

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

UNCLASSIFIED

NORTH DAKOTA

Nothing Significant to Report

REGIONAL

(Colorado) Copper thefts cause \$250k in damage to rail system. Two Colorado brothers are accused of stealing more than \$96,000 worth of overhead copper wiring from two light rail construction sites. The Denver Post reported January 17 the thefts caused \$250,000 damage to the RTD FasTracks system under construction in Jefferson County, Colorado. Two suspects were being held in Jefferson County jail. One faced charges of theft by receiving, and his brother faced felony charges of criminal mischief and theft. Investigators said about 7,000 feet of copper wire was stolen from one RTD site and another 150 feet from a second, causing I-beams supporting the overhead wires to bend. Source:

<http://www.noco5.com/story/16540529/copper-thefts-cause-250k-in-damage-to-rail-system>

(South Dakota) Repairs planned for Pierre causeway. A causeway that connects the city of Pierre, South Dakota, to LaFramboise Island on the Missouri River will be rebuilt. Parts of the causeway were washed away last spring and summer by Missouri River flooding. Now the U.S. Army Corps of Engineers said it will spend up to \$2 million for repairs. The causeway provides access to four city drinking water wells on LaFramboise Island that have not been used since last year's flooding. The Oahe Dam project manager is hopeful the rebuilding will be finished this year. The mayor of Pierre said the city will pay part of the repair cost. Source:

<http://www.therepublic.com/view/story/39e6f9579874499c92bb70fac75e83f4/SD--Causeway-Construction/>

NATIONAL

Nothing Significant to Report

INTERNATIONAL

Israeli hackers target UAE, Arab Bank sites. In the wake of recent hacks that targeted Israeli Web sites, a group known as IDF Team January 19 went after the Web sites for two major Arab banks. As of 1:30 p.m. Eastern Time, the Web sites for the Central Bank of the United Arab Emirates and Arab Bank were both offline. In a note posted to Pastebin, IDF Team said its attacks were in retaliation for a January 18 hack of Israel's Anti-Drug Authority Web site, which IDF called terrorist activity and "attempts to disrupt the normal course of life in Israel." If the attacks on Israeli sites don't stop, IDF Team pledged to also target stock market and government Web sites, such as the Arab Emirates Web portal at government.ae, as well as "sites related to the country's economy and even security." According to the Financial Times, the January 19 bank attacks were likely distributed denial of service (DDoS) attacks. Source:

<http://www.pcmag.com/article2/0,2817,2399095,00.asp>

UNCLASSIFIED

UNCLASSIFIED

Radioactive material stolen from Egyptian nuclear power station. Radioactive material has been stolen from an under-construction nuclear power station on Egypt's Mediterranean coast that was the site of violent protests, the Egyptian state-run al-Ahram newspaper reported January 19. A safe containing radioactive material at the Dabaa nuclear power plant was seized while another safe containing radioactive material was broken open and part of its contents taken, the newspaper said. The Egyptian government alerted security authorities and asked that specialized teams help in the search for the stolen material. More than a dozen people were wounded the week of January 9 when military police tried to disperse hundreds of protesters demanding the relocation of the plant. Source:

<http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/9024293/Radioactive-material-stolen-from-Egyptian-nuclear-power-station.html>

BANKING AND FINANCE INDUSTRY

U.S. charges Chinese man with NY Fed software theft. U.S. prosecutors arrested a Chinese computer programmer January 18 on charges that he stole software code valued at nearly \$10 million from the Federal Reserve Bank of New York. The man was a contract programmer. He was accused of illegally copying software to an external hard drive, according to a criminal complaint filed in U.S. district court in Manhattan. Authorities said the software, owned by the U.S. Treasury Department, cost about \$9.5 million to develop. A New York Fed spokesman said in a statement the bank immediately investigated the breach when it was uncovered and promptly notified authorities. The programmer was charged with one count of stealing U.S. government property, which carries a maximum 10-year prison term. The complaint, signed by an FBI agent, said the man admitted to copying the code onto a drive and taking it home. He told investigators he took the code "for private use and in order to ensure that it was available to him in the event that he lost his job," the complaint said. While U.S. intelligence officials have become increasingly worried about economic espionage, cybercrime experts said the case appeared to be one of simple theft. The programmer was hired as a contract employee in May by an unnamed technology consulting company used by the Fed to work on its computers, the complaint said. The code, called the Government-wide Accounting and Reporting Program (GWA), was developed to track the billions the U.S. government transfers daily. The GWA provides federal agencies with a statement of their account balance, the complaint said. Investigators uncovered the suspected breach only after one of the programmer's colleagues told a supervisor the programmer had claimed to have lost a hard drive containing the code, the complaint said. Source: <http://www.reuters.com/article/2012/01/19/us-nyfed-theft-idUSTRE80H27L20120119>

New stealthy botnet Trojan holds Facebook users hostage. A new strain of cybercrime trojan is targeting Facebook users by taking over their machines and shaking them down for cash, The Register reported January 18. Carberp, like its predecessors Zeus and SpyEye, infects machines by tricking users into opening PDFs and Excel documents loaded with malicious code, or attacks computers in drive-by downloads. The hidden malware is designed to steal account information and harvest credentials for e-mail and social-networking sites. A new configuration of the Carberp trojan targets Facebook users to ultimately steal e-cash vouchers. Previous malware

UNCLASSIFIED

UNCLASSIFIED

attacks on Facebook have been designed purely to steal log-in info, so this latest trojan, spotted by security firm Trusteer, can be considered an escalation. The Carberp variant replaces any Facebook page the user navigates to with a fake page notifying the victim their Facebook account is temporarily locked. The page asks the mark for their first name, last name, e-mail, date of birth, password, and a Ukash 20 euro (\$25) voucher number to verify their identity and unlock the account. The use of anti-debugging and rootkit techniques make Carberp trojan difficult to detect, warns security consultancy Context Information Security. Context said: "Carberp is also part of a botnet that can take full control over infected hosts, while its complicated infection mechanisms and extensive functionality make it a prime candidate for more targeted attacks." Context adds Carberp, which creates a backdoor on infected machines, can be controlled from a central administrator control panel, allowing botnet herders to more easily mine stolen data. Trusteer said it has reported the attack to Facebook. Source: http://www.theregister.co.uk/2012/01/18/carberp_steals_e_cash_facebook/

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

TEPCO left backup power for nuclear data equipment detached for 4 months. Tokyo Electric Power Co. (TEPCO) left the backup power source of a reactor-monitoring device at Japan's Fukushima Nuclear Power Plant disconnected for 4 months until the March 2011 earthquake and tsunami triggered a disaster at the plant, the Mainichi Daily News reported January 20. Failure to connect the backup source is said to have prevented data on the status of the plant being sent to the government for about 2 hours after the outbreak of the crisis. It is believed this may have affected the initial response to the disaster and the predictions on the spread of radioactive materials. TEPCO officials said workers tried to connect the backup power supply to the media converter during renewal work in November 2010, but the cable was too short so it was left disconnected. Source: <http://mdn.mainichi.jp/mdnnews/news/20120120p2a00m0na008000c.html>

(New Jersey) Chemist admits to stealing sanofi-aventis secrets. A former research chemist with global pharmaceutical company sanofi-aventis headquartered in Bridgewater, New Jersey, pleaded guilty January 17 to stealing trade secrets and making them available for sale through a U.S. subsidiary of a Chinese chemical company, authorities said. The 29-year-old Chinese national is a resident of Franklin, New Jersey, who worked for sanofi-aventis. The convict worked as a research scientist at the firm from August 2006 to June 2011, where she directly assisted in the development of many compounds sanofi-aventis viewed as building blocks for future drugs. The compounds were trade secrets and had not been disclosed outside in any manner, including by means of a patent application. While employed at the firm, the convict was a 50 percent partner in Abby Pharmatech Inc., a subsidiary of Chinese chemical products company Xiamon KAK Science and Technology Co. Ltd. Abby also is engaged in the sale and distribution of pharmaceuticals. The convict admitted that between October 2008 and June 2011, she accessed an internal sanofi-aventis database and downloaded data and chemical structures related to many compounds onto her company-issued laptop. She said she then transferred the data to her home computer via e-mail or a USB thumb drive. The convict further admitted she made the stolen compounds available for sale on the Abby Catalog on Abby

UNCLASSIFIED

UNCLASSIFIED

Pharmatech Web sites, as well as through a well-known online database. The convict's lawyer said she only listed the items for sale but never had the compounds. He said she did this to make the size of the Abby Catalog, which included legitimate compounds, look bigger. The charge to which the convict pleaded guilty carries a maximum potential penalty of 10 years in prison and a \$250,000 fine. Source:

<http://www.mycentraljersey.com/article/20120117/NJNEWS/301170036/Chemist-admits-to-stealing-sanofi-aventis-secrets>

COMMERCIAL FACILITIES

Hackers zap Zappos: Info from 24 million users stolen. Popular online shoe retailer Zappos.com said January 15 that hackers accessed its network and stole account information from as many as 24 million customers. Credit card information was not stolen, the company CEO said in a statement sent to users, but e-mail addresses, billing, and shipping addresses, phone numbers, the last four digits from credit cards — and more — may have been compromised. The company said it already reset the passwords for existing customers to prevent abuse of the stolen data. Source:

<http://www.foxnews.com/scitech/2012/01/16/zappos-zapped-hackers-steal-info-from-24-million-users/?test=latestnews>

COMMUNICATIONS SECTOR

(Arizona) Copper thieves target Century Link. A \$1,000 reward is being offered for information leading to an arrest in the case of copper theft from Century Link, KVOA 4 Tucson reported January 19. The phone, Internet, and TV company said copper was stolen from more than 80 sites in Pima County, Arizona, and the Phoenix area. Forty-three of those sites are in Tucson alone. The vice president and general manager of Century Link said the theft has cost the company hundreds of thousands of dollars, but has really impacted its customers. “[W]e’re most concerned about the outages this causes for people that rely on the service day in and day out.” Each theft causes hours of service outage for thousands of customers and takes crews several hours to repair. Authorities from throughout Pima County are investigating. A deputy said the Pima County’s Sheriff’s Office is looking at 11 cases from Century Link alone. Century Link believes citizens may not contact authorities because, in some instances, the thieves are driving utility type trucks posing as landscapers. “The thieves typically target areas that are a little bit more rural. Where they probably stand a better chance of doing this and some of the theft has actually taken place in the middle of the day,” the vice president said. Source:

<http://www.kvoa.com/news/copper-thieves-target-century-link/>

Federal body concludes LightSquared can’t work with GPS. A key federal agency involved in testing the proposed LightSquared Long-Term Evolution (LTE) network has concluded there is no practical way to solve interference between that network and the Global Positioning System (GPS), possibly dealing a crippling blow to the startup carrier’s hopes for a terrestrial mobile network. In a memo released January 13, the National Space-Based Positioning, Navigation, and Timing Executive Committee (PNT ExComm) said the nine federal agencies that make up the

UNCLASSIFIED

UNCLASSIFIED

body had concluded unanimously that none of LightSquared's proposals would overcome significant interference with GPS. LightSquared in 2010 received a waiver from the Federal Communications Commission (FCC) allowing it to operate a terrestrial LTE network on frequencies that have until now been devoted to much weaker satellite signals. The PNT ExComm has been involved in testing and results analysis at the request of the FCC and the National Telecommunications and Information Administration (NTIA). Both the original and modified proposals by LightSquared would cause harmful interference to many GPS receivers, the PNT ExComm chairs said in the memo. The agency also said a Federal Aviation Administration analysis had concluded the network would be incompatible with aircraft safety systems. Source:

http://www.computerworld.com/s/article/9223447/Federal_body_concludes_LightSquared_cant_work_with_GPS

T-Mobile USA hacked. A group of hackers that goes by the name "TeaMp0ison" claims to have obtained access credentials belonging to staff at US Deutsche Telekom subsidiary T-Mobile USA, H Security reported January 17. To back up their claim, the hackers posted data to the Pastebin anonymous text hosting service. One member of the group told Softpedia the hack involved exploiting SQL injection vulnerabilities on the t-mobile.com and newsroom.t-mobile.com Web sites. According to T-Mobile, the problem was limited to the T-Mobile USA newsroom. This would limit the scale of any problems arising as a result — the intruders may be able to publish fake press releases. Based on the information provided, private customer data was never at risk. Most of the passwords consist of a simple six-digit number composed of two numbers repeated such as "112112." T-Mobile USA said it has now fixed the vulnerabilities. Source: <http://www.h-online.com/security/news/item/T-Mobile-USA-hacked-1414307.html>

CRITICAL MANUFACTURING

NHTSA Safety Recall - Kia Optima and Kia Rondo. Kia Motors America, Inc., announced the recall January 20 of 145,755 model year 2006-2008 Kia Optima and model year 2007 and 2008 Kia Rondo vehicles. The clock spring contact assembly for the driver's side air bag supplemental restraint system (SRS) may become damaged through usage over time. If the clock spring contact assembly becomes damaged, the driver's side air bag electrical circuit will experience a high resistance condition potentially causing the driver's air bag to not deploy. If the clock spring develops high resistance, in the event of a crash, the driver's air bag will not deploy and will not be able to properly protect the driver, increasing the risk of injuries. Kia will notify owners, and dealers will replace the vehicle's air bag clock spring contact assembly as necessary. The safety recall is expected to begin during March. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V014000&summary=true&prod_id=288668&PrintVersion=YES

Thousands of Minis and Mini Coopers recalled. BMW announced January 16 the recall of nearly 89,000 of its Mini and Mini Cooper cars in the United States, and more than 235,000 worldwide. The company said a water pump that cools the turbocharger in some models has a circuit board that can malfunction and overheat. "In an extreme case, this overheating can lead

UNCLASSIFIED

UNCLASSIFIED

to a smoldering of the water pump and eventually can create a vehicle fire,” according to a BMW spokeswoman. She said about 12 fires have been reported to the National Highway Transportation Safety Administration, though none have resulted in accidents or injuries. The fires started when the vehicles were standing still. The recalled models include: 2007-11 Mini Cooper S; 2008-11 Mini Cooper Clubman; 2009-11 Mini Cooper S Convertible; 2009-11 Mini JCW; 2009-11 Mini JCW Clubman; 2009-11 Mini JCW Convertible; and the 2011 Mini Cooper S Countryman. Source: http://www.cbsnews.com/8301-500395_162-57359874/thousands-of-minis-and-mini-coopers-recalled/

DEFENSE/ INDUSTRY BASE SECTOR

F-22 Raptor pilots suffer more apparent oxygen problems. ABC News reported January 13, pilots for the F-22 fighter plane reported several new instances of experiencing “hypoxia-like” symptoms while at the controls the jet, the U.S. Air Force (USAF) said, an apparently rare but potentially deadly oxygen problem that has stumped the military for the last 4 years. From 2008 to 2011, pilots for the jet reported at least 12 incidents of experiencing the “hypoxia-like” symptoms, prompting the full fleet of F-22s to be grounded in May. After an intense, nearly 5-month investigation, the USAF said it could not figure out what could be making the pilots feel the effects of hypoxia and cautiously sent the pilots back into the skies in October. However, the USAF told ABC News the problem persists — in the 6,000 sorties flown since the grounding, pilots reported another eight instances of suffering “hypoxia-like symptoms.” In each of the new cases, the pilot followed proper procedures, returned to base and landed “without incident,” the USAF said. “The Air Force has not yet identified a root cause or a single mechanical deficiency, but through a range of both engineering and physiological actions we can mitigate the risk; this includes rigorous inspections, enhanced safety procedures, new training on life support systems, improved physiological monitoring, and continued data collection,” a USAF spokesperson said in a statement to ABC News. Source: <http://abcnews.go.com/Blotter/22-raptors-suffer-apparent-oxygen-problems/story?id=15357696#.Txbt3IHpjXN>

F-35C tailhook design blamed for landing issues. Lockheed Martin traced the U.S. Navy F-35C Joint Strike Fighter’s troubles with catching a carrier’s arresting gear wires to the tailhook design, Defense News reported January 17. Efforts to fix the problem are well underway, a top company official said. The rest of the design of the tailhook system, which include the doors and bay that conceal the device and other ancillary hardware, is sound, the Lockheed program manager for the F-35 program said. A preliminary review has already been completed and was done in conjunction with the Naval Air Systems Command and F-35 Joint Program Office. The program manager said the hook system is already being modified in accordance with the new test data. Tests with the newly modified tailhook should start at Lakehurst, New Jersey, in the second quarter of 2012, he said. That will give the F-35 program another set of data to study to make sure the new design works as promised. However, until those tests are done, there is no ironclad guarantee the redesign of the tailhook will work, but the program manager said he is confident the modified design will be successful. Source:

UNCLASSIFIED

UNCLASSIFIED

<http://www.defensenews.com/article/20120117/DEFREG02/301170010/F-35C-Tailhook-Design-Blamed-Landing-Issues?odyssey=tab|topnews|img|FRONTPAGE>

EMERGENCY SERVICES

FBI: Nationwide trend of ‘swatting’ both dangerous and costly. The FBI has grown increasingly concerned about the number of prank calls to police that warrant mobilizing SWAT teams to respond to hostage situations, which pose a very real threat to citizens and law enforcement officers, Examiner.com reported January 18. On average, each prank call cost \$10,000 in resources. The FBI coined the term “swatting” to describe the phenomenon. The latest incident which took place in early January in a Georgia town, demonstrates the serious risks posed to law enforcement officers and communities. Cyber criminals are using modified telephone caller identification that allows them to mask their identities while reporting hostage situations or bomb incidents with the purpose of getting SWAT forces deployed on innocent victims, either for revenge or for bragging rights. Advanced technology allows swatters to appear as though they are calling 911 from the home phone number of their targets while reporting a gruesome murder or a home intrusion. State and local law enforcement agencies around the country are working together with the FBI and telecommunications providers to address swatting incidents. Source: <http://www.examiner.com/homeland-security-in-chicago/fbi-nationwide-trend-of-swatting-both-dangerous-and-costly>

(Indiana) Police gear taken from undercover officer’s car. Police are looking for suspects in the theft of several items from an undercover Indianapolis police officer’s vehicle. The thefts happened January 12. The officer said he had stopped at a coffee shop and parked the undercover police car next to the building, WRTV 6 Indianapolis reported. The officer was inside for just a few minutes and found the back window of the car broken when he returned, police said. The officer’s .40-caliber police-issued handgun and three loaded magazines were taken, along with his personal 9mm Taurus handgun, a protective vest, handcuffs, two badges, and other equipment. Source: <http://www.theindychannel.com/news/30206156/detail.html>

(Maryland) State Police arrest six members of Occupy Baltimore. Maryland State Police arrested six members of Occupy Baltimore January 16 for allegedly trespassing on the state-owned site of a proposed juvenile detention center in East Baltimore. The arrests of four men and two women came about 2 hours after they began erecting a plywood structure — painted red and representing a schoolhouse — inside the fenced site at East Madison and Graves streets near the city’s complex of jails and prisons. A state police spokesman said the six individuals were told they were entering private property, which is owned by the Maryland Department of Public Safety and Correctional Services. Several troopers stationed inside the site tried to negotiate with the protesters building the structure, encouraging them to leave, he said. The six individuals had erected four walls and six roof trusses before they were arrested. They were being processed at central booking and each was charged with trespassing, the spokesman said. He stated troopers were securing the area January 16 when members of Occupy Baltimore pulled up and started moving materials over the chain link fence. Source:

UNCLASSIFIED

UNCLASSIFIED

http://articles.baltimoresun.com/2012-01-16/news/bs-md-ci-occupy-school-20120116-13_1_juvenile-detention-center-chain-link-fence-arrest

ENERGY

(U.S. Virgin Islands) Major oil refinery to close in US Virgin Islands. One of the world's largest oil refineries in the U.S. Virgin Islands will close next month, the company announced January 18. Industry analysts said the closure is unlikely to have a major effect on the global oil market. Losses at Hovensa, a joint venture of U.S.-based Hess Corp. and Venezuela's state-owned oil company, have totaled \$1.3 billion over the past 3 years and were projected to continue due to reduced demand caused by the global economic slowdown, and increased refining capacity in emerging markets. Hovensa was the third largest U.S. refinery before it cuts its capacity of 500,000 barrels by 30 percent last year. It is now the eighth largest, according to the U.S. Energy Information Administration. Source: <http://abcnews.go.com/Business/wireStory/major-oil-refinery-close-us-virgin-islands-15385253#.TxhlpYHLIBk>

SCADA-Logical: DoS Vulnerabilities In Rockwell Automation FactoryTalk Disclosed: Researcher Luigi Auriemma has uncovered multiple denial of service (DoS) vulnerabilities in Rockwell Automation's FactoryTalk supervisory control and data acquisition (SCADA) product, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) announced. The vulnerabilities are exploitable by sending specially crafted packets to the server, which can result in a DoS attack, according to an ICS-CERT advisory. [HSEC-1.1; Date: 18 January 2012; Source: <http://www.infosecurity-magazine.com/view/23317/>]

FOOD AND AGRICULTURE

USDA announces \$308 million in aid to states. The nation's top agriculture official announced January 18 that more than \$300 million in emergency assistance was awarded to 33 states and Puerto Rico to help them recover from an unusually intense year for natural disasters across the United States. Utah and Missouri will receive the most disaster aid, together taking in \$109 million, or more than one-third of the \$308 million in aid from Department of Agriculture (USDA) watershed and conservation emergency funds, the USDA Secretary said. Flooding last spring in Utah inundated thousands of acres of farmland, costing farmers tens of millions of dollars lost to damaged and destroyed crops or delayed planting. Utah will receive \$60 million in watershed money for repair work and preventative measures, said the state conservation engineer for the U.S. Natural Resources Conservation Service. Missouri suffered months of flooding along the Missouri River after the U.S. Army Corps of Engineers authorized unprecedented releases from reservoirs in the northern river basin all summer to deal with unexpectedly heavy rain in May and above-average mountain snow-pack. Missouri will receive around \$49 million, of which \$35 million will come from the watershed program, and the rest from the Farm Service Agency's Emergency Conservation Program. Source: <http://online.wsj.com/article/AP78a8805aa36b40eab19b4d873702b121.html>

UNCLASSIFIED

UNCLASSIFIED

Allergen alert: Soy in sunflower seeds. Ryt-way Industries is recalling select sunflower seeds because they may contain soy ingredients that were not declared on the packaging, Food Safety News reported January 18. The recall is of BIGS Dill Pickle Sunflower Seeds. The sunflower seeds were distributed nationwide in supermarkets, convenience stores, and U.S. military commissaries. Source: <http://www.foodsafetynews.com/2012/01/allergen-alert-soy-in-sunflower-seeds/>

(Washington) Washington state dairy recalls raw milk. Frisia Dairy and Creamery of Tenino, Washington, is recalling its raw milk because it may be contaminated with a dangerous strain of E. coli, according to a January 17 news release issued by the Washington State Department of Agriculture (WSDA) at the dairy's request. The recall, which covers all expiration dates, was voluntarily initiated by the dairy after the department's routine monthly sampling discovered toxin-producing E. coli in a skim milk sample. The unpasteurized fluid milk products, including whole, skim, and cream, were distributed through on-farm sales and at eight retail outlets in Lewis, Thurston, and Pierce counties. Frisia and the department are continuing their investigation into the source of the problem. The department's news release said E. coli was not found in other samples collected at the same time, nor was it found in previous routine monthly samples. Source: <http://www.foodsafetynews.com/2012/01/washington-state-dairy-recalls-raw-milk/>

New animal virus takes northern Europe by surprise. Scientists in northern Europe are scrambling to learn more about a new virus that causes fetal malformations and stillbirths in cattle, sheep, and goats, Wired reported January 13. For now, scientists do not know about the virus' origins or why it is suddenly causing an outbreak; in order to speed up the process, they want to share the virus and protocols for detecting it with anyone interested in studying the disease or developing diagnostic tools and vaccines. The virus, provisionally named "Schmallenberg virus" after the German town from which the first positive samples came, was detected in November 2011 in dairy cows that showed signs of infection with fever and a drastic reduction in milk production. Now, the virus has also been detected in sheep and goats, and it has shown up at dozens of farms in the Netherlands, and in Belgium. According to the European Commission's Standing Committee on the Food Chain and Animal Health, cases have been detected on 20 farms in Germany, 52 in the Netherlands, and 14 in Belgium. Many more suspected cases are being investigated. Source: <http://www.wired.com/wiredscience/2012/01/new-animal-virus/>

(Illinois) 146 norovirus cases linked to Illinois restaurant. Many of 146 people sickened with norovirus in Wheeling, Illinois, may have been exposed at Bob Chinn's Crab House, the Cook County Health Department said January 13. Bob Chinn's, which bills itself as the nation's fourth busiest restaurant, closed its doors January 10, after receiving complaints from customers who said they had become sick, and then reopened January 11. "We worked with the [Cook County Department of] Public Health to clean and sanitize the restaurant," said a restaurant spokesman. "We've satisfied all of the requirements, and they've allowed us to reopen." A health department spokeswoman said her agency received dozens of calls from people who said they became sick after eating at the restaurant, but that it is unclear whether the eatery is

UNCLASSIFIED

UNCLASSIFIED

the source of illness in all of those cases. Source:

<http://www.foodsafetynews.com/2012/01/146-norovirus-cases-linked-to-illinois-restaurant/>

Allergen alert: Stuffed clams with milk, wheat, eggs. Price Chopper Supermarkets is recalling stuffed clams from its seafood departments because three ingredients — milk, wheat, and eggs — are allergens and are not listed on the label, Food Safety News reported January 14. The recall is for Gourmet Stuffed Clams, sold chain-wide in Price Chopper seafood departments between September 30 and December 30, 2011. According to the company's news release, the store-generated label was updated December 30, 2011 to correctly reflect all of the ingredients contained in the product. The news release did not explain whether the recalled clams would still be available in stores. Source: <http://www.foodsafetynews.com/2012/01/allergen-alert-stuffed-clams-with-milk-wheat-eggs/>

Allergen alert: Barbecue sauce with anchovies. Herbadashery of Casper, Wyoming, is recalling certain bottles of barbecue dipping sauce because the labels do not specify that the sauce contains anchovies, an allergen, Food Safety News reported January 14. The recall was initiated after an onsite U.S. Food and Drug Administration inspection November 23, found one ingredient, Worcestershire sauce, included anchovies. The recall is for Pine Ridge BBQ and Dipping Sauce, and Pine Ridge Jalapeno BBQ and Dipping Sauce manufactured after January 1, 2011, and distributed through Internet sales and in retail stores from January 1 to September 1. Source: <http://www.foodsafetynews.com/2012/01/allergen-alert-barbecue-sauce-with-anchovies/>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Missouri) School bus thefts mystify police in Jefferson and St. Louis counties. At least one full-size regulation school bus has disappeared each month since September — plus one in May — from five locations in south St. Louis County or Jefferson County, Missouri. “It’s not your usual stolen vehicle,” said a sergeant with the St. Louis County police auto crime unit. “Most vehicles come up recovered, and not having these school buses surface anywhere is unusual too.” The FBI was notified. Officials said that new, each bus is worth about \$60,000. Exactly when these were stolen is hard to pinpoint because they went missing on weekends or when school was otherwise not in session. The most recent theft is so far the only one at least partially caught on video. In that case, Jefferson County deputies believe the thieves used bolt cutters to sever chains securing the gates and then fastened them again with new padlocks. Source: http://www.stltoday.com/news/local/crime-and-courts/series-of-school-bus-thefts-mystifies-police-in-jefferson-st/article_49fd3268-f123-54e8-95c3-c01b3a69a749.html

(District of Columbia) Man accused of shooting at White House charged in 17-count indictment. An Idaho man accused of firing a rifle at the White House faces 17 charges, including attempting to assassinate the U.S. President, after being formally indicted by a grand jury in Washington, D.C. January 17. The indictment against the suspect includes new charges

UNCLASSIFIED

UNCLASSIFIED

such as assaulting officers of the U.S. government with a deadly weapon, injury to U.S. property, namely the White House, use of a firearm during a crime of violence, and assault with a dangerous weapon. The man allegedly fired a rifle at the White House November 11 and then fled. The indictment says the suspect “did forcibly assault, intimidate, and interfere” with three Secret Service employees by firing at the White House. Several rounds hit the exterior of the White House near the second story residence area for the first family. The suspect was arrested 5 days later in Pennsylvania, and has been jailed ever since. Source:

<http://www.cnn.com/2012/01/17/justice/white-house-shooting/index.html>

(District of Columbia) ‘Occupy’ protesters suspected of throwing smoke bomb over White House fence. An apparent smoke bomb was thrown over the fence of the White House in Washington, D.C., as hundreds of Occupy protesters massed outside the gates. The crowds were dispersed January 17, and the White House was all clear. A U.S. Secret Service spokesman said there were no arrests. The U.S. President and First Lady were not home at the time of the incident. The scene outside the White House followed an earlier protest on the West Lawn of the Capitol, in which several hundred protesters affiliated with the Occupy Wall Street movement decried the influence of corporate money in politics and voiced myriad other grievances. Organizers touted the rally, known as Occupy Congress, as the largest national gathering of Occupy protesters to date, and secured a permit that would have allowed up to 10,000 people to participate. While the rally was mostly peaceful, there were some scuffles between police and protesters. U.S. Capitol Police said four people were arrested, one for allegedly assaulting a police officer, and three accused of crossing a police line. Source: <http://www.foxnews.com/politics/2012/01/17/occupy-protesters-suspected-throwing-smoke-bomb-over-white-house-fence/?test=latestnews>

(Florida) Suspicious package found at St. Lucie County Clerk of Courts office. State health officials investigated a package that forced the evacuation of a building in Fort Pierce, Florida, January 13. The clerk of courts office was on lockdown for a few hours when a suspicious package was discovered. Sheriff’s officials, fire-rescue, and haz-mat crews were called to the scene. The package was delivered to the fourth floor of the clerk of courts office. Three St. Lucie County deputies, and five clerk of courts employees were taken to the hospital as a precaution. Source: <http://www.cbs12.com/articles/pierce-4738061-courts-office.html>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Koobface C&C goes silent after alleged controllers exposed. The Koobface network is apparently down, according to Facebook. A Facebook security official told Reuters the company’s decision to expose the five men alleged to be behind the malware had an effect within 24 hours: “The thing that we are most excited about is that the botnet is down.” On January 18, Facebook decided to publish the names of alleged gang members based on details of research carried out in 2009-2010 by two German researchers. One of the researchers works for Security company Sophos. A Sophos researcher told H Security the command and control servers are not down, they just have not sent out any new commands since 08:40 GMT January 17. “Now they just reply with 404 errors” he said. He did note though the five men identified by

UNCLASSIFIED

UNCLASSIFIED

the investigation “appear to have been busy deleting their social networking accounts.” Source: <http://www.h-online.com/security/news/item/Koobface-C-C-goes-silent-after-alleged-controllers-exposed-1416869.html>

Cisco security response: Wi-Fi protected setup PIN brute force vulnerability. On December 27, the U.S. Computer Emergency Readiness Team released Vulnerability Note #723755, describing a vulnerability that exists in the Wi-Fi Alliance Wi-Fi Protected Setup (WPS) protocol, also known as Wi-Fi Simple Config, when devices are operating in PIN External Registrar (PIN-ER) mode. Devices operating in PIN-ER mode allow a WPS capable client to supply only the correct WPS PIN to configure their client on a properly secured network. A weakness in the protocol affects all devices that operate in the PIN-ER mode, and may allow an unauthenticated, remote attacker to brute force the WPS configuration PIN in a short amount of time. Now, Cisco announced exploit code and functional attack tools that exploit the weakness within the WPS protocol have been released. The vulnerability is due to a flaw that allows an attacker to determine when the first 4-digits of the 8-digit PIN are known. The eighth digit of the PIN is utilized as a checksum of the first 7 digits and does not contribute to the available PIN space. Because the PIN space has been significantly reduced, an attacker could brute force the WPS pin in as little as a few hours. While the affected devices implement the WPS 1.0 standard that requires that a 60-second lockout be implemented after three unsuccessful attempts to authenticate to the device, this does not substantially mitigate this issue as it only increases the time to exploit the protocol weakness from a few hours to at most several days. It is Cisco’s recommendation to disable the WPS feature to prevent exploitation of this vulnerability. Source: <https://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20120111-wps>

Facebook ‘free mobile recharge’ scam hijacks accounts. A phishing and survey scam rolled into one is currently targeting Facebook users and ends up hijacking their accounts and makes it difficult for users to get them back, warns a McAfee researcher. The victims are lured with messages seemingly posted by friends claiming they received a “100rs free recharge.” Following the offered link, users connect to a page asking them to enter Facebook log-in credentials to receive it. Once the account details are entered and the “Log In” button is pressed, the page redirects users to a page mimicking a Facebook one, which asks the user to complete a survey to unlock the recharge option. In the background, the page sends the recorded log-in credentials — in clear text via a HTTP POST request — to a remote server operated by the scammers. The scammers then use the credentials to access the victims’ Facebook accounts, change information contained in them (including the password and the e-mail address), and post the same message that lured in the victims in the first place. The affected users are unable to immediately do anything about it. “Even if the victims try to reset their passwords, they will never get the password reset email from Facebook,” said the researcher. Source: <http://www.net-security.org/secworld.php?id=12234>

Popular live-blogging site says data files were breached. CoveritLive, a popular, Web-based live-blogging program used worldwide, said January 13 it discovered “certain proprietary data files” of its users “were accessed without authorization,” but “no financial account information

UNCLASSIFIED

UNCLASSIFIED

has been compromised. We have not yet determined if, or to what extent, CoveritLive account information (i.e., user names, email addresses and/or passwords) was accessed,” Demand Media, which bought CoveritLive in 2011, said in an e-mail to its users. Those users include bloggers, journalists, and mainstream media organizations, including msnbc.com, FoxNews.com, ESPN, and the BBC. Many people use CoveritLive’s free services, but there are premium accounts. Live-blogged events hosted by CoveritLive draw more than 60 million people every month, the company says, 60 percent of whom are from outside the United States. CoveritLive said the files were breached “starting on or about” January 7, and an investigation is “ongoing.” In the meantime, as a “precautionary measure,” all users were asked to re-set their passwords January 14. Source:

<http://technolog.msnbc.msn.com/news/2012/01/13/10152434-popular-live-blogging-site-says-data-files-were-breached>

Facebook chat phishing attack impersonates Facebook security team. A new phishing attack spreading through Facebook chat modifies hijacked accounts to impersonate the social network’s security team. The attackers replace the profile picture of compromised accounts with the Facebook logo and change their names to a variation of “Facebook Security” written with special Unicode characters, said a Kaspersky Lab expert. Facebook claims changing the profile name can take up to 24 hours and is subject to confirmation. However, in the expert’s tests the change occurred almost instantly and required only the password. This was also confirmed by a victim whose profile name was modified within 5 minutes of their account being compromised, he said. After the victim’s profile name and picture get changed, the attackers send out a chat message to all of their contacts informing them their accounts will be suspended unless they re-confirm their information. The rogue messages appear to be signed by “The Facebook Team” and contain a link to a phishing page hosted on an external domain. The Web page mimics Facebook’s design and asks for name, e-mail, password, security question, country, birth date, and other information needed to hijack the account. However, the attack does not stop there. According to the expert, a second form asks users for their credit card details and billing address. This is unusual for Facebook phishing attacks, the majority of which target only social networking account information. Source:

http://www.computerworld.com/s/article/9223432/Facebook_chat_phishing_attack_impersonates_Facebook_security_team?taxonomyId=17

NATIONAL MONUMENTS AND ICONS

(Florida) Arson ruled out in fire that toppled ‘The Senator’ at Big Tree Park. Fire officials said arson is not to blame in a fire that toppled “The Senator,” one of the oldest cypress trees in the world, which was reduced to a stump January 16 at Big Tree Park in Seminole County, Florida. Investigators initially said arson was a possibility because a pile of twigs was found at the base of the tree, there had not been recent lightning strike, and no power lines are located nearby. The official cause is not yet known, and an investigation is ongoing. An arson investigator said the possible cause was a lightning strike from a few weeks ago. The tree, named after a Florida senator who in 1927 donated the property on which the landmark sits, was about 120 feet tall and its trunk had a diameter of nearly 18 feet. It was the main attraction in the park dedicated

UNCLASSIFIED

UNCLASSIFIED

in 1929. The tree had reached a height of 165 feet before a 1925 hurricane lopped off its top. Afterward, lightning rods were installed to protect the tree. More than a dozen firefighters were at the park when the fire occurred but hoses and water from a helicopter could not save the tree. Source: <http://www.clickorlando.com/news/Arson-ruled-out-in-fire-that-toppled-The-Senator-at-Big-Tree-Park/-/1637132/8136768/-/tp6dmc/-/>

POSTAL AND SHIPPING

(Pennsylvania) Police say man raided post office in pursuit of bath salt delivery. A man broke into a closed Clarks Summit, Pennsylvania post office January 16 looking for a package of designer drugs he thought would be there waiting for him, police said. Instead, the man made off with a U.S. Postal Service (USPS) hat and jacket, pieces of mail, a scale, and a coin-operated machine after he could not find the bath salts, even though a tracking of the package indicated it would be at the branch, police said. The man was charged with felony counts of burglary, theft, receiving stolen property, and a misdemeanor count of criminal trespass, after he was spotted driving erratically in a pickup truck. Police found in the truck several opened pieces of mail and the USPS jacket beside him on the front seat, arrest papers said. The man was arraigned January 16 and placed in the county prison in lieu of \$35,000 straight bail. Source: <http://thetimes-tribune.com/police-say-man-raided-post-office-in-pursuit-of-bath-salt-delivery-1.1258376#axzz1jiMMNog2>

PUBLIC HEALTH

Drug shortages raise risk of cancer counterfeits, U.S. says. Shortages of some injectable cancer drugs have created an opening for dangerous unapproved versions of Roche Holding AG's Herceptin and Amgen Inc.'s Neupogen to be sold to clinics and other health-care providers. The Food and Drug Administration (FDA) issued a notice January 13 warning providers to avoid direct solicitations from unproven sources and only buy drugs through approved channels. Unapproved versions of Roche's Rituxan and AstraZeneca Plc's Faslodex have also been sold. The quality of such products is often jeopardized, putting patients at risk, the agency said. Though some injectable cancer medications are in short supply, none of the unapproved products are on the shortage list. "Amgen is aware of and is cooperating with the FDA on investigations related to the illegal importation of Amgen product that is approved for sale in other regions, but unapproved for sale in the U.S. and being sold on the Internet and directly to U.S. clinics," a spokeswoman for the Thousand Oaks, California-based company said in an e-mail. Source: <http://www.businessweek.com/news/2012-01-15/drug-shortages-raise-risk-of-cancer-counterfeits-u-s-says.html>

FDA fingers. The Food and Drug Administration (DOT) said January 12 a preliminary investigation suggests "improper usage" of CardioGen-82 generators led to the increased patient radiation exposure that triggered last summer's product recall. In a safety announcement, the FDA said ongoing tests carried out by the nuclear medicine agent's manufacturer, Bracco Diagnostics Inc., have shown manufacturing "deficiencies" noted by the agency do not seem related to the heightened radiation exposure detected in some patients.

UNCLASSIFIED

UNCLASSIFIED

The CardioGen-82 generator was recalled in July, after three patients set off very sensitive radiation detectors at the U.S. border. It turned out the patients had all undergone PET stress tests using the substance several months earlier. The FDA said the problem that led to the recall, which was voluntarily ordered by Bracco, was likely caused by a “strontium breakthrough,” meaning radioactive strontium isotopes used to create the PET agent were inadvertently injected into the patients. “None of the tested generators showed signs of [strontium] breakthrough. FDA continues to work with the manufacturer to resolve their manufacturing deficiencies,” the agency said. Source:

<http://www.dotmed.com/news/story/17843/>

TRANSPORTATION

TSA adopts Coast Guard’s emergency notification system. The Transportation Security Administration (TSA) will begin using the U.S. Coast Guard’s (USCG) enterprisewide emergency mass notification system. Interagency cooperation is allowing TSA to integrate the infrastructure of the USCG Alert and Warning System (AWS). The system is designed to provide emergency alerts over multiple channels such as landlines, mobile and satellite phones, e-mail, text messages, and facsimile to units across the agency, AtHoc company officials said. The emergency notification system is based on AtHoc’s IWSAlerts software. The system will reach 50,000 TSA employees nationwide via a virtual private cloud. The notification will contact units at more than 100 ports and 45 airports, across TSA’s Transportation Threat Assessment and Credentialing network, and TSA facilities. The system’s enterprisewide architecture allows deployment in centralized data centers to support TSA facilities. A unified design methodology provides centralized alert activation, control and management from a Web-based console. The USCG has used AWS since 2007. It uses AWS 2.0 for emergency alerts; staff recall; personnel accountability; and disaster response to events. Source:

<http://gcn.com/articles/2012/01/18/tsa-coast-guard-emergency-alert-system.aspx>

(Illinois) Alleged railroad yard thief nabbed. The Cook County, Illinois Sheriff’s Office announced January 16 the arrest of a man who allegedly helped steal more than \$100,000 in property from a South Side Chicago railroad yard. One of three suspects in a January 11 theft at the Canadian National rail yard was arrested January 14, the sheriff’s office said in a release. Authorities learned January 11 about a possible theft where three people allegedly removed railroad ties and other scrap metal, the release said. The property was valued at about \$100,000. A witness positively identified a getaway vehicle used in the crime, the release said. On January 12, authorities found the suspect and his vehicle, presumably the getaway vehicle. He was charged with one count of felony theft and one count of criminal trespass to real property. Detectives were eventually able to recover some of the items stolen from the rail yard at local scrap yards, the release said. Source:

<http://abclocal.go.com/wls/story?section=news/local&id=8507977>

UNCLASSIFIED

WATER AND DAMS

(Pennsylvania) EPA to test water near Penn. fracking site. Regulators at the U.S. Environmental Protection Agency (EPA) said January 19 they will perform water tests at about 60 homes in Dimock, Pennsylvania where residents say natural gas drilling has polluted wells. The EPA also plans to truck water to four homes in the town where some households have relied on water deliveries since drilling by Cabot Oil & Gas Corp began 3 years ago, it said in a statement. The tests, which will begin in the coming days, are being carried out “to further assess whether any residents are being exposed to hazardous substances that cause health concerns,” the agency said. The announcement represents a reversal for the EPA, which 6 weeks ago declared the water in the 1,400-person town safe to drink before receiving more data provided by residents. It is also the clearest sign yet regulators are concerned about the effect of drilling on drinking water there. A Cabot spokesman said the company has tested and sampled water from more than 2,000 wells in the area over the past several years and does not have data showing drilling is the cause of “alleged health concerns purported by the EPA.” Dimock residents began complaining of cloudy, foul-smelling water in 2008 after Cabot began fracking nearby. The company trucked water to a dozen Dimock households for 3 years until November when state regulators agreed it could stop. Since then, residents have relied on water deliveries arranged by environmental groups including Water Defense and Sierra Club, though the sporadic deliveries have barely been enough. Some have been using pond water for showers. Source: <http://www.reuters.com/article/2012/01/20/us-usa-fracking-pennsylvania-idUSTRE80I29A20120120>

Three area towns to receive \$350,000 infrastructure grants. Three Bureau County communities will each receive \$350,000 in federal grant funds for infrastructure improvements, the governor of Illinois said January 18. Receiving the grants are Neponset, for water treatment plant improvements; Sheffield, to install new water mains and replace two failing lift stations; and Wyanet, for sewer system improvements. The governor announced nearly \$19 million in federal funding to address the infrastructure needs of 59 small and rural communities. Awarded through the Community Development Assistance Program, the funding will be used to make improvements to water and sewer lines, including replacing water mains, and upgrading stormwater systems. Source: <http://www.starcourier.com/news/x3506992/Three-area-towns-to-receive-350-000-infrastructure-grants>

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.

UNCLASSIFIED

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