymity said officials found what appeared to be an unknown quantity of ammonium nitrate. The official, who was not authorized to release the information, said

UNCLASSIFIED

## UNCLASSIFIED

nothing else was found that would have enabled an explosion. The official said tests were being done to determine the substance and the exact concentration. A law enforcement source said the suspect was carrying a notebook that contained the phrases “al Qaeda,” “Taliban rules,” and “Mujahid defeated croatian forces” when he was detained. The law enforcement source said the backpack also contained 20 spent 9 mm shell casings and 3 cans of black spray paint. The suspect was detained after the U.S. Park Police came across him early June 17 in Arlington National Cemetery, when it was closed, triggering the investigation. The Park Police then launched a search for a vehicle, which was found near the Pentagon. The 2011 red Nissan prompted the Arlington County Fire Department’s bomb disposal unit to follow protocols, including the use of a water cannon, to render the vehicle safe, an Arlington Police spokeswoman told reporters. CBS News reports the Marine Corps Memorial is open to the public. Arlington National Cemetery was briefly closed, but has since reopened. A DHS spokesman said federal agencies were involved with the investigation. “DHS is monitoring a suspicious vehicle incident causing road closures around the Pentagon,” he said. “This is a law enforcement matter at this time, with the U.S. Park Police and the Arlington County Police Department as leads and other federal agencies on the scene.” Source:

<http://www.cbsnews.com/stories/2011/06/17/national/main20071998.shtml>

**(Michigan) Video: Authorities detonate suspicious package near IRS building in Detroit.** A backpack that set off a bomb scare outside the IRS building on Michigan Avenue in Detroit, Michigan was detonated by the Detroit Police Bomb Squad June 15. The backpack was found at about 4:30 a.m. at the corner of Third and Michigan, a Detroit police inspector said. A power source spotted after an X-ray of the bag, prompted authorities to detonate the bag at the scene, versus remove it and detonate it elsewhere, he said. The police inspector, who would not elaborate on what the power source was, said investigators will review surveillance video to determine whether the bag was left accidentally or intentionally. The discovery forced the evacuation of the IRS building and, by 6:30 a.m., dozens of police and fire vehicles were on the scene. Michigan Avenue was closed, along with surrounding streets and sidewalks. By 7:30 a.m., Michigan Avenue was reopened and people were allowed back in the building. An IRS spokesman said about 900 people work in the building, one of three IRS computing centers in the United States. Source:

<http://www.freep.com/article/20110615/NEWS01/110615009/Authorities-detonate-suspicious-package-near-IRS-building-Detroit?odyssey=tab|topnews|text|FRONTPAGE>

**(New York) Williamsville students charged in bomb threats.** Amherst, New York police charged two students at Transit Middle School in East Amherst June 13 in a series of bomb threats directed at the school. After a week-long investigation and with the help of the school’s resource officer, police were able to identify the suspects. Both are charged with falsely reporting an incident, a felony. After having their mugshots taken and being fingerprinted, each was released to their parents until their court date. Source:

<http://www.wgrz.com/news/article/124553/37/Williamsville-Students-Charged-in-Bomb-Threats>

UNCLASSIFIED

## UNCLASSIFIED

**(Washington, D.C.) U.S. government Website hacked.** The U.S. Senate's Web site, [www.Senate.Gov](http://www.Senate.Gov) was hacked June 12, by Lulz Security. This is the same team of hackers who are responsible for security breaches at Sony, Nintendo, and even the FBI. The company tweeted June 13 that they were "releasing their Bethesda and Senate.gov double surprise releases." On its Web site, the company listed codes and dates taken from Senate.gov. The Senate's Sergeant at Arms said the network firewall prevented the hackers from gaining access to any vital information. He said the only information seized was already public. Still, the Senate is working to beef up security. The weakness has been identified and the problem has been fixed. Lulzsec also said the usernames and passwords of gamers from Bethesda Softworks in Rockville, Maryland were hacked. Source: <http://wusa9.com/news/article/154768/77/US-Government-Website-Hacked>

**(Virginia) Police: Man found with gun, package near Pentagon.** Virginia State Police said a motorist found with a gun and what appeared to be a suspicious package near the Pentagon in Arlington June 13 has been taken into custody. Police said a trooper saw the vehicle backing up on a southbound Interstate 395 ramp around 8:30 p.m. Police stopped the car and found a handgun and what they described as a "suspicious-looking package" inside. State police bomb technicians and the Arlington County Fire Department responded and determined there was no explosive or suspicious device. Police said the driver has been taken into custody with charges pending. The incident shut down the ramp for hours June 13. Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2011/06/14/national/a033331D02.DTL>

**(Tennessee) 'Suspicious letter' sent to state capitol.** A suspicious letter was intercepted in the Tennessee capitol hill mail room June 9 and has been turned over to the FBI, according to state government officials. Officials have declined to identify who the letter was addressed to or what it contained that drew attention to it. Upon noticing the letter in the morning, mail room staff contacted the Tennessee Highway Patrol, who contacted the state's emergency management agency, according to a spokeswoman for the department of safety. The case is now in the hands of the FBI, she said. The mail room, located on the ground floor of the capitol building, was blocked off in the morning and remained blocked off in the afternoon. Source: <http://missouri-news.org/midwest-news/tennessee/suspicious-letter-sent-to-state-capitol/5911>

**U.S. reaches plea deal in classified leaks case.** The Justice Department June 9 reached a plea agreement in the leak case against a former National Security Agency (NSA) official. In court papers, the government said the man will plead guilty to exceeding authorized use of a computer, a misdemeanor. The suspect had been charged with obstruction of justice, lying to the FBI, and illegal possession of classified NSA documents under the seldom-used Espionage Act of 1917, even though he was not charged with spying. If he had been convicted of those crimes, he could have faced up to 35 years in prison. The court documents in the plea deal contain no recommendation on sentencing for the man, but misdemeanors carry a maximum penalty of 1 year in jail. The documents filed June 9 by federal prosecutors said the government and the suspect agreed that if the case had gone to trial, the government would have proved that from February 2006 through about March 2007, the suspect intentionally accessed a

UNCLASSIFIED

## UNCLASSIFIED

system called NSANet, obtained official NSA information, and provided it orally and in writing to another person who was not permitted or authorized to receive it. The suspect “knew that NSA restricted the use of and access to its computers and NSANet to official use only,” the court papers said. Source: <http://www.longislandpress.com/2011/06/09/us-reaches-plea-deal-in-classified-leaks-case/>

**(Wisconsin) Woman arrested for alleged bomb threats at state office buildings.** A 24-year-old Fitchburg, Wisconsin woman was arrested by Wisconsin Capitol Police for allegedly making two bomb threats to two state office buildings June 7 in Madison. The woman was tentatively charged with two counts of making a bomb scare, according to a press release issued June 10 by the Wisconsin Department of Military Affairs on behalf of the capitol police. According to the release, the woman was working for a cleaning company contracted by the state. Police were notified of written bomb threats to the GEF-2 and GEF-3 state office buildings on Webster Street in Madison at about 7 p.m. The threats were found by cleaning crews. Both buildings were evacuated and searched, but nothing was found. The case has been turned over to the Dane County District Attorney’s Office. Source: [http://host.madison.com/ct/news/local/crime\\_and\\_courts/article\\_d25126aa-9377-11e0-92fc-001cc4c002e0.html](http://host.madison.com/ct/news/local/crime_and_courts/article_d25126aa-9377-11e0-92fc-001cc4c002e0.html)

## **INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**Free Web hosting is a boon to phishers.** According to a Zscaler researcher, free hosting services are a boon for scammers, since they need a place to set up malicious sites as quickly as they get pulled down. There are many such services on the Web, and among them is PasteHtml.com a free anonymous Web hosting. Although the intentions of the people behind the service are honorable, the site has proven very handy for phishers. “Try searches on the site for terms such as ‘site:pastehtml(dot)com facebook login’ or ‘site:pastehtml(dot)com paypal’,” points out a the researcher. “Most of the pages are malicious.” While the service tries to keep the pace and take down or block the pages in question — or sets up warnings for users to see when they try to view it — it is a constant race against the clock, not to mention a drain on its resources. Unfortunately, there is no easy solution for them, and until there is one, users must become accustomed to checking the URL in the address bar to be sure they have landed on the right pages. Source: <http://www.net-security.org/secworld.php?id=11180>

**Malware targets custom Android ROMs.** Malware designed to exploit a flaw that granted extra permissions to applications on devices with custom Android ROMs has been identified by Lookout Mobile Security. A CyanogenMod developer confirmed the vulnerability was closed in version 7.0.3 of CyanogenMod in May, when the popular ROM was updated for a mystery “important security fix.” The problem is if applications are signed with the same private key as the operating system, Android grants them permission to install and uninstall applications without user intervention. Normally, this would not be an issue as the private key would be secret, but many custom ROMs are built from the Android Open Source Project (AOSP) source code that includes publicly available private keys. Lookout found malware, which it dubbed

UNCLASSIFIED

## UNCLASSIFIED

jSMShider, in several applications in alternative Chinese app markets. jSMShider is signed with the “private key” from AOSP and uses the permissions flaw to install a secondary payload onto the system that could read, send, and process SMS messages, download and install more applications, communicate with a C&C remote server, and open URLs silently. Source:

<http://www.h-online.com/security/news/item/Malware-targets-custom-Android-ROMs-1262462.html>

**‘Anonymous’ hacker group identifies Fed as target on YouTube.** A group of online hackers identified the Federal Reserve as a target, using a video on the YouTube Web site to call on its chairman to resign. In the video, the group, which calls itself Anonymous, said June 14 would mark the “first step” of protests against the Federal Reserve Chairman and urged those wanting him to quit to occupy a public space. “The Federal Reserve’s policies are systematically looting the country to enrich one 10th of 1 percent of the population,” a distorted voice said on the video. The group attacked several Turkish government Web sites the week of June 6 to protest an Internet filter it said will restrict Web surfing, the Hurriyet newspaper reported. Source:

<http://www.bloomberg.com/news/2011-06-14/-anonymous-hacker-group-identifies-fed-as-target-on-youtube.html>

**CO.TV free domain provider abused in Google News BHSEO campaign.** Security researchers from cloud security provider Zscaler have come across a Google News black hat SEO campaign that uses numerous co(dot)tv rogue domains. The targeted keywords are related to an actor’s departure from a popular television series. The news generated noticeable attention online the week of June 6, and was apparently popular enough for cyber crooks to try and exploit. Experts note search results poisoning has moved away from the traditional Web search and towards complementary services such as image search or news search. This switch has also been influenced by the fact Google has gotten better at preventing the rogue links from appearing at the top of its search results. However, Google has not paid the same attention to the other types of searches it offers. Black hat SEO attacks involve the creation of keyword-riddled pages on compromised domains and leveraging their Google rank to push the links at the top of the results for particular topics. Source: <http://news.softpedia.com/news/CO-TV-Free-Domain-Provider-Abused-in-Google-News-BHSEO-Campaign-205566.shtml>

**PlayBook OS updated after Adobe Flash security issue.** A new version of the BlackBerry Tablet OS will soon be available to all BlackBerry PlayBook tablet users, to address a security issue raised by Adobe about its Flash Player, Research In Motion said June 12. The new version of the operating system, version 1.0.5.2342, will contain an updated version of the Flash Player, RIM said in a blog post. Adobe issued an update the week of June 6 for its Flash Player to deal with a cross-site scripting vulnerability. The problem could be exploited to perform actions on behalf of a BlackBerry PlayBook tablet user on any Web site or Web mail provider if the user visits a malicious Web site that loads Adobe Flash content, RIM said on a support page. The PlayBook’s operating system is built from the ground up to run Adobe Flash. Source:

[http://www.computerworld.com/s/article/9217557/PlayBook\\_OS\\_updated\\_after\\_Adobe\\_Flash\\_security\\_issue](http://www.computerworld.com/s/article/9217557/PlayBook_OS_updated_after_Adobe_Flash_security_issue)

## UNCLASSIFIED

## UNCLASSIFIED

**Some top apps put data at risk.** Computer security firm viaForensics found the applications for top Internet companies LinkedIn Corp., Netflix, Inc., Foursquare, and Square, Inc. stored various forms of users' personal data in plain text on a mobile device, putting sensitive information at risk to computer criminals. The Android applications of LinkedIn, Netflix, and Foursquare stored user names and passwords in unencrypted form on their Google-powered devices. Storing that data in plain text violates a commonly accepted best practice in computer security. Since many people tend to use the same usernames and passwords across any number of sites, the failing could help hackers penetrate other accounts. ViaForensics also found the iPhone version of Square's mobile payments app exposed a user's transaction amount history and the most recent digital signature of a person who signed an electronic receipt on the app. The apps exposed other types of personal data in plain text on cell phones, including e-mails sent from the app by a LinkedIn member, the movie queue of a Netflix app user, and the search history under Foursquare's Places tab. Source: <http://blogs.wsj.com/digits/2011/06/08/some-top-apps-put-data-at-risk/>

**Spanish police arrest 'Anonymous' PlayStation hackers.** Spanish police arrested three suspected members of the so-called "Anonymous" group June 10 on charges of cyber-attacks against targets including Sony's PlayStation network, governments, businesses, and banks. The police said the accused, arrested in Almeria, Barcelona, and Alicante, were guilty of coordinated computer hacking attacks from a server set up in a house in Gijon in the north of Spain. Spanish police alleged the three arrested "hacktivists" had been involved in the recent attack on Sony's PlayStation online gaming store which crippled the service for over a month, as well as cyber-attacks on Spanish banks BBVA and Bankia, and the Italian energy group Enel. Source: <http://www.reuters.com/article/2011/06/10/rc-spain-anonymous-idUSLDE7591FV20110610>

**Phishers LAMP Web hosts.** Phishers compromise LAMP-based Web sites for days at a time and hit the same victims over and over again, according to an Anti-Phishing Working Group (APWG) survey. Sites built on Linux, Apache, MySQL, and PHP are the favored targets of phishing attackers, the APWG report found, with between 76 and 82 percent of respondents using one or more components of the LAMP architecture. All 270 Web sites surveyed had been cracked. In the vast majority of cases, the sites were not the primary targets, but were compromised to act as launching pads for phishing attacks against third parties. "While we acknowledge that LAMP — Linux, Apache, MySQL, PHP — is the most popular web operating environment, the APWG IPC is concerned that this profile is exploited with such apparent frequency," the report noted. According to the latest numbers from Netcraft, Apache has about a 63 percent market share. The APWG survey also found that 37 percent of sites had been compromised more than once in the last 12 months, and that 35 percent were under the control of the attackers for 2 days or more. The report also showed that many Web masters were largely clueless about how and when the attackers managed to break in — 52 percent of respondents had to be notified about the breach by anti-phishing companies. Thirty-four percent of respondents blamed their PHP applications for the compromise, but 45 percent admitted they had no idea how the attackers got in. Source: [http://www.theregister.co.uk/2011/06/10/domains\\_lamped/](http://www.theregister.co.uk/2011/06/10/domains_lamped/)

## UNCLASSIFIED

## **NATIONAL MONUMENTS AND ICONS**

**(Arizona) Arizona fires: Monument Fire forces chaotic evacuation.** Firefighters at the Wallow Fire in the northeastern part of Arizona battled intense winds, which were expected to continue June 16 with gusts up to 42 mph. A surprise flare-up 1 mile south of Eagar prompted fire crews to alert residents of several of the town's subdivisions to prepare to evacuate if the situation worsened. But fire officials said areas previously burned nearby would help control the newly spreading fire. The Wallow Fire, which had consumed 487,016 acres, was 33 percent contained. Firefighters raced June 16 to build break lines ahead of the wind-whipped Monument Fire in southern Arizona, but the fire jumped Arizona 92 and forced the evacuation of Hereford, an unincorporated area south of Sierra Vista that has 3,200 homes. Local police, county sheriff's deputies, and fire officials swarmed neighborhoods with sirens blaring and officers on speakers imploring, "You've gotta get out now!" The fast-moving fire burned 50 homes earlier the week of June 13, and more June 16 near Stump Canyon Road as wind and rough terrain hampered fire crews' efforts. Steep canyons full of pine and oak trees and grasslands made firefighting a challenge. More than 1,500 people have been evacuated, the chief deputy for the Cochise County Sheriff's Office said. Source: <http://tucsoncitizen.com/arizona-news/2011/06/17/arizona-fires-monument-fire-forces-chaotic-evacuation/>

**(Florida) 4 wildfires burn more than 4,700 acres in Big Cypress National Preserve.** Four wildfires are burning in the Big Cypress National Preserve in Florida after lightning started them June 13, the National Park Service reported June 15. Due to the location of one of the fires, the Concho Billie, Windmill Tram, and Burns Lake access points are closed to all backcountry activity. In all, the fires are burning more than 4,700 acres of federally managed land, according to the Park Service. The Florida Division of Forestry is reinforcing fire lines on the northern boundary of the Monkey Fire, a wildfire estimated at 2,800 areas burning in Big Cypress. Two units were working on the fire lines, according to a wildfire mitigation specialist with the state's Caloosahatchee Forestry Center. Source: <http://www.marconews.com/news/2011/jun/15/4-wildfires-burn-more-4700-acres-big-cypress-natio/>

**(Arizona; New Mexico) Arizona wildfire is now the state's largest ever.** The Wallow Fire in Arizona became the largest wildfire in the state's history June 14, surpassing the 2002 Rodeo-Chediski fire, according to officials with Apache-Sitgreaves National Forest. The amount of land burned by the fire grew to about 733 square miles, forest officials reported June 14. The Rodeo fire covered 732 square miles. The blaze was about 18 percent contained, fire officials said June 14, nearly double the containment figure reported the day before, when officials reported the northward advance had been stopped. Meanwhile, another fire broke out June 13 in southern New Mexico at Carlsbad Caverns National Park, officials said. Hundreds of visitors were evacuated as crews tackled the 3,000-acre wildfire inside the park. Calmer winds were helping firefighters get the upper hand on the Wallow Fire in Arizona, which has been burning since late May, said the operations chief for the Southwest Incident Management team. In the town of Greer, part of which was burned by the fire, work was under way to make it safe for people to return, the town's fire chief said. Residents were already moving back to Springerville, Eagar, and South Fork after authorities lifted evacuation orders June 12. Authorities warned residents

## UNCLASSIFIED

of the towns that air quality could continue to be a problem, and food in refrigerators may have spoiled. Source: [http://www.cnn.com/2011/US/06/14/arizona.wildfires/index.html?hpt=hp\\_t1](http://www.cnn.com/2011/US/06/14/arizona.wildfires/index.html?hpt=hp_t1)

**(Colorado; New Mexico) Wildfire in NM keeps Raton Pass closed Monday.** Interstate 25 was closed June 13 over Raton Pass because of a large wildfire burning just south of the Colorado border with New Mexico. The Track Fire has now grown to 2,700 acres. About 200 structures, both residential and commercial, were threatened by the fire. The fire started on the west side of Interstate 25 and jumped to the east side June 12. It was moving north toward the Colorado/New Mexico state line, and also to the east-south east toward Raton, Sugarite State Park, and Bartlett Mesa. There were evacuations in northern Raton, north of I-25, and north of County Road 72. Sugarite State Park was also evacuated. Drivers on southbound I-25 were being stopped at mile marker 11. Local traffic was still permitted to use the interstate, but no one was allowed to cross the state line. The fire was burning actively in pinon and juniper in rugged terrain. Source: <http://www.kktv.com/home/headlines/123716349.html>

**(Oregon) Forest Service: Cave vandals caught.** Law enforcement officers with the U.S. Forest Service said they have apprehended suspects whom they believe may have vandalized a historic cave in Central Oregon. The vandalism occurred sometime in late April of 2011 at the Hidden Forest Cave in the Deschutes National Forest. Vandals chopped down trees and set a fire inside the cave. They also spray-painted extensively both outside and inside the cave, covering native pictographs. "Through that we received some tips that have lead us to apprehend five suspects in that damage. Their case has been sent to the Department of Justice and the Department of Justice will consider what kind of charges to take in the matter," a spokeswoman for the Deschutes National Forest said. The suspects could face misdemeanor or felony charges under the Archaeological Resources Protection Act. If convicted, they could face up to 10 years in jail, and up to \$100,-000 in fines. Source: <http://news.opb.org/article/forest-service-cave-vandals-caught/>

## **POSTAL AND SHIPPING**

**UK blocks UPS sites over security.** United-States based shipping company United Parcel Service (UPS) has been barred from moving air cargo through some United Kingdom facilities because of security deficiencies, the British government said June 17. The department for transport disclosed the action, but gave no information on the security issues and did not identify the locations involved. It said: "following careful consideration, the department has restricted the number of sites in the U.K. at which UPS Ltd. are permitted to screen air cargo until it has satisfied current security requirements." The department said it could not give details of the sites for security reasons. UPS told customers June 17 that shipments from Britain were being delayed, but did not give further details. The vulnerability of air cargo to terrorist attacks is a major worry for international security agencies. Source:

<http://www.google.com/hostednews/ap/article/ALegM5iJVWPbYe5shYiHGLW4rUpRCT1ag?docId=6010a231fbff4ebcb8e56288ed211954>

UNCLASSIFIED

## UNCLASSIFIED

**(Utah) Suspicious letter found at Utah IRS office.** Utah fire officials said a suspicious envelope prompted authorities to evacuate a single Internal Revenue Service worker from an Ogden federal building June 14. A deputy fire chief said the worker noticed some white powder in an envelope while opening the mail on the sixth floor of the 25th Street building. He said the worker immediately placed the envelope and letter opener inside of a large envelope, shut down the office ventilation system, and called authorities. The fire department's hazardous materials team determined the powder was harmless and turned the material over to the FBI for testing. The worker suffered no injury or illness and returned to work. The incident is under investigation by federal authorities. Source:

<http://www.therepublic.com/view/story/dae3432991fb49fa9b63ca2ddeebfe68/UT--Suspicious-Letter/>

## **PUBLIC HEALTH**

**FDA says Takeda diabetes drug raises cancer risk.** Takeda Pharmaceutical's Actos diabetes drug can increase the risk of bladder cancer if used for more than a year, U.S. drug regulators said June 15. The Food and Drug Administration (FDA) said it is adding this information to the label for the drug after reviewing the preliminary 5-year results of an ongoing 10-year study. The announcement comes after France and Germany suspended sales of Actos the week of June 6 due to similar worries about a possible risk to bladder cancer. Japan's Takeda has garnered close to \$5 billion in worldwide sales from Actos, its best-selling drug. However, Actos faces looming generic competition, potentially muting any financial impact from regulatory actions. About 2.3 million patients filled a prescription for a product containing pioglitazone, the clinical name for Actos, from January to October of 2010, the FDA said. It said it will continue to evaluate data from the ongoing 10-year epidemiological study, and will also review the results from a French study, which prompted the suspension of Actos in France. Source:

<http://www.reuters.com/article/2011/06/15/us-drugs-fda-actos-idUSTRE75E5Q220110615>

**Feds move toward health claims database despite privacy fears.** Despite lingering privacy concerns, the U.S. Office of Personnel Management (OPM) is plowing ahead with plans to build a massive centralized database containing detailed healthcare claims information on millions of federal employees and their families. The agency June 15 released two formal notices in the Federal Register detailing plans for the new Health Claims Data Warehouse. One of the notices describes how the OPM will use the database, the other describes how the OPM Inspector General's office will use it. Work on the database begins July 15. The notices — known in government parlance as systems-of-records notices — are aimed at addressing some of the concerns raised by several privacy groups when the OPM first detailed its plans last October. The outcry prompted the OPM to push back its original deadline. Source:

[http://www.computerworld.com/s/article/9217680/Feds\\_move\\_toward\\_health\\_claims\\_database\\_despite\\_privacy\\_fears](http://www.computerworld.com/s/article/9217680/Feds_move_toward_health_claims_database_despite_privacy_fears)

**Childhood diseases return as parents refuse vaccines.** There have been at least 152 cases of measles diagnosed in the United States so far this year — twice the number seen in a typical

UNCLASSIFIED

## UNCLASSIFIED

year and the biggest outbreak in 15 years, said the Centers for Disease Control and Prevention (CDC). Half of patients have had to be hospitalized. For the doctors and nurses caring for patients, the return of vaccine-preventable diseases such as measles — a viral illness that once killed 3,000 to 5,000 Americans a year — is both frightening and all too predictable. All can be deadly. Although overall vaccine coverage remains high, about 40 percent of parents say they have deliberately skipped or delayed a shot for their children. Worldwide, the disease killed 164,000 people in 2008. Before a vaccine was available, 3.5 million Americans got measles each year, 100,000 were hospitalized, and 3,000 to 5,000 died, a spokesman from the Children's Hospital of Philadelphia said. In the past 3 years, doctors also have seen outbreaks of other vaccine-preventable diseases, such as mumps, whooping cough and a life-threatening bacterial infection called Hib. All can be deadly. The CDC said travelers should consider getting a measles shot if going abroad, due to major outbreaks in Europe, and Southeast Asia. Source:

<http://yourlife.usatoday.com/health/medical/story/2011/06/Childhood-diseases-return-as-parents-refuse-vaccines/48414234/1?csp=34news>

**Government lists formaldehyde as cancer causer.** The strong-smelling chemical formaldehyde causes cancer, while styrene, a second industrial chemical that's used worldwide in the manufacture of fiberglass and food containers, may cause cancer, the National Institutes of Health (NIH) said. The NIH said June 10 that people with higher measures of exposure to formaldehyde are at increased risk for certain types of rare cancers, including those affecting the upper part of the throat behind the nose. The chemical is widely used to make resins for household items, including paper product coatings, plastics and textile finishes. It also is commonly used as a preservative in medical laboratories, mortuaries and consumer products including some hair straightening products. The government said styrene is a component of tobacco smoke, and NIH said the greatest exposure to the chemical is through cigarette smoking. The two chemicals were among eight added to the government's list submitted to Congress of chemicals and biological agents that may put people at increased risk of cancer.

Source: <http://yourlife.usatoday.com/health/medical/cancer/story/2011/06/Government-lists-formaldehyde-as-cancer-causer/48352682/1>

**(Missouri) Fungal infection adds to Missouri toll from tornado.** The death toll from the tornado that destroyed much of Joplin, Missouri has risen to 151, and three of the latest victims suffered from a rare fungal infection that can occur when dirt becomes embedded under the skin, authorities said June 10. The Jasper County coroner said the three had been hospitalized with the unusually aggressive infection sometimes found in survivors of other natural disasters. He said it was difficult to identify the fungus as a cause of death since the people infected also suffered other severe injuries. A doctor said his hospital treated five Joplin tornado victims for the infection, known as zygomycosis. Overall infection numbers were not available. The health department in Springfield-Greene County, where some patients were treated, declined to release information about patients sickened by the fungus, citing patient privacy concerns. The Springfield News-Leader reported that the department sent a memo June 13 to area health providers warning them to be on the lookout for the infections. Source:

## UNCLASSIFIED

## UNCLASSIFIED

<http://www.washingtontimes.com/news/2011/jun/12/fungal-infection-adds-to-missouri-toll-from-tornad/?page=all#pagebreak>

**(Wisconsin) Federal government takes action against drug manufacturer and distributor.** The U.S. Food and Drug Administration (FDA) announced June 13 that a consent decree of condemnation, forfeiture, and permanent injunction has been filed against H&P Industries Inc., The Triad Group Inc., and three individuals that would prevent them from manufacturing and distributing products from their Hartland, Wisconsin facility, or any other location. The Triad Group distributes and H&P Industries manufactures a variety of over-the-counter drug products including povidone-iodine and benzalkonium chloride antiseptic products, cough and cold products, nasal sprays, suppositories, medicated wipes, antifungal creams, and hemorrhoidal wipes. Under the decree, the defendants cannot resume manufacturing and distributing drugs or medical devices until they establish an acceptable Quality Assurance and Quality Control program to ensure that all products manufactured in their facilities comply with federal standards for quality and have the identity, purity, potency, and safety they are expected or are represented to possess. FDA inspections from 2009 to 2011 determined H&P failed to comply with rules intended to assure the safety, quality, and purity of manufactured drugs. Since December 2010, H&P has initiated five voluntary product recalls, including two because of bacterial contamination of their products. The FDA's most recent inspection of H&P, completed on March 28, found multiple violations. In April, U.S. Marshals seized more than \$6 million in products at the Hartland facility. Under the decree, the seized products are condemned and forfeited to the United States. The defendants, after posting a \$4 million bond with the court, may seek FDA's approval to "recondition" the seized articles. If the defendants' proposals are unacceptable to FDA, however, the company must destroy them at its own expense. Source: <http://www.mmdnewswire.com/federal-government-takes-action-against-drug-manufacturer-and-distributor-48764.html>

## **TRANSPORTATION**

**(Iowa) Amtrak steps up security following Iowa train sabotage.** Amtrak said it is taking additional security countermeasures after someone tried to derail a train carrying highly flammable ethanol in Iowa June 12. The Iowa Interstate Railroad CEO said a lock was cut off a track switch box just outside Menlo, a town that sits along the rail line between Des Moines and Omaha, Nebraska. The track was also "gapped open" about 2 inches, and a black bag was used to cover the switch signal so the tampering would be harder to notice. The CEO said the switch tampering, and the creation of the gap in the tracks, clearly indicated to him that someone was trying to derail one of the 130-car trains that were running the track. The Amtrak chief of police announced June 14 the company is expanding its comprehensive rail security efforts to provide increased right of way protection to detect and deter terrorists seeking to derail passenger trains. Amtrak said the additional security countermeasures would focus first on passenger trains, particularly those operating on the Amtrak-owned Northeast corridor. Amtrak said it already had security in place, which was focused on the threat of improvised

UNCLASSIFIED

## UNCLASSIFIED

explosive devices, in a station or on a train, or on an active shooter scenario. Source: <http://www.kgoam810.com/rssItem.asp?feedid=118&itemid=29680065>

**(West Virginia; Kentucky; Ohio) Exercise focuses on security.** The Transportation Security Administration in conjunction with federal, state, and local agencies planned to conduct an all-day training exercise June 15 in Wood County, West Virginia, designed to enhance security in the tri-state area. The Visible Intermodal Prevention and Response operation was slated to take place from 8 a.m. to 4 p.m. throughout 5,000 square miles in Kentucky, Ohio, and West Virginia. In Wood County, training was scheduled to be focused in and around the Ohio River and its tributaries, according to the director of the Wood County 911 Center. Participating teams include federal air marshals, canine teams, inspectors, and bomb appraisal officers. Source: <http://www.newsandsentinel.com/page/content.detail/id/549003/Exercise-focuses-on-security.html?nav=5061>

**(Iowa) Iowa railroad finds switch had been tampered with.** Railroad officials said someone tampered with a switch near Menlo, Iowa to try and derail a train. The Iowa Interstate Railroad's chief operating officer told Des Moines television station KCCI 8 that the switch box was broken into the morning of June 12. It sits about a quarter of a mile west of Menlo, which is about 40 miles west of Des Moines. The railroad official said a train went through the area and a crew member noticed there was something wrong with the switch. The dispatch office was notified, and a following train was stopped short of Menlo. He said the tampering would have caused a train to derail. The FBI is helping the Iowa State Patrol and the Guthrie County Sheriff's Office with the investigation. Source: <http://www.mysanantonio.com/news/article/iowa-railroad-finds-switch-had-been-tampered-with-1421433.php>

**Some flights resume in Melbourne after ash cloud strands 60,000 in Australia, New Zealand.** Airlines started flying a backlog of thousands of stranded passengers to and from Australia's second-largest city June 13 as ash from a Chilean volcano began to clear after forcing hundreds of cancellations. Most flights between Australia and New Zealand, however, remained grounded due to the drifting cloud of fine grit, which can damage airplane engines. Australia's Bureau of Meteorology said the ash cloud was large enough to continue disrupting flights. Several flights to and from Melbourne, the island state of Tasmania, and New Zealand were canceled June 12 after the ash moved across the Pacific from Chile, where it has been spewing from the Cordon Caulle volcano since June 4. In total, more than 60,000 passengers were stranded by the disruptions, which came amid a 3-day holiday weekend in Australia. Qantas estimated it could take 24 to 48 hours to clear just the Melbourne backlog. Source: [http://www.washingtonpost.com/world/asia-pacific/some-flights-resume-in-melbourne-after-ash-cloud-stranded-55000-in-australia-new-zealand/2011/06/13/AGdhJiSH\\_story.html](http://www.washingtonpost.com/world/asia-pacific/some-flights-resume-in-melbourne-after-ash-cloud-stranded-55000-in-australia-new-zealand/2011/06/13/AGdhJiSH_story.html)

## **WATER AND DAMS**

Nothing Significant to Report

UNCLASSIFIED

UNCLASSIFIED

## **NORTH DAKOTA HOMELAND SECURITY CONTACTS**

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center: 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 (BCI): 701-328-5500; North Dakota 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