

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**

### **International task force established to help form management plan for Souris River next year.**

An international task force was been formed December 8 to help develop a plan for management of the Souris River in 2012. The basin experienced record flooding earlier this year due to heavy spring snowmelt and rain, flooding that affected more than 4,000 homes and businesses in Minot, North Dakota. The task force will have state, federal, and Canadian provincial officials. It was set up during a meeting December 8 in St. Paul, Minnesota, that included representatives of the U.S. Army Corps of Engineers, U.S. Fish and Wildlife Service, Saskatchewan Watershed Authority, North Dakota Water Commission, the North Dakota congressional delegation, and the governor of North Dakota. Source:

<http://www.therepublic.com/view/story/4b9c0e36fc3c4f72a38e1c12bba158bf/ND--ND-Flooding-Souris-River/>

## **REGIONAL**

**(Montana) Lockwood Irrigation District repairs river dike.** Repair work on a Yellowstone River dike that serves the Lockwood Irrigation District in Montana is nearing completion, the manager of the irrigation district said December 13. The half-mile-long dike was heavily damaged by flooding last spring. The repair project started July 27, and December 12 trucks dumped their 400th load of sandstone. The work cost \$170,000 so far, of which the Federal Emergency Management Agency (FEMA) has paid \$35,000. The district is applying for additional financial help from FEMA. The dike funnels Yellowstone River water into the district's pumping station, ensuring a steady supply of water when the river is low. The Lockwood Water and Sewer District also uses that water supply when needed, the manager said. Source:

[http://billingsgazette.com/news/local/lockwood-irrigation-district-repairs-river-dike/article\\_ec2e9d44-14e0-5612-9d35-d50f07571093.html?oCampaign=hottopics](http://billingsgazette.com/news/local/lockwood-irrigation-district-repairs-river-dike/article_ec2e9d44-14e0-5612-9d35-d50f07571093.html?oCampaign=hottopics)

**(Montana) Contamination scare leaves Eureka without water for days.** Eureka, Montana residents were asked not to use any water for fear of contamination December 9 after people were seen on top of the town water tank. A person living nearby saw people on top of the tank December 5 and called authorities. The tank was immediately shut off for fear of spreading contaminated water to Eureka residents. To prevent sickness, the town was instructed to not use any water. The water was tested twice and by December 8, the results showed the water was safe. City officials held a meeting December 9 to decide whether or not to pursue those who may have caused the disruption of service. Source:

<http://www.ktvq.com/news/contamination-scare-leaves-eureka-without-water-for-days/>

## **NATIONAL**

**(Midwest) Corps shy of Missouri River levee-repair money.** The U.S. Army Corps of Engineers currently has only enough money available to fix 11 of 68 Missouri River levees, and is draining extra water from upstream reservoirs to nurse the flood-battered system through 2012. Officials made the announcement December 12 during a meeting of the Missouri River Flood

## UNCLASSIFIED

Task Force in suburban Kansas City. The damaged levees are located in Missouri, Nebraska, Iowa, and Kansas. The Corps said the \$68 million available is sufficient only to help pay for the most crucial projects. The goal is to fix those levees at least enough to protect against a 25-year flood, although many previously provided 100-year flood protection. The Corps said it would cost \$253 million to make all the repairs needed in the Missouri River Basin. Source:

<http://www.kcautv.com/story/16309021/corps-shy-of-missouri-river-levee-repair-money>

### **INTERNATIONAL**

**Parcel bomb intercepted at public office in Rome.** Authorities intercepted a parcel bomb December 15 at a branch of Italy's tax-collecting organization Equitalia, almost a week after another parcel bomb exploded at a separate branch in Rome. The device was handed over to police for further investigation, the ANSA news agency reported. Experts examining the package had found a "dark powder inside [the parcel]," a police spokesman told Agence France-Press. The parcel bomb discovery follows two recent similar incidents, one at another Equitalia branch in Rome. The Italian far-left group Federazione Anarchia Informale (Informal Anarchist Federation), also known as FAI, claimed responsibility for sending a bubble-wrapped parcel bomb to an Equitalia branch December 9. The director who opened the parcel bomb suffered burns to his right hand. The group also claimed responsibility for sending a parcel bomb addressed to the CEO of Deutsche Bank in Frankfurt on December 7. That bomb was intercepted by authorities, who confirmed it contained explosives and shrapnel. In claiming responsibility for the Frankfurt attack, the FAI said it would target "banks, bankers, ticks and bloodsuckers" with three attacks. Source: [http://www.myfoxphoenix.com/dpps/news/parcel-bomb-intercepted-at-public-office-in-rome-dpgonc-20111215-fc\\_16395158](http://www.myfoxphoenix.com/dpps/news/parcel-bomb-intercepted-at-public-office-in-rome-dpgonc-20111215-fc_16395158)

**Slovaks hold 7 suspected of radioactive sale plan.** Slovak police said December 15 that they have arrested seven men suspected of planning to sell an unspecified radioactive material. A police chief said the material originated in a former Soviet country, has an estimated value of \$649,650, and had not yet been transported to Slovakia. Six suspects are Slovak nationals and one is a Czech. Slovak and Czech police, who have followed the group since 2009, cooperated in the arrests. The Slovak police chief declined to give more details, including what the material was and who may want to buy it. The suspects face up to 10 years in prison if convicted of illegal trade with radioactive materials. Source: <http://www.google.com/hostednews/ap/article/ALegM5gTxVaQmRfbvXEaVabrRVIWNB0bOw?docId=07b9548d3e9b4eeebb6e500bc880f2c3>

**Swiss charge 3 men in nuclear smuggling case.** Three Swiss engineers were charged with breaking arms export laws by aiding a Pakistani-led nuclear smuggling ring that supplied Libya's atomic weapons program, Swiss prosecutors said December 13. The formal indictment followed almost a decade of politically charged investigation. The three engineers are suspected of providing technology and know-how to the nuclear smuggling network of a well-known Pakistani scientist who was the architect of Pakistan's nuclear weapons program, the federal prosecutors office in Bern said in a statement. An unidentified fourth defendant will be charged in separate legal proceedings with breaking Swiss arms exports laws, prosecutors said. Source:

UNCLASSIFIED

## UNCLASSIFIED

[http://www.google.com/hostednews/ap/article/ALeqM5jf6wSjVK\\_6bzo44cg5hga90cdqtA?docId=ae93c8602aa144d7bc230184edde0a69](http://www.google.com/hostednews/ap/article/ALeqM5jf6wSjVK_6bzo44cg5hga90cdqtA?docId=ae93c8602aa144d7bc230184edde0a69)

### **BANKING AND FINANCE INDUSTRY**

**Hackers feast on unencrypted credit card data stored by merchants.** A report released by Security Metrics December 15 states the number of merchants that store customer credit card data in an unencrypted form is higher than ever. The latest Merchant Data Security Report reveals that 71 percent of the businesses that participated in the study stored unencrypted credit card data, and many were highly vulnerable to SQL injection attacks. With the use of a tool called PANscan, Security Metrics scanned the systems of 2,736 merchants, including hard drives, networks, and attached storage devices in search of unencrypted primary account numbers (PAN) and magnetic stripe track data. The scan found a total of 378,748,700 cards, which translates into an 8 percent increase when compared to 2010. Old, non-PCI compliant, payment applications are problematic and easy to hack, but new payment systems can turn out to be just as insecure if they are not configured correctly. Other problems emerge from the improper removal of payment-information-containing files. Many believe if they delete a file, it is as good as gone, but this is not the case. Even if the information is not available for the user, hackers can easily recover it from the device's unassigned storage space. While a large part of the sensitive data is stored unknowingly by employees who are just not trained to handle sensitive data, in many situations merchants do not bother to make sure the data is safely tucked away from malicious cybercriminal operations. Source:

<http://news.softpedia.com/news/Hackers-Feast-on-Unencrypted-Credit-Card-Data-Stored-by-Merchants-240850.shtml>

**Phishing targets FDIC.** The Federal Deposit Insurance Corporation (FDIC) is warning banks about another strand of phishing attacks feigning to come from the FDIC, Bank Info Security reported December 9. In an e-mail alert, the FDIC warned that the e-mails appear to be coming from "insurance@fdic.gov", "subscriptions@fdic.gov", "alert@fdic.gov", and "accounts@fdic.gov." The fraudulent e-mails include the subject lines "FDIC: Your business account", "FDIC: About your business account", "Insurance coverage of your business account", or other similar variations. The e-mails also include a malicious link that claims to offer critical information about financial institutions. The claim states: "We have important news regarding your bank. This includes information on the acquiring bank (if applicable), how your accounts and loans are affected, and how vendors can file claims against the receivership." The FDIC said recipients of the e-mails should be mindful of any electronic correspondence that appears to come from the FDIC, and reiterated that it does not issue unsolicited e-mails to consumers or business account holders. Source: [http://www.bankinfosecurity.com/articles.php?art\\_id=4318](http://www.bankinfosecurity.com/articles.php?art_id=4318)

**Three Bulgarians arrested in connection with phishing scheme against US banks.** Bulgarian authorities arrested three men December 7 on charges of being part of an international cybercriminal gang that targeted U.S. bank customers. The men were detained last week in Sofia and Burgas following a joint investigation by the computer crime division of the Bulgarian Chief Directorate for Combating Organized Crime and the FBI. The gang sent phishing e-mails

UNCLASSIFIED

## UNCLASSIFIED

that appeared to originate from major U.S. banks and directed recipients to fake online banking Web sites with the purpose of stealing user names and passwords, the Bulgarian Interior Ministry said in a statement. The men allegedly used the stolen information to transfer money from bank accounts belonging to victims. Investigators said the three suspects used online payment services such as libertyreserve.com, paypal.com, webmoney.ru, moneybookers.com, and others. During raids at the three men's homes police officers seized mobile phones, computer systems containing hacking programs, laptops, storage media devices, receipts of numerous money transactions, as well as stolen online banking credentials. Source: [http://www.pcworld.com/businesscenter/article/246022/three\\_bulgarians\\_arrested\\_in\\_connection\\_with\\_phishing\\_scheme\\_against\\_us\\_banks.html](http://www.pcworld.com/businesscenter/article/246022/three_bulgarians_arrested_in_connection_with_phishing_scheme_against_us_banks.html)

**SEC probes major companies' Syria, Iran ties.** The Securities and Exchange Commission (SEC) has asked at least a dozen U.S.-listed companies to fully explain their business relations — which were apparently undisclosed in some cases — with Iran and Syria, the Financial Times (FT) reported December 11. Among the companies being asked to provide the information are global giants including Sony, Caterpillar, and American Express. The article says the companies have conducted business with the countries, listed as “state sponsors” of terrorism by the U.S. government and heavily sanctioned as a result, in many cases by going through international subsidiaries which operate outside the confines of U.S. sanctions. As global outrage rises in light of the Syrian regime's crackdown on opposition protests, and an Iranian student siege on the British Embassy in Tehran, some U.S. lawmakers have pushed for the subsidiary loophole to be closed, according to the FT. “The notion that a foreign subsidiary of a U.S. company can conduct business that would be sanctionable in the US ... undermines our efforts to prevent Iran from achieving a nuclear-weapons capability,” the ranking Democrat on the House foreign affairs committee, told the FT. Source: [http://www.cbsnews.com/8301-503543\\_162-57341135-503543/sec-probes-major-companies-syria-iran-ties/](http://www.cbsnews.com/8301-503543_162-57341135-503543/sec-probes-major-companies-syria-iran-ties/)

## **CHEMICAL AND HAZARDOUS MATERIALS SECTOR**

**(Colorado) Colorado approves disclosure of fracking chemicals.** Colorado will require energy companies to disclose the concentrations of all chemicals in hydraulic fracturing and also ask drillers to make public some information about ingredients considered trade secrets after new rules were approved December 13. Colorado regulators unanimously approved the new rules, which take effect in April. The guidelines are similar to those required by a first-in-the-nation law passed in Texas this year, but go further by requiring the concentrations of chemicals to be disclosed. Also, if Colorado drillers claim a trade secret, they would still have to disclose the ingredient's chemical family. In emergencies, companies would have to tell health care workers what those secret ingredients were. Source: <http://www.google.com/hostednews/ap/article/ALeqM5g9ORd4ntZGYIkAZQADqLWypXF9tg?dclid=155fc21d4ccf4a04bac0aeea04889754>

**(Texas) Texas drillers must disclose fracking chemicals.** Oil and natural gas drillers in Texas will be required to report the chemicals they use in hydraulic fracturing effective February 1. The Texas Railroad Commission approved the new rule December 13 and said companies will also

UNCLASSIFIED

## UNCLASSIFIED

be required to disclose the amount of water they use. Drillers will be required to report all information to the public Web site FracFocus.org. However, if a chemical is deemed a trade secret it does not have to be listed, unless the Texas attorney general or a court determines otherwise. Source: [http://www.bizjournals.com/houston/morning\\_call/2011/12/texas-drillers-must-disclose-chemicals.html](http://www.bizjournals.com/houston/morning_call/2011/12/texas-drillers-must-disclose-chemicals.html)

### **International task force established to help form management plan for Souris River next year.**

An international task force was been formed December 8 to help develop a plan for management of the Souris River in 2012. The basin experienced record flooding earlier this year due to heavy spring snowmelt and rain, flooding that affected more than 4,000 homes and businesses in Minot, North Dakota. The task force will have state, federal, and Canadian provincial officials. It was set up during a meeting December 8 in St. Paul, Minnesota, that included representatives of the U.S. Army Corps of Engineers, U.S. Fish and Wildlife Service, Saskatchewan Watershed Authority, North Dakota Water Commission, the North Dakota congressional delegation, and the governor of North Dakota. Source:

<http://www.therepublic.com/view/story/4b9c0e36fc3c4f72a38e1c12bba158bf/ND--ND-Flooding-Souris-River/>

## **COMMERCIAL FACILITIES**

**Occupy protesters blocking gates at West Coast ports, halt operations at some.** Hundreds of Wall Street protesters blocked gates at some of the West Coast's busiest ports December 12, causing the partial shutdown of several in a day of demonstrations they hope will cut into the profits of the corporations that run the docks. The closures affected some of the terminals at the ports in Oakland, California, Portland, Oregon, and Longview, Washington, though it was not immediately clear how much the shutdowns would affect operations and what the economic loss would be. From California to as far away as Vancouver, British Columbia, protesters picketed gates, beating drums, carrying signs such as "Shutdown Wall St. on the Waterfront" and causing longer wait times for trucks. There were a handful of arrests by the late afternoon, but no major clashes with police. While the demonstrations were largely peaceful and isolated to a few gates at each port, local officials in the union that represents longshoremen and, in some cases, port officials, determined the conditions were unsafe for workers. In Oakland, shipping companies and the longshoremen's union agreed to send home about 150 workers, essentially halting operations at two terminals, and leaving a long line of big rigs outside one of the entrances. In Portland, authorities shuttered two terminals after protestors blocked semitrailers from making deliveries, and arrested two people who were carrying weapons. And in Longview, workers were sent home out of concerns for their "health and safety." Port officials erected fences and told workers to stay home, a port spokesman said. Source: [http://www.washingtonpost.com/business/occupy-protesters-seek-to-shut-down-west-coast-ports-despite-rejection-by-longshore-union/2011/12/12/gIQA3zP3oO\\_story.html](http://www.washingtonpost.com/business/occupy-protesters-seek-to-shut-down-west-coast-ports-despite-rejection-by-longshore-union/2011/12/12/gIQA3zP3oO_story.html)

UNCLASSIFIED

## UNCLASSIFIED

### **COMMUNICATIONS SECTOR**

Nothing Significant to Report

### **CRITICAL MANUFACTURING**

**NHTSA recall notice - Ford F-series theft protection standard violation.** Ford announced December 15 the recall of 16,091 model year 2011 F-150 vehicles manufactured from September 9 through September 22, and model year 2012 F-250, F-350, F-450, and F-550 Heavy Duty vehicles manufactured from September 12 through September 22. These vehicles fail to comply with the requirements of federal motor vehicle safety standards regarding theft protection. The transmission can be shifted out of the park position without pressing the brake pedal due to a brake shift interlock switch problem. This will allow the operator to inadvertently shift the vehicle into gear without the brake pedal being depressed, increasing the risk of a crash or injury to a nearby pedestrian. Ford will notify owners, and dealers will inspect the brake shift interlock switch function and replace the switch if necessary. Source: [http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl\\_ID=11V582000&summary=true&prod\\_id=1033769&PrintVersion=YES](http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=11V582000&summary=true&prod_id=1033769&PrintVersion=YES)

### **DEFENSE/ INDUSTRY BASE SECTOR**

**Balance issue contributed to Libya F-15 crash.** An F-15E crashed in Libya March 21 in part because of a lack of balance on the aircraft, as well as the pilot conducting a maneuver at untested altitude, U.S. Air Forces in Europe (USAFE) announced December 13. An accident investigation board found the Strike Eagle departed from controlled flight because it “exceeded the critical angle of attack,” according to a USAFE news release. Although the pilot was performing an acceptable maneuver, he performed it at an altitude that had never been tested. Lateral asymmetry — an unbalanced aircraft — was also faulted. The pilot and his weapons system officer successfully ejected in rebel-held territory east of Benghazi. What remained of the aircraft was destroyed so foreign forces could not salvage it later, according to the release. Source: <http://www.militarytimes.com/news/2011/12/air-force-f-15-board-maneuver-resulted-libya-crash-121411w/>

### **EMERGENCY SERVICES**

**Major US law enforcement Website shut down after data breach.** The official website of the Coalition of Law Enforcement and Retail (clearusa.org) has been shut down after hackers supporting the AntiSec movement managed to obtain access to thousands of account details, leaking them all online. A hacker called Exphin1ty is responsible for this latest operation against a government institution. He states this is a form of retaliation against the “American law enforcement’s inhumane treatments of occupiers.” Identification numbers, the dates when accounts were created, names, titles, agency names, addresses, cities, states, zip codes, e-mail addresses, phone numbers, and hashed passwords were posted online by the hacker. Exphin1ty claims military and law enforcement personnel, federal agents, security companies, and even

UNCLASSIFIED

## UNCLASSIFIED

large corporations such as Microsoft may be affected by the breach. The CLEAR USA Web site is now displaying a message that states the “account has been suspended”, which means that its owners are working on fixing the security issues that left it vulnerable. Source:

<http://news.softpedia.com/news/Major-US-Law-Enforcement-Website-Shut-Down-After-Data-Breach-239859.shtml>

### **ENERGY**

**BP oil spill shows blowout systems need redesign, panel says.** Blowout preventers, which are supposed to seal off an oil well in an emergency, must be redesigned to prevent failures like the one in 2010 at BP Plc’s Macondo well in the Gulf of Mexico, according to the final report of a technical panel. The U.S. government and the energy industry “misplaced trust” in the ability of blowout preventers to act as fail-safe mechanisms, a committee of the National Academy of Engineering and National Research Council said in a report December 14. The 57-foot valve systems, which stand atop deep-water wells, were not designed or tested for the conditions that existed when the Macondo well exploded, the report found. A blowout at the Macondo well in April 2010 killed 11 workers aboard Transocean Ltd.’s Deepwater Horizon drilling rig off the coast of Louisiana, causing it to sink and resulting in the biggest offshore U.S. oil spill in history. An estimated 4.9 million barrels of crude went into the Gulf while operators fought for 87 days to seal the well. If the blowout preventer had cut off the flow of oil and gas from the well, the rig might not have sunk and the spill probably would have been smaller, the report found. Source: <http://www.businessweek.com/news/2011-12-14/bp-oil-spill-shows-blowout-systems-need-redesign-panel-says.html>

**(Nebraska) Magellan pipeline ruptures near Nemaha, Neb.** A pipeline carrying petroleum from Kansas City, Missouri, to Omaha, Nebraska, ruptured, spilling an estimated 252,000 gallons. A Magellan Midstream Partners spokesman said a landowner hit the pipeline with a bulldozer December 10 near Nemaha, Nebraska. Magellan’s control room in Tulsa, Oklahoma, noticed a drop in pressure and quickly shut down the line. The company spokesman said there are two pipes that run through the area and both were affected. He said an initial estimate put the spill at 252,000 gallons but that could be revised as a crew cleans up the area and fixes the pipes. A Magellan crew was at the site December 11. Source:

<http://www.kmov.com/news/mobile/Magellan-pipeline-ruptures-near-Nemaha-Neb-135409203.html>

### **FOOD AND AGRICULTURE**

**(Florida) Pesticide to blame for dead bees in Brevard County.** Officials said they know what killed hundreds of thousands of bees in Brevard County, Florida, Central Florida News 13 Orlando reported December 13. It was a pesticide that wiped out hundreds of beehives in the Malabar area. Two beekeepers were affected. In September, state agriculture investigators thought a pesticide was to blame. Tests now confirm that finding, but nobody knows where the pesticide came from. Beehive owners said the mass kill-off cost them as much as \$500,000.

UNCLASSIFIED

## UNCLASSIFIED

Source: [http://www.cfnews13.com/article/news/2011/december/357358/Pesticide-to-blame-for-dead-bees-in-Brevard-County.html?hpt=us\\_bn5](http://www.cfnews13.com/article/news/2011/december/357358/Pesticide-to-blame-for-dead-bees-in-Brevard-County.html?hpt=us_bn5)

**More dog food recalled due to aflatoxins.** Three more labels of dry dog food from another manufacturer have been added to the recall list because of levels of aflatoxins above acceptable limits, Food Safety News reported December 13. Advanced Animal Nutrition, which said it had no reports of adverse health effects related to the dog food, become the third company with the problem. Advanced Animal Nutrition said the recalled dog food was distributed in Missouri, Arkansas, and Louisiana. Like Iams and Cargill, at issue for Advanced Animal Nutrition are levels of fungus or mold growth, often associated with corn, that at high levels can cause liver damage. Source: <http://www.foodsafetynews.com/2011/12/three-more-labels-of-dry/>

**Chicken recalled for possible Listeria contamination.** A Raeford, North Carolina-based company is recalling about 4,140 pounds of cooked chicken breasts that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced December 9. According to the recall news release, a customer's laboratory sample of House of Raeford Farms chicken breasts tested positive for Listeria monocytogenes. The recall is of 18- to 22-pound boxes containing two 9- to 11-pound "BONELESS OVEN ROASTED CHICKEN BREAST." The products were shipped to delicatessens and food service institutions for further processing in Florida, Georgia, North Carolina, and South Carolina. Source: <http://www.foodsafetynews.com/2011/12/chicken-breasts-recalled-for-possible-listeria-contamination/>

**Cilantro recalled due to possible Salmonella.** A California produce distributor, Pacific International Marketing, or Pacific, is recalling 6,141 cartons of cilantro due to potential Salmonella contamination, Food Safety News reported December 11. A sample of the cilantro tested positive for Salmonella, according to the U.S. Food and Drug Administration (FDA). The source of the contamination is unknown, the Salinas-based distributor said. The cilantro came from Salt River farming, located in Phoenix, and was distributed through retailers in California, Arizona, Massachusetts, New Jersey, Indiana, South Carolina, and Missouri. The California Department of Public Health, FDA, and Pacific are coordinating the recall. Source: <http://www.foodsafetynews.com/2011/12/cilantro-recalled-due-to-possible-salmonella/>

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

**Hospital turns away patients after 'virus' disrupts network.** Gwinnett Medical Center in Lawrenceville, Georgia, had to turn away patients December 7 after being hit by a computer virus that downed the institution's network, and sent staff back to using paper records. The unidentified malware started to cause problems for the medical center and got progressively worse until the hospital was forced to divert all non-emergency admissions to other medical centers. By December 9, the IT team had the outbreak under control and it was able to go back

UNCLASSIFIED

## UNCLASSIFIED

to using the computerized records system the following day, local media reported. The source of the outbreak is still not clear, nor has the malware been identified. But given the symptoms mentioned in reports, a worm infection seems the most likely cause, which could have spread rapidly across the hospital's network forcing IT to pull connectivity to avoid it spreading further. The standard procedure for a fast-spreading worm is immediate isolation followed by a hunt for the point where the malware entered the network, most likely a laptop or USB stick brought into the hospital by a staff member. "It's not affecting patient care in any way, shape or form," a spokeswoman said, adding patient data was not at risk. Source:

<http://news.techworld.com/security/3324420/hospital-turns-away-patients-after-virus-downs-network/>

### **INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**Cybercriminals steal more than \$1 million from Android users in 2011.** A recent study by Lookout Mobile Security reveals mobile malware has become a reality as cyber criminals managed to illegally earn more than \$1 million from Android users alone. Experts estimate that in 2012 things will worsen. The figures show the likelihood for an Android user to encounter a malicious element has risen from 1 percent to 4 percent from the beginning of 2011.

Reportedly, Android customers worldwide have a 36 percent chance of clicking on a link that will eventually point to a malware-filled Web site. When it comes to monetization trends, experts believe malevolent software that sends SMS messages to premium rate numbers will represent the favorite method utilized by crooks to fill their pockets. Even though many believed botnet networks will be used at a larger scale, so far they have not made their presence felt. Source: <http://news.softpedia.com/news/Cybercriminals-Steal-More-than-1-Million-from-Android-Users-in-2011-240949.shtml>

**Google pulls more SMS fraud-related Android apps.** Google removed five additional apps from the Android Market that mobile-security firm Lookout alleges appear to be engaged in SMS fraud targeting Europeans. The apps were removed after Lookout discovered them December 13, a Lookout representative told CNET. That brings the total number of apps removed that Lookout has dubbed "RuFraud" (Russian Fraud) to 27, the representative said. The apps, which appear to be free versions of legitimate games or wallpaper, are designed to charge premium SMS toll rates on European phones, Lookout said. The rates are buried within the terms of service, and users may not realize they will be charged \$5 per SMS, according to the firm. Google confirmed December 12 it removed 22 Lookout-identified fraudulent apps before the firm found the 5 additional ones. Source: [http://news.cnet.com/8301-1009\\_3-57342638-83/](http://news.cnet.com/8301-1009_3-57342638-83/)

**SCADA vuln imperils critical infrastructure, feds warn.** An electronic device used to control machinery in water plants and other industrial facilities contains serious weaknesses that allow attackers to take it over remotely, the U.S. Industrial Control Systems Cyber Emergency Response Team warned. Some models of the Modicon Quantum PLC used in industrial control systems contain multiple hidden accounts that use predetermined passwords to grant remote access, the agency said in an advisory issued December 14. Palatine, Illinois-based Schneider Electric, the maker of the device, produced fixes for some of the weaknesses, and continues to

UNCLASSIFIED

## UNCLASSIFIED

develop additional mitigations. The programmable logic controllers reside at the lowest levels of an industrial plant, where computerized sensors meet the valves, turbines, or other machinery being controlled. The default passwords are hard-coded into Ethernet cards the systems use to funnel commands into the devices, and gets temperatures and other data out of them. The Ethernet modules also allow administrators to remotely log into the machinery using protocols such as telnet, FTP, and the Windriver Debug port. According to a blog post published December 12 by an independent security researcher, the NOE 100 and NOE 771 modules contain at least 14 hard-coded passwords, some of which are published in support manuals. Even in cases where the passcodes are obscured using cryptographic hashes, they are easy to recover thanks to documented weaknesses in the underlying VxWorks operating system. As a result, attackers can exploit the weakness to log into devices and gain privileged access to their controls. Source:

[http://www.theregister.co.uk/2011/12/14/scada\\_bugs\\_threaten\\_critical\\_infrastructure/](http://www.theregister.co.uk/2011/12/14/scada_bugs_threaten_critical_infrastructure/)

**ICS-ALERT-11-343-01—Control System Internet Accessibility.** October 28, 2010, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) published an alert titled “ICS-ALERT-10-301-01 — Control System Internet Accessibility.” The alert warned control system owners and operators a search engine called SHODAN was being used to locate Internet facing control systems. ICS-CERT is issuing this new alert to warn of an uptick in related activity and urge asset owners and operators to audit their control systems configurations and verify whether or not they are susceptible to an attack via this vector. ICS-CERT is tracking and responded to multiple reports of researchers using SHODAN, Every Routable IP Project, Google, and other search engines to discover Internet facing control systems. ICS-CERT coordinated this information with the identified control system owners and operators to notify them of their potential vulnerability to cyber intrusion and attack. When appropriate, ICS-CERT also coordinates with the corresponding sector Information Sharing and Analysis Centers or international Computer Incident Response Team to notify asset owners. In many instances, the exposed systems were unknowingly or unintentionally configured with potentially unsecure access authentication and authorization mechanisms. ICS-CERT works with the asset owner/operators and vendor or systems integrators whenever possible to remove any default credentials and secure these systems from attack. In cases where unauthorized access was identified, ICS-CERT assisted control system owners and operators with system and firewall data analysis to determine the extent of the intrusion and whether any configuration changes might have been made to the system. The use of readily available and generally free search tools significantly reduces time and resources required to identify Internet facing control systems. In turn, hackers can use these tools to easily identify exposed control systems, posing an increased risk of attack. Conversely, owners and operators can also use these same tools to audit their assets for unsecured Internet facing devices. Source: [http://www.us-cert.gov/control\\_systems/pdf/ICS-ALERT-11-343-01.pdf](http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-343-01.pdf)

**Windows Phone bug reportedly disables messaging.** A reported vulnerability in Windows Phone causes its messaging features to be disabled after the device is sent a specific SMS or chat message. The bug was reported to the blog Winrumors, according to the researcher who administers the Web site. He wrote he and the reporter were notifying Microsoft. In a video,

UNCLASSIFIED

## UNCLASSIFIED

the Winrums administrator shows that after a Windows Phone device receives the message, it shuts down. Upon reboot, the messaging hub tile does not work despite repeated attempts. The denial-of-service issue also occurs if a person is sent a specific Facebook or Windows Live Messenger chat message. Winrums ran tests on the HTC Titan, the Samsung Focus Flash, and others running the 7740 version of Windows Phone 7.5 and the Mango RTM build 7720, the administrator wrote. "At this stage, there doesn't appear to be a workaround to fix the messaging hub apart from hard resetting and wiping the device," he wrote. The bug appears to have other strange effects. He found a live tile featuring updates from a Facebook friend will lock up if that friend posts a particular message. He wrote that problem could be avoided by initially booting up a device, getting past the lock screen quickly, and then removing the live tile before it flips over and locks the device. Source:

[http://www.computerworld.com/s/article/9222620/Windows\\_Phone\\_bug\\_reportedly\\_disables\\_messaging?taxonomyId=17](http://www.computerworld.com/s/article/9222620/Windows_Phone_bug_reportedly_disables_messaging?taxonomyId=17)

**Major US law enforcement Website shut down after data breach.** The official website of the Coalition of Law Enforcement and Retail (clearusa.org) has been shut down after hackers supporting the AntiSec movement managed to obtain access to thousands of account details, leaking them all online. A hacker called Exphin1ty is responsible for this latest operation against a government institution. He states this is a form of retaliation against the "American law enforcement's inhumane treatments of occupiers." Identification numbers, the dates when accounts were created, names, titles, agency names, addresses, cities, states, zip codes, e-mail addresses, phone numbers, and hashed passwords were posted online by the hacker. Exphin1ty claims military and law enforcement personnel, federal agents, security companies, and even large corporations such as Microsoft may be affected by the breach. The CLEAR USA Web site is now displaying a message that states the "account has been suspended", which means that its owners are working on fixing the security issues that left it vulnerable. Source:

<http://news.softpedia.com/news/Major-US-Law-Enforcement-Website-Shut-Down-After-Data-Breach-239859.shtml>

## **NATIONAL MONUMENTS AND ICONS**

Nothing Significant to Report

## **POSTAL AND SHIPPING**

Nothing Significant to Report

## **PUBLIC HEALTH**

(Illinois) **Whooping cough cases increasing across Chicago area.** Pertussis — whooping cough — cases have grown throughout the Chicago area, with some counties reporting their highest numbers in nearly 5 years. Statewide, 1,100 people have contracted pertussis in 2011 through November, health officials said. There were 1,057 cases all of last year. There have been more than 650 confirmed cases of whooping cough in McHenry, DuPage and Lake counties.

UNCLASSIFIED

## UNCLASSIFIED

Confirmed cases have spiked over the last few weeks. In McHenry County, what started with eight cases among students at Cary-Grove High School in Cary has grown into an outbreak with more than 200 cases — a county record — affecting as many as 16 communities and at least 33 schools. "The majority of cases are definitely at the schools," a spokeswoman for the McHenry County Health Department said. There have been 138 confirmed cases in Lake County, prompting health officials last week to issue an alert urging residents to be aware of the symptoms, including coughing, spasms, and vomiting. The county expects to surpass its previous record of 164, which is its highest number in 5 years, according to a Lake County Health Department epidemiologist. Source: [http://articles.chicagotribune.com/2011-12-12/news/ct-met-whooping-cough-1211-20111212\\_1\\_whooping-cough-cases-public-health-outbreaks](http://articles.chicagotribune.com/2011-12-12/news/ct-met-whooping-cough-1211-20111212_1_whooping-cough-cases-public-health-outbreaks)

**Hospital turns away patients after 'virus' disrupts network.** Gwinnett Medical Center in Lawrenceville, Georgia, had to turn away patients December 7 after being hit by a computer virus that downed the institution's network, and sent staff back to using paper records. The unidentified malware started to cause problems for the medical center and got progressively worse until the hospital was forced to divert all non-emergency admissions to other medical centers. By December 9, the IT team had the outbreak under control and it was able to go back to using the computerized records system the following day, local media reported. The source of the outbreak is still not clear, nor has the malware been identified. But given the symptoms mentioned in reports, a worm infection seems the most likely cause, which could have spread rapidly across the hospital's network forcing IT to pull connectivity to avoid it spreading further. The standard procedure for a fast-spreading worm is immediate isolation followed by a hunt for the point where the malware entered the network, most likely a laptop or USB stick brought into the hospital by a staff member. "It's not affecting patient care in any way, shape or form," a spokeswoman said, adding patient data was not at risk. Source: <http://news.techworld.com/security/3324420/hospital-turns-away-patients-after-virus-downs-network/>

## **TRANSPORTATION**

**Oakland Port reopens after protesters disrupt overnight operations.** California's Oakland port terminal re-opened December 13 after Occupy protestors shut the facility down overnight, but the disruption "cost the Port and City of Oakland vital resources," a statement from officials said. "They hurt the many businesses that pay taxes and help us create jobs," said the communications manager for the port. On December 12, a statement from the port authority said there were "some delays of truck traffic" but said the port remained operational. But by Monday night, the protests had disrupted workers ability to get to work and impaired the port's ability to operate, officials said. Officials said the disruptions resulted in a backlog of work to get through, cost workers shifts and wages, and caused a negative ripple effect for people up and down the West Coast. Demonstrations took place December 12 in Los Angeles, Seattle, Houston, and Portland, Oregon. Organizers said the goal was to shut down ports to "disrupt the economic machine that benefits the wealthiest individuals and corporations." In Houston, police arrested 20 protesters after dozens of police on foot and on horseback confronted a

UNCLASSIFIED

## UNCLASSIFIED

group who blocked an interstate on-ramp, authorities said. Groups of up to six protesters got down on the pavement and interlocked arms and legs, while a larger group stood near them yelling slogans. Officers set up barricades to cordon off protesters to free the ramp for traffic. Most protesters could be seen moving behind the barricades, with a few exceptions, including those who had lain down. Police handcuffed some protesters. Six face felony charges of using criminal instruments to block a public roadway, said a Houston police department spokesman. In Long Beach, California, protests caused isolated traffic delays but did not hinder port operations, according to the police chief. About 80 protesters demonstrated outside the gate of San Diego's port but caused no disruption, a port spokesman said. A spokesman for the port in Portland said the protests had partially shut down the port there. In addition to the West Coast port blockades, demonstrators in Salt Lake City and Denver said they were planning to disrupt operations of Wal-Mart distribution facilities. About 40 to 50 people protested at the Denver facility, CNN affiliate KCNC 4 Denver reported. Source: [http://www.cnn.com/2011/12/13/us/occupy-ports/?hpt=hp\\_t2](http://www.cnn.com/2011/12/13/us/occupy-ports/?hpt=hp_t2)

### **WATER AND DAMS**

**Coal ash taints 20 U.S. sites: report.** Toxic contamination from coal ash, a waste product of coal-fired power plants, has been detected in groundwater and soil at 20 sites in 10 states, an environmental watchdog group reported December 13. These sites are the latest to contribute to a total of 157 identified by the U.S. Environmental Protection Agency (EPA) and the Environmental Integrity Project, which released the report. Most states do not require ash ponds to be lined, have any construction standards, or any monitoring or cleanup requirements, the report's editor said, adding that almost half the wastes from coal-burning in the United States are dumped this way. Nineteen of the 20 newly identified sites show groundwater contaminated with arsenic or other toxic metals exceeding the maximum contaminant level listed in the Safe Drinking Water Act. The 20th site showed contaminated soil with arsenic 900 times the federal screening level for site cleanups, the report said. Source: <http://www.reuters.com/article/2011/12/14/us-coal-ash-report-idUSTRE7BD2D220111214>

### **NORTH DAKOTA HOMELAND SECURITY CONTACTS**

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

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

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

UNCLASSIFIED

**UNCLASSIFIED**

**UNCLASSIFIED**