



**UNCLASSIFIED**



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



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

**UNCLASSIFIED**

**NDSLIC DISCLAIMER**

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

**QUICK LINKS**

[North Dakota](#)

[Energy](#)

[Regional](#)

[Food and Agriculture](#)

[National](#)

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

[International](#)

[Information Technology and Telecommunications](#)

[Banking and Finance Industry](#)

[National Monuments and Icons](#)

[Chemical and Hazardous Materials Sector](#)

[Postal and Shipping](#)

[Commercial Facilities](#)

[Public Health](#)

[Communications Sector](#)

[Transportation](#)

[Critical Manufacturing](#)

[Water and Dams](#)

[Defense Industrial Base Sector](#)

[North Dakota Homeland Security Contacts](#)

[Emergency Services](#)

## **NORTH DAKOTA**

**Fire destroys classrooms at Lidgerwood, N.D., school.** A fire November 9 at the K-12 school in Lidgerwood, North Dakota, destroyed at least two classrooms and caused extensive smoke damage to the first floor of the building. The school was hosting a regional volleyball tournament, and fans, students, and players were evacuated from the gymnasium. Officials estimated that more than 100 people were in the building. No injuries were reported. Firefighters from Hankinson and Lidgerwood battled the blaze for more than an hour. The cause was not immediately determined. The school's principal said students likely will be sent to another school for classes during cleanup and repairs. Source: <http://www.grandforksherald.com/event/article/id/182888/group/homepage/>

**Pipe rupture kills one; two injured.** One is dead in a Montrail County gas line explosion. Police received a call around 1 p.m. from a caller who said he hit a gas line northwest of Tioga, North Dakota. The police and the fire department responded. They said a 30-year-old individual was working installing electrical lines when a plow hit Williston Basin Interstate Pipeline's high pressure gas line. It was charged with 650 pounds of pressure. The rupture threw the individual 100 feet to his death. Two other workers were taken to Tioga medical center and were later released. Police were still investigating the incident. Source: [http://www.kfyrtv.com/News\\_Stories.asp?news=44371](http://www.kfyrtv.com/News_Stories.asp?news=44371)

## **REGIONAL**

**(Minnesota) Firefighters contain anhydrous ammonia leak.** Red Wing, Minnesota firefighters safely contained a tank that had been leaking hazardous gas November 8. Firefighters were called at 3:10 a.m. to County Road 18 and Brink Road for an anhydrous ammonia leak. According to a press release from Red Wing Fire chief, firefighters could see a small plume of gas and discovered a trailer about 50 yards off County Road 18 in an open field. Firefighters, who first conferred with the state duty officer, closed the tank's valves and secured the leak. It appeared someone had cut a one-inch hose, causing the leak. The chief said investigation of the apparent tampering was turned over to Red Wing police. Anhydrous ammonia can be used in the illegal manufacturing of methamphetamines. Farmers use anhydrous ammonia as a fertilizer, but it can become dangerous if inhaled. No firefighters were exposed to the ammonia. Though County Road 18 was closed during the incident, no evacuations were necessary. He said it was unclear how long the tank had been leaking before firefighters were called. Source: <http://www.republican-eagle.com/event/article/id/70288/>

**(Minnesota) Minneapolis opens Emergency Operations Training Facility.** The City of Minneapolis, Minnesota has opened its new Emergency Operations Training Facility, which will help emergency responders and other city staff better prepare for and respond to emergencies. The multi-purpose building helps meet the training and response needs of the Minneapolis Fire Department, the Minneapolis Police Department, and the city's emergency management division, along with other regional partners. The facility includes training classrooms for Minneapolis firefighters and metro emergency managers, a strategic information center for the Minneapolis police, the main training site

## UNCLASSIFIED

for the State of Minnesota Structural Collapse Team, and an emergency operations center that will be used during significant emergencies or disasters. It will include apparatus bays for storage of emergency response vehicles and specialty equipment for the Coast Guard, state, city and Metro West region of Homeland Security. The U.S. Coast Guard will also use the facility as a monitoring location for cameras placed along the Mississippi River from St. Louis to the metro area. Source: <http://www.ci.minneapolis.mn.us/news/20101104NewEOTF.asp>

**(South Dakota) Wildfire burning south of Rapid City.** The Beretta Road off U.S. Highway 16 in South Dakota will remain closed November 9 and possibly November 10 as firefighters battle the Dead End Beretta Fire. The 18-acre fire is under investigation. The incident commander of Black Hills National Forest, Mystic Ranger District, was leading efforts to contain the fire by November 8. Fire crews had dug a fire line that day around 50 percent of the blaze northwest of Rockerville near Storm Mountain. No structures were threatened. The man-caused blaze was spotted early November 8 while fire officials were doing a routine check on a previous prescribed burn. Two hand crews, four U.S. Forest Service engines, and fire engines from Rockerville Volunteer Fire Department, Keystone Volunteer Fire Department, and Rapid City Fire Department were on site. Source: [http://www.rapidcityjournal.com/news/article\\_5ed1443c-eb55-11df-bea6-001cc4c002e0.html](http://www.rapidcityjournal.com/news/article_5ed1443c-eb55-11df-bea6-001cc4c002e0.html)

**(South Dakota) Flood-control work on target.** The second phase of the Sioux Falls, South Dakota, flood-control project around the Big Sioux River and Skunk Creek is on track to be finished at the end of next year. It is good news for the 1,800 homeowners who live in the floodplain and are required to buy flood insurance unless they do not have a mortgage. A dam near the union of Skunk Creek and the Big Sioux River is the main part of Phase 2 and is two-thirds complete, the principal city engineer said. The \$4 million dam is designed to stop water from going upstream and keep the estimated \$750 million worth of area property and buildings near it dry, the public works director said. It cost the city \$1.2 million to acquire the additional land and to cover the cost of fixing the affected holes. Construction on Phase 3, which includes raising levees at a different location and building a diversion dam, is expected to be finished by the end of next year. The project dates to 2000, when the mayor signed an agreement with the U.S. Army Corps of Engineers for an upgrade to the 1961 flood-control system. Work on the \$55 million project to purchase land and raise the levees at least 5 feet began in 2002. It will take an additional 8 to 12 months after the work is finished to get maps updated with the federal government to reflect the reduction of the flood plain. Source: <http://www.argusleader.com/article/20101106/NEWS/11060314/1001>

**(South Dakota) Power failure darkens Aberdeen, South Dakota-area towns.** Nearly 20 Aberdeen, South Dakota-area towns were without power November 6 after an electric substation went down in Redfield. NorthWestern Energy customers in Doland, Conde, Miranda, Loyaltown, Brentford, Redfield, Raymond, Rockford, Orient, Tulare, Chelsea, Northville, Zell, Cresbard, Athol, Frankfort, Mellette, and Ashton all lost power around 5:30 p.m., said the communications coordinator for NorthWestern. By 9:45 p.m., power had been restored to everyone. Many towns were back online within a few hours. Tulare and half of Redfield were the last to see electricity return. A cause for the outage was still being investigated the night of November 6. While the towns lost power when the substation in Redfield went down, the issue could have occurred elsewhere in the system. Extra crews were brought in to try to identify the cause. But because of the darkness, it was a difficult task. "It could be something as simple as an animal in a substation," the coordinator said. Source: <http://www.istockanalyst.com/article/viewiStockNews/articleid/4646584>

UNCLASSIFIED

## **NATIONAL**

**Testimony indicates poor cementing of drilling rigs is a widespread problem.** Drilling engineers and government officials are almost lackadaisical in their approach to the critical steps of closing down an offshore oil drilling rig and sealing it, 2 days of testimony before a Presidential commission investigating the explosion of BP's Deepwater Horizon drilling rig indicate. In testimony that concluded November 9, government officials, representatives of the companies drilling the well, and outside engineers all testified to shortfalls that showed the critical task of sealing the well with cement was filled with missteps and what the commission co-chairman called "a series of almost inexplicable failures." The panel's deputy legal counsel used the 2 days of detailed questioning to suggest the failings aboard the Deepwater Horizon rig were not a one-time event but the result of lax oversight, inadequate regulation, and inattention to detail that may exist on all deepwater drilling operations. One example of the problems that emerged November 9 was illustrated on BP's drilling application for the Deepwater Horizon well in the Gulf of Mexico, which the deputy legal counsel said called for using only a fraction of the cement needed to seal such a well. That fact did not trigger any questions from government engineers who approved the plan. Investigators now think the cement intended to seal the well failed, and that crude oil and natural gas surged up the Deepwater Horizon's drilling pipe when the rig's crew began to remove heavy drilling mud and then replaced it with lighter seawater. Source: <http://www.miamiherald.com/2010/11/09/1917737/testimony-indicates-poor-cementing.html>

## **INTERNATIONAL**

**Nuclear smuggling: Armenia arrests suspected supplier.** The Armenian government said November 8 it had detained a man suspected of supplying nuclear bomb-grade uranium to two smugglers caught in the Republic of Georgia earlier this year trying to sell it on the black market. The Armenian national security service said the man, who served several months in 2005 for a previous attempt to smuggle highly enriched uranium (HEU), had been arrested based on information from Georgian investigators. Officials said Armenian security officials were conducting a joint investigation into the March incident with their Georgian counterparts. Two Armenians pled guilty in a Tbilisi court to an attempt to sell a weapons-grade sample of HEU in the Georgian capital to a man they believed to be a representative of an Islamist jihadist group. The would-be buyer in the alleged March 11 deal was an undercover Georgian security agent. The two men admitted smuggling 18 grams of uranium into Georgia from Yerevan, the Armenian capital. The smugglers told Georgian investigators they were given the HEU by the supplier, a petty trader and an acquaintance of one of the men, who had boasted he could get hold of much more from contacts in the Urals and in Siberia. The Armenian smugglers were asking \$50,000 per gram for their sample and were offering more if the sale was successful. Source: <http://www.guardian.co.uk/world/2010/nov/08/nuclear-smuggling-armenia-arrest>

**Al Qaeda group takes credit for mail bomb plot.** A Yemen-based al Qaeda group is claiming responsibility for the international mail bomb plot uncovered the week of October 25. A week after authorities intercepted packages in Dubai and England that were bound for the United States, Al Qaeda in the Arabian Peninsula issued a message November 5 saying it will continue to strike American interests. Both mail bombs were wired to detonators that used cell phone technology. U.S. officials have said they believe it was the Yemen group. The claim was reported by the private SITE

## UNCLASSIFIED

Intelligence Group. On November 4, the French Interior Minister said the bomb was defused at England's East Midlands airport just 17 minutes before it was due to go off. The White House said November 4 they could not confirm that. Source:

<http://www.cbsnews.com/stories/2010/11/05/world/main7026751.shtml>

**Furious villagers storm water station.** About 100 residents from Sing Buri have stormed a water station in Ang Thong, Thailand, to demand the opening of sluice gates that they blame for causing persistent floods in their villages. Villagers from Tha Chang district turned out at Yang Manee water station in Pho Thong district about midnight November 2. They were infuriated when they discovered all of the sluice gates were closed. Villagers said closing the gates resulted in floodwaters from the Noi River accumulating in Sing Buri's Tha Chang district. Tensions flared when the Sing Buri villagers demanded some gates be opened. Officials at the water station refused to lift the gates. Some local villagers also turned up and insisted the gates be kept closed to prevent further flooding in their area. Station officials claimed they had been ordered by the "higher-ups" to close all sluice gates. Gunfire was heard as the Tha Chang villagers advanced to the station. The angry villagers demanded to know who had issued the order to shut the water gates. Police were called to the scene. Officials gave in and opened one gate in a bid to calm the situation. A village head in tambon Thorn Samor of Tha Chang district, said the irrigation department had assured the villagers the flooding situation would not get any worse. But the water levels in their villages rose quickly. Source:

<http://www.bangkokpost.com/news/local/204659/furious-villagers-storm-water-station>

**U.S. seeks to aid Africa in securing deadly bioagents.** A group of U.S. Defense Department arms control specialists is scheduled to travel to Africa the week of November 8 to support regional efforts to secure deadly pathogens that could be turned into biological weapons, a U.S. Senator announced. "Deadly diseases like Ebola, Marburg, and anthrax are prevalent in Africa," the Republican Senator from Indiana said in released remarks. "These pathogens can be made into horrible weapons aimed at our troops, our friends and allies, and even the American public. This is a threat we cannot ignore." He planned to accompany Pentagon experts in their examinations of scientific facilities in Uganda and Kenya. The laboratories are involved in infectious disease diagnosis and research and in supporting pandemic-curbing treatments. "We've discovered through [the U.S. Cooperative Threat Reduction program] that Soviet scientists used pathogens from Africa to make biological weapons during the Cold War," the Senator said in the release. "Those weapons are being destroyed. Now we have to secure their sources." Source: [http://gsn.nti.org/gsn/nw\\_20101104\\_6903.php](http://gsn.nti.org/gsn/nw_20101104_6903.php)

**Man in disguise boards international flight.** Canadian authorities are investigating an "unbelievable" incident in which a passenger boarded an Air Canada flight disguised as an elderly man, according to a confidential alert obtained by CNN. The incident occurred October 29 on Air Canada flight AC018 to Vancouver originating in Hong Kong. An intelligence alert from the Canada Border Services Agency described the incident as an "unbelievable" case of concealment. "Information was received from Air Canada Corporate Security regarding a possible impostor on a flight originating from Hong Kong," the alert said. "The passenger in question was observed at the beginning of the flight to be an elderly Caucasian male who appeared to have young looking hands. During the flight the subject attended the washroom and emerged an Asian looking male that appeared to be in his early 20s." After landing in Canada, border services officers escorted the man off the plane where he "proceeded to make a claim for refugee protection," the alert said. Source:

<http://www.cnn.com/2010/WORLD/americas/11/04/canada.disguised.passenger/index.html?hpt=C1>

UNCLASSIFIED

## UNCLASSIFIED

**Delta plane cleared after search at airport in India.** Security officials in Mumbai, India, have now given the all-clear after searching a Delta flight that landed at the city's airport. The plane was checked for suspicious cargo after a warning from airline staff in Amsterdam, where the flight originated. The plane was flanked by fire trucks and other emergency vehicles after landing, and was taken to an isolated area where it was inspected by bomb squads and airport security. An airport official said nothing was found, and the cargo was cleared. He said all 244 passengers on board Delta flight 70 were evacuated safely after the landing. Source:

[http://www.wlos.com/template/inews\\_wire/wires.international/2d16da3f-www.wlos.com.shtml](http://www.wlos.com/template/inews_wire/wires.international/2d16da3f-www.wlos.com.shtml)

**Seven Israeli defendants charged in multi-million dollar lottery telemarketing fraud scheme.**

Federal prosecutors and the FBI announced the extradition from Israel to the United States of seven individuals, all residents of Israel, on charges relating to a lottery telemarketing fraud scheme through which they stole approximately \$2 million from elderly victims in the United States between 2007 and September 2008. This is the largest number of Israeli citizens ever extradited to a foreign country in a single case. The defendants participated in a phoney "lottery prize" scheme that targeted hundreds of victims, mostly elderly, throughout the United States. They identified victims by purchasing the names and contact information of U.S. residents who subscribed to sweepstakes lotteries from list brokers. They then contacted the victims and solicited information about their finances by falsely telling them they had won a substantial cash prize they would receive as soon as they paid the necessary fees and taxes. In reality, there was no lottery prize and the victims were ultimately robbed. All seven defendants were provisionally arrested in Israel in September 2008 based on the indictments. Source: <http://www.empirestatenews.net/News/20101105-2.html>

## **BANKING AND FINANCE INDUSTRY**

**New, improved Trojans target banks.** Security researchers are warning financial institutions about the Qakbot Trojan, a rare kind of malware that is allegedly infiltrating large banks and other global financial institutions. It is unlike other types of malware because it has the ability to spread like a worm, but still infect users like a Trojan. Named for its primary executable file, \_qakbot.dll, the Trojan is not new, but its qualities and difference in attack set it head and shoulders above other more well-known Trojans, such as Zeus, in that it can infect multiple computers at a time. It is the only Trojan known to exclusively target U.S. banks, said an RSA security researcher. The more well-known Trojans and their variants, Zeus and Spyeeye, are all available for sale on the black market, said the researcher who is head of new technologies, consumer identity protection at RSA, the security division of EMC. First discovered by Symantec in 2007, Qakbot is likely being run by one group. It is likely an organized crime group developed it, focusing on their own specific methods, and tailored the Trojan to a specific segment — large banks and their commercial customers. Source:

[http://www.bankinfosecurity.com/articles.php?art\\_id=3075](http://www.bankinfosecurity.com/articles.php?art_id=3075)

**Online banking, ATM outage: malware likely to blame.** Malware is likely to blame for the so-called "computer glitch" that took down a handful of the country's largest banks' ATMs and online banking sites over the weekend of November 5. The nation's three largest banks and a handful of others were derailed over the weekend when their ATM and online banking channels were taken down. All of the institutions affected — Bank of America, Chase, U.S. Bank, Wells Fargo, Compass, USAA, Suntrust, Chase, Fairwinds Credit Union, American Express, BB&T on the East Coast, and PNC — are blaming

UNCLASSIFIED

## UNCLASSIFIED

the outage on a computer glitch related to the time-zone change. But a senior analyst at Aite Group LLC who covers banking and payments fraud said there is likely a great deal more going on behind the scenes. In fact, she suspects the weekend outage is related to a widespread malware attack. "It has all the hallmarks of that, based on the geographic spread of it, the targeted systems and the banks in question," she said. Source: <http://www.bankinfosecurity.com/podcasts.php?podcastID=837>

**ATMs crash across the country after 'Bank Holiday' warning.** Following rumors of a "bank holiday" that could limit or prevent altogether cash withdrawals later the week of November 8, Twitter and other Internet forums were raging November 7 about numerous ATMs across the United States that crashed early November 7, preventing customers from performing basic transactions. It is unknown whether the crashes were partly a result of a surge of people trying to withdraw money in preparation for any feared bank shutdown, or if mere technical glitches were to blame. The fact that the problem affected numerous different banks in different parts of the United States would seem to indicate the former. The Orange County Register reported that the problems were "part of a national outage" which prevented people from performing simple transactions such as cashing checks and withdrawing money. "Computer issues" were blamed for similar issues in Phoenix, Arizona, while in Birmingham, Alabama, Wells Fargo customers' online banking accounts and ATMs displayed incorrect balances. The banks primarily affected were Wells Fargo, Chase, and Bank of America, but according to a blogger who studied Twitter feeds and other Internet message boards that were alight with the story, numerous other financial institutions were also affected, including US Bank, Compass, USAA, Sun Trust, Fairwinds Credit Union, American Express, BB&T on the East Coast, and PNC. Source: <http://www.prisonplanet.com/atms-crash-across-the-country-after-bank-holiday-warning.html>

**Firm finds security holes in mobile bank apps.** A security firm disclosed holes November 4 in mobile apps from Bank of America, USAA, Chase, Wells Fargo, and TD Ameritrade, prompting a scramble by most of the companies to update the apps. "Since Monday [November 1], we have been communicating and coordinating with the financial institutions to eliminate the flaws," research firm viaForensics wrote in a post on its site. "The findings we published reflect testing completed on November 3. Since that time, several of the institutions have released new versions and we will post updated findings shortly." The company had reported its findings to The Wall Street Journal earlier in the day. On November 3, viaForensics went public with problems in PayPal's iPhone app, spurring the online payment provider to action. Specifically, viaForensics concluded that: the USAA's Android app stored copies of Web pages a user visited on the phone; TD Ameritrade's iPhone and Android apps were storing the user name in plain text on the phone; Wells Fargo's Android app stored user name, password, and account data in plain text on the phone; Bank of America's Android app saves a security question (used if a user was accessing the site from an unrecognized device) in plain text on the phone; and Chase's iPhone app stores the username on a phone if the user chose that option, according to the report. Source: [http://news.cnet.com/8301-27080\\_3-20021874-245.html](http://news.cnet.com/8301-27080_3-20021874-245.html)

## **CHEMICAL AND HAZARDOUS MATERIALS SECTOR**

**AP1000 impact study not adequate.** Westinghouse has been told to resubmit its assessment of aircraft impact on the AP1000 reactor. The Nuclear Regulatory Commission (NRC) said documents put to it in order to demonstrate a 2009 requirement did not include "realistic" analyses, which amounted to a violation of requirements Westinghouse must explain and rectify. A 2009 NRC rule states that new nuclear power plant buildings and safety systems must maintain containment,

UNCLASSIFIED

## UNCLASSIFIED

cooling of the reactor core, and the integrity or cooling of used fuel facilities in the event of the impact of a large passenger jet. All reactor vendors must fulfill this requirement for their designs. For Westinghouse, this regulatory work comes in addition to a 2007 design amendment to the original AP1000 design, which was certified by the NRC in 2006. Source: [http://www.world-nuclear-news.org/IT AP1000 impact study not adequate 0911101.html](http://www.world-nuclear-news.org/IT_AP1000_impact_study_not_adequate_0911101.html)

**(Vermont) Vt. nuke plant closes after radioactive water leak.** Technicians at the Vermont Yankee nuclear power plant are getting into the section of the plant where a pipe began leaking radioactive water, forcing the Vernon, Vermont plant to shut down. A plant spokesman said November 8 technicians had begun checking repair options and trying to determine how long the plant will be offline. The reactor was shut November 7 after the leak was spotted during routine surveillance. The cause was unknown. The Nuclear Regulatory Commission said the public was not in danger. It was the second shutdown within 1 hour at a plant owned by New Orleans-based Entergy Corp. A transformer exploded at a nuclear power plant north of New York City, forcing an emergency shutdown. No one was injured and no radioactive materials leaked. Source: <http://www.google.com/hostednews/ap/article/ALeqM5j2iEnkuCw7AlhkdiMAKUP6a-wO3A?docId=102bef213be848efada97029a4a89271>

**(New York) Entergy's Indian Point reactor unit shut by explosion.** An explosion on Entergy Corp's main transformer November 7 shut the 1,020-megawatt Unit 2 at the Indian Point nuclear power plant in Buchanan, New York, the second shutdown at the company's nuclear plants within 1 hour. The company has also shut its 605-megawatt nuclear plant in Vernon, Vermont due to a system pipe leakage. The reactor is known to have leaked tritium twice this year and the Vermont Senate has voted to permanently shut the plant in 2012. News of the two shutdowns arrive at a time when Entergy faces a civil investigation by the U.S. Department of Justice into the way the power utility operates its transmission system and power plants in Louisiana, Arkansas, Mississippi, and Texas. There were no casualties or injuries associated with the November 7 explosion at the Indian Point reactor and no resulting fire, a company spokesman said. Source: <http://uk.reuters.com/article/idUKSGE6A707A20101108>

## **COMMERCIAL FACILITIES**

**(Indiana) Bomb squad sent to Mishawaka shopping plaza.** Police, the bomb squad, and the FBI were on high alert in Mishawaka, Indiana, while responding to a suspicious package November 8. Police were called to the Boxes Plus store in the Wilshire Plaza around 1:30 p.m.. They blocked off five store fronts. Police said the bomb squad and FBI arrived shortly after. WSBT saw an officer in a blast suit and a robot being sent in to investigate before being asked to leave by the FBI. According to police, an addressed package was left unattended in front of the store. A worker then picked the package up and took it to the back of the building before notifying police. Police blew up the package. There was nothing explosive inside. Police are still investigating what was inside. Source: <http://www.wsbt.com/news/wsbt-bomb-squad-sent-to-mishawaka-s-110810,0,3881699.story>

**(Maryland) Possible pipe bomb found in apartment near NASA center.** The Prince George's County bomb squad blew up a possible pipe bomb November 8, which was found in a Lanham, Maryland apartment complex across the street from NASA's Goddard Space Flight Center. The suspicious device was reported to the Prince George's County Fire/EMS Department around 9 a.m. when a

UNCLASSIFIED

## UNCLASSIFIED

maintenance man found it in a vacant apartment at the Glendale Apartments, the battalion chief said. When bomb technicians entered the building at Good Luck Road, they found a device with wires coming out of it that resembled a pipe bomb. The device was placed inside a bomb squad robot and detonated. The remains have been turned over to authorities in the Bureau of Alcohol, Tobacco, Firearms and Explosives for evaluation, the chief said. Residents were evacuated from two buildings in the apartment complex as a precaution, but no one was injured, she said. The apartment where the device was found was vacant for a short time, though the battalion chief could not say exactly how long. Source: [http://www.gazette.net/stories/11082010/prinnew135838\\_32560.php](http://www.gazette.net/stories/11082010/prinnew135838_32560.php)

**(Nevada) Las Vegas Walmart: Wal-mart evacuated after shot fired, bomb threat.** A Las Vegas, Nevada Walmart was evacuated November 6 after an armed man dropped what appeared to be an explosive device, police said. The incident happened at a store on South Rainbow Boulevard near I-215, Las Vegas police said. Store security had tried to confront a man who wrote a bad check. The suspect struck the security officer with a gun and fled, dropping a backpack with the device inside, police said. A Las Vegas police lieutenant said the bomb squad removed the device. The suspect got away, but police said he left identification at the store. Source: <http://www.lvrj.com/news/wal-mart-evacuated-after-shot-fired--bomb-threat-106874013.html?ref=013>

**(West Virginia) Possible explosive devices found at local religious community.** Residents in the New Vrindaban Community in Marshall County, West Virginia, which houses the Palace of Gold, believe they were the target to a hate crime. It was during a festival just after 12:30 a.m. October 31 when someone drove down a community road, threw some sort of explosive device out the window, and onto the community's property. The night guard said he, along with several hundred community members and tourists, were inside the Hare Krishna Temple when he heard a loud boom outside. Some of the remnants are still left on site where witnesses said the explosive device ignited. A piece of tinfoil was found melted on the cement. The guard described the device as a Lipton tea bottle with tinfoil and some sort of chemical inside. Three other devices were found in the surrounding area. He said none of those ignited. The Marshall County sheriff said he wants the Bureau of Alcohol, Tobacco and Firearms to take a look at the devices. Source: <http://www.wtrf.com/story.cfm?func=viewstory&storyid=89122&catid=3>

**(California) Bomb scare at Clovis shopping center.** A bomb scare forced several Clovis, California businesses to evacuate November 6. It happened at the Wild West Village Shopping Center near Shaw and Villa. Witnesses reported seeing a pipe with wires sticking out of it — in a trash can in front of a store. Officers from the Clovis Police Department's Bomb Squad responded. They set a small charge on the pipe to destroy it. Nobody was hurt in the incident and there was no major damage. Nearby businesses were evacuated as a precaution. Source: <http://abclocal.go.com/kfsn/story?section=news/local&id=7768177>

## **COMMUNICATIONS SECTOR**

**iPhone's Safari dials calls without warning, says security expert.** A security researcher is asserting that Apple has made a poor security decision by allowing its Safari browser to honor requests from third-party applications to perform actions such as making a phone call without warning a user. Safari, like other browsers, can launch other applications to handle certain URL protocols. These might be in clickable links, or in embedded iframes. An iframe containing a URL with a telephone

UNCLASSIFIED

## UNCLASSIFIED

number, for example, will cause Safari to ask if the user wants to make a phone call to that particular number, wrote a security researcher, on the SANS Application Security Street Fighter blog. Users can tap a button to make or cancel the call. But the researcher found that behavior changes in some cases. For example, if a user has Skype installed and stays logged into the application, Safari does not give an alert when it encounters a Skype URL in an iframe, and immediately starts a Skype call, he said. The researcher said he contacted Apple. The company said third-party applications should be coded to ask permission before performing a transaction. But in the current arrangement, third-party applications can only ask for authorization after a person has been “yanked” out of Safari and the application has been fully launched. “A solution to this issue is for Apple to allow third-party applications an option register their URL schemes with strings for Safari to prompt and authorize prior to launching the external application,” he wrote. Source:

[http://www.computerworld.com/s/article/9195578/iPhone\\_s\\_Safari\\_dials\\_calls\\_without\\_warning\\_s\\_ays\\_security\\_expert](http://www.computerworld.com/s/article/9195578/iPhone_s_Safari_dials_calls_without_warning_s_ays_security_expert)

**Report: Sprint rejected Huawei, ZTE for security concerns.** Sprint Nextel turned down bids from ZTE and Huawei Technologies because of U.S. government concerns over possible dangers to national security from the Chinese vendors building critical infrastructure in the United States, the Wall Street Journal reported November 5. Sprint, the nation’s third-largest mobile operator, rejected ZTE and Huawei’s bids to modernize its network even though they were lower than those of three rival companies, the Journal reported. The other bidders were Ericsson of Sweden, Samsung Electronics of South Korea, and Alcatel-Lucent, which is based in Paris and incorporates the former U.S. telecom vendor Lucent. Some U.S. lawmakers have expressed concern over letting Huawei or ZTE participate in major infrastructure projects because of concerns over possible links with the Chinese government and military. They worry the Chinese military could use equipment from the companies to disrupt U.S. communications. The Journal reported that the U.S. Secretary of Commerce had called the Sprint CEO the week of November 1 to voice concerns about possible deals between Sprint and the two companies, though not to ask him to reject the companies’ bids. Source:

[http://www.computerworld.com/s/article/9195278/Report\\_Sprint\\_rejected\\_Huawei\\_ZTE\\_for\\_security\\_concerns](http://www.computerworld.com/s/article/9195278/Report_Sprint_rejected_Huawei_ZTE_for_security_concerns)

**FCC warns of looming wireless spectrum shortage.** Mobile data traffic in the United States will be 35 times higher in 2014 than it was in 2009, leading to a massive wireless spectrum shortage if the government fails to make more available, the Federal Communications Commission (FCC) said in a paper released October 2010. About 42 percent of U.S. mobile customers now own a smartphone, up from 16 percent 3 years ago, and between the first quarter of 2009 and the second quarter of 2010, data use per mobile line grew by 450 percent, the paper said. The FCC expects smartphone use — and a corresponding increase in mobile data use — to continue to skyrocket, the FCC Chairman said. “If we don’t act to update our spectrum policies for the 21st century, we’re going to run into a wall — a spectrum crunch — that will stifle American innovation and economic growth and cost us the opportunity to lead the world in mobile communications,” he warned. In a national broadband plan released in March 2010, the FCC called for 300 MHz of spectrum to be made available for mobile broadband uses in the next 5 years, and an additional 200 MHz in the subsequent 5 years. Much of that spectrum would come from bands now controlled by the FCC or other government agencies, but 120 MHz would come from spectrum now owned but unused by U.S. television stations. Under the broadband plan, the stations would give back unused spectrum in exchange for part of the profits when the spectrum is sold at auction. The FCC would need congressional approval to hold these so-

UNCLASSIFIED

## UNCLASSIFIED

called incentive auctions. Source:

[http://www.computerworld.com/s/article/352502/FCC\\_Wireless\\_Spectrum\\_Shortage\\_Looms?taxonomyId=70](http://www.computerworld.com/s/article/352502/FCC_Wireless_Spectrum_Shortage_Looms?taxonomyId=70)

**(Texas) Researcher releases Web-based Android attack.** A computer security researcher released code November 4 that could be used to attack some versions of Google's Android phones over the Internet. The attack targets the browser in older, Android 2.1-and-earlier versions of the phones. It was disclosed November 4 at the HouSecCon conference in Houston by a security researcher with Alert Logic. The researcher said he has written code that allows him to run a simple command line shell in Android when the victim visits a Web site that contains his attack code. The bug used in the attack lies in the WebKit browser engine used by Android. Google said it knows about the vulnerability. "We're aware of an issue in WebKit that could potentially impact only old versions of the Android browser," a Google spokesman confirmed in an e-mail. "The issue does not affect Android 2.2 or later versions." Version 2.2 runs on 36.2% of Android phones, Google says. Older phones such as the G1 and HTC Droid Eris, which may not get the updated software, could be at risk from this attack. Android 2.2 is found on phones such as the Droid and the HTC EVO 4. Source: [http://www.computerworld.com/s/article/9195058/Researcher\\_releases\\_Web\\_based\\_Android\\_attack](http://www.computerworld.com/s/article/9195058/Researcher_releases_Web_based_Android_attack)

## **CRITICAL MANUFACTURING**

**Hackers' future target: automobiles.** the chief technology officer and vice president at integrator Northrop Grumman Information Systems said most cars contain 50, perhaps 100 or more tiny computers accessed through a diagnostic port that could be used to "take over a car by controlling the brakes, the accelerator, the steering wheel, despite whatever the driver might want to do." A paper, Experimental Security Analysis of a Modern Automobile, delivered earlier this year at an IEEE journal symposium, said the potential attack window could widen as more automakers provide vehicle-to-vehicle and vehicle-to-infrastructure communications networks to third-party development: "An attacker who is able to infiltrate virtually any electronic control unit can leverage this ability to completely circumvent a broad array of safety-critical systems," the paper said. In the lab and road tests, the researchers took control of a number of a car's functions and the driver could do nothing about it. They bypassed basic network security protection within the car, and embedded malicious code in its telematics unit to erase any evidence of the hack's presence after a crash. The Northrop Grumman CEO sees the threat to cars as more theoretical than practical. But he said it shows people must think about cybersecurity more broadly than they have in the past. Source: <http://blogs.govinfosecurity.com/posts.php?postID=780>

**In Qantas blowout, concern for jet engine maker.** Shares of Rolls-Royce, the British aircraft engine maker, extended their declines November 5 after the chief executive of Qantas suggested that a design flaw or manufacturing defect was the most likely explanation for a engine blow-out that forced one of the Australian carrier's A380 jets to make an emergency landing in Singapore November 4. "We believe this is probably, most likely, a material failure or some sort of design issue," the Qantas chief executive said at a news conference in Sydney. "We don't believe this is related to maintenance in any way." The episode, involving a Qantas A380 jetliner carrying more than 450 people, was particularly alarming because it occurred on the world's largest passenger plane and a flagship for Airbus, a unit of the European Aeronautic Defense and Space Company, or EADS. Rolls-

UNCLASSIFIED

# UNCLASSIFIED

Royce of London, which is a separate company from the carmaker owned by BMW, is also developing an engine for Boeing's latest aircraft, the 787 Dreamliner. Problems with that engine have contributed to that program's delays. Source:

[http://www.nytimes.com/2010/11/06/business/global/06engine.html?\\_r=1&partner=rss&emc=rss](http://www.nytimes.com/2010/11/06/business/global/06engine.html?_r=1&partner=rss&emc=rss)

## **DEFENSE/ INDUSTRY BASE SECTOR**

**Navy suspends Alliant Techsystems missile tests following software failure.** The U.S. Navy halted tests of an Alliant Techsystems Inc. anti-radar missile following 6 software or circuit-card failures in the first 12 trials. It is "a rare occurrence" to stop combat testing so soon, the Pentagon's office of operational testing said. The office said it does not know how long it will take the Navy and Alliant Techsystems to evaluate fixes and resume testing. Testing stopped September 3. One hundred flights are planned to evaluate the missile's effectiveness in destroying enemy missile radar, with the initial flights to assess missile guidance, internal diagnostics and pre-launch communications with the pilot, Navy and Pentagon officials said. The test glitches included one that gave a pilot a "substantial electrical shock" during a post-flight inspection, according to the Pentagon's test office. The Advanced Anti-Radiation Guided Missile is intended as an upgrade to the existing Harm missile made by Waltham, Massachusetts-based Raytheon Co. The Alliant Techsystems version is equipped with a more modern homing receiver and navigation systems that let it detect the radar signals of stationary and mobile air defense systems. Source: <http://www.bloomberg.com/news/2010-11-04/navy-suspends-alliant-techsystems-missile-tests-following-software-failure.html>

## **EMERGENCY SERVICES**

**(Texas) Suspicious package found at PD.** Plano, Texas police officers discovered an unknown substance while searching a vehicle in the back parking lot of the Plano Police Department November 4. Officers located an unknown powdery substance while they were searching the vehicle for narcotics. They immediately backed off for safety and notified the Plano Fire Department's hazardous materials unit for further investigation. The Plano Police Department public information officer said officers took all safety precautions. There were no evacuations, and local businesses were notified of the proceedings. The investigation is ongoing. Source:

[http://www.planostar.com/articles/2010/11/04/plano\\_star-courier/news/471.txt](http://www.planostar.com/articles/2010/11/04/plano_star-courier/news/471.txt)

**Adapting emergency evacuation to human decision-making.** A team of scientists developed a disaster-response planning model that considers human decisions made in real-time, before establishing an effective law-enforcement strategy during evacuations. The model they developed is for pedestrian traffic but could also be applied to vehicle traffic management. This new model could help government entities train first responders and determine the best policies to put in place to prepare for emergencies. It can tell emergency planners how many police officers are necessary on the disaster scene to speed up the evacuation, or how a certain percentage of tourists can slow it down. In a desire to program the simulation after real human behavior, the team recorded human choices during a virtual reality experiment. After gathering information about behaviors and reactions, the researchers built a model that considers the way that different types of people react in emergency situations. The paper is titled "An integrated human decision making model for evacuation scenarios under a BDI framework," and will be published in the ACM Transactions on

UNCLASSIFIED

# UNCLASSIFIED

Modeling and Computer Simulation. Source: <http://news.softpedia.com/news/Adapting-Emergency-Evacuation-to-Human-Decision-Making-164899.shtml>

## **ENERGY**

**(Maine) More copper wire reported stolen from Ellsworth, Maine area utility poles.** Copper thieves have struck again, targeting Bangor Hydro-Electric Co. utility poles in Ellsworth and Surry, Maine. A deputy of the Hancock County Sheriff's Department said November 4 the thieves took copper ground wire from about 30 utility poles along the North Bend Road between Route 1 in Ellsworth and Route 172 in Surry. Based on information from Bangor Hydro crews, it appears the copper wire was taken within the last week. This is the second time in a week that police have opened investigations into copper wire thefts from Bangor Hydro poles. Ellsworth police still are investigating the theft of ground wires from about 23 poles on Gary Moore Road and Sunset Park Road. Although that investigation began last week, it appeared that the copper wire could have been taken months ago. A Bangor Hydro spokesperson said that crews also have reported missing wires from poles in Hancock. Source: <http://www.istockanalyst.com/article/viewiStockNews/articleid/4643032>

**(New York) Bad part shorts National Grid transmission line, cuts power to 14,100 customers northeast of Syracuse.** A power outage that cut electricity to about 14,100 National Grid customers November 4 in Madison and Onondaga counties in New York was caused by an equipment failure at a substation in Peterboro, utility officials said. The outage began about 9:44 p.m. with the failure of a lightning arrester, a piece of equipment that protects the substation against lightning strikes, said a utility spokesman. The failure allowed an arc that shorted out a transmission line, he said. That shut down power to customers in parts of Cicero, DeWitt, and East Syracuse in Onondaga County and in Oneida, Lenox, Bridgeport, and Canastota in Madison County, said another Grid spokesman. It took about 45 minutes to complete the restoration of power. All customers were back on line by 11:01 p.m. The arrester was not hit by lightning. "It just happened to fail," the spokesman said. Source: [http://www.syracuse.com/news/index.ssf/2010/11/bad\\_part\\_shorts\\_national\\_grid.html](http://www.syracuse.com/news/index.ssf/2010/11/bad_part_shorts_national_grid.html)

## **FOOD AND AGRICULTURE**

**Oil traces found in Gulf food chain, scientists say.** A "shadow" of oil from the Deepwater Horizon spill is in the Gulf of Mexico's food chain, scientists at Alabama's Dauphin Island Sea Lab have found. But that is not necessarily a bad thing. "Signatures" of oil carbon turned up in zooplankton, animals such as fish larvae and microscopic crustaceans that form the base of the food chain, said the lead author of a study published the week of November 8. Plankton is consumed by other organisms, such as crabs, mussels, oysters, and shrimp, which are in turn consumed by humans and other species. Scientists tracked a particular isotope of carbon identified with oil and found it turned up in zooplankton. The study concludes that oil was consumed by microbes, or oil-eating bacteria, which were then consumed by micro-organisms in the plankton food web. "What we found was that the system works. It doesn't mean everything is OK and it doesn't mean that there isn't anything out there that isn't toxic. It just explains that the ecosystem is working to process this oil as if it were food," the author said. Source: <http://www.cnn.com/2010/US/11/09/gulf.spill.food.chain/>

**USDA plan could partially lift sugar beet ban.** Federal agriculture officials have released a plan to let farmers plant genetically modified sugar beets while a lawsuit over them is resolved, but farmers fear

UNCLASSIFIED

## UNCLASSIFIED

a partial lifting of a court-ordered ban will not come in time for 2011's crop. A federal judge in California issued an order the summer of 2010, halting the planting of genetically modified sugar beets until the U.S. Department of Agriculture completes an environmental impact study on how the beets could affect conventional crops. The ruling had a widespread effect since nearly all the nation's sugar beet farmers had converted to genetically modified seed. Half of the nation's sugar comes from sugar beets, and 95 percent of them are grown using so-called Roundup Ready seed produced by St. Louis-based Monsanto Co. The seeds are engineered to withstand the weed killer Roundup, allowing farmers to reduce the use of other chemicals and limit tilling, which kills weeds but can contribute to erosion. Source:

<http://www.google.com/hostednews/ap/article/ALeqM5jeXCGKlkg2YtQtBkl5X3DsoJ235A?docId=81e756ee7866466f84a6f2ede93880ee>

**Food wrapper chemicals may leach into food.** Chemicals applied to fast-food wrappers and microwave popcorn bags are migrating into food and being ingested by consumers, researchers in Canada said. Perfluorinated carboxylic acids (PFCAs) are the breakdown products of chemicals used to make non-stick and water- and stain-repellent products ranging from kitchen pans to clothing to food packaging. PFCAs, the best known of which is perfluorooctanoic acid (PFOA), are found in humans all over the world, University of Toronto (UT) scientists said. A UT graduate student said the study exposed rats to polyfluoroalkyl phosphate esters orally or by injection, and the rats were monitored for a 3-week period to track concentrations of the polyfluoroalkyl phosphate esters and PFOA metabolites, including PFOA. The researchers used the concentrations previously observed in human blood together with the esters and PFOA concentrations observed in the rats to calculate human PFOA exposure from polyfluoroalkyl phosphate esters metabolism. The findings are published in the journal *Environmental Health Perspectives*. Source:

[http://www.upi.com/Health\\_News/2010/11/08/Food-wrapper-chemicals-may-leach-into-food/UPI-62541289275374/](http://www.upi.com/Health_News/2010/11/08/Food-wrapper-chemicals-may-leach-into-food/UPI-62541289275374/)

**Salmonella detected in eggs from Ohio Fresh Eggs in Croton.** A recall was ordered November 8 of eggs produced by Ohio Fresh Eggs in Croton. According to a press release from egg distributor Cal-Maine Foods Inc., the company was notified by the Food and Drug Administration (FDA) that a supplier, Ohio Fresh Eggs LLC, had a routine environmental study sample test positive for salmonella enteritidis. Cal-Maine said it bought about 24,000 dozen unprocessed eggs from Ohio Fresh Eggs that were processed and re-packaged by the company's Green Forest, Arkansas, facility between October 9 and October 12. Cal-Maine said in the release it was not notified of the test results until November 8. In a statement from company officials, Ohio Fresh Eggs said the farm had held back eggs from the Croton barn where the salmonella was found. However, through discussions with the FDA, the company discovered some eggs from that barn mistakenly were sent to a distributor. The eggs involved, which were not produced from Cal-Maine flocks, were distributed to food wholesalers and retailers in Arkansas, California, Illinois, Iowa, Kansas, Missouri, Oklahoma, and Texas. Source:

<http://www.newarkadvocate.com/article/20101109/NEWS01/11090311>

**Death by grain entrapments at record high.** Grain bin entrapment has set a record in 2010. The Purdue University Agricultural Safety and Health Program reported 46 entrapments nationwide this year, the most since the university began tracking farming accidents in 1978. The 2010 record tops the record of 42 set in 1993. Twenty-five of the 46 entrapments resulted in death. Of the entrapments, 33 were on farms and 13 were at commercial grain facilities. The increase was expected

UNCLASSIFIED

## UNCLASSIFIED

in part due to the late harvest and poor crop conditions in 2009, which created moldy and caked grain in bins, a Purdue farm safety specialist said. Because many non-fatal grain-related entrapments go unreported, he estimated the total number of actual cases could be 20 percent to 30 percent higher nationwide. Illinois has had 10 entrapments, Minnesota had eight, and Iowa and Wisconsin each had five. Source: <http://www.pal-item.com/article/20101107/NEWS01/11070308/100832>

**Cilantro problem prompts Trader Joe's recalls.** Cilantro in several Trader Joe's products may be contaminated with Salmonella. The company has alerted its customers to a recall of: Cilantro Dressing with a sell-by date of February 9, 2011, sold nationwide in all Trader Joe's stores; Spicy Peanut Vinaigrette with a sell-by date of January 9, 2011 sold nationwide in all Trader Joe's stores; Cilantro Pecan Dip with sell-by dates of November 20, 2010 and November 24, 2010 sold in California, Arizona, New Mexico, Nevada, and Washington Trader Joe's stores; Spicy Thai Pasta Salad with sell-by dates of October 30, 2010 through November 6, 2010, sold in the chain's California stores and in one Trader Joe's location each in Tucson, Arizona and Carson City, Nevada. The potentially contaminated cilantro prompted APPA Fine Food of Corona, California, to recall approximately 7,325 pounds of ready-to-eat chicken pasta salad, the U.S. Department of Agriculture's Food Safety and Inspection Service announced November 5. Source: <http://www.foodsafetynews.com/2010/11/pasta-recalled-due-to-possible-salmonella/>

**(Michigan) Equine encephalitis toll reaches 133: Economy contributes to horse deaths from EEE in Southwest Michigan.** Michigan has reported a final tally for one of the worst outbreaks of eastern equine encephalitis (EEE) in 30 years — by veterinarians' counts 133 horses were stricken, with all but four killed by the mosquito-borne disease, most in Southwest Michigan. At 55 confirmed EEE cases, 2010 is tied with 1981 for having the second highest number on record, the Michigan Department of Agriculture state veterinarian said. In 1980, there were 93 confirmed cases. Source: [http://www.mlive.com/living/kalamazoo/index.ssf/2010/11/equine\\_encephalitis\\_toll\\_reach.html](http://www.mlive.com/living/kalamazoo/index.ssf/2010/11/equine_encephalitis_toll_reach.html)

**(California) Some Fresh Choice red leaf lettuce may contain Salmonella.** California state health officials warn consumers not to eat certain Fresh Choice red leaf lettuce sold at three Southern California grocers due to possible Salmonella contamination. The lettuce was sold between October 20 and November 1 at Canton Food Co. in Los Angeles, Cardenas Market, and Numero Uno Market locations throughout Southern California, according to the California Department of Public Health director. Fresh Choice Marketing of Oxnard produced the lettuce and made it available in grocery stores as whole head lettuce without identifying labels, he said. Source: <http://www.news10.net/news/local/story.aspx?storyid=104337&catid=2>

**Cheese sold at Costco in 5 states linked to E. coli.** Federal health officials are warning consumers to avoid a cheese sold in five states over an E. coli outbreak that has left 25 people sick. The Gouda cheese was sold at Costco stores in Arizona, California, Colorado, New Mexico, and Nevada. Costco offered the Bravo Farms Dutch Style Raw Milk Gouda Cheese for sale and in-store tasting between October 5 and November 1. Source: <http://www.cnn.com/2010/HEALTH/11/05/cheese.warning/index.html?hpt=T2>

**(Illinois) Illinois firm recalls canned meat and poultry products.** Eickman's Processing, Establishment Number 31776, in Seward, Illinois, is recalling approximately 12,086 pounds of meat and poultry products because they may have been underprocessed, the U.S. Department of Agriculture's Food

UNCLASSIFIED

## UNCLASSIFIED

Safety and Inspection Service (FSIS) announced November 5. The following products in 14-ounce glass jars are subject to recall: “Lena UMW Country Mince Meat”; “Eickman’s Canned Chicken” with bar code # 03340 00050; “Eickman’s Canned Pork” with bar code # 03340 00040; “Eickman’s Canned Beef” with bar code # 03340 00030; and “CJ’s Country Canned Beef” with bar code # 91411 00001. The products subject to recall were produced between November 4, 2007, and April 7, 2010, and distributed to retail establishments in the northern Illinois area. Source:

<http://myhealthnewsdaily.com/illinois-firm-recalls-canned-meat-and-poultry-products-0681/>

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

**Campus watch.** After gunfire on the Texas-Mexico border in Matamoros, Mexico, came in contact with parts of the University of Texas-Brownsville (UTB) campus November 5, students, faculty, and staff were evacuated and classes and activities were canceled, CNN reported. The shooting killed at least 55 people in Matamoros, according to a statement released by the Mexican Navy. Students expressed disbelief when they heard the gunshots. “I was shocked that this could happen so close to campus,” a junior, who heard the shots from the soccer field, said to the Brownsville Herald. “I don’t think the other (out-of-state) teams realized how close we were to the border, what we are dealing with down here.” Although violence has been spilling across the Mexican border into Texas, students said they still felt safe going back to campus November 8 after the evacuation and cancellation.

Source: <http://dailyuw.com/2010/11/10/campus-watch/>

**(Florida) Hundreds of Florida schools on lockdown after threat.** Hundreds of schools in Broward County, Florida, were on lockdown November 10 after a threat of a shooting. A captain with the Pembroke Pines Police Department said police initially received information from a local radio station indicating a woman had called the station to say her husband was going to show up at a school in Pembroke Pines and start shooting. Subsequently, an e-mail threat was sent but it is not clear to whom. The FBI was contacted. Source:

<http://www.670kboi.com/rssItem.asp?feedid=118&itemid=29596351>

**U.S. workers are on alert after breach of data.** Federal workers at the General Services Administration are on alert against identity theft after an employee sent the names and Social Security numbers of the agency’s entire staff to a private e-mail address. The agency, which manages federal property, employs more than 12,000 people. Officials apologized to employees for the incident in a letter dated October 25 — almost 6 weeks after the breach occurred. The agency said it paid for employees to enroll in a 1-year program to monitor their credit reports, along with up to \$25,000 in identity theft insurance coverage. The letter was signed by the chief information officer and the agency’s senior privacy official. An agency spokeswoman said in a statement November 3: “Ensuring the security of employee data is no small challenge in large organizations. We will continue to evolve our protocols to protect the employee information entrusted to us.” Source:

[http://www.nytimes.com/2010/11/07/us/07breach.html?\\_r=1](http://www.nytimes.com/2010/11/07/us/07breach.html?_r=1)

**(Washington) V For Vendetta hacker infiltrates Washington State University.** A sophisticated hacker managed to infiltrate dozens of Washington State University (WSU) classrooms the week of November 1 with a video featuring a call for student involvement from someone dressed as V from the film V for Vendetta November 5. The Chronicle of Higher Education reports: After hacking into

UNCLASSIFIED

## UNCLASSIFIED

the university's academic media system, which manages classroom-presentation and distance-learning technology, the as-of-yet-unidentified culprit or culprits programmed motorized screens to unfurl themselves and scheduled projectors to broadcast the 5-minute-long video once every hour. The video — ostensibly a diatribe against campus squirrels and a call to end student apathy — interrupted lectures and cut off access for distance-learning students until the IT staff was able to shut down the program in the early afternoon. According to the university's executive director for external communications, IT officials in some cases had to unplug computer hard drives in order to stop the hack. "It was a rather sophisticated program," he said. "Traditional ways of shutting down the software wouldn't work." The video featured the Web address for WSU 1812, a blog purporting to have "have grown tired of this university's disregard for the opinion of it's [sic] students" and naming the school's student government as a "prime culprit in this problem." Source:

[http://www.huffingtonpost.com/2010/11/09/v-for-venetta-hacker-inf\\_n\\_780840.html](http://www.huffingtonpost.com/2010/11/09/v-for-venetta-hacker-inf_n_780840.html)

**US Mission in Geneva evacuated: suspicious package.** The U.S. Mission in Geneva, Switzerland, was evacuated shortly before 4 p.m. November 5 after a suspicious package was found on the premises. The Swiss bomb squad was called to the scene but further details were not available. The incident occurred on a day when the United States had a particularly high-powered team in Geneva for its first-ever Universal Periodic Review by the U.N. Human Rights Council, and a town hall style meeting for non-governmental organizations was organized nearby for 5 p.m.. Bombs were delivered to several embassies and government offices in Europe the week of November 1, and consulates, embassies and other areas are on high alert. Source: <http://genevalunch.com/blog/2010/11/05/us-mission-in-geneva-evacuated-suspicious-package/>

**(District of Columbia) Secret Service detains vehicle suspected of explosives at White House entrance.** The U.S. Secret Service detained a suspicious vehicle at a White House entrance November 6 after a dog alerted officers to possible explosives. The vehicle was later cleared and considered to be no threat, a Secret Service spokesperson said. The area around the entrance at 15th and Pennsylvania Ave., NW, was cordoned off. The explosive ordinance disposal unit of the D.C. Police and the D.C. Fire Department were called to the scene. Source: <http://www.tbd.com/articles/2010/11/secret-service-detains-vehicle-suspected-of-explosives-at-white-house-entrance-29537.html>

**(Illinois) Western Illinois receives three bomb threats.** The University of Western Illinois, which is recovering from the shocks of two bomb threats over the past 2 weeks, was the target of a yet another bomb threat November 5. The previous two threats — on October 25 and November 4 — were found to have no immediate danger, a WIU spokesperson said. The target of the bomb threats on all three occasions was Tanner Hall, a student dormitory on the Moline, Illinois, campus that houses over 800 freshmen. All three threats were called into the Tanner Hall clerk's office, according to a police report. The third bomb threat was reported at 2:30 p.m., and evacuations began almost immediately. According to a police report, Tanner Hall was reopened to student residents at 4:30 p.m. after the office of public safety searched the building and found no danger. Source: [http://badgerherald.com/news/2010/11/07/western\\_ilinois\\_rece.php](http://badgerherald.com/news/2010/11/07/western_ilinois_rece.php)

**Security boosted at U.S. military posts.** In the year since an Army major is accused of bringing two handguns and 400 rounds of ammunition onto Fort Hood in Fort Hood, Texas and shooting dozens of people in a busy medical processing building and killing 13 in the process, Army officials have taken

UNCLASSIFIED

## UNCLASSIFIED

steps to improve security on American military installations and ferret out similar threats from American soldiers. Department of Defense (DOD) officials are recommending an array of fixes aimed at identifying future threats at all U.S. military installations, and improving response time to incidents. Among the recommendations made by the U.S. Defense Secretary in response to an independent review of the shooting at Fort Hood are: bringing enhanced 911 services to military installations, which would notify dispatchers of call locations and broadcast emergency notifications to designated areas; strengthening background checks of recruits entering the military and foreign nationals working for the DOD abroad; conducting violence risk assessments for service members before and after they deploy; developing a policy to help commanders distinguish between “appropriate religious practices” and those that indicate the “potential for violence or self-radicalization”; and standardizing personal firearms policies, which vary by installation. Source:

<http://www.statesman.com/news/texas/security-boosted-at-u-s-military-posts-1022445.html>

**US Cyber Command becomes ‘fully operational’.** The US military’s new Cyber Command has formally “achieved full operational capability”, according to the Department of Defense (DOD). “I am confident in the great service members and civilians we have here at US Cyber Command. Cyberspace is essential to our way of life and US Cyber Command synchronizes our efforts in the defense of DOD networks. We also work closely with our interagency partners to assist them in accomplishing their critical missions,” said the chief of Cyber Command and also of the National Security Agency, with which the Command shares a headquarters. According to a statement issued November 3 announcing Full Operational Capability (FOC) for the cyber force: Some of the critical FOC tasks included establishing a Joint Operations Center and transitioning personnel and functions from two existing organizations, the Joint Task Force for Global Network Operations and the Joint Functional Component Command for Network Warfare. U.S. Cyber Command’s development will not end at FOC, and the department will continue to grow the capacity and capability essential to operate and defend our networks effectively. Source:

[http://www.theregister.co.uk/2010/11/04/cyber\\_command\\_go/](http://www.theregister.co.uk/2010/11/04/cyber_command_go/)

## **INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**Researchers see real-time phishing jump.** Real-time phishing attacks that cheat two-factor authentication are on the rise around the globe as phishers adapt to the latest barriers put in their way, according to a team of researchers. Researchers at Trusteer November 9 said 30 percent of all attacks during the past two-and-a-half months against Web sites using two-factor authentication have been real-time, man-in-the-middle (MITM) methods that allow attackers to bypass this stronger authentication. The data comes from a sampling of thousands of phishing attacks. Phishing attacks typically are static, so they are mostly rendered powerless when a bank uses two-factor authentication, such as one-time passwords. That is because the attacker may be able to capture the first level of credentials, but they are not able to easily capture and use OTPs, which quickly expire. So phishers are adapting their attacks to find ways around stronger authentication, and security experts said it was only a matter of time until they routinely started cheating banks and other transactional sites’ two-factor authentication. This type of real-time MITM attack has been isolated and rare thus far, experts said. Trusteer researchers have spotted these attacks in South Africa, Europe, and now in the United States, the firm’s CEO said. And while these attacks are not a new concept, this is the first time his team has seen them in such high numbers, he said. Source:

UNCLASSIFIED

<http://www.darkreading.com/authentication/security/attacks/showArticle.jhtml?articleID=228200550>

**Microsoft forgets to patch Mac Office 2004, 2008.** Microsoft November 9 revealed four vulnerabilities in the Mac version of its Office suite, but then failed to produce patches for the 2004 and 2008 editions. Office for Mac 2011, which launched October 26, was the only version updated as part of Microsoft's monthly Patch November 9. Microsoft did not explain the omission of Office for Mac 2004 and Office for Mac 2008 patches, or say when it would ship updates for those editions. According to that bulletin, Office for Mac contains four vulnerabilities, all rated "important," the second-highest threat ranking in Microsoft's four-step scoring system. Microsoft confirmed that each bug could be used by attackers to infect a Mac with malware by labeling them with the phrase "remote code execution." Along with a fifth bug, the same four flaws were patched November 9 in all still-supported versions of Office for Windows. Source:

[http://www.computerworld.com/s/article/9195819/Microsoft\\_forgets\\_to\\_patch\\_Mac\\_Office\\_2004\\_2008](http://www.computerworld.com/s/article/9195819/Microsoft_forgets_to_patch_Mac_Office_2004_2008)

**AOL Mail goes down again?** Less than 3 weeks after AOL Mail went down, the service appeared to be having some downtime issues again November 8. Some users have reported that they were unable to access their AOL Mail accounts. In addition, various affected users have taken their frustrations to Twitter. Source: <http://erictric.com/2010/11/08/aol-mail-goes-down-again/>

**PayPal network problems worsen.** PayPal's recent outage was the result of a network hardware failure, and the problem worsened when the failover systems did not spring into action as designed, reported Fierce CIO. PayPal has more than 87 million active accounts in 24 currencies around the world. It is owned by e-Bay, who acquired the company for \$1.5 billion in 2002. The outage illustrates the challenges inherent to maintaining a cloud-based system in which zero downtime is tolerated, with merchants and customers globally relying on PayPal to be able to complete orders and transfer funds. Source:

[http://www.itweb.co.za/index.php?option=com\\_content&view=article&id=38514:paypal-network-problems-worsen&catid=69](http://www.itweb.co.za/index.php?option=com_content&view=article&id=38514:paypal-network-problems-worsen&catid=69)

**Zscaler develops free tool to detect Firesheep snooping.** A security company has developed a free Firefox add-on that warns when someone on the same network is using Firesheep, a tool that has raised alarm over how it simplifies an attack against a long-known weakness in Internet security. Firesheep, which was unveiled at the ToorCon security conference in San Diego October 2010, collects session information that is stored in a Web browser's cookie. The session information is easily collected if transmitted back and forth between a user's computer and an unencrypted Wi-Fi router while a person is logged into a Web service such as Facebook. While most Web sites encrypt the traffic transmitted when logging into a Web site, indicated by the padlock on browsers, many then revert to passing unencrypted information during the rest of the session, a weakness security analysts have warned of for years, particularly for users of public open Wi-Fi networks. Firesheep identifies that unencrypted traffic and allows an interloper to "hijack" the session, or log into a Web site as the victim, with just a few clicks. The style of attack has been possible for a long time, but because of its simple design, Firesheep has given less-sophisticated users a powerful hacking tool. Zscaler's The Blacksheep add-on, however, will detect when someone on the same network is using Firesheep, allowing its users to make a more informed security decision about their behavior while on an open

## UNCLASSIFIED

Wi-Fi network, for example. Source:

[http://www.computerworld.com/s/article/9195398/Zscaler\\_develops\\_free\\_tool\\_to\\_detect\\_Firesheep\\_snooping](http://www.computerworld.com/s/article/9195398/Zscaler_develops_free_tool_to_detect_Firesheep_snooping)

**Zeus Trojan defeats Microsoft security tool.** Only weeks after Microsoft added anti-Zeus Trojan detection to its free Malicious Software Removal Tool (MSRT), it is unable to detect the latest versions, a rival security company has claimed. The analysis by Trusteer is a reminder that ordinary users face a battle to keep state-of-the-art Trojans such as Zeus (or Zbot or WnspoeM), which targets online bank accounts, off their PCs. According to Trusteer, MSRT detected and removed Zeus version 2.0 about 46 percent of the time in its tests, but failed to spot updated versions, which are now circulating. The company also thinks that such Zeus detection is seriously flawed because it relies on the user downloading and running a tool when it might already be too late — Zeus typically steals banking logins soon after infection. Ironically, because MSRT's effectiveness is still superior to many antivirus products, it might cause criminals to up their game once again, shortening the infection-to-theft period and even attacking MSRT itself. Source:

<http://www.networkworld.com/news/2010/110510-zeus-trojan-defeats-microsoft-security.html>

**Facebook and Twitter flunk security report card.** Digital Society, a self-professed security think tank, has given failing security grades to both Twitter and Facebook. Both sites are vulnerable to attacks that can give someone partial or full control over one's account, the group claimed. According to Digital Society, the main problem with Facebook and Twitter is that neither site allows full Secure Sockets Layer (SSL) protection. Both sites create unencrypted sessions for the user by default. Although the actual logins are encrypted, they're not authenticated — which means one cannot pull up security information in one's browser to verify the sites' identities. Even if a user forces a secure session by going to the main sites for Twitter and Facebook, the sites still have links to non-secure parts of the site and JavaScript code that transmit authentication cookies without SSL, Digital Society found. These are not new concerns, but the news fits hand-in-hand with the release of FireSheep, a Firefox add-on that lets people with limited technical knowledge hijack other people's Web accounts over unencrypted Wi-Fi networks. Digital Society's report card essentially spells out what an attacker using FireSheep or another packet-sniffing program could accomplish. In Facebook, for instance, an attacker can gain access to every part of an account except username and password, allowing the attacker to send status updates and read private messages. Source:

[http://www.computerworld.com/s/article/9195021/Facebook\\_and\\_Twitter\\_Flunk\\_Security\\_Report\\_Card](http://www.computerworld.com/s/article/9195021/Facebook_and_Twitter_Flunk_Security_Report_Card)

**Stock traders become targets for hackers exploiting mobile platforms.** Once mobile online trading platforms become popular, the nature of the cyber-crime scene will most likely change, according to an Internet security expert. It is just a matter of time when Internet crime, which mostly has targeted personal computers, will expand to the mobile platform, according to a McAfee Labs Technical Product Manager. He outlined the possible threats to traders who use mobile platforms, including denial of service (DoS) attacks, session hijacking, cross-site scripting and SQL injection. When a lot of data is sent around the same time, systems are likely to slow down and block access to thousands of users, as seen with a DoS attack, he said. This is particularly crucial in trading sessions, where the price of stocks can fluctuate by the minute, he added. With session hijacking, the hacker can eavesdrop or pose as the legitimate user. If session hijacking takes place during an online stock trading, it can be dangerous as the details of the transaction are compromised. It could also mean the

UNCLASSIFIED

## UNCLASSIFIED

customer is dealing with a hacker, not his trader. Source:

<http://www.thenewnewinternet.com/2010/11/04/stock-traders-become-targets-for-hackers-exploiting-mobile-platforms/>

### **NATIONAL MONUMENTS AND ICONS**

**(Illinois) Man arrested for state park arsons.** After weeks of investigation, police arrest a man suspected in several arsons in the Jasper County, Illinois, area. The suspect, of Yale, was arrested November 3. The fires took place inside Sam Parr State Park and on private property throughout the county. The suspect appeared in court November 4 facing charges of arson and criminal damage to government supported property. The Jasper County state attorney said he could face additional charges in relation to the fires. Source: <http://www.wthitv.com/dpp/news/local/man-arrested-for-state-park-arsons>

### **POSTAL AND SHIPPING**

**(New York) Suspicious envelope prompts evacuation of Elmsford offices.** The corporate offices of Town Sports International, the company that owns and operates New York Sports Clubs, was evacuated this morning after receiving a suspicious envelope, Greenburgh police said. The office at 399 Executive Blvd. called police at 11:15 a.m. after receiving a white business-sized envelope addressed there. Four employees made contact with the letter after it was delivered at 10 a.m., including a woman who touched an unknown white powdery substance along the folding ridge line of the letter. She reported skin irritation and itching. More than 70 people were evacuated from the first floor of the building. The Greenburgh and Fairview Fire Department's joint Hazmat-Tech Rescue Team was assisted by the Westchester County police bomb squad, the county Department of Emergency Services and Hazmat team, the county Office of Emergency Management, the state police Joint Terrorist Task Force, the FBI, and the Elmsford Volunteer Fire Department and Emergency Medical Services. A mobile decontamination station was set up to treat the four employees and one postal worker. The letter containing the unknown substance was removed from the scene and transported to the county lab for further testing. Source: <http://www.lohud.com/article/20101109/NEWS02/11090373/-1/newsfront/Suspicious-envelope-prompts-evacuation-of-Elmsford-offices>

**Saudis warned U.S. of package bomb plot weeks ago.** Western officials are crediting a Saudi intelligence tip they received in early October, nearly 3 weeks before terrorists in Yemen managed to smuggle mail bombs onto airplanes, with heading off what could have been a series of catastrophic explosions on jets. The Yemen-based al-Qaeda in the Arabian Peninsula claimed responsibility November 5 for sending the two bombs addressed to synagogues in the U.S. and intercepted in Dubai and Britain. The group also said it was responsible for the crash of a UPS cargo plane in Dubai in September, and threatened even more attacks on passenger and cargo aircraft. Investigators said they believe the UPS crash was an accident, not a terror attack, but they are not discounting the al-Qaeda claim. The Saudi tip contained no mention of cargo planes, or any details of the plot carried out last week, said U.S. officials, speaking on condition of anonymity to discuss classified matters. But they said it gave the U.S. and other Western officials enough of a warning to know what to look for when another Saudi tip arrived last week. A CIA spokesman cited several allies that have provided key

UNCLASSIFIED

## UNCLASSIFIED

intelligence about terrorist activities. Source: [http://www.usatoday.com/news/world/2010-11-05-al-qaeda-bomb-plot\\_N.htm](http://www.usatoday.com/news/world/2010-11-05-al-qaeda-bomb-plot_N.htm)

**(Texas) Bomb threat empties Downtown Post Office.** A Texarkana, Texas, man is in custody after allegedly making a bomb threat November 4 that led to a 5.5-hour evacuation of the Downtown Post Office and federal building. The 49-year-old has been charged with terroristic threatening. The offense is punishable by two to 10 years in prison. An FBI spokesman said the suspect's case will likely be presented to a grand jury in the Eastern District of Texas during the week of November 8-12 for indictment on violations of federal law. Source: <http://www.texarkanagazette.com/news/localnews/2010/11/05/bomb-threat-empties-downtown-post-office-54.php>

## **PUBLIC HEALTH**

**Hospitals 'struggling' to protect patient data.** The healthcare industry is spending an estimated \$6 billion annually on data breaches of patient information, according to the latest benchmark study by Ponemon Institute. On November 9, the Ponemon Institute and ID Experts released Benchmark Study on Patient Privacy and Data Security. The study indicated that protecting patient data is a low priority for hospitals, and that organizations have little confidence in their ability to secure patient records. Among the findings, researchers found that the cost of a data breach over a 2-year period is approximately \$2 million per organization, and the lifetime value of a lost patient is \$107,580. The average organization had 2.4 data breach incidents over the past 2 years. The researchers also found that 70 percent of hospitals stated that protecting patient data is not a top priority, and that patient billing (35 percent) and medical records (26 percent) are the most susceptible to data loss or theft. A majority of organizations have less than two staff dedicated to data protection management (67 percent). Source: <http://www.healthcareitnews.com/news/hospitals-struggling-protect-patient-data>

**(Florida) Gunman an apparent suicide in Florida hospital.** A former employee who had recently been fired from Palm Bay Hospital in Miami, Florida returned there November 4 carrying a gun, holed himself up in an office, then apparently killed himself, officials said. The incident began about 2:20 p.m., when Palm Bay police got a call from people in the hospital cafeteria who said a man was pointing the gun at anyone who tried to talk to him, said a police spokeswoman. Earlier she said that during the police response, "we were told that shots had been fired," but "nobody was injured." But she later told reporters the shots may have been the gunman taking his own life. As police officers and SWAT personnel from Palm Bay and nearby agencies assembled outside the hospital, the hospital was locked down and emergency vehicles were diverted to other hospitals. A few hours later, a robot found the man's body inside an administrative office near the cafeteria's food-preparation area. Source: <http://www.cnn.com/2010/CRIME/11/04/florida.gunman.hospital/index.html>

## **TRANSPORTATION**

**(North Carolina) Rowan airport closed for explosive search.** The Rowan County Airport in Salisbury, North Carolina, closed November 9 as police investigated reports of an explosive in the area. Salisbury police said there was a possibility that there was an explosive in a vehicle located on Airport Road. Police said the vehicle is not at the airport or at the National Guard Armory; instead it is near

UNCLASSIFIED

## UNCLASSIFIED

those facilities. Police have restricted traffic access to the area during the investigation. Source:

<http://www.charlotteobserver.com/2010/11/09/1825251/rowan-airport-closed-for-explosive.html>

**U.S. bans toner and ink cartridges on passenger planes, extends air cargo ban to Somalia.** The United States announced an immediate ban on toner and ink cartridges over 16 ounces (453 grams) on passenger aircraft in both carry-on bags and checked bags on domestic and international flights inbound to the United States, while extending a Yemeni air cargo ban to Somalia. The new security measures were announced by DHS in wake of a failed al-Qaeda plot to bomb two U.S.-bound cargo planes. In addition, no cargo deemed "high risk" will be allowed on passenger aircraft. The DHS Secretary said the U.S. administration is working closely with industry international partners to expedite the receipt of cargo manifests for international flights to the United States prior to departure in order to identify and screen items based on risk and current intelligence. Source:

<http://channel6news.com/2010/11/u-s-bans-toner-and-ink-cartridges-on-passenger-planes-extends-air-cargo-ban-to-somalia/>

**Cruise ship loses power after engine room catches fire in seas south of San Diego.** Tugboats headed about 150 miles south of San Diego, California, to tow in a 952-foot Carnival Splendor cruise ship that lost power after a November 8 engine-room fire. The ship is about 55 miles off the northern Baja coast, and tugboats will take it to the Mexican port of Ensenada. Miami, Florida-based Carnival Cruise Lines said the ship, on a 7-day cruise to the Mexican Riviera, has auxiliary power, but air conditioning, hot food service, hot water and telephones were knocked out. The cruise line said toilets and cold water were restored overnight. Carnival said the tugboats were expected to arrive about midday November 9. Source:

[http://www.google.com/hostednews/canadianpress/article/ALeqM5gGHWUWTx7iAcGX6\\_FRT2NaNZ\\_WNSw?docId=5077454](http://www.google.com/hostednews/canadianpress/article/ALeqM5gGHWUWTx7iAcGX6_FRT2NaNZ_WNSw?docId=5077454)

**FMCSA bans truckers from texting.** The Federal Motor Carrier Safety Administration (FMCSA) has issued a formal rule banning truck and bus drivers from texting while driving. Carriers are also prohibited from requiring or allowing texting by their drivers. The ban codifies current federal enforcement practices and follows up on guidance the FMCSA issued earlier in the year. The rule affects commercial motor vehicle (CMV) drivers who operate within interstate commerce. Sanctions for violators include a \$2,750 fine for drivers and \$11,000 fine for carriers. Drivers can also be disqualified from operating CMVs in interstate commerce. Source: <http://www.24-7pressrelease.com/press-release/fmcsa-bans-truckers-from-texting-179926.php>

**(District of Columbia; Maryland; Virginia) Metro to boost improvised explosives protection.** The Washington Metropolitan Area Transit Authority (Metro) is working to boost protection against improvised explosive devices. Metro said a \$351,000 grant will pay for new equipment that can jam radio signals of remote-controlled devices. It will also fund training for bomb squad members, and allow Metro to participate in the FBI's National Electronic Countermeasures system. The equipment includes two vehicles and two systems with a vehicle-mounted jammer and portable jammer. Metro plans to make the equipment available to other accredited bomb squads in the region. Metro's board of directors will vote later in November on a measure to add the grant to the 2011 budget and authorize Metro to award a contract for the equipment. Source:

<http://www.wset.com/Global/story.asp?S=13444834>

UNCLASSIFIED

**WATER AND DAMS**

Nothing Significant to Report

**NORTH DAKOTA HOMELAND SECURITY CONTACTS**

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **Fusion Center (24/7):** 866-885-8295(IN ND ONLY); Email: [ndslic@nd.gov](mailto:ndslic@nd.gov) ; Fax: 701-328-8175  
**State Radio:** 800-472-2121 **Bureau of Criminal Investigation:** 701-328-5500 **Highway Patrol:** 701-328-2455  
**US Attorney's Office Intel Analyst:** 701-297-7400 **Bismarck FBI:** 701-223-4875 **Fargo FBI:** 701-232-7241

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

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



**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**