

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

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

NORTH DAKOTA

Nothing Significant to Report

REGIONAL

(Minnesota) Lanesboro dam needs reconstruction. The Lanesboro Power Dam on the Root River in Lanesboro, Minnesota, is in need of reconstruction, as it is putting the city at risk. The trouble began with a letter from the state department of natural resources stating the dam had to be fixed or torn down because it is high hazard, said a Lanesboro city administrator. The dam is at the center of a debate between the Lanesboro and the state's historic preservation office, which says because it is in a historic location it needs to be built with similar materials from when it was first built, making it a much more costly project for the city. Source: <http://kaaltv.com/article/stories/S2480678.shtml?cat=10219>

(Colorado; Wyoming; South Dakota) Mountain pine beetle epidemic slows in some areas. U.S. Forest Service officials said the mountain pine beetle epidemic in Colorado and southern Wyoming is slowing, as insects have largely depleted the large pine trees they attack. The assistant director for forest health projects said February 1 that a 2011 aerial survey showed about 4.6 million acres in Colorado, Wyoming, and South Dakota have been affected since the first signs of the outbreak in 1996, up from about 4.3 million in 2010. The increase includes 140,000 more acres infested in Colorado, 68,000 more acres in Wyoming, and about 23,000 more acres in South Dakota. The Forest Service spent about \$32 million in fiscal 2011 removing dead trees that threatened to fall along 275 miles of roads, 162 miles of trails, and about 12,000 acres in the region. Source: <http://www.kjct8.com/news/30344202/detail.html>

NATIONAL

Oregon prepares for tsunami debris. As the 1 year anniversary of the devastating March 11, 2011, Japanese earthquake approaches, and debris from the ensuing tsunami moves closer to the West Coast, a group of Oregon agencies, university scientists, political staff, non-governmental organizations, and others is preparing for its arrival. The week of January 30, the group held a conference call to review Oregon's response to the potential arrival of the debris and to chart a communication strategy to educate residents about what may happen. An Oregon State University (OSU) oceanographer and expert in ocean currents, said the debris is still months away from arriving on the West Coast, though it is possible that strong winds may push some floating items that rise high above the surface more quickly to the North American shore. He said it is difficult to calculate how much debris remains in the ocean, and what exactly will arrive on the shore. What does arrive is unlikely to be dangerous, according to a professor and head of the Department of Nuclear Engineering and Radiation Health Physics at OSU. The National Oceanic and Atmospheric Administration is monitoring the debris from a national perspective. Source: <http://www.kpic.com/news/local/Oregon-prepares-for-tsunami-debris-138493054.html>

INTERNATIONAL

Four men admit London Stock Exchange bomb plot. Four men inspired by al-Qa'ida admitted planning to detonate a bomb at the London Stock Exchange, BBC News reported February 1. The men all pleaded guilty in court in England to engaging in conduct in preparation for acts of terrorism. The men, from London and Cardiff, were arrested in December 2010. Five other men linked to the plot pleaded guilty to other terrorism offenses and all nine will be sentenced the week of February 6. It emerged that those who targeted the London Stock Exchange wanted to send five mail bombs to various targets during the run up to Christmas 2010, and discussed launching a "Mumbai-style" atrocity. A hand-written target list discovered at the home of one of the men listed the names and addresses of London's mayor, two rabbis, the U.S. embassy, and the stock exchange. The conspiracy was stopped by undercover anti-terror police before firm dates could be set for attacks. The terrorists met because of their membership of various radical groups and stayed in touch over the Internet, through mobile phones, and at specially arranged meetings. The quartet talked about leaving homemade bombs in the toilets of their city's pubs and discussed traveling abroad for terror training. Source:

<http://www.bbc.co.uk/news/uk-16833032>

Experts: US ill-prepared for oil spill off Cuba. The United States is not ready to handle an oil spill if drilling off the Cuban coast should go awry but can be better prepared with monitoring systems and other basic steps, experts told government officials January 30. The comments at a congressional subcommittee hearing in Sunny Isles, Florida, come more than a week after a huge oil rig leased by Repsol YPF arrived in Cuban waters to begin drilling a deep water exploratory well. Similar development is expected off the Bahamas next year, but decades of tense relations between the United States and Cuba makes cooperation in protecting the Florida Straits difficult. State and federal officials fear even the perception of any oil flowing toward Florida beaches could devastate an economy that claims about \$57 billion from tourism. Source: <http://www.foxnews.com/us/2012/01/30/experts-us-ill-prepared-for-oil-spill-off-cuba/>

BANKING AND FINANCE INDUSTRY

U.S. indicts Wegelin bank for helping Americans avoid tax. The United States indicted Wegelin, the oldest Swiss private bank, on charges it enabled wealthy Americans to evade taxes on at least \$1.2 billion hidden in offshore bank accounts, the U.S. Justice Department said February 2. The announcement, made by federal prosecutors in Manhattan, New York, represents the first time an overseas bank was indicted by the United States for enabling tax fraud by U.S. taxpayers. The indictment said the U.S. government seized more than \$16 million from Wegelin's correspondent bank, the Swiss giant UBS AG, in Stamford, Connecticut, via a separate civil forfeiture complaint. Because Wegelin has no branches outside Switzerland, it used correspondent banking services, a standard industry practice, to handle money for U.S.-based clients. The charges against Wegelin are fraud and conspiracy. Wegelin "affirmatively decided to capture for Wegelin the illegal U.S. cross-border banking business lost by UBS and deliberately set out to open new undeclared accounts for U.S. taxpayer-clients leaving UBS,"

UNCLASSIFIED

the indictment said. The indictment also accused Wegelin of helping two unnamed Swiss banks “repatriate undeclared funds to their own U.S. taxpayer-clients by issuing checks drawn on Wegelin’s Stamford correspondent account.” The transfers were separated into chunks below the \$10,000 threshold at which such transfers are reported to the Internal Revenue Service. Wegelin, the indictment said, “co-mingled” the repatriated funds with other, unrelated funds, to better conceal their origin and nature. The charges against Wegelin were filed as a superseding indictment of three previously charged Wegelin bankers, naming several unindicted co-conspirators. Source: <http://www.reuters.com/article/2012/02/03/us-usa-tax-swiss-indictment-idUSTRE81203M20120203>

Hacker extracts RFID credit card details. The widespread use, especially in U.S. credit cards, of radio frequency identification (RFID) chips which can be read through clothing or wallets for contactless payments can lead to cards being read without the owners knowledge or permission, H Security reported February 1. Forbes reported January 30 that a hacker at the Shmoocoon security conference in Washington D.C. demonstrated the ability to read data on RFID chipped credit cards and make a payment that had not been authorized by the card owner. With about 100 million RFID cards issued, this could now be done without card owners handing over their cards. No security measures such as card reader authentication are in place. However, the RFID data does not include the three-digit CVV number printed on the back of the card that is usually required when making an online transaction. Instead, the chip issues a one-time CVV that is only valid for one transaction. Using this CVV repeatedly will cause the card to be blocked. In the United States, Visa markets RFID credit cards as payWave, and in the United Kingdom (UK) as Contactless by Visa. Mastercard markets their RFID credit cards as Paypass in the United States and UK. Source: <http://www.h-online.com/security/news/item/Hacker-extracts-RFID-credit-card-details-1425974.html>

Malware redirects bank phone calls to attackers. Trusteer has discovered a concerning development in new configurations of Ice IX, a modified variant of the ZeuS financial malware platform, that are targeting online banking customers in the United Kingdom (UK) and United States. “In addition to stealing bank account data, these Ice IX configurations are capturing information on telephone accounts belonging to the victims ... allow[ing] attackers to divert calls from the bank intended for their customer to attacker controlled phone numbers,” the chief technology officer (CTO) of Trusteer said. He believes “the fraudsters are executing fraudulent transactions using the stolen credentials and redirecting the bank’s post-transaction verification phone calls to professional criminal caller services that approve the transactions.” In one captured attack, at login the malware steals the victim’s user ID and password, memorable information/secret question answer, date of birth, and account balance. Next, the victim is asked to update phone numbers and select the name of their service provider from a drop-down list. To enable the attacker to modify phone service settings, the victim is then asked by the malware to submit telephone account number. The fraudsters justify this request by stating this data is required as a part of verification process caused by “a malfunction of the bank’s anti-fraud system with its landline phone service provider.” Source: http://www.net-security.org/malware_news.php?id=1984

UNCLASSIFIED

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

NRC wants U.S. nuclear operators to adopt new seismic model. The Nuclear Regulatory Commission (NRC) said January 31 that the agency wants nuclear plant operators in the central and eastern United States to use a new seismic model to reassess the potential for earthquakes in their area. A NRC study focused on this area because it is considered a “stable continental region” where big earthquakes are rare. The study, which gathered historical earthquake and geological data from 1568 through 2008, determined the largest potential earthquakes in the eastern and central parts of the country could occur near New Madrid, Missouri, and also in Charleston, South Carolina, where large magnitude seismic activity has occurred in the past.

Source: <http://www.reuters.com/article/2012/01/31/us-utilities-nrc-earthquakes-idUSTRE80U1OS20120131>

US alleges DuPont TiO₂ technology stolen for China. A man was ordered to stay in a U.S. jail February 1 in connection with an alleged scheme to steal titanium dioxide (TiO₂) trade secrets from DuPont on behalf of Chinese government officials. A federal judge in San Francisco ordered the businessman to remain in detention as a flight risk pending trial, said a spokesman for the U.S. attorney’s office. Prosecutors opposed his release and alleged in a court document that investigators found a “trove of evidence” which shows [he] was selling trade secrets belonging to [DuPont] to companies controlled by the government of the People’s Republic of China.” The man was charged with witness tampering, conspiracy to tamper with witnesses, and making a false statement in connection with the U.S. probe. Prosecutors said they have evidence showing he obtained over \$20 million from the sale of TiO₂ technologies to Chinese companies. Source: <http://www.icis.com/Articles/2012/02/01/9528663/us-alleges-dupont-tio2-technology-stolen-for-china.html>

EPA rethinks chemical plant emissions. The U.S. Environmental Protection Agency (EPA) is reconsidering national emission standards for hazardous air pollutants for nine chemical manufacturers. In a final regulation brief issued January 30, the agency seeks comment on several provisions of an October 29, 2009 final rule it is reconsidering. The EPA also proposes revisions to its approach for addressing malfunctions, and asks for comments on those revisions and on the standards applicable during start-up and shutdown periods, as described in the final rule. Source: <http://www.courthousenews.com/2012/01/30/43477.htm>

COMMERCIAL FACILITIES

(Nevada) Nevada officials: Luxor guests had Legionnaires’. Health officials in Las Vegas said January 30 the bacteria that causes Legionnaires’ disease was found in water samples at the Luxor hotel-casino in January after a guest died of the form of pneumonia. The Southern Nevada Health District said the Centers for Disease Control and Prevention national surveillance program reported three cases in the past year of Luxor guests being diagnosed with the disease caused by Legionella bacteria. The Las Vegas Strip resort’s water was tested after the first two cases were reported during the spring of 2011, but no Legionella bacteria was detected, district officials said. Officials said the Luxor, owned by MGM Resorts International, immediately began

UNCLASSIFIED

a remediation process once the bacteria was found. An MGM Resorts spokesman said treatment procedures include superheating and super-chlorination of the water system. The spokesman said the company's resorts regularly test for Legionella and treat water systems preventatively, before bacteria are detected. The new cases come as the company is already facing a civil lawsuit from guests who said they were infected with Legionella at the Aria Resort & Casino, part of the CityCenter complex that is half-owned by MGM Resorts. MGM Resorts notified guests that they might have been exposed to the bacteria between June 21 and July 4, 2011 after the district reported six cases of Legionnaires' disease in July. Source:

http://www.google.com/hostednews/ap/article/ALegM5ixz-INAaCBfnEhVp_MZSqge3YVeg?docId=a235210765334c6fb3032a4023d9c788

(New Jersey) NJ synagogue attack suspect charged with 3rd plot. Authorities leveled additional charges January 27 against a teenager accused in the firebombings of two northern New Jersey synagogues, saying he had plotted a similar attack on a Jewish community center, and had conducted Internet searches for building Molotov cocktails and instructions on blowing up buildings. A Bergen County prosecutor said investigators found multiple Molotov cocktails the week of January 23 in a wooded area near the Jewish Community Center of Paramus, and they traced the evidence to a foiled attack they said the suspect was planning for January 7. The suspect was charged with aggravated arson, bias intimidation, and other charges for the planned attack on the center. He was arrested earlier the week of January 23, and has already pleaded not guilty to nine counts of attempted murder as well as bias intimidation and arson charges for a January 11 attack on a Rutherford synagogue, and a January 3 firebombing of a Paramus synagogue. If convicted on all charges, the suspect could face at least 95 years in prison. Source: http://www.stltoday.com/news/national/prosecutor-new-charges-in-nj-synagogue-attacks/article_61932c09-3ee7-5dbe-be8c-c2d92592a177.html

(California) Arrests in Oakland protests rise to more than 400. Crews cleaned up Oakland's historic city hall January 29 from damage inflicted overnight during violent anti-Wall Street protests that resulted in about 400 arrests, marking one of the largest mass arrests since nationwide protests began last year in Oakland, California. The skirmishes injured three officers and at least one demonstrator. Police said a group of protesters burned an American flag in front of city hall, then entered the building and destroyed a vending machine, light fixtures, and a historic scale model of the edifice. The city's 911 emergency system was overwhelmed during the disturbances. "While city hall sustained damage, we anticipate that all city offices will be open for regular business January 31," said the Oakland city administrator. Violence erupted again in Oakland January 28 when protesters attempted to take over the apparently empty downtown convention center to establish a new headquarters and draw attention to the problem of homelessness. Police in riot gear moved in to drive back the crowd, which they estimated at about 500 protesters. Source: <http://www.reuters.com/article/2012/01/30/us-oakland-protests-idUSTRE80S00520120130>

UNCLASSIFIED

COMMUNICATIONS SECTOR

(New Jersey) Copper thieves caught red-handed in Old Bridge. A police officer thwarted two men intent on stealing copper grounding plates from cell towers near a Garden State Parkway commuter parking lot in New Jersey February 1. A patrolman arrested the men, one of whom is an employee of Metro RF, on charges of burglary by entering a locked structure, theft of movable property, and possession of burglary tools, an Old Bridge Police captain said. "There has been a problem with copper grounding plates being stolen from cell tower areas," he said. "Not having the copper grounding bars can be extremely dangerous. Should lightning hit the cell towers, the entire communications system for the area, for all of the state, really, could be out." While on his usual rounds, the patrolman noticed an unoccupied vehicle parked in the commuter lot. A short time later, the same vehicle appeared to have its lights on, and as the officer approached the car he observed a man asleep in the passenger seat. As he was questioning the the man, the second suspect, approached them from the direction of the cell tower area, police said. Police said during his questioning of the men, the patrolman noticed a black bag filled with copper grounding plates in the vehicle. Upon closer inspection of the cell towers, numerous nuts and bolts were found discarded on the ground while wires were seen hanging loose from the cell towers where the copper grounding plates should have been attached, police said. Source: <http://www.mycentraljersey.com/article/20120201/NJNEWS/302010047/Copper-thieves-caught-red-handed-Old-Bridge?odyssey=mod|newswell|text|lp>

CRITICAL MANUFACTURING

HP recalls fax machines due to fire and burn hazards. The U.S. Consumer Product Safety Commission, in cooperation with Hewlett-Packard (HP) announced a voluntary recall February 2 of about 928,000 HP fax 1040 and 1050 machines. The importer was Hewlett-Packard Co., of Palo Alto, California. The machines were manufactured in China. The fax machines can overheat due to an internal electrical component failure, posing fire and burn hazards. HP is aware of seven reports of machines overheating and catching fire, resulting in property damage, including one instance of significant property damage and one instance of a minor burn injury to a consumer's finger. Six incidents were reported in the United States. The machines were sold at electronics, computer, and camera stores nationwide, and online at www.shopping.hp.com and other Web sites from November 2004 through December 2011. Some of the recalled fax machines were replacement units for a previous recall involving HP fax model 1010 in June 2008. Source: <http://www.cpsc.gov/cpsc/pub/prerel/prhtml12/12101.html>

Arctic Cat recalls snowmobiles due to crash hazard. Arctic Cat announced January 31 the recall of about 19,000 model year 2012 F, XF, and M model snowmobiles. The lower steering tie-rod attachment can loosen and cause loss of steering control, posing a crash hazard. Arctic Cat has received four reports of incidents, including one complete loss of steering control. No injuries have been reported. Consumers should immediately stop using these snowmobiles and contact their local Arctic Cat snowmobile dealer to schedule a free inspection and repair. Arctic Cat has

UNCLASSIFIED

notified owners of these snowmobiles directly by mail. Source:

<http://www.cpsc.gov/cpscpub/prerel/prhtml12/12716.html>

NHTSA recall notice - Mazda Tribute master cylinder cap. Mazda January 30 announced the recall of 52,390 model year 2001-2002 Mazda Tribute vehicles manufactured from April 20, 2000 through July 19, 2002. The brake master cylinder reservoir cap can leak brake fluid. If brake fluid leaks, it could come in contact with the antilock brake system (ABS) module wiring harness connector. Corrosion may develop in the electrical connector leading to melting, smoking, or possible fire. Mazda will notify owners, and dealers will replace the vehicle's brake master cylinder reservoir cap and modify the ABS electrical system. Mazda advised owners to park their vehicles outside, rather than in garages, until the repair has been performed. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V016000&summary=true&prod_id=240555&PrintVersion=YES

DEFENSE/ INDUSTRY BASE SECTOR

Fake Windows updater targets government contractors, stealing sensitive data. Two security companies released a joint report January 31 describing an ongoing series of attacks against government contractors that have been occurring since at least early 2009. According to the vendors Seculert and Zscaler, attackers are sending firms phishing e-mails with fake invitations to conferences, often in the form of PDF files that exploit flaws in Adobe Reader. The file installs what the vendors call an "MSUpdater" trojan that poses as a legitimate Windows Update process. In reality, the trojan is a remote access tool that can steal data from a company's network for as long as the breach remains undiscovered. "Foreign and domestic (United States) companies with intellectual property dealing in aero/geospace and defense seem to be some of the recent industries targeted in these attacks," the report states, without identifying specific attack targets. The vendors believe the attacks are either state-sponsored or perpetrated by a high-profile group of attackers, but they have not yet been able to determine their identities, according to Seculert's CTO. Source: <http://arstechnica.com/business/news/2012/01/fake-windows-updater-targets-government-contractors-stealing-sensitive-data.ars>

Parachute problem grounds some Lockheed F-35 jets. The Pentagon, January 30, said it was temporarily suspending high-speed ground and flight operations of more than 15 Lockheed Martin Corp F-35 fighter jets after discovering improperly packed parachutes under the pilot's ejection seat. The move affects six Air Force variants of the F-35 fighter jet based at Edwards Air Force Base in California, halting testing until the parachute issues are resolved, according to a Lockheed spokeswoman. The suspension also affects nine F-35 fighters to be used for training at Eglin Air Force Base in Florida, and three planes nearly completed at Lockheed's Fort Worth, Texas, factory, according to Lockheed and the Pentagon's F-35 program office. It will not affect eight F-35 test aircraft at Naval Air Station Patuxent River, Maryland, because they had received older ejection seats whose parachutes were properly packed. It estimated that it would take about 10 days until the first set of repacked parachutes were available. The grounding comes as the \$382 billion F-35 Joint Strike Fighter program braces for a third restructuring in 3 years. The

UNCLASSIFIED

UNCLASSIFIED

Pentagon's program office, in a joint statement with Lockheed, said the affected ejection seats were packed in reverse order by privately owned UK-based Martin Baker Aircraft Corp, apparently due to improperly drafted procedures. Source:

<http://www.reuters.com/article/2012/01/30/us-lockheed-fighter-pentagon-idUSTRE80T1S120120130>

Insight into Sykipot Operations. The Sykipot campaign has been persistent in the past few months targeting various industries, the majority of which belong to the defense industry, Symantec reported January 26. Each campaign was marked with a unique identifier comprised of a few letters followed by a date hard-coded within the Sykipot Trojan itself, researchers found. These campaign markers allowed the attackers to correlate different attacks on different organizations and industries. The attackers also left additional clues that allowed Symantec to gain insight into what appears to be a staging server that is used prior to the delivery of new binaries to targeted users. In addition, Symantec was able to confirm the server was also used as a command and control server for a period of time as well. The server is based in the Beijing region of China and was running on one of the largest ISPs in China. Source:

<http://www.symantec.com/connect/fr/blogs/insight-sykipot-operations-0>

EMERGENCY SERVICES

(New York; Utah; Texas) 'Anonymous' hackers shut down Syracuse police Website. Hackers affiliated with the group "Anonymous" hacked the police Web site in Syracuse, New York and in Salt Lake City, and Texas, according to Syracuse police. The Syracuse public information site was hacked, but that did not include police reports or other sensitive information, said a sergeant. The Web site, www.syracusepolice.org, will likely be shut down for a few days, he said.

Syracuse police department names and apparent passwords were posted February 1 to sites where hackers often post snippets of code. The hackers cited the department's knowledge of a case, as well as the case of a former Auburn police officer, a convicted felon suing the city of Auburn for back pay and pension. The officer's case is not related to the Syracuse Police Department in any way. The sergeant stressed the hacked site was maintained by a third-party host and was not linked to departmental records. In Salt Lake City, hackers who broke into the police department site compromised more data than originally thought, police said February 1. "We have learned that citizen complaints regarding drug crimes in the community were also accessed. These forms included phone numbers, addresses, e-mail addresses, other personal information, and details about suspicious activity from a variety of sources," a news release stated. The hackers also attacked Texas police agencies, especially in the Fort Worth area.

Source:

http://www.syracuse.com/news/index.ssf/2012/02/anonymous_hackers_shut_down_sy.html

Hackers claim to have intercepted call between FBI, Scotland Yard. A sensitive conference call between the FBI and Scotland Yard was recorded by the hacking group Anonymous, it claimed February 3. The group released a roughly 15-minute-long recording of what appears to be a January 17 conference call devoted to tracking and prosecuting members of the loose-knit hacking group. There was no classified information on the call, FBI sources told Fox News,

UNCLASSIFIED

UNCLASSIFIED

noting unsecure phones are not used for sensitive information. The source indicated those responsible will be held accountable. Names of some of the suspects being discussed were apparently edited from the recording. "The information was illegally obtained and a criminal investigation is underway," a FBI spokesman told Fox News. Anonymous also published an e-mail purportedly sent by an FBI agent that gave details and a password for accessing the call. Amid the material published by the hackers was a message purportedly sent by an FBI agent to international law enforcement agencies. It invites his foreign counterparts to join the call to "discuss the on-going investigations related to Anonymous ... and other associated splinter groups." The e-mail contained a phone number and password for accessing the call. The e-mail was addressed to officials in England, Ireland, the Netherlands, Sweden, and France, but only American and British officials can be heard on the recording. Source:

<http://www.foxnews.com/scitech/2012/02/03/hackers-claim-to-have-intercepted-call-between-fbi-scotland-yard/?test=latestnews>

(West Virginia) State to beef up training for emergency responders. West Virginia officials apparently plan to increase the training requirements for emergency medical personnel to improve their ability to respond to hazardous material accidents. Word of the plan emerged January 30, on the fifth anniversary of a propane explosion that killed four people at a Raleigh County convenience store. U.S. Chemical Safety Board (CSB) officials said they were told of the plan January 27, after they issued a news release that criticized West Virginia's Office of Emergency Medical Services for not requiring annual hazardous materials response refresher training for all emergency medical personnel. To date, training occurs only once every 2 years. Source: <http://sundaygazette.com/News/201201300177>

(Kentucky; Tennessee) Bridge collapse causes changes in ambulance routes. The partial collapse of the Eggners Ferry Bridge has a Murray, Kentucky, hospital working to reassure the community, WPSD 6 Paducah reported January 30. The Murray-Calloway County Ambulance Service is having to detour around the collapse that occurred January 26 when a cargo ship slammed into the bridge. Paramedics used the bridge to take patients needing more specialized medical care to Nashville, Tennessee. The ambulance service makes between 10 and 15 trips to Nashville a month. The Murray-Calloway County Hospital also takes in about eight patients a month from Trigg County Hospital. If a patient must go to Nashville, there are two options. The first takes them onto Interstate 24. The ride is smoother but about 30 minutes longer. The other option takes the patient through Dover, Tennessee. The roads are rougher and tough on ambulances. The CEO of Murray-Calloway said critically injured patients are always flown out. That will not change. Many people travel across the bridge from Trigg County to Murray-Calloway for outpatient procedures and doctor's visits. Administrators are afraid some of those folks will look to get services elsewhere because of the added distance. Source: <http://www.wpsdlocal6.com/news/local/Bridge-collapse-causes-changes-in-ambulance-routes-138362674.htm>

(Florida) Guns stolen from police cruiser. Police in Orlando, Florida are looking for someone who stole an assault rifle, shotgun, and ammunition from a parked police car. Officials said the door of the marked police cruiser was pried open between January 23 and January 29.

UNCLASSIFIED

UNCLASSIFIED

Authorities said a department-issued Bushmaster AR 15 and unknown caliber Remington shotgun were removed from the vehicle. Each gun was loaded with ammunition, officials said. It is unknown if the police cruiser was parked in the same spot the entire time or if there was a delay in reporting the theft. The theft is still under investigation. Source:

<http://www.wesh.com/r/30333644/detail.html>

(Virginia) Missing street signs cause 911 problems. A spike in the number of street sign thefts has prompted the sheriff's office to increase patrols and ask residents for assistance. The thefts usually average about 30 per month, according to the lieutenant with the Franklin County, Virginia Sheriff's Office. But in December and January, the number of thefts significantly increased, especially in Truevine and Boones Mill. "The thefts cause a problem for first responders, who rely on those street signs to locate residences," he said. "Missing street signs also interfere with Fed Ex and UPS deliveries." Anyone found with a street sign will be charged with possession of stolen property, he said. And anyone found in the act of taking the signs will be charged with larceny. Source: <http://www.thefranklinnews.com/article.cfm?ID=21198>

ENERGY

Researchers postpone release of free smart meter security testing tool. Smart grid researchers pulled their talk and planned release of a new security assessment tool for smart grid meters during the ShmooCon conference after a vendor voiced concerns about the research. A senior security analyst with InGuardians had planned to introduce January 28 a new homegrown tool that tests for both vulnerabilities and functionality in smart grid meters — via the devices' infrared ports. A spokesman said there were no official threats of legal action by the vendor, which he declined to name. InGuardians had not planned to name any vendors in Weber's presentation, either. Legal threats and vendor pressure are nothing new in the security research community: There have been multiple occasions where vendor backlash has forced researchers to pull their presentations at Black Hat, DefCon, and at TakeDownCon in 2011.

Source: <http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/232500808/>

(Texas) Copper spools worth \$10K stolen from Xcel. Amarillo, Texas police are seeking four large spools of copper wire taken from an Xcel Energy site, the Amarillo Globe News reported January 31. On January 24, Xcel Energy reported four commercial-grade copper spools worth more than \$10,000 missing from its property. Police said property surveillance equipment recorded a four-door Nissan Frontier hauling a red trailer in the area. An Xcel Protection Services consultant said the 3- and 4-foot copper spools were going to be used for new construction. Three of the spools were small enough to load onto the truck or trailer and the fourth was likely rolled on. The stolen copper was insulated, or covered with plastic, which is typically harder to recycle. Source: <http://amarillo.com/news/local-news/2012-01-31/more-10k-copper-stolen-xcel-site#.TylMnoHLlBk>

(Oklahoma) Oil storage tank in Kingfisher explodes after being struck by bullet. Fire officials said someone intentionally shot at an oil well tank in Kingfisher County, Oklahoma, January 29,

UNCLASSIFIED

UNCLASSIFIED

causing it to explode and start a fire. The bullet struck the tank and caused enough pressure for the top to explode. About 12 firefighters responded to the scene and were able to extinguish the fire with oil well foam before the blaze reached nearby wheat crops. The fire damaged two of the three Continental Operating Company oil tanks at the site, causing \$20,000 in damage. Company officials worked with firefighters to help shut the well down so the fire could be put out. Source: <http://newsok.com/oil-storage-tank-in-kingfisher-explodes-after-being-struck-by-bullet/article/3644563>

FOOD AND AGRICULTURE

Hard-cooked egg recall expands, potato salads included. One week after a company began notifying customers in 34 states about potential Listeria contamination in hard-cooked eggs, the Food and Drug Administration announced that Michael Foods, Inc. is expanding its recall of certain hard-cooked eggs, Food Safety News reported February 2. Michael Foods said it was widening the initial call back for three lot dates, announced January 26 after lab testing revealed some of the eggs may have been contaminated with Listeria monocytogenes. Additional lot dates were added, the company said, because of new evidence a repair project in its Wakefield, Nebraska, packaging room “was the likely source of the contamination.” While Michael Foods said its eggs were not sold directly to retailers or consumers, the company acknowledged food distributors and manufacturers who purchased the eggs could have used them in products sold to retail outlets, or used them in food service settings. Source: <http://www.foodsafetynews.com/2012/02/hard-cooked-egg-recall-expands-potato-salads-included/>

Cantaloupe Listeria outbreak still claiming victims. One more victim of the nationwide outbreak of Listeria infection linked to Colorado cantaloupes died January 29, bringing the death toll up to 32. When the epidemic was declared over in December 2011, it was already the deadliest foodborne illness outbreak in the United States in nearly 100 years, having killed 30 of the 146 people sickened, and caused a pregnant woman to miscarry. However, while the contaminated cantaloupes — distributed by Jensen Farms — were long off the market by that time, the disease continued to wreak havoc on its victims, claiming two more lives. December 18, 10 days after the Centers for Disease Control and Prevention (CDC) issued its final outbreak report, a man died after weeks suffering from listeriosis. January 29, a woman died from complications due to stage IV breast cancer and listeriosis. Listeriosis is especially devastating for individuals with compromised immune systems, making it harder to combat alongside chemotherapy, which weakens the body’s defenses. The CDC may not update its outbreak report to include either of these deaths. If this remains the case, it is likely these deaths will go unreported in the official count. According to investigators, traces of Listeria could have come into the packing plant via a truck used to ferry culled cantaloupes to a cattle operation. The bacteria then could have flourished in pooled water, and been tracked and spread around the packing shed, contaminating walkways and equipment. Source: <http://www.foodsafetynews.com/2012/02/cantaloupe-listeria-outbreak-still-claiming-victims/>

UNCLASSIFIED

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Utah) Suspect in Utah school bomb plot charged. Authorities filed charges against a 16-year-old boy accused in a plot to detonate a bomb at a Utah high school, the Associated Press reported January 31. Police said the teenager, along with an 18-year-old, planned to bomb an assembly at Roy High School, in Roy, Utah. Both were arrested the week of January 23. The 18-year-old has been charged with possession of a weapon of mass destruction. Prosecutors January 31 charged the 16-year-old with the same count in juvenile court, but have filed a motion seeking to try him as an adult. Police said the plot was foiled when another student came forward after receiving ominous text messages from one of the suspects hinting at their plan. Source: <http://www.cachevalleydaily.com/news/local/Suspect-in-Utah-school-bomb-plot-charged-138445339.html>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Symantec warns of Android trojans that mutate with every download. Researchers from Symantec identified a new premium-rate SMS Android trojan that modifies its code every time it gets downloaded to bypass antivirus detection. This technique is known as server-side polymorphism and already existed in the world of desktop malware for many years, but mobile malware creators have only now begun to adopt it. A special mechanism that runs on the distribution server modifies certain parts of the trojan to ensure every malicious app that gets downloaded is unique. This is different from local polymorphism where the malware modifies its own code every time it gets executed. Symantec identified multiple variants of this trojan horse, which it detects as Android.Opfake, and all of them are distributed from Russian Web sites. However, the malware contains instructions to automatically send SMS messages to premium-rate numbers from many European and former Soviet Union countries. In some cases, especially when security products rely heavily on static signatures, detecting malware threats that make use of server-side polymorphism can be difficult. Source: [http://www.computerworld.com/s/article/9223950/Symantec warns of Android Trojans that mutate with every download?taxonomyId=17](http://www.computerworld.com/s/article/9223950/Symantec_warns_of_Android_Trojans_that_mutate_with_every_download?taxonomyId=17)

HTC Android phones expose Wi-Fi passwords to apps. HTC has confirmed the way some of its Android smartphones handle requests for passwords allows applications to obtain the passwords for Wi-Fi networks the phones are connected to. If that application also has permission to connect to the Internet it could take that information and transfer it to an unknown server. Researchers discovered applications with the android.permission.ACCESS_WIFI_STATE permission could obtain the password, user name, and other settings by executing the .toString() method of the WiFiConfiguration class. On most Android devices, the .toString() leaves the password field blank or marked with a "*" to show a password is set, but on the affected HTC devices, the password is shown in clear text. The flaw was found in September 2011 and the researchers have been working with Google and HTC to resolve the issue. Google changed the Android code to better protect the credentials store and performed a code scan of applications in the Android Market and found no applications that

UNCLASSIFIED

exploit the vulnerability there, though this may not apply to other sources of Android applications. HTC has released updates for the affected smartphones. HTC said most devices will have already received the fix with over the air updates but some devices will need a manual update and asks users to check the help page for more information in the coming week. Source: <http://www.h-online.com/security/news/item/HTC-Android-phones-expose-Wi-Fi-passwords-to-apps-1427099.html>

Android malware makes use of steganography. Security firm F-Secure released details on how Android malware makes use of steganography to hide the control parameters for rogue code. Steganography is the technique of hiding messages within something else, in this case, an icon file. F-Secure first suspected Android malware was making use of steganography when researchers came across a particular line of code. Further research revealed more code, and it soon became clear the image file being referenced was the icon file bundled with the rogue application. The hidden data is used to control how and when premium rate SMS messages are sent from the victim's handset, which is the primary purpose of the rogue application. Source: <http://www.zdnet.com/blog/hardware/android-malware-makes-use-of-steganography/17903>

Facebook Valentine's Day Theme Leads to Trojan. Trend Micro researchers came across a Valentine's Day-themed Facebook scam that attempts to dupe victims into downloading a malicious Trojan that later places itself in the browser with the purpose of helping crooks make money, Softpedia reported January 31. Facebook customers who fall for the phony advertisement and click it are taken to a Web site that displays a large Install button. Once clicked, the page prompts the user to download a file called FacebookChrome.crx, identified by the security firm as Troj.Fookbace.A. Upon execution, the Trojan executes a script that is capable of displaying ads from other sites, as well as installing itself on the browser as an extension named Facebook Improvement. After it is successfully installed, the malicious extension monitors Web activities, redirects sessions to survey pages that request sensitive data, performs like-jacking attacks, and posts ill-intended messages on behalf of the victim. Experts believe these attacks are specially designed to target Chrome users, but note they also work with Mozilla Firefox. Facebook members that utilize Internet Explorer are directly taken to the survey site because the extension does not work that browser. Source: <http://news.softpedia.com/news/Facebook-Valentine-s-Day-Theme-Leads-to-Trojan-249729.shtml>

Massive Android malware op may have infected 5 million users. The largest-ever Android malware campaign may have duped as many as 5 million users into downloading infected apps from Google's Android Market, Symantec said January 27. Dubbed "Android.Counterclank" by Symantec, the malware was packaged in 13 different apps from three different publishers, with titles ranging from "Sexy Girls Puzzle" to "Counter Strike Ground Force." "They don't appear to be real publishers," a director with Symantec's security response team said in an interview. "These aren't rebundled apps, as we've seen so many times before." Symantec estimated the impact by combining the download totals of the 13 apps, arriving at a figure between 1 million on the low end and 5 million on the high. When installed on an Android smartphone, Android.Counterclank collects a wide range of information, including copies of the bookmarks and the

UNCLASSIFIED

UNCLASSIFIED

handset maker. It also modifies the browser's home page. Source:

[http://www.computerworld.com/s/article/9223777/Massive Android malware op may have infected 5 million users](http://www.computerworld.com/s/article/9223777/Massive_Android_malware_op_may_have_infected_5_million_users)

Drive-by-download attack exploits critical vulnerability in Windows Media Player. Security researchers from antivirus vendor Trend Micro have come across a Web-based attack that exploits a known vulnerability in Windows Media Player, a threat response engineer said in a blog post January 26. The security flaw can be exploited by tricking the victim into opening a specially crafted MIDI (Musical Instrument Digital Interface) file in Windows Media Player. Microsoft released a security fix for it January 10, as part of its monthly patch cycle. If successful, the exploit downloads and executes a computer Trojan on the targeted system, which Trend Micro detects as TROJ_DLOAD.QYUA. “[So] far we’ve been seeing some serious payload, including rootkit capabilities,” the Trend Micro engineer said. The attack is not widespread at the moment, but it is possible other attackers will start exploiting the same vulnerability in the near future, a senior antivirus researcher said. Source:

[http://www.computerworld.com/s/article/9223768/Drive by download attack exploits critical vulnerability in Windows Media Player](http://www.computerworld.com/s/article/9223768/Drive_by_download_attack_exploits_critical_vulnerability_in_Windows_Media_Player)

New drive-by spam infects those who open email — no attachment needed. Attackers have developed a new way to infect a user's PC through e-mail. According to researchers at eleven, a German security firm, the new drive-by spam automatically downloads malware when an e-mail is opened in the e-mail client. The user does not have to click on a link or open an attachment — just opening the e-mail is enough. The current wave of drive-by spam contains the subject “Banking security update” and has a sender address with the domain fdic.com. If the e-mail client allows HTML e-mails to be displayed, the HTML code is immediately activated. Source: <http://www.darkreading.com/security/attacks-breaches/232500660/new-drive-by-spam-infects-those-who-open-email-no-attachment-needed.html>

Technology firms create DMarc to fight phishing. A crackdown on “phishing” scams has been announced by 15 of the top technology companies. E-mail providers such as Google and Microsoft will work with companies like Paypal and the Bank of America to improve authentication. The Domain-based Message Authentication, Reporting and Conformance (DMarc) coalition has released plans to produce a “feedback loop” between e-mail receivers and senders. The initiative is the first significant attempt to bring together e-mail and service providers along with key security organizations. DMarc said this industry-wide involvement — which covers the receivers, senders, and intermediaries of e-mail use — will mean e-mail providers will for the first time be able to reliably filter out unwanted e-mails, rather than use “complex and imperfect measurements” to determine threats. Source:

<http://www.bbc.co.uk/news/technology-16787503>

NATIONAL MONUMENTS AND ICONS

Nothing Significant to Report

UNCLASSIFIED

POSTAL AND SHIPPING

Nothing Significant to Report

PUBLIC HEALTH

Number of patient record data breaches nearly doubled last year. The total number of patient records compromised in the United States increased by 97 percent in 2011 compared with 2010, according to a report released this week by the Redspin consulting firm. Redspin cites the increasing concentration of protected health information (PHI) on unencrypted portable devices and the lack of sufficient oversight of PHI disclosed to hospital's business associates as the main reasons for the increase. Malicious attacks (theft, hacking, and insider incidents) continue to cause 60 percent of all breaches due to the economic value of personal health records sold on the black market, and for medical ID theft used to commit Medicare fraud. Redspin examined data breach information on the U.S. Department of Health and Human Services Web site, which lists a total of 385 breaches affecting more than 19 million individuals since breach reporting notification requirements went into effect in August 2009. For a breach to be reported, it must affect 500 individuals or more. In addition, the average number of records affected by a single breach has almost doubled. Source: <http://www.infosecurity-us.com/view/23648/number-of-patient-record-data-breaches-nearly-doubled-last-year/>

Pfizer recalls 1M birth control packs after mixup. Pfizer Inc. is recalling 1 million packets of birth control pills due to a packaging error that could raise the risk of an accidental pregnancy by leaving women with an inadequate dose. Pfizer found some packets of the drugs had too many active tablets, while others had too few. Oral birth control products use a series of 21 hormone tablets and 7 inactive sugar tablets to regulate the menstrual period while providing contraception. The problem affects 14 lots of Lo/Ovral-28 tablets and 14 lots of generic Norgestrel and Ethinyl Estradiol tablets. Both products are manufactured by Pfizer and marketed in the United States by Akrimax Rx Products under the Akrimax Pharmaceuticals brand. A Pfizer spokeswoman said the problem was caused by mechanical and visual inspection failures on the packaging line. She said the problem has been corrected. Patients with the affected lot numbers should return them to the pharmacy. The affected packets have expiration dates ranging between July 31, 2013, and March 31, 2014. The drugs were distributed to warehouses, clinics and retail pharmacies throughout the United States. Source: http://www.google.com/hostednews/ap/article/ALegM5h7oszk1RBsQuNjBK_8wMMkiqKDaA?docId=0cc71c595a72410a8375533c9c5eb70c

(Kentucky) Stolen Lexington Clinic laptop contained patient information. Kentucky's Lexington Clinic in Lexington was notifying the public of a privacy breach involving 1,018 patients 6 weeks after a medical clinic laptop was stolen, the Lexington Herald-Leader reported January 31. The laptop was stolen December 7 from the clinic's neurology department. A clinic spokeswoman said it took weeks to pinpoint exactly what information was on the laptop, which was used in conjunction with the clinic's electromyography machine. Clinic officials determined the laptop contained data such as names, contact information, and diagnoses gathered from patients as

UNCLASSIFIED

long as 5 years ago. The stolen laptop did not contain personal financial information such as Social Security numbers, credit card numbers, and bank account numbers. Officials from St. Joseph Hospital, which runs the office park, said the incident appears to have been an isolated theft. Letters to affected patients were sent the week of January 23, and the security breach was made public January 30. Source: <http://www.kentucky.com/2012/01/31/2049109/stolen-lexington-clinic-laptop.html>

(Florida) UM patient data stolen. Limited data on 1,219 University of Miami (UM) Miller School of Medicine patients in Miami, Florida, was stolen in November when someone broke the back window of a pathologist's car and took a briefcase that contained a flash drive. The drive contained information on the patients' age, sex, diagnosis, and treatment data from 2005 to 2011, the UM said in a press release January 27. No financial information or Social Security numbers were on the drive, the university said. Following federal law, UM is informing the patients involved, according to the press release, but "there is no indication that the information was accessed or misused in any way." More information on the theft is available on the UM Web site. Source: <http://www.miamiherald.com/2012/01/30/2615588/um-patient-data-stolen.html>

TRANSPORTATION

Scientists worry Alaska volcano, 'Cleveland', could blow soon. Scientists in Alaska are worried that a massive volcano on a remote island about 1,000 miles southwest of Anchorage is primed to erupt and spew a giant ash plume that could paralyze intercontinental travel. The Alaska Volcano Observatory January 31 bumped the alert status for the Cleveland Volcano from yellow to orange — one step below the highest alert level. "Renewed eruptive activity of Cleveland Volcano has been observed in satellite data," the observatory said, noting a new 130-foot lava dome — a visible bulge of gathering lava — had formed in the mountaintop's crater. About 90 percent of air freight from Asia to North America and Europe flies over Alaska, along with some 20,000 commercial travelers a day, according to CNN. Experts say a significant eruption could lead to a shutdown of the airspace, sparking the worst travel nightmare since a giant ash curtain from an Iceland volcano grounded millions of global travelers in April 2010. Source: <http://www.nydailynews.com/news/national/scientists-worry-alaska-volcano-cleveland-blow-article-1.1015974>

FTA lacks rail safety data, says OIG. The Federal Transit Administration (FTA) lacks the data necessary to nationally oversee transit safety, said the Transportation Department Office of Inspector General (OIG) in a January 31 report. The Transportation Secretary in 2009 called on Congress to approve legislation giving the FTA a direct role in setting rail transit safety standards and overseeing their implementation in localities that take federal rail dollars. Currently, 28 oversight agencies oversee 35 light rail and 13 heavy rail systems operated by 48 transit agencies across the country, leading to a disparity in standards such as rail car crash-worthiness and train operator certification. The only way the FTA would be able to step into an expanded oversight role would be to adopt data-driven, risk-based oversight, the OIG report says. But, while the FTA captures basic safety incident data such as fatalities and injuries, it does

UNCLASSIFIED

UNCLASSIFIED

not have detailed information on matters such as the condition of rail transit assets. Were the FTA to increase its responsibilities, it would also have to institute new practices to ensure data quality, a problem that has plagued other Transportation Department regulators such as the Federal Highway Administration, the report adds. The agency would also face the difficult task of articulating a uniform set of national safety performance measures, since without standardization in the measures, it would be unable to assess how well local agencies do. Even without expanded authority, the report recommends the FTA improve its data collection, an effort FTA officials say they are undertaking in an assessment of current data gaps. Source: <http://www.fiercehomelandsecurity.com/story/fta-lacks-rail-safety-data-says-oig/2012-02-02>

Sea trafficking report reveals how ships move guns and drugs. Most ships involved in reported cases of sanctions-busting or illicit transfers of arms, drugs, and equipment that could be used in the development of missiles and weapons of mass destruction are owned by companies based in the world's richest countries, according to the first comprehensive study of maritime trafficking. The ships are primarily commercial lines based in Germany, Greece, and the United States, according to the report, released January 30 by the Stockholm International Peace Research Institute. "This doesn't mean the ship owners, or even the captains, know what they are carrying. But it is relatively easy for traffickers to hide arms and drugs in among legitimate cargoes," said the report's co-author. The report shows the methods adopted by arms trafficking networks in response to United Nations embargoes on Iran and North Korea were pioneered by drug traffickers. They included hiding goods in sealed shipping containers that claim to carry legitimate items; sending the goods on foreign-owned ships engaged in legitimate trade; and using circuitous routes to make the shipments harder for surveillance operations to track. The report shows that in cases where the ship owners, operators, and captains appear to have been directly involved in the trafficking attempt, the ships tended to be older and to be sailing under "flags of convenience." They regularly performed badly in safety and pollution inspections when they entered ports. Source: <http://www.guardian.co.uk/world/2012/jan/30/sea-trafficking-report-guns-drugs>

FAA faces shortage of air traffic controllers because of retirements. Despite a 5-year hiring surge, the Federal Aviation Administration (FAA) is at risk of not having enough senior air traffic controllers for its busiest and most critical facilities, where they are needed to run operations and train less-experienced controllers, according to the agency's independent inspector general (IG). Nearly one-third of the senior controllers at the nation's most critical facilities are eligible for retirement, according to the report. At a Dallas-Ft. Worth FAA facility, 65 percent of the controllers are eligible for retirement, it says. Meanwhile, trainees are quitting jobs at high rates at those demanding, high-volume facilities. Between fiscal year 2008 and fiscal year 2010, critical facilities lost 40 percent of their trainees to attrition, well above the national average of 24 percent, the report says. The IG looks at 21 facilities deemed "critical" to the nation because of the high volume of air traffic they control. The list includes several control towers at the nation's busiest airports — Atlanta Hartsfield-Jackson, Chicago O'Hare, and the New York area's Kennedy, Newark, and LaGuardia fields — as well as several regional and high-altitude facilities. The FAA said January 30 it has "progressively improved" hiring, training, and certification of new controllers and has increased its ranks of senior controllers, known as "certified

UNCLASSIFIED

UNCLASSIFIED

professional controllers.” The FAA told the inspector general’s office it recognizes the “failure rate” of new controllers is unacceptably high at some facilities, and it is addressing the issue.

Source: <http://fox6now.com/2012/01/30/faa-faces-shortage-of-air-traffic-controllers-because-of-retirements/>

(Florida) ‘Low visibility’ reported hours before Florida interstate pileup that killed 10.

Troopers reopened Interstate 75 January 30 as the investigation continued into the massive pileup that killed 10 people on the highway near Gainesville, Florida the weekend of January 28. The Florida Highway Patrol (FHP) released an accident report January 30 showing there was a three-way crash at 11:55 p.m., involving a tractor-trailer and two SUVs, that preceded the massive pileup early January 29, according to the Associated Press. One person was seriously injured in the January 28 crash. A trooper noted in his report “there was heavy smoke in the area, causing low visibility.” The highway was closed to traffic a short time later. The 19-vehicle crash happened after the smoke- and fog-shrouded highway reopened at about 4 a.m. Besides the 10 people killed, 18 people were hospitalized. Wreckage, some of it burned and twisted, stretched for about a mile along the high-traffic road, the main transit route down the middle of the state. It was closed in both directions for hours. Troopers re-opened lanes the evening of January 29, but shut the interstate down again early January 30 because of smoke and visibility issues, a FHP spokesperson said. All lanes reopened at about 11 a.m. January 30. A 62-acre fire broke out January 28 in Paynes Prairie, a wildlife area that straddles the freeway just south of Gainesville, but a spokeswoman for the Florida Forest Service said it was not clear how it started. Source: <http://www.chicagotribune.com/news/nationworld/os-florida-highway-deaths-killed-i-75-20120130,0,2598249.story>

WATER AND DAMS

Irrigation causing declines in the High Plains Aquifer. Groundwater withdrawals for crop irrigation have increased to over 16 million acre-feet per year in the High Plains Aquifer, according to a recent U.S. Geological Survey (USGS) study released February 3. The USGS study shows recharge, or the amount of water entering the aquifer, is less than the amount of groundwater being withdrawn, causing groundwater losses in this already diminished natural resource. Crop irrigation is the largest use of groundwater in the aquifer, and, over the past 60 years, has caused severe water-level declines of up to 100 feet in some areas. The new USGS findings address concerns about the long-term sustainability of the aquifer. The High Plains aquifer underlies about 175,000 square miles in parts of eight states – Colorado, Kansas, Nebraska, New Mexico, Oklahoma, South Dakota, Texas, and Wyoming – and is a major source of groundwater irrigation in the region. The High Plains region supplies about one-fourth of the nation’s agricultural production. The new USGS study also compares previously published data with new methods for estimating recharge and groundwater withdrawals, and provides an assessment of the strengths and weaknesses of those methods. This USGS report is part of a larger study to evaluate groundwater availability of the High Plains Aquifer. Source:

<http://www.wateronline.com/article.mvc/Irrigation-Causing-Delcines-In-The-High-0001>

UNCLASSIFIED

UNCLASSIFIED

(Illinois) Chicago water sampling shows high levels of lead. In a new round of water testing by the Environmental Protection Agency (EPA), half of the 29 Chicago homes visited yielded at least one sample containing more than 15 parts per billion (ppb) of lead, a level that can trigger regulatory action if detected during routine screening, the Chicago Tribune reported January 31. Agency officials said the results will help regulators evaluate whether the 20-year-old procedures used nationwide to test homes' tap water for lead should be updated. Current procedures require only the first liter of water that comes out of homeowners' faucets to be checked, and action is taken if more than 10 percent of tested homes exceed 15 ppb. Under that standard, Chicago has passed its tests for nearly 20 years. EPA researchers, however, tested samples from at least the first 11 liters to come out of the sink in each home. Only one home had a level more than 15 ppb in its first sample, but at least one of the next 10 samples exceeded that level in 15 of 29 homes. A representative from the Chicago Department of Water Management, which tests tap water under current procedures, said it was aware of and analyzing the results. The latest results, based on EPA testing in September and October, are similar to results of sampling carried out in June. Lead levels found in the homes went as high as 36.7 ppb and as low as 1.5. The EPA says there is no safe level of lead exposure. New national standards for lead content on the "wetted" contact surface of plumbing and fixtures will take effect in 2014. The weighted average lead content will be restricted to 0.25 percent or less.

Source: <http://www.chicagotribune.com/health/ct-met-epa-lead-tests-20120131,0,4490886.story>

Water quality said to affect herbicides. The quality of water used to spray herbicides can affect their efficiency and crop producers should test water sources, U.S. researchers said. Research by Purdue University found hard water or water with pH values as low as 4 or as high as 9 can lessen the efficacy of certain common plant herbicides. "At this point, it seems to be specific to a limited number of compounds," a professor of botany and plant pathology said in a news release January 27. Some common herbicides sensitive to spray water quality included glyphosate, nicosulfuron, and saflufenacil, he said. Testing spray water for pH and hardness is especially important if producers are getting water from multiple sources because levels can vary from well to well, he said. Source: <http://outcomemag.com/science/2012/01/27/water-quality-said-to-affect-herbicides/>

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; 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, 701-328-8168

UNCLASSIFIED