

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

(Montana) Sweeping clean water settlement approved for Montana. A federal judge approved a settlement giving Montana until 2014 to clean up polluted streams and lakes in 28 watersheds across the state, capping nearly 15 years of legal battles, officials said October 3. Reuters reported the deal covers more than 17,000 miles of rivers and streams and 461,000 surface acres of lakes, requiring them to meet water-quality standards set for uses such as drinking, swimming, and fishing, under the federal Clean Water Act (CWA). The settlement, signed by a U.S. district judge September 27 and made public October 3, addresses hundreds of types of pollutants, including hazardous chemicals such as polychlorinated biphenyls (PCBs), and heavy metals such as mercury. The deal stems from a 1997 lawsuit that said the U.S. Environmental Protection Agency and the Montana Department of Environmental Quality had violated the CWA by permitting contaminants to be released into the state's already degraded waters. Source: <http://news.yahoo.com/sweeping-clean-water-settlement-approved-montana-030829778.html>

NATIONAL

Nothing Significant to Report

INTERNATIONAL

Nothing Significant to Report

BANKING AND FINANCE INDUSTRY

(Colorado) Police: man steals \$100K using skimmer on local ATMs. Boulder County, Colorado, sheriff's deputies October 5 released a picture of a man they said has stolen more than \$100,000. Deputies said the man put a skimming device on an ATM to get bank account information. He took more than \$11,000 from one person's account, deputies said. As deputies investigated, they said they found other incidents throughout the Denver metropolitan area involving the same man. Some skimmers, like the thief in this case, put a device over the card slot of an ATM, which reads the magnetic strip as the user unknowingly passes their card through it. These devices are often used in conjunction with a miniature camera (inconspicuously attached to the ATM) to read the user's PIN at the same time, deputies said. Source: <http://www.thedenverchannel.com/money/29395290/detail.html>

Banks losing ground on card security. U.S. banks are losing ground in the battle to combat credit and debit card fraud, a new report shows, underscoring the growing threat thieves and hackers pose for the financial system. Globally, security is improving in the payment industry,

UNCLASSIFIED

UNCLASSIFIED

according to data released the week of October 3 by the Nilson Report, a California trade publication. For every \$100 worth of credit and debit card transactions last year, 4.46 cents were lost to fraud worldwide in 2010, down from 4.71 cents in 2009. But many of the security gains were at banks in Europe and Asia, which have adopted stricter security procedures such as issuing cards with computerized chips to help verify purchases, said the publisher of the Nilson Report. Meanwhile, U.S. banks and merchants have balked at the expense of conversion. As a result, fraud in the United States accounted for 47 percent of global fraud losses last year — up from about 46.5 percent in 2009, and 44 percent in the middle of the last decade, he said. Total fraud losses worldwide were \$7.6 billion in 2010, up 10 percent from 2009, the report found. Source: <http://www.reuters.com/article/2011/10/04/us-banks-security-idUSTRE7935XO20111004>

SpyEye Trojan hijacks mobile SMS security for online fraud. A stealth new attack carried out by the SpyEye Trojan circumvents mobile SMS security measures implemented by many banks, Help Net Security reported October 5. Using captured code, Trusteer found a two-step, Web-based attack that allows fraudsters to change the mobile phone number in a victim's online banking account and reroute SMS confirmation codes used to verify online transactions. This attack, when successful, enables the thieves to make transactions on the user's account and confirm them without the user's knowledge. In the first step of the attack, SpyEye steals online banking log-in details. This allows fraudsters to access the account without raising red flags. In the second step, SpyEye changes the victim's phone number of record in the online application to one of several random, attacker-controlled numbers. To complete the operation, the attacker needs the confirmation code sent by the bank to the customer's original phone number. To steal this code, SpyEye injects a fraudulent page in the customer's browser that appears to be from the online banking application. The fake page purports to introduce a new security system "required" by the bank and for which customers must register. The page explains the customer will be assigned a unique telephone number and will receive a special SIM card via mail. Next, the user is told to enter the confirmation number they receive on their mobile telephone into the fake Web page to complete the registration process for the new security system. This allows the criminals to steal the confirmation code they need to authorize changing the customer's mobile number. Now the fraudsters can receive all future SMS transaction verification codes for the hijacked account via their own telephone network. This latest SpyEye configuration shows that out-of-band authentication (OOBA) systems, including SMS-based solutions, are not fool-proof. Using a combination of man-in-the-browser injection technology and social engineering, fraudsters can bypass OOBA, and buy themselves more time since the transactions have been verified. Source: http://www.netsecurity.org/malware_news.php?id=1864

PayPal emails replicated in phishing campaign. An e-mail reading "Your PayPal account has been limited" has been received by many users, in what turned out to be a well-thought-out phishing expedition. Mxlabs informed Softpedia October 3 that the scam e-mails were very well designed and because the seemingly genuine address was spoofed, they looked even more credible. The body of the note reads "Unfortunately one of your recent transaction with PayPal is not successful because your PayPal account has been limited. It is a measure taken to protect

UNCLASSIFIED

UNCLASSIFIED

your account and help ensure the safety of the PayPal platform. We want to help you remove this limitation as soon as possible so he can continue to take advantage of the benefits from PayPal.” The whole layout of the e-mail is very well conceived, and all the graphics and content elements are a perfect match to what would normally be seen in a message coming from PayPal. Once the Click Here button is hit, the user is transferred to a site hosted on a domain called mittemaedchen(dot)de. The full address contains some fragments that refer to “pay pal” to make it look more realistic. The next page, which is also well built, contains a form in which the customer is asked for information such as name, date of birth, country, address, and credit card information. After the form is completed, the victim is redirected to the PayPal genuine site. Source: <http://news.softpedia.com/news/PayPal-Emails-Replicated-in-Phishing-Campaign-225118.shtml>

(New York) Anonymous threatens to 'erase NYSE from the Internet'. Anonymous declared "war" on the New York Stock Exchange (NYSE) the weekend of September 30 and vowed to "erase" it from the Internet October 10 as the Occupy Wall Street protest entered its third week in New York City after a weekend that saw hundreds of protesters arrested during a planned march across the Brooklyn Bridge. "On October 10, NYSE shall be erased from the Internet. On October 10, expect a day that will never, ever be forgotten," intoned a computer-generated male voice common to many Anonymous videos, in a warning posted on TheAnonMessage YouTube channel. The channel has been used to post several Occupy Wall Street-related video messages since the protest against lax regulation of the financial sector and economic inequality began September 17. Those messages include Anonymous' initial "official" video regarding Occupy Wall Street, and a warning sent last week to the New York Police Department that threatened retaliation if "the brutality does not stop" against Occupy Wall Street protestors. The threat to "erase" the NYSE from the Internet was not explained, though some speculated Anonymous was planning a Distributed Denial-of-Service (DDoS) attack on the public-facing NYSE.com Web site, similar to DDoS attacks the group has used to take down sites in the past. Others felt that would only be a minor setback for the NYSE and guessed that Anonymous was planning a larger attack, perhaps even an attempt to actually disable trading on the exchange. Source: <http://www.pcmag.com/article2/0,2817,2394071,00.asp#fbid=HVPcnsT7BOR>

SEC finds failures at credit raters. U.S. Securities and Exchange Commission (SEC) staff found “apparent failures” at each of the 10 credit rating agencies they examined, including Standard & Poor’s, Moody’s, and Fitch, the agency said September 30 in its first annual report on credit raters. The SEC sent letters outlining concerns to each ratings firm and demanded a remediation plan with 30 days, an agency official said in a conference call with reporters. SEC staff said concerns include failures to follow ratings methodologies, failures in making timely and accurate disclosures, and failures to manage conflicts of interest. The report was required by last year’s Dodd-Frank financial oversight law. The staff report did not single out by name any credit-rating agency for questionable actions, but it did describe specific problems it found. Two of the three largest firms, for example, did not have specific policies in place to manage conflicts of interest when rating an offering from an issuer who is also a large shareholder of the firm. One of the large firms, the report said, did not have effective procedures in place to

UNCLASSIFIED

UNCLASSIFIED

prevent leaks of ratings before they are published, the report said. One of the three firms also failed to follow its methodology in rating certain asset-backed securities, was slow to discover, disclose and fix the errors, and may have let business interests influence its mistakes, the report said. It said the SEC has not determined that any of the findings constituted a “material regulatory deficiency”, but said it might do so in the future. Source:

<http://www.reuters.com/article/2011/09/30/us-sec-raters-idUSTRE78S50920110930?feedType=RSS&feedName=topNews>

FTC: Debit card scheme defrauded merchants. The Federal Trade Commission (FTC) said September 30 it is paying \$350,000 in refunds to 100 small U.S. merchants defrauded in a debit and credit card scheme. The scheme involved several firms that falsely promised they would save small businesses money in credit and debit card processing fees by offering lower rates than those of other card-processing services. However, the firms failed to disclose fees and concealed pages of fine print until after the merchants had signed contracts for their services, the FTC said. The FTC identified the firms that perpetrated the scheme as Merchant Processing Inc., Direct Merchant Processing Inc., Vequity Financial Group Inc., and PPI Services Inc. The agency reached settlements with two defendants that banned them from marketing card processing goods or services for sale or lease. Merchants due to receive refunds were to get between \$100 and more than \$25,000, depending on how much the merchant paid, the FTC said. Source: http://www.forbes.com/feeds/ap/2011/09/30/business-us-debit-card-fraud_8710414.html

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

States continue to ban chemicals. Fueled by consumer concerns about exposure to toxic chemicals, state legislatures in 2011 have continued a trend of recent years by banning specific uses of certain compounds. Thus far this year, lawmakers in six states have adopted laws to restrict bisphenol A (BPA), a phosphate-based flame retardant, according to Safer States, a group that tracks chemical legislation in states. Two states broke new ground on chemical policy this year. New York became the first state to prohibit the use of tris (2-chloroethyl) phosphate in children’s goods. And although four other states adopted measures to stop use of BPA in certain products for babies and toddlers, Connecticut became the nation’s first state to ban this chemical from thermal paper used in cash register tapes and other receipts. Four other states took action against BPA. Three states, Maine, Delaware, and California, moved to bar BPA in baby bottles and cups for young children. They joined eight other states with similar bans. Maryland, meanwhile, banned sales of infant formula in containers with more than 0.5 part per billion of BPA. Source: <http://pubs.acs.org/cen/government/89/8940gov3.html>

(Virginia) U.S. NRC finds no damage at Dominion's quake-hit plant. An inspection team for the U.S. Nuclear Regulatory Commission (NRC) said October 3 it has found no significant damage at Dominion Resource's quake-hit North Anna power plant in Mineral, Virginia, but that more evaluation is needed. The NRC team said the plant's safety system functions were maintained, and the plant's staff reacted in manner that protected public health and safety. Still, the team said there were issues that needed further review. They said some "anomalies" were observed

UNCLASSIFIED

UNCLASSIFIED

on safety-related equipment that will need more evaluation. The NRC said it had sent Dominion a letter laying out the requirements for the restart of the plant. Source:

<http://www.reuters.com/article/2011/10/03/usa-nuclear-dominion-idUSN1E79219J20111003>

No explosion at No. 2 reactor / TEPCO: Only 3 hydrogen blasts occurred at Fukushima N-plant. The Tokyo Electric Power Co. (TEPCO) panel investigating the nuclear crisis at Japan's Fukushima No. 1 power plant has concluded a hydrogen explosion did not occur at the plant's No. 2 reactor, overturning its previous conclusion an explosion took place March 15, according to a draft of the panel's interim report October 3. According to TEPCO, the first hydrogen explosion took place in the No. 1 reactor building March 12, followed by an explosion at the No. 3 reactor March 14. Early on the morning of March 15, TEPCO confirmed the sound of an explosion, and then found damage in the No. 4 reactor building as well as significantly lower pressure at the No. 2 reactor's pressure suppression pool. This led them to conclude in June that explosions occurred almost simultaneously. However, the panel studied a seismometer at the plant and found only one explosion tremor was recorded, at the No. 4 reactor. Due to the fact the pressure at the No. 2 reactor's pressure suppression pool dropped around that time, the panel said the reactor's containment vessel may have sustained other damage. The interim report also referred to a possible reason why hydrogen explosions occurred at the Nos. 1 and 3 reactors. The report said silicon rubber used to seal the spaces between doors and wall, and between the containment vessels and their lids, may have not functioned properly due to the high temperatures, opening gaps that allowed the release of hydrogen into the reactor building. Source: <http://www.yomiuri.co.jp/dy/national/T111002003221.htm>

COMMERCIAL FACILITIES

(California) Manhunt after 2 die in Calif. workplace shooting. Authorities were searching door to door with guns drawn in a neighborhood about 5 miles from the Cupertino, California quarry where a gunman killed two and wounded six at a morning meeting October 5. Schools were on lockdown or closed in Cupertino as SWAT teams sought the 47-year-old suspect. He also is suspected of wounding a woman in an attempted carjacking in Cupertino more than 2 hours later. A Santa Clara County sheriff's lieutenant said the suspect was at the routine safety meeting at 4:30 a.m., became disgruntled and left. He said he then returned with a 9 mm handgun and a rifle and started shooting people. In the early afternoon October 5, authorities were searching the quarry for possible victims. About 15 workers were evacuated and being kept at a safe location. The suspect is a San Jose resident who was a truck operator at the Permanente Cement Plant, and also produced and hosted a public access television show for CreaTV in San Jose. After leaving the quarry, the suspect attempted a carjacking at a nearby Hewlett-Packard parking lot, shooting a female driver in the leg. He did not get the car from her. Three of the victims were taken to Santa Clara Valley Medical Center, including the woman shot in the carjacking, a hospital spokeswoman said. One victim was treated and released, while the other two were in fair condition, she said. In nearby Sunnyvale, another injured person was found in a parking lot, reported KNTV 11 San Jose, but it was not clear if that was connected to the workplace shooting. The suspect is described as African American, 5'11", and 260 pounds, with numerous tattoos, according to KNTV. Permanente Cement Plant, owned by

UNCLASSIFIED

UNCLASSIFIED

Lehigh Hanson, Inc., is a limestone and aggregate mining operation and cement plant. Source: http://www.msnbc.msn.com/id/44785704/ns/us_news-crime_and_courts/#.ToyWjnLm9_6

(Alabama) Suspicious package causes evacuation at Montgomery shopping complex. A suspicious package shut down a shopping center in Montgomery, Alabama for 3 hours October 3, causing businesses to be evacuated, and the bomb squad to be brought in to investigate. According to Montgomery's Department of Public Safety, a call from a UPS employee was made around 5 p.m. describing a suspicious package that was dropped off by a customer. Montgomery's police and fire departments were involved along with the explosives ordinance disposal unit and even the FBI to X-ray the package and safely remove it from the property. According to police, the package was detonated on their firing range and was not determined to be hazardous, but a Montgomery County commissioner said all precautions were necessary because the customers' actions were unusual. Source: <http://www.waka.com/news/9554-suspicious-package-causes-evacuation-at-montgomery-shopping-complex.html>

COMMUNICATIONS SECTOR

FCC tells retailers to stop selling mobile phone jammers. The Federal Communications Commission (FCC) has issued warnings to 20 online retailers selling illegal mobile phone jammers, GPS jammers, Wi-Fi jammers, and other signal jamming devices, the agency said October 5. The sale and use of devices that jam the signals of authorized radio communications are illegal in the United States, the FCC said in its enforcement action. The agency will "vigorously" prosecute violations going forward, it said in a press release. "Jamming devices pose significant risks to public safety and can have unintended and sometimes dangerous consequences for consumers and first responders," the chief of the FCC's enforcement bureau said in a statement. Jammers, sometimes used in classrooms, theaters and churches, are prohibited because they can prevent individuals from contacting police and fire departments or family members during an emergency, the FCC said. The 20 retailers were marketing more than 200 jamming devices, the FCC said. Among the jammers being sold were GPS blockers for vehicles, high-tech signal blockers with remote control capabilities, and jammers disguised as paintings and cigarette packs, the agency said. The FCC ordered each online retailer to immediately stop marketing signal-jamming devices in the United States. If a retailer gets a second citation from the FCC, it could face fines ranging from \$16,000 to \$112,500, with a separate penalty possible for each device sold or each day a device is marketed, the agency said. Additional violations could result in the seizure of equipment and prison time, the FCC said. Source:

http://www.computerworld.com/s/article/9220573/FCC_tells_retailers_to_stop_selling_mobile_phone_jammer

CRITICAL MANUFACTURING

NHTSA recall notice - Volkswagen Golf, Jetta; Audi A3 fuel system defect. Volkswagen is recalling 168,275 model year 2009-2012 Jetta and Jetta Sportwagen vehicles, model year 2010-2012 Golf vehicles, and model year 2010-2012 Audi A3 vehicles that are equipped with a 2.0L

UNCLASSIFIED

UNCLASSIFIED

TDI common rail diesel engine/clean diesel engine. The fuel injection pulses could coincide with the natural frequency of the injector line #2, in specific load and revolutions per minute conditions. This resonance creates additional stress in the fuel line. Due to the resonance condition, injector line number 2 could develop small cracks that would lead to a fuel leakage. Leaking fuel in the presence of an ignition source may lead to a fire. Volkswagen will install an improved fuel injector line for the number 2 cylinder, and will install vibration dampers on all injector lines. Volkswagen and Audi will notify owners to have the vehicles repaired free of charge. The safety recall is expected to begin in November. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=11V490000&summary=true&prod_id=779783&PrintVersion=

DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

EMERGENCY SERVICES

(Connecticut) Responders train for hybrid, electric car rescues. In 2010, the National Fire Protection Association received a \$4.4 million grant from the U.S. Department of Energy to develop a training program to instruct fire department personnel on the potential hazards they may encounter at a motor vehicle accident with all-electric and hybrid vehicles, or cars with both combustion engines and battery packs. Instructors from 38 fire departments across Connecticut recently attended a train-the-trainer course at the Connecticut Fire Academy to view procedures in handling all-electric and hybrid vehicle accidents, the Associated Press reported October 5. The fire association took the data and created a 2-page Emergency Response Guide, so emergency crews could focus on critical information when they arrive at the scene of an accident. The fire association instructor said the high strength steel being used in electric and hybrid cars is creating additional concerns. Although the cars are 75 percent lighter, they are now 15 percent stronger, making it difficult for firefighters to cut through to reach anyone trapped inside, he said. Another possible danger is a battery breach, he said, in which fluids can leak onto the ground, creating an environmental hazard. Source: <http://www.courant.com/community/manchester/hc-ap-ct-electriccarrescueoct05,0,3939571.story>

Medical identity theft a growing problem. According to a recent report on a nationwide survey of 600 executives from U.S. hospitals, doctors' organizations, health insurance companies, pharmaceutical manufacturers, and life sciences companies, accounting firm PricewaterhouseCoopers (PwC) found medical identify theft is the fastest-growing form of identity theft, affecting 1.42 million Americans in 2010, and costing more than \$28 billion. Theft accounted for 66 percent of the publicly reported security breaches documented since 2009, which included stolen laptops, stolen smart phones, using patient data to submit fraudulent claims, and people seeking medical care in another person's name. The single most commonly reported breach in the security of patients' private health information was improper use of patient data by a person who works for a doctor's office, hospital, insurance company, or life

UNCLASSIFIED

UNCLASSIFIED

sciences organization. The breaches ranged from an employee leaving private documents out in plain sight, to making improper comments on Facebook, or even talking in the elevator about a person's protected health information. Nearly four out of 10 doctors and hospitals surveyed have caught a patient trying to use someone else's identity to obtain healthcare services. Patients seeking medical services under someone else's name was the second most common privacy or security issue reported by healthcare providers. Rounding out the top three most common breaches was improper transfer of files containing personal health data to people who were not authorized to view the information. One in four insurers reported improperly transferring files that contained protected health information. Source:

<http://www.medpagetoday.com/PracticeManagement/InformationTechnology/28696>

ENERGY

(New York) Copper thieves target power company in Central New York. National Grid is pushing back against copper thieves, who have targeted 24 electric substations in Onondaga County, New York, since the beginning of the year, the Syracuse Post-Standard reported October 4. In the last month, Onondaga County sheriff's deputies have investigated 20 reports of copper thefts at National Grid substations and other facilities, the sheriff said. Syracuse police are investigating at least 15 cases, the police chief said. Recently, thieves stole \$800 in scrap metal and caused \$10,000 in damage at the Glenwood and Peat Street substations in Syracuse. The two substations have been hit at least three times apiece. In another case, someone was charged with stealing less than \$200 in copper from 35 utility poles near Syracuse University. The repairs cost \$14,000 — or \$400 a pole. A theft in southern Onondaga County required a 6-hour planned outage September 11 to fix. The price of copper — between \$3 and \$4 a pound — has led to “skyrocketing” copper thefts in the past year, authorities said. Source:

http://www.syracuse.com/news/index.ssf/2011/10/copper_thieves_target_power_co.html

FOOD AND AGRICULTURE

Soybean meal, flour recalled for Salmonella. A Michigan company is recalling 2,623 40-pound bags, 360 1,500-pound totes of soybean flour, and 924 .08-ton loads of bulk soy meal because they may be contaminated with Salmonella, Food Safety News reported October 5. The soy meal and flour was used to manufacture human and animal food, and had been distributed since November 2010. Thumb Oilseed Producer's Cooperative of Ubly, Michigan said in a news release the recall resulted from routine sampling conducted by the company and U.S. Food and Drug Administration (FDA) that revealed Salmonella in finished product, and the manufacturing plant. Thumb Oilseed is cooperating with the FDA. The soy flour was distributed in 40-pound paper bags under the names: Nex Soy (lot numbers TF112310 thru TF033011) and Soy Beginnings (product code 285100-NFB; lot numbers TF112310 thru TF033011). The soy flour was also distributed in 1,500-pound polyurethane totes under the name: Soy Beginnings (product code 285100-NFT, lot numbers TF112310 thru TF082311). The soy meal was distributed as .08 ton loads after custom processing with lot numbers O011711 thru O081711. The recalled soybean flour and meal was distributed from November 2010 to September 2011 to a limited group of wholesale customers in Illinois, Vermont, Minnesota, Pennsylvania,

UNCLASSIFIED

UNCLASSIFIED

Wisconsin, New Hampshire, and Canada. Source:

<http://www.foodsafetynews.com/2011/10/soybean-meal-flour-recalled-for-salmonella/>

Europe cancels consumer caution about sprouts. The European Food Safety Authority (EFSA) October 4 dropped its consumer advisory against eating raw sprouts and growing sprouts from seed at home, and recommended consumers refer to the various national food safety agencies for specific guidance on sprouts. EFSA said the reason for canceling the advisory was fenugreek seeds from Egypt, the most likely cause of the massive outbreak of E. coli O104:H4 centered in Germany in the spring of 2011, are no longer on the market. The agency also said its biological hazards panel, by request from the European Commission, was carrying out a risk assessment on the EU production chain for sprouts and sprouting seeds, and would publish a scientific opinion "in the coming weeks." In a wrap-up report on the E. coli O104:H4 outbreak, which ended July 26, EFSA said there were at least 3,134 cases and 47 deaths. E. coli O104:H4 was never detected in any of the batches of suspect fenugreek seeds, something that "is not unexpected," according to EFSA, because it was possible the contaminated seeds were no longer in stock when sampling took place, or that the pathogen was present at such a low level that isolating the organism was not possible. Source:

<http://www.foodsafetynews.com/2011/10/europe-cancels-consumer-caution-about-sprouts/>

CDC: 84 infected, 15 dead from Listeria outbreak. New statistics from the U.S. Centers for Disease Control and Prevention show that the recent listeria outbreak in 19 states has killed 15 people and sickened 84, according to FoxNews.com reported September 30. Infections have occurred in the following states: Alabama (1), Arkansas (1), California (1), Colorado (17), Illinois (1), Indiana (2), Kansas (5), Maryland (1), Missouri (3), Montana (1), Nebraska (6), New Mexico (13), North Dakota (1), Oklahoma (11), Texas (14), Virginia (1), West Virginia (1), Wisconsin (2), and Wyoming (2). Deaths have occurred in the following states: 3 in Colorado, 1 in Kansas, 1 in Maryland, 1 in Missouri, 1 in Nebraska, 5 in New Mexico, 1 in Oklahoma, and 2 in Texas. A California company said it was recalling 90 cartons of chopped romaine lettuce shipped to Oregon and then further distributed to Idaho, Washington, and perhaps elsewhere after the U.S. Food and Drug Administration found listeria in a sample. True Leaf Farms said there have been no illnesses linked to the lettuce. Listeria is very dangerous and is the bacteria behind an ongoing outbreak that has sickened and killed people in several states who ate contaminated cantaloupes that were produced in Colorado. Source:

<http://www.foxnews.com/health/2011/09/30/lettuce-recalled-after-listeria-found/>

Cargill ground turkey outbreak toll climbs to 129. Ten more cases and two more states have been added to the Salmonella Heidelberg outbreak associated with Cargill ground turkey, the U.S. Centers for Disease Control and Prevention (CDC) reported September 29. The outbreak, which prompted the largest Class I recall in history, has so far spread over 34 states, sickening 129, and killing a California man. In its update on the outbreak, the CDC said the patients became sick between February 27 and September 13. Texas reported 17 cases; Illinois 16; Michigan and Ohio 12 each; Missouri 7; California and Pennsylvania 6 each; Colorado, North Carolina, and Wisconsin 4 each; Arizona, Kansas, Massachusetts, and South Dakota 3 each; Georgia, Iowa, Kentucky, Minnesota, Mississippi, Nebraska, New York, Oklahoma, and

UNCLASSIFIED

UNCLASSIFIED

Tennessee 2 each; and Alabama, Arkansas, Connecticut, Indiana, Louisiana, Maryland, Nevada, New Jersey, Oregon, Utah, and Vermont 1 each. The patients ranged in age from less than 1 year to 90. Among 88 people with information about treatment available, 33 were hospitalized. Source: <http://www.foodsafetynews.com/2011/10/cargill-ground-turkey-outbreak-toll-climbs-to-129/>

Kraft recalls Velveeta Shells & Cheese cups. Kraft Foods Inc. is recalling three varieties of its Velveeta Shells & Cheese single-serve microwaveable cups because small, thin wire bristle pieces may be inside the cups, Food Safety News reported October 2. The recall includes 137,000 cases of the affected products shipped to customers across the United States. There have been no reports of consumer injuries or complaints, the company said September 30. The recall includes the: 2.39 ounce Velveeta Shells & Cheese original microwaveable cups with a best-when-used-by date of May 16, 2012 and UPC 2100002322; Velveeta Shells & Cheese original four-pack microwaveable 2.39-ounce cups that have best-when-used-by dates of April 24, 2012 to May 16, 2012 and a UPC of 2100002339; the 2.19-ounce Velveeta Shells & Cheese made with 2% milk microwaveable cups with best-when-used-by dates of March 25, 2012 to March 30, 2012 and UPC of 2100002323; Velveeta Shells & Cheese made with 2% milk four-pack 2.19-ounce microwaveable cups with best-when-used-by dates of March 29, 2012 to April 12, 2012 and UPC 2100002946; and 2.44-ounce Velveeta Rotini & Cheese Broccoli microwaveable cups with best-when-used-by dates of April 29, 2012 to May 14, 2012 and UPC of 2100002318. Source: <http://www.foodsafetynews.com/2011/10/kraft-recalls-velveeta-shell-cheese-cups/>

(California; Arizona; Nebraska) E. Coli contamination prompts beef recall. The U.S. Department of Agriculture announced Manning Beef is issuing a voluntary recall on its beef cuts, including top-round, tri-tip, and trimmings, due to unsanitary conditions and the discovery of E. Coli bacteria contamination at its Los Angeles manufacturing plant, the State Column reported October 2. Officials said 80,000 pounds of beef have been recalled. This tainted meat was shipped to retail establishments and food services in Arizona, California, and Nebraska. There have been no reported illnesses related to the consumption of the tainted beef. Source: <http://www.thestatecolumn.com/health/e-coli-contamination-prompts-beef-recall/>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(District of Columbia) Suspicious device near Capitol identified. Capitol Police discovered a small metal cylinder on Pennsylvania Avenue NW near the reflecting pool in front of the U.S. Capitol in Washington D.C., October 6. Streets were shut down and a robot was called in to investigate. But the suspicious device was eventually found to be nothing more than a piece of equipment used to inspect sewer pipes, an NBC News correspondent reported. An officer spotted the object at about 7 a.m., and law enforcement officials said they were investigating it as a suspicious device. Investigators put the device into an X-ray machine, but Capitol police said "it was too dense to see what's inside." A team placed the cylinder inside a bomb squad

UNCLASSIFIED

UNCLASSIFIED

vehicle, and it was to be transported to Quantico, Virginia. Surrounding roadways were shut down for the investigation. The affected roads: First Street NW from Garfield Circle to Constitution Avenue and Pennsylvania Ave SE from First Street to 3rd street SE. Source: http://www.msnbc.msn.com/id/44800111/ns/local_news-washington_dc/

Security breaches in federal agencies hard to contain despite efforts. A report released by the U.S. Government Accountability Office (GAO) October 4 revealed that in the past 5 years, the number of security breaches in federal networks have increased constantly. The figures show that in 2006, there were just over 5,000 incidents reported, while in 2010 the number skyrocketed to 41,000. About 30 percent of the incidents from last year were attacks in which malicious code was injected into the networks of federal organizations. The paper concludes "Inadequacies exist in access controls, which include identification and authentication, authorization, cryptography, audit and monitoring, boundary protection, and physical security." Source: <http://news.softpedia.com/news/Security-Breaches-in-Federal-Agencies-Hard-to-Contain-Despite-Efforts-225271.shtml>

(California) 4 hurt in Calif. high school campus attack. A male student stabbed two fellow students and a dean at South East High School in South Gate, California, September 30, forcing the school to temporarily lock down. Five people were taken to area hospitals after the attack, including the assailant, a Los Angeles County Fire Department inspector said. A campus police officer hurt his back in the scuffle. A Los Angeles Unified School District police officer said the argument started with the male student arguing with and choking another female student. "The dean tried to intervene and during that, the dean realized the male had a knife and was attacking the female student," the officer said. Another student was injured while trying to intervene. The initial victim was initially in serious condition, but her injury, along with the others' injuries, appeared non-life threatening. Students told local television stations the attacker was the former boyfriend of the female student. It was not immediately clear what triggered the initial confrontation. The lockdown was lifted a few hours later, and classes resumed. Source: <http://www.cbsnews.com/stories/2011/09/30/national/main20114190.shtml>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Facebook scammers exploit Steve Jobs' death. Facebook scammers are exploiting news of the death of Apple's founder as a theme for survey scams. The users targeted by the scam are told an unnamed firm is giving away 50 iPads in memory of the deceased. Applicants are invited to complete an online survey to "qualify" for the prize. The offer is entirely bogus. Even so, more than 15,000 people have already clicked through to the bogus survey site, net security firm Sophos reported. Source: http://www.theregister.co.uk/2011/10/06/jobs_death_facebook_scam_lur

Facebook to scrub itself clean of filthy malware links. Facebook has recruited Websense to scan its social network for links to malicious sites. Scammers are increasingly using Facebook as a means to drive traffic towards malware and exploit portals or Internet scam sites. In

UNCLASSIFIED

UNCLASSIFIED

response, Facebook is tapping Websense for technology that will analyze the jump off points to links. Cloudy technology will assign a security classification to sites, presenting users with a warning if the location is considered dangerous. This warning page will explain why a site might be considered malicious. Users can still proceed, at their own risk, to potentially dodgy sites. Before, individual users had the option to add additional security filtering apps, such as Bitdefender Safego, to their profiles as a means to scan for spam and malicious links. Facebook is now offering this type of technology by default as an extension of its previous relationship with Websense. Source:

http://www.theregister.co.uk/2011/10/04/facebook_websense_scam_scanning/

XSS Web attacks could live forever, researcher warns. Web sites that accidentally distribute rogue code could find it harder to undo the damage if attackers exploit widespread browser support for HTML5 local storage, and an increasing tendency for heavy users of Web apps never to close their browsers. If browsers do not provide a mechanism for Web sites to recover from certain cross-site scripting attacks, the attacks could become invincible and the site at the origin of the attack remain compromised indefinitely, a vulnerability researcher and Google security engineer warned October 1. The scope of client-side programming languages such as JavaScript within browsers is limited by a critical security concept known as the same-origin policy. This prevents scripts running on certain Web pages from interfering with Web sites opened in separate tabs or windows. In the case of cross-site scripting (XSS), attackers manage to insert rogue JavaScript code in targeted pages, where it is then executed in the context of their origin, defined by the domain, the protocol, and the port number. JavaScript is very powerful and is used in most Web-based attacks. Despite this, browsers do not currently provide a mechanism to invalidate such code, something that would provide compromised Web sites with a way to request a clean slate once they had resolved the problem. A normal response to XSS attacks is to patch the vulnerability, invalidate session cookies so that everyone is forced to re-authenticate, and optionally force a password change. But this is not enough, because, according to the researcher, once compromised a Web origin can stay tainted indefinitely. Source:

http://www.computerworld.com/s/article/9220511/XSS_web_attacks_could_live_forever_researcher_warns

Firefox and SeaMonkey users warned to disable McAfee ScriptScan. A major incompatibility between Mozilla's browsers Firefox and SeaMonkey, and McAfee's ScriptScan plug-in has caused "a high volume of crashes," according to Mozilla. The problem first came to light in September, when members of the McAfee forum began reporting problems with version 14.4.0 of ScriptScan, a tool that checks Web pages, as they are loaded into the browser, for malicious code. This is the first time since July that Mozilla has found it necessary to block a plug-in. All versions of Firefox and SeaMonkey are affected by the problem, as are all current versions of McAfee ScriptScan. Mozilla recommends ScriptScan users disable the browser plug-in. The issue only affects version 7 of the browsers, according to a McAfee spokesperson. Source:

<http://www.h-online.com/security/news/item/Firefox-and-SeaMonkey-users-warned-to-disable-McAfee-ScriptScan-1355098.html>

UNCLASSIFIED

UNCLASSIFIED

Security hole in HTC phones gives up e-mail addresses, location. A security hole found in some HTC Android phones could give apps with Internet permissions access to information such as a user's location and their text messages, Android Police reported October 2. The vulnerability is part of HTC's Sense UI and affects a subset of the brand's most popular phones, including the HTC Thunderbolt, and the EVO 4G. The affected HTC phones have an application package titled HTCLoggers.apk installed with root-level access. Apps with Internet permissions can access HTCLoggers.apk, which provides access to information such as GPS data, WiFi network data, memory information, running processes, SMS data (including phone numbers and encoded text), and system logs that can include information such as e-mail addresses and phone numbers. When called upon, the logging program opens a local port that will provide this data to any app that asks for it. Apps can send the data off to a remote server for safekeeping, as shown by a proof-of-concept app that Android Police researchers developed. Source: <http://arstechnica.com/gadgets/news/2011/10/security-hole-in-htc-phones-gives-up-e-mail-addresses-location.ars>

Children's online games hide bank account stealing malware. Bitdefender experts warn users to pay closer attention to what their children access on the Internet as in many cases, harmless looking games hide dangerous malware that could compromise the entire information from a device. According to a Bitdefender researcher, "Some of these dangerous games are easily identified by adults — who suspect that something is abnormal about them when they require permission to install various programs in the computer or they redirect to other Web sites," he said. "Thus, attackers choose targets that are easier to dupe. Furthermore, a 4-year-old doesn't understand the concept of online vulnerability." The colorful images and playful sounds might look innocent, but in some cases they hide backdoor applications that surrender control of the machine to hackers looking to steal sensitive data. The phenomenon is expected to take off, as recent studies show that in the United States and in the United Kingdom, more than 40 percent of children are highly active in social networking environments. Also, 24 percent of parents do not monitor their children's Internet activity. Malware containing Flash applications seem to be among the most unsafe as in many cases they look like regular games. When they are executed, redirects are made, which lead kids to insecure locations that host malicious elements. Legitimate sites can also be overtaken by cybercriminals and infested with malevolent code that could hand over the controls to the system to a third party. Source: <http://news.softpedia.com/news/Children-s-Online-Games-Hide-Bank-Account-Stealing-Malware-225093.shtml>

Mobile malware masqueraded as Opera Mini. Cybercriminals are taking advantage of the fact that Opera Mini is one of the most popular mobile browsers and creating a fake Web site which stores a piece of malware that looks like a genuine installation file. Trend Micro discovered the site that resembles the official Opera page and that was specially made to be accessed from mobile devices. The content of the page is in Russian so that is the most likely origin of the hackers. The visitor is immediately alerted that "Your version of Opera Mini browser is out of date, further work may not be correct and lead to unexpected errors and crashes! You need to urgently upgrade Opera Mini to version 6.1!" The java file that is downloaded was detected as being J2ME_FAKEBROWS.A. Upon execution, the virus checks if the mobile device uses specific

UNCLASSIFIED

UNCLASSIFIED

message service centers and if a match is found, it starts sending simple text messages to a phone number encoded in the data.res file. The string "424626 357 OX" is sent to specified premium numbers using the SMS service of the machine. Devices that support MIDlets are the ones vulnerable in front of this piece of malware. Source:

<http://news.softpedia.com/news/Mobile-Malware-Masqueraded-as-Opera-Mini-224863.shtml>

Symantec IM Manager multiple vulnerabilities. Multiple vulnerabilities have been reported in Symantec IM Manager, which can be exploited by malicious users to compromise a vulnerable system and by malicious people to conduct cross-site scripting attacks, according to Secunia. Input passed to the "refreshRateSetting" parameter in IMManager/Admin/IMAdminSystemDashboard.asp, "nav" and "menuItem" parameters in IMManager/Admin/IMAdminTOC_simple.asp, and "action" parameter in IMManager/Admin/IMAdminEdituser.asp is not properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a browser session in context of an affected site. Also, an input validation error exists within the Administrator Console. Successful exploitation of this vulnerability may allow execution of arbitrary code. The vulnerabilities are reported in version 8.4.17 and prior. Source: <http://www.net-security.org/secworld.php?id=11716>

Crazy square barcodes can point your phone to malware. Russian VXers have begun using QR codes as a launchpad for mobile malware. A recently identified malicious Quick Response code on a Russian Web site links through a series of redirections to a site punting a trojan version of the Jimm mobile ICQ client. Android users who follow the links and install the application will be infected with malware that sends text messages to premium-rate SMS numbers, net security firm Kaspersky warned. Source:

http://www.theregister.co.uk/2011/10/03/qr_code_mobile_malware_risk/

NATIONAL MONUMENTS AND ICONS

(District of Columbia) Washington Monument assessment to begin anew. Assessment of the earthquake-damaged Washington Monument were expected to begin anew October 3. Authorities halted inspections September 30 after wind gusts blew one of the roped-in workers off the monument, and moved him 30 feet away. In an earlier statement, the National Park Police said as the engineering team was finishing September 30, a climber, who works for the Difficult Access Team from Wiss, Janney, Elstner Associates, was lifted by wind and pushed from the west face of the monument to the south face. The team is assessing the exterior of the monument following damage from an 5.8 magnitude earthquake that shook much of the East Coast August 23. The park service said an interior assessment of the monument found it to be structurally sound and in no danger of collapse. The Difficult Access Team has mainly focused on the top of the monument, but will eventually rappel down the sides for a full inspection. Park service officials said they hoped the assessment would be finished by October 14, at which point they would have a better idea when the monument could be reopened to the public.

UNCLASSIFIED

UNCLASSIFIED

Source: http://articles.cnn.com/2011-10-03/us/us_washington-monument_1_washington-monument-assessment-magnitude-earthquake?_s=PM:US

(California) Sequoias falling in forest prompts closing of Trail of 100 Giants. Two giant Sequoia trees fell side by side October 1 in the Giant Sequoia National Monument, prompting the closure of the Trail of 100 Giants in the Sequoia National Forest in California. Sequoias in that area are 245 feet tall with 18-foot diameters, a U.S. Forest Service spokeswoman said. The mile-long, paved trail is a popular tourist spot that allows people to see the giant sequoias up close. She said there were no reports of any injuries, but Forest Service crews were on their way to the area to check, as well as to ensure nobody still was in the area. Because of concerns that the falling tree knocked loose branches and other heavy debris that could fall from the branches of the trees still standing, the trail was closed while officials assessed the risks.

Source: <http://www.visaliatimesdelta.com/article/20111003/NEWS01/110030305>

POSTAL AND SHIPPING

(Florida) Suspicious package probed on Biden brother's road. On October 1, the FBI investigated a suspicious package containing a powdery substance that was delivered to a home on a Florida street where the U.S. Vice President's brother lives in Ocean Ridge. Two residents of Ridge Boulevard were taken to the hospital as a precaution after the package was delivered to their home. It was not clear if the Vice President's brother was affected. The Boynton Beach Fire-Rescue spokesman said the Palm Beach County sheriff's bomb squad and the county fire-rescue hazardous materials team responded. The bomb squad determined the package was not explosive. The package was later taken to Miami for FBI lab testing. The spokesman said the U.S. Postal Service and Secret Service were also on the scene. The FBI issued a statement saying, "Preliminary tests indicate the contents of the package were deemed not to be threatening in nature." Source:

http://www.google.com/hostednews/ap/article/ALeqM5gl3tOU7DV8-i6mS_SU3Gp8k0zpFA?docId=b2dee8d5bf224168a6f20ba7d262d715

PUBLIC HEALTH

Medical identity theft a growing problem. According to a recent report on a nationwide survey of 600 executives from U.S. hospitals, doctors' organizations, health insurance companies, pharmaceutical manufacturers, and life sciences companies, accounting firm PricewaterhouseCoopers (PwC) found medical identity theft is the fastest-growing form of identity theft, affecting 1.42 million Americans in 2010, and costing more than \$28 billion. Theft accounted for 66 percent of the publicly reported security breaches documented since 2009, which included stolen laptops, stolen smart phones, using patient data to submit fraudulent claims, and people seeking medical care in another person's name. The single most commonly reported breach in the security of patients' private health information was improper use of patient data by a person who works for a doctor's office, hospital, insurance company, or life sciences organization. The breaches ranged from an employee leaving private documents out in plain sight, to making improper comments on Facebook, or even talking in the elevator about a

UNCLASSIFIED

UNCLASSIFIED

person's protected health information. Nearly four out of 10 doctors and hospitals surveyed have caught a patient trying to use someone else's identity to obtain healthcare services. Patients seeking medical services under someone else's name was the second most common privacy or security issue reported by healthcare providers. Rounding out the top three most common breaches was improper transfer of files containing personal health data to people who were not authorized to view the information. One in four insurers reported improperly transferring files that contained protected health information. Source: <http://www.medpagetoday.com/PracticeManagement/InformationTechnology/28696>

TRANSPORTATION

Nothing Significant to Report

WATER AND DAMS

Chemical-munching mussels contaminating Great Lakes. Zebra mussels from the Caspian Sea, introduced to North America by accident, are becoming a veritable plague releasing toxic chemicals into the Great Lakes, Canadian biologists said, according to PhysOrg.com October 1. The mussels hitch-hiked to Canada on the ballasts of cargo ships arriving on the continent in 1986. And in the past two decades, the thumbnail-sized creatures have spread and are found in more than a third of the Great Lakes. The mussels are sucking on toxic polychlorinated biphenyls (PCBs) trapped in the lakes' sediment and releasing the chemicals into the freshwaters, a biologist at Queens University in Kingston, Ontario told Agence France-Presse. The concern is the mussels are releasing PCBs that had been trapped in sediment for decades in waters where they are then absorbed by algae and other animals up the food chain until they eventually reach fish eaten by humans. Health Canada said small amounts of PCBs are unlikely to cause adverse health effects. But an accumulation of the chemicals in the body can lead to problems of the nervous system, and liver and kidney cancer. The mussels blanket vast areas in clusters, interfering with and even suffocating indigenous mollusks and crustaceans, and cause billions of dollars in infrastructure damage. Source: <http://www.physorg.com/news/2011-10-chemical-munching-mussels-contaminating-great-lakes.html>

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

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