

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**

**OSHA cites oil well for violations.** A Wyoming-based oil company is facing over \$65,000 in fines from the U.S Department of Labor's Occupational Safety and Health Administration (OSHA) for safety violations in an oil field near Ray, North Dakota, KFVR 5 Bismarck reported April 10. According to an OSHA release, Cyclone Drilling, based out of Gillette, Wyoming, was cited with two repeat, five serious, and one other than serious violation of safety and health standards for exposing workers on an oil drilling rig to electrical, fire, and fall hazards, among others. Source: [http://www.kfyrtv.com/News\\_Stories.asp?news=56364](http://www.kfyrtv.com/News_Stories.asp?news=56364)

## **REGIONAL**

**Dry spring frees reservoir space.** The U.S. Army Corps of Engineers said drier-than-normal weather has helped keep space free for floodwaters in the reservoirs along the Missouri River this spring. The Corps said April 6 nearly all of the 16.3 million acre-feet of the planned storage space for floodwater remains free because March was so dry. In 2011, late spring rains combined with heavy snowpack to force the release of massive amounts of water from the dams and record flooding along the 2,300-mile-long river. Source: <http://www.columbiatribune.com/news/2012/apr/06/dry-spring-frees-reservoir-space/>

**(Montana) Better spill plan eyed by Exxon, agencies.** State and federal officials said Exxon Mobil Corp. is working with government agencies on a plan to speed up the response to oil spills along Montana's upper Yellowstone River, after a major spill in 2011 left local officials scrambling to deal with an ill-defined threat, the Great Falls Tribune reported April 6. The goal is to provide enough training and resources to take action on major pipeline, refinery, or railway spills within 24 hours, or before outside help can arrive. Exxon would pay to plan and possibly equip the stepped-up response under a settlement with the state over pollution violations from its July 2011 pipeline break near Laurel. The effort is in the early stages and the company has not yet submitted a formal proposal. State approval is needed for the work to count toward Exxon's remaining \$1.3 million obligation under the settlement. The company's 12-inch Silvertip pipeline broke beneath the Yellowstone River in July 2011, releasing about 63,000 gallons of oil. Less than 1 percent of the oil that spilled was recovered during a cleanup that cost an estimated \$135 million after pipeline repairs were factored in. Source: <http://www.greatfallstribune.com/article/20120407/NEWS01/204070302/Better-spill-plan-eyed-by-Exxon-agencies?odyssey=tab|topnews|text|Frontpage>

## **NATIONAL**

**European court OKs extradition to U.S. of five terrorism suspects.** A man who celebrated the September 11th attacks in sermons and allegedly tried to set up a terrorist training camp in Oregon can be extradited to the United States from Britain, the European Court of Human Rights ruled April 10. The court said the man and four other terrorism suspects, including two accused of involvement in the 1998 bombings of U.S. embassies in Kenya and Tanzania that killed hundreds and wounded thousands, could be sent to face trial in the United States

## UNCLASSIFIED

without fear that they would face “inhuman and degrading” conditions in a maximum-security prison if convicted. The men had argued that they could be subject to solitary confinement for the rest of their lives in a “supermax” prison in Colorado where many terrorism convicts are serving time. The suspects have 3 months to appeal the decision to the European court’s grand chamber, but such appeals are rarely taken up. U.S. authorities want the man extradited to face allegations he tried to set up a training camp in Bly, Oregon, for would-be insurgents in Afghanistan, and that he was involved in the kidnapping of a group of Western tourists in Yemen in 1998. The other suspects covered by the European court ruling included one of the man’s alleged conspirators in trying to establish the Oregon terrorist training camp. Source: [http://latimesblogs.latimes.com/world\\_now/2012/04/european-court-rules-on-extradition-of-cleric.html](http://latimesblogs.latimes.com/world_now/2012/04/european-court-rules-on-extradition-of-cleric.html)

**Botulism worries spur recall of fish, not yet gutted, sold in Twin Cities.** Minnesota state authorities are warning consumers about a threat to their health involving many hundreds of pounds of fish that have yet to be gutted being sold at ethnic grocery outlets in the Twin Cities, as well as elsewhere in the Upper Midwest. The Minnesota Department of Agriculture said April 10, more than 1,500 pounds of dried, uneviscerated fish are being recalled because of a “high risk” the food is contaminated with a botulism-producing bacteria. While no illnesses were reported in connection with the recall, consumers were advised to throw away any dried, uneviscerated fish they may have bought. Import Foods Wholesale Inc., of St. Paul, was cooperating with the recall of smoked croaker, barracuda, big eye, and red snapper that originated from Guyana in South America. Seng Ong Wholesale Inc., also of St. Paul, was cooperating as well and recalling dried mackerel and round scad. State agriculture officials were working with the U.S. Food and Drug Administration to determine additional product origins and distribution channels. Import Foods sold its fish in 10-pound boxes in Minnesota, North Dakota, South Dakota, and Iowa. Source: <http://www.startribune.com/local/146966635.html>

**Federal study ties fracking to earthquakes.** A new study from the U.S. Geological Survey (USGS) suggests oil and gas production may explain a sharp increase in small earthquakes in the nation’s midsection, the Associated Press reported April 9. The rate has jumped six-fold from the late 20th century through 2011, the team reports, and the changes are “almost certainly man-made.” The study said a relatively mild increase starting in 2001 comes from increased quake activity in a methane production area along the state line between Colorado and New Mexico. The increase began about the time that methane production began there, so there is a “clear possibility” of a link, said the lead author of the study. The increase over the nation’s midsection has gotten steeper since 2009, due to more quakes in a variety of oil and gas production areas, including some in Arkansas and Oklahoma, the researchers say. It is not clear how the earthquake rates might be related to oil and gas production, the study authors indicated. They note others have linked earthquakes to injecting huge amounts of leftover wastewater deep into the earth. Source: <http://www.theintelligencer.net/page/content.detail/id/568353/Federal-Study-Ties-Fracking-to-Earthquakes.html?nav=515>

UNCLASSIFIED

## **INTERNATIONAL**

**Gendarmes seize smuggled radioactive substance in Ankara.** Teams from a Turkish anti-smuggling unit seized two glass tubes containing 500 grams of Cesium-137, a radioactive isotope of cesium, which they suspected was smuggled to Turkey from Russia through Georgia, Today's Zaman reported April 11. The teams acted after a tip-off that radioactive substances had been brought into Turkey from Georgia by means of a car with a German license plate. Upon searching the car, they found the Cesium-137 as well as an unlicensed gun and 18 coins thought to have historical value. Three people in the car, all Turkish nationals living in Germany, were detained. Sources said they all had prior charges related to smuggling on their criminal records. Cesium-137, the most common radioactive form of the metal cesium, is commonly used for the treatment of cancer and in a variety of gauges in the construction and drilling industries, but it can be used in nuclear weapon production as well. The half-life of cesium-137 is 30 years. Source: <http://www.todayszaman.com/news-277106-gendarmes-seize-smuggled-radioactive-substance-in-ankara.html>

## **BANKING AND FINANCE INDUSTRY**

**HSBC customers under phishing attack.** Customers of HSBC, one of the largest banking and financial services organizations in the world, are being targeted with a fake warning of account suspension, Help Net Security reported April 12. The e-mail claims someone tried to access the user's account and failed, and that the bank suspended the account to protect the customer. Unfortunately, the offered link takes the victims to a phishing site made to look like the bank's legitimate Internet banking log-in page, where they are asked to input their user ID, name, date of birth, Social Security number, sort code, account number, and ATM PIN code to prove their identity. Once the information is submitted by pressing on the "Continue" button, it is immediately sent to the phishers and the victims are redirected to the bank's legitimate page. Source: <http://www.net-security.org/secworld.php?id=12739&utm>

**U.S. SEC sues AutoChina for securities fraud.** U.S. securities regulators sued AutoChina International Ltd, its executives, and others for securities fraud April 11. The U.S. Securities and Exchange Commission (SEC) said the company's employees, board members, and other Chinese citizens unlawfully bought and sold AutoChina stock to boost its trading volume as the company sought loans. AutoChina, which is based in China and owns and operates a commercial vehicle leasing business there, traded its shares on the NASDAQ stock market until October 2011. Its listing was suspended for failing to file required documents with the SEC. The defendants opened brokerage accounts beginning in October 2010, deposited some \$60 million in the accounts, and bought and sold millions of shares of AutoChina stock, the SEC said. The lawsuit comes as the SEC steps up its inquiries into Chinese companies whose shares trade in the United States for accounting violations and other misconduct. The SEC lawsuit, filed in federal court in Massachusetts, is seeking civil penalties and other sanctions. Source: <http://www.reuters.com/article/2012/04/11/sec-autochina-idUSL2E8FB75S20120411>

## UNCLASSIFIED

**New Zeus-based trojan leeches cash from cloud-based payrolls.** Cybercrooks have forged a Zeus-based trojan that targets cloud-based payroll service providers. A new attack, detected by transaction security firm Trusteer, shows crooks are going up the food chain. Researchers captured a Zeus configuration that targets Ceridian, a Canadian human resources and payroll services provider. The trojan works by capturing a screenshot of the payroll services Web page when a malware-infected PC visits the site. This data is uploaded, allowing crooks to obtain user ID, password, company number, and the icon selected by the user for the image-based authentication system – enough information to siphon funds from compromised accounts into those controlled by money mules. Trusteer thinks crooks are targeting the small cloud service provider to get around the tougher problem of how to bypass industrial strength security controls typically maintained by larger businesses. Cloud services can be accessed using unmanaged devices that are typically less secure and more vulnerable to infection by Zeus-style financial malware. Source:

[http://www.theregister.co.uk/2012/04/11/zeus\\_based\\_trojan\\_targets\\_payrolls/](http://www.theregister.co.uk/2012/04/11/zeus_based_trojan_targets_payrolls/)

### **CHEMICAL AND HAZARDOUS MATERIALS SECTOR**

**EPA rejects petition to ban 2,4-D weed killer.** An environmental group's petition to ban the widely used herbicide 2,4-D was rejected by the U.S. Environmental Protection Agency (EPA), HealthDay reported April 10. The agency said the petition from the Natural Resources Defense Council (NRDC) did not adequately show 2,4-D was harmful under the conditions in which it is used, the New York Times reported. The herbicide, first approved in the late 1940s, is one of the most widely used weed killers in the world. It is used by farmers and is an ingredient in many home lawn-care products. In its petition, the NRDC cited studies suggesting that exposure to 2,4-D could cause problems such as cancer, genetic mutations, and hormone disruption, the Times reported. While some of the studies did suggest high doses of the herbicide could be harmful, they did not establish lack of safety, the EPA said in its ruling. Source:

<http://health.usnews.com/health-news/news/articles/2012/04/10/health-highlights-april-10-2012>

### **COMMERCIAL FACILITIES**

**(New York) Novelty grenade prompts bomb scare near New York's 'Ground Zero'.** A novelty hand grenade briefly prompted the evacuation of one of the buildings near the site where New York City's World Trade Center towers stood until they were brought down in the September 11th attacks, police said April 12. The evacuation of 2 World Financial Center in Manhattan was triggered around 11 a.m. after an X-ray of a package at the building appeared to reveal an explosive device inside, a New York City Police Department (NYPD) spokesman said. It was actually a novelty hand grenade on a plaque that read "complaint department, pull the pin" that had been sent to one of the tenants, Nomura Holdings, the NYPD spokesman said. Police have given the all-clear, allowing employees to return to the building, which houses a number of financial services firms. Source: <http://www.reuters.com/article/2012/04/12/us-usa-newyork-wtc-idUSBRE83B11O20120412>

UNCLASSIFIED

## UNCLASSIFIED

**(Nevada) NTSB releases recommendations for air races.** Air race pilots should take their modified aircraft on a dry run before participating in certain types of competitions and should possibly wear flight suits to help them withstand high gravitational forces, the National Transportation Safety Board (NTSB) said April 10. The recommendations were among seven the board offered during a news conference in Reno, Nevada, nearly 6 months after a crash at the Reno National Championship Air Races that killed 11 people and seriously injured more than 70 spectators. The NTSB also called on the Federal Aviation Administration (FAA) to correct what it said were numerous errors and discrepancies in its guidance for race course designs, including the distance that spectators should be from the edge of the course. The FAA said it was already acting on the NTSB recommendation. Source: <http://www.businessweek.com/ap/2012-04/D9U28GT80.htm>

**(Virginia) Navy begins compensation after crash.** The U.S. Navy was scheduled to begin cutting compensation checks April 9 to victims of a fiery crash of a fighter jet into apartment buildings in Virginia Beach, Virginia, April 6. Initial payments will begin at \$2,300 per person to cover immediate needs, such as housing, meals, and clothing. The F/A-18 fighter jet experienced a “catastrophic mechanical malfunction” during takeoff, raining jet fuel over Virginia Beach before plunging to the ground, damaging five apartment buildings, according to residents and Navy officials. The jet carried a student pilot in the front seat and an experienced instructor behind him, and the leakage of fuel was “one of the indications that there was a mechanical malfunction,” a Navy captain said. The two pilots, a Virginia Beach police officer, an EMS volunteer, and three other people were treated for injuries at the hospital. The jet, which was not carrying live ordnance, was part of a training squadron at Naval Air Station Oceana, the Navy and Federal Aviation Administration said. It crashed 2.2 miles from the runway, a senior Defense Department official told CNN. Source: <http://www.cnn.com/2012/04/09/us/virginia-plane-crash/>

## **COMMUNICATIONS SECTOR**

**ICANN postpones cutoff date for new gTLD applications after glitch.** The Internet Corporation for Assigned Names and Numbers (ICANN) has postponed the last date for applications for new generic top-level domains (gTLDs) on its application system to April 20, after it detected a technical issue with the software. The organization said in a statement that it had to take the TLD application system (TAS) offline temporarily after it learned of a possible glitch in the software that has allowed “a limited number of users to view some other users’ file names and user names in certain scenarios. Out of an abundance of caution, we took the system offline to protect applicant data. We are examining how this issue occurred and considering appropriate steps forward,” ICANN’s chief operating officer said in a statement April 12. TAS will be shut down until April 17, unless otherwise notified before that time, the ICANN said. Source: <http://www.networkworld.com/news/2012/041312-icann-postpones-cutoff-date-for-258247.html?hpg1=bn>

**Fake Verizon emails contain malicious links.** An e-mail that fraudulently claims to come from Verizon Wireless is making the rounds in Wisconsin and could lead to a serious breach of data

UNCLASSIFIED

## UNCLASSIFIED

for consumers who click the links in its text, Agri-view reported April 6. The fake Verizon Wireless account e-mail has been sent to citizens and to businesses. The sender, subject, graphics, and text are nearly identical to an actual Verizon message. The scam e-mail claims the recipient owes a large amount of money on a Verizon account — current versions say more than \$900. When a person clicks any of the links in the e-mail to learn more, they may unintentionally download malicious software onto the computer or be driven to a site that will harvest personal information. Verizon Wireless notes on its Web site that the company does not send e-mail notices asking for customer payment information, usernames, or passwords used to manage accounts. Source: [http://www.agriview.com/news/regional/fake-verizon-emails-contain-malicious-links/article\\_0c48ab8a-7ff4-11e1-9190-001a4bcf887a.html](http://www.agriview.com/news/regional/fake-verizon-emails-contain-malicious-links/article_0c48ab8a-7ff4-11e1-9190-001a4bcf887a.html)

### **CRITICAL MANUFACTURING**

**Anonymous hackers attack Boeing website to protest CISPA; Is Microsoft next?** Boeing's Web site was the target of an attack staged by the hacking collective Anonymous, April 10, part of a widespread hacktivism campaign against companies and trade groups that support the Cyber Intelligence Sharing and Protection Act (CISPA). The Twitter account @YourAnonNews posted April 10 announcing that Boeing.com was down as part of Anonymous' "OpDefense" campaign. Boeing's Web site was reportedly offline for about 3 hours, and still was not working properly as of early April 11. Anonymous also managed to take down the Web sites of TechAmerica and USTelecom, tech industry trade groups that have lobbied in favor of CISPA. Source: [http://blogs.seattleweekly.com/dailyweekly/2012/04/anonymous\\_hackers\\_attack\\_boein.php](http://blogs.seattleweekly.com/dailyweekly/2012/04/anonymous_hackers_attack_boein.php)

**NHTSA recall notice - Buick Enclave, Chevrolet Traverse, and GMC Acadia windshield wiper linkages.** General Motors (GM), April 12 announced the recall of 50,001 model year 2011-2012 Chevrolet Traverse, Buick Enclave, and GMC Acadia vehicles currently registered in 28 states and the District of Columbia. If snow or ice buildup on the windshield or on the wiper restricts the movement of the wiper arm, the wiper arm may loosen and cause the wiper to become inoperative. If this occurs, driver visibility could be reduced, increasing the risk of a crash. GM will notify owners, and dealers will tighten the wiper arm nuts. Source: [http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl\\_ID=12V151000&summary=true&prod\\_id=971774&PrintVersion=YES](http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V151000&summary=true&prod_id=971774&PrintVersion=YES)

**Ford recalls more than 140,000 Focus cars in U.S.** According to U.S. safety regulators, Ford Motor Co. is recalling 140,310 Focus cars from model year 2012 in the United States to repair a potential problem with the passenger-side windshield wiper motor, Reuters reported April 9. A seal plug in the wiper motor electrical connector may be missing, allowing water into the motor's electrical connection, according to documents filed with the National Highway Traffic Safety Administration (NHTSA). That could result in an inoperative wiper, reducing visibility and increasing the risk of a crash. Owners will be notified the week of May 21, and the wiper motor connector will be cleaned and sealed as needed, the NHTSA said. In separate NHTSA documents, Chrysler, which is controlled by Fiat, is recalling 1,689 2012 model Jeep Patriot and Compass sport utility vehicles that may have been built with a fuel tank assembly containing a damaged rollover valve. In an accident or rollover, fuel could leak and increase the risk of a fire,

UNCLASSIFIED

## UNCLASSIFIED

the NHTSA said. Chrysler said in an NHTSA filing that it was not aware of any accidents, leaks, fires, or injuries related to the issue. The recall is expected to begin by June. Source:

<http://www.reuters.com/article/2012/04/09/us-ford-usrecall-idUSBRE8380BD20120409>

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

Nothing Significant to Report

### **EMERGENCY SERVICES**

**(Massachusetts) Police officers, ambulance crew taken to hospital after toxic suicide in South End.** Twelve people were evacuated from an apartment building in the South End area of Boston, and four police officers and an ambulance crew were taken to a hospital after a woman committed suicide April 9 inside an apartment by ingesting a toxic chemical, fire officials said. The Boston deputy fire chief said at the HAZMAT scene that the woman ingested the chemical on the first floor and was later pronounced dead at the hospital. He said four police officers and the ambulance team of two EMS workers were quarantined at the hospital to determine whether they were affected by the substance. He said the woman is believed to have ingested sodium azide, a chemical used to make airbags. "But it can metabolize into some kind of cyanide," he said. He said April 10 crews were preparing to reenter the apartment building to see if it presented a safety risk, a process expected to take a few hours. He also said the officers and EMS workers who were quarantined did not appear to be showing signs of being adversely affected by the chemical. Source: <http://www.boston.com/Boston/metrodesk/2012/04/police-officers-ambulance-crew-taken-hospital-after-suicide-sparks-hazmat-scene-south-end/da0IFfoxlNkIAWwHXzJ9TK/index.html>

**U.S. to offer anthrax vaccine to first responders on trial basis.** The U.S. Presidential administration is preparing to make unused federal stocks of anthrax vaccine available to certain nonmilitary emergency personnel in a trial effort that could lead to wider distribution of the countermeasure to first responders. The initiative would offer certain state and local officials the option to accept a federally funded course of anthrax vaccination doses and would consider broader distribution in part through demand from individual response personnel, senior medical officials with the Homeland Security Department and the Centers for Disease Control and Prevention told Global Security Newswire April 6. The program would draw from inventory that is within months of expiration in the U.S. Strategic National Stockpile of medical countermeasures. The federal government formally deems stockpiled anthrax vaccine to be unusable once it ages beyond its 4-year shelf life, but officials have not ruled out the possibility that some lapsed material could remain sufficiently potent to distribute to the public if a shortage of unexpired stocks develops following an outbreak. Source:

<http://www.nti.org/gsn/article/us-offer-anthrax-vaccine-first-responders-trial-basis/>

UNCLASSIFIED

## **ENERGY**

**DOJ, EPA reach refining flare gas settlement with Marathon.** Marathon Petroleum Corp. has reached an agreement with the U.S. Department of Justice (DOJ) and Environmental Protection Agency (EPA) after developing and installing equipment to cap waste gases at its refinery flares, Oil & Gas Journal reported April 9. They said the Findlay, Ohio, refining and marketing company spent more than \$45 million to develop the equipment for use at its 6 refineries' 22 flares, but expects to save \$5 million per year from reduced steam use and product recovery while cutting air pollution by 5,400 tons per year. The DOJ and EPA said that Marathon, under EPA direction and oversight, spent more than \$2.4 million to develop and conduct pioneering combustion efficiency testing of flares and to advance the understanding of the relationship between flare operating parameters and flare combustion efficiency. Beginning in 2009, they added, Marathon installed flow monitors, gas chromatographs, and other equipment to improve combustion efficiency. Marathon also agreed to pay a \$460,000 fine under a consent decree filed in federal court, the DOJ and EPA said. The decree is subject to a 30-day comment period and court approval before it becomes final. Source: <http://www.ogj.com/articles/2012/04/doj-epa-reach-refining-flare-gas-settlement-with-marathon.html>

**Refinery closures risk Northeast gas price spike.** While gas prices soar to record levels, many U.S. refineries that make and sell gasoline are going broke. Nearly 50 percent of the refining capacity on the East Coast has either shut down or may shut down within the next few months, CNNMoney reported April 10. If gas shortages develop due to the closed refineries, East Coast drivers could face higher prices than they otherwise would later in 2012. Sunoco, which closed its Philadelphia-area Marcus Hook refinery in December and is trying to sell another facility nearby, said its refining businesses has been losing \$1 million dollars a day for 3 years running. In fall 2010, ConocoPhillips closed its Trainer refinery, also in the Philadelphia area. If all three refineries were closed, that would leave just six operating refineries in the northeast. The refineries are losing money because they are old and cannot process the cheaper, heavier types of oil that are increasingly in supply from Canada's oil sands, Saudi Arabia, Venezuela, and elsewhere. Source: [http://money.cnn.com/2012/04/10/news/economy/refineries-gas-prices/?source=cnn\\_bin](http://money.cnn.com/2012/04/10/news/economy/refineries-gas-prices/?source=cnn_bin)

**Industry insiders: Insufficient security controls for smart meters.** False data injection attacks exploit the configuration of power grids by introducing arbitrary errors into state variables while bypassing existing techniques for bad measurement detection; experts say the current generation of smart meters are not secure enough against false data injection attacks, Homeland Security Newswire reported April 10. nCircle recently announced results of a survey of 104 energy security professionals. The survey was sponsored by nCircle and EnergySec, a Department of Energy-funded public-private partnership that works to enhance cyber security of electric infrastructure. The online survey was conducted March 12 to 31. When asked, "Do smart meter installations have sufficient security controls to protect against false data injection?" 61 percent of respondents said "no." Source: <http://www.homelandsecuritynewswire.com/dr20120410-industry-insiders-insufficient-security-controls-for-smart-meters>

## UNCLASSIFIED

**MSHA publishes final rule on examinations in underground coal mines.** The U.S. Department of Labor's Mine Safety and Health Administration (MSHA) recently published the final rule "Examinations of Work Areas in Underground Coal Mines for Violations of Mandatory Health or Safety Standards," Occupational Health & Safety reported April 9. The rule is geared to enhance miners' health and safety by requiring mine operators to identify and correct hazardous conditions and violations of nine health and safety standards that pose the greatest risk to miners, including the kinds of conditions that led to the April 2010 explosion at the Upper Big Branch Mine in Montcoal, West Virginia that killed 29 miners. The nine standards address ventilation, methane, roof control, combustible materials, rock dust, and equipment guarding. They are consistent with guidance emphasized in the MSHA's "Rules to Live By" initiative, and the types of violations cited in the agency's report on the Upper Big Branch Mine explosion as contributing to the cause of that deadly accident. Source:

<http://ohsonline.com/articles/2012/04/09/msha-publishes-final-rule-on-examinations-in-underground-coal-mines.aspx?admgarea=news>

## **FOOD AND AGRICULTURE**

**Drought expands throughout USA.** The United States has not been as dry as it is now in almost 5 years, USA Today reported April 12. Still reeling from devastating drought in 2011 that led to at least \$10 billion in agricultural losses across Texas and the South, the nation is enduring another unusually parched year. A mostly dry, mild winter put nearly 61 percent of the lower 48 states in "abnormally dry" or drought conditions, according to the U.S. Drought Monitor, a weekly federal tracking of drought. That is the highest percentage of dry or drought conditions since September 2007. Only two states — Ohio and Alaska — are entirely free of abnormally dry or drought conditions. The drought is expanding into some areas where dryness is rare. According to the U.S. Geological Survey, stream levels are at near-record or record lows in much of New England. The Drought Monitor lists all of Vermont as "abnormally dry," just 6 months after the state's wettest August on record that stemmed mainly from disastrous flooding by the remnants of Hurricane Irene. The rest of the East is also very dry. More than 63 percent of Georgia is in the worst two levels of drought, the highest percentage of any state. Wildfires and brush fires have been common along the East Coast from New England to Florida in recent weeks. Trouble also looms for water-dependent California. The state department of water resources announced the week of April 2 that water content in California's mountain snowpack is 45 percent below normal. Source:

<http://www.usatoday.com/weather/drought/story/2012-04-11/mild-winter-expands-usa-drought/54225018/1>

**Outbreak potentially linked to sushi expands to 116 cases.** A multistate outbreak of Salmonella Bareilly that previously sickened 100 expanded to include at least 116 victims across 20 states, according to new data from the Centers for Disease Control and Prevention (CDC). In this latest outbreak report, released April 11, CDC reported, "The investigation has not conclusively identified a food source," however evidence suggests sushi may be the contaminated product. Cases are largely centered in states on the Eastern Seaboard and the Gulf of Mexico, but also

UNCLASSIFIED

## UNCLASSIFIED

extend to the Midwest. The number of sickened individuals in each state is as follows: Alabama (2), Arkansas (1), Connecticut (5), District of Columbia (2), Florida (1), Georgia (5), Illinois (10), Louisiana (2), Maryland (11), Massachusetts (8), Mississippi (1), Missouri (2), New Jersey (7), New York (24), North Carolina (2), Pennsylvania (5), Rhode Island (5), South Carolina (3), Texas (3), Virginia (5), and Wisconsin (12). Among those infected, 12 are reported to have been hospitalized. Illnesses related to the outbreak were first reported January 28, and current case counts are accurate as of March 31. Source: <http://www.foodsafetynews.com/2012/04/more-victims-in-outbreak-potentially-linked-to-sushi/>

**(Wisconsin; Iowa; Minnesota) Allergen alert: Donuts with traces of egg.** Kwik Trip of La Crosse, Wisconsin, is recalling certain Glazers Donuts because they may contain undeclared traces of egg, Food Safety News reported April 10. The recall was initiated after it was discovered that the company's supplier had added egg to a key ingredient. The company said the problem has been corrected. The recalled Glazers Donuts were sold in Iowa, Minnesota, and Wisconsin. Source: <http://www.foodsafetynews.com/2012/04/allergen-alert-donuts-with-traces-of-egg-1/>

**Diamond Naturals Lamb Meal & Rice dog food may contain Salmonella.** Diamond Pet Foods is recalling its Diamond Naturals Lamb Meal & Rice because it may be contaminated with Salmonella. According to a recall notice posted by the company April 6, the recalled dry dog food was distributed to customers in Alabama, Florida, Georgia, Kentucky, Maryland, Michigan, New York, North Carolina, Ohio, Pennsylvania, South Carolina, and Virginia. However, it then could have been further distributed to other states, through pet food channels. Handling contaminated dry pet food can cause humans to become infected with Salmonella, especially if they have not thoroughly washed their hands after having contact with surfaces exposed to the product. Source: <http://www.foodsafetynews.com/2012/04/diamond-naturals-lamb-meal-rice-dog-food-may-contain-salmonella/>

**Beef recalled for Salmonella in Canada.** The Canadian Food Inspection Agency (CFIA) issued a joint announcement with Intercity Packers (East) Ltd. April 7, warning the public, distributors, and food service establishments in Canada to avoid consuming, selling, serving, or using beef burger meat mix produced by Integrity Packers due to potential Salmonella contamination. The warning comes on the heels of a Salmonella outbreak in Ottawa and southern Ontario. Public health partners from CFIA, Health Canada and the Public Health Agency of Canada are investigating the outbreak, which may have been caused by Intercity Beef. The product has been distributed to public and commercial food establishments in Ontario and Newfoundland, and possibly retailers in Newfoundland. Source: <http://www.foodsafetynews.com/2012/04/beef-recalled-for-salmonella-in-canada/>

**Allergen alert: MSG in steamed pork buns.** Quality Food Distributor of Las Vegas is recalling about 50,820 pounds of Steamed BBQ Flavored Pork Buns because they contain monosodium glutamate (MSG), which is not declared on the label, the U.S. Department of Agriculture's Food Safety and Inspection Service said in a news release, Food Safety News reported April 9. During a label review and routine food safety assessment, FSIS personnel determined the MSG was used in marinade used during the cooking process and was left off the label of the final product.

UNCLASSIFIED

## UNCLASSIFIED

This product was produced April 4 and 5, 2011 and was sold to a distributor in Las Vegas. This product may have been further distributed to restaurants. Source:

<http://www.foodsafetynews.com/2012/04/allergen-alert-msg-in-steamed-pork-buns/>

**Some Planters cocktail peanuts recalled.** Kraft Foods Group, Inc. is recalling about 3,000 cases of Planters Cocktail Peanuts because there is a possibility the product was exposed to water not intended for use in food during the production process, Food Safety News reported April 9. Consumers who purchased the affected code date of this product should not eat them, according to the Kraft Foods news release. The recall is for nuts sold in 12-ounce canisters.

About 3,000 cases of the recalled peanuts, which were processed at the Kraft Foods facility in Suffolk, Virginia, were shipped to retail customers across the United States and Puerto Rico.

Source: <http://www.foodsafetynews.com/2012/04/some-planters-cocktail-peanuts-recalled/>

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

**Oak Ridge team using advanced machine learning to counter cyber threats.** Oak Ridge National Lab in Oak Ridge, Tennessee, is developing many cybersecurity tools that use advanced machine learning to counter cyber threats, Government Computer News reported April 12. One tool under development looks for data being sent from inside an enterprise by insiders, leveraging data from each host on the network to identify bad behavior. The lab was the victim of one of the most notable breaches of 2011, after which it was offline for more than a week. A successful phishing attack infected its network with what a spokesperson called a “very sophisticated” piece of malware apparently designed to steal information from the lab’s network. E-mail and Internet access at the lab were shut down until the infection could be identified and removed. Source: <http://gcn.com/articles/2012/05/07/feature-1-oak-ridge-big-security-sidebar.aspx>

**(Alaska) 2 dead in shooting at Alaska station; FBI on scene.** Two U.S. Coast Guard members were found shot to death at work in Kodiak Island, Alaska, in what officials said appeared to be a double homicide. Another Coast Guard member found the victims April 12 at their work areas inside the communications station, a spokeswoman said. She said officials believed a third person was involved, but no suspect was in custody or identified as of April 12. A captain said he was not aware of any threats or anything else that might have indicated problems at the station. After the shooting, security was increased at the base, about 8 miles from the island’s largest city of Kodiak. Added security also was put in place at an adjacent school. A petty officer said the station has “secure front doors,” and requires staff and visitors to show identification. The spokeswoman said visitors and those not actually working at the station are usually provided escorts. Source: <http://www.foxnews.com/us/2012/04/13/2-dead-in-shooting-at-alaska-station-fbi-on-scene/>

**IG report finds flaws in VA’s information security program.** An inspector general audit revealed that the Department of Veterans Affairs (VA) failure to fully comply with the Federal

UNCLASSIFIED

## UNCLASSIFIED

Information Security Management Act (FISMA) resulted in more than 15,000 outstanding security risks, Federal Computer Week reported April 6. The fiscal year 2011 performance audit examined the extent to which VA's information security program complied with FISMA requirements and National Institute for Standards and Technology guidelines. Substantial inadequacies were discovered in areas related to access controls, configuration management controls, continuous monitoring, and services continuity practices. Also, VA has not effectively implemented procedures to identify and correct system security flaws on network devices, database and server platforms, and Web applications. Deficiencies were also found in reporting, managing, and closing plans of action and milestones. The report accentuated a larger compliance issue government-wide. A March 7 review by the Office of Management and Budget showed that only 7 out of 24 agencies are more than 90 percent compliant with FISMA directives. Source: <http://fcw.com/articles/2012/04/06/fisma-compliance-va-failure.aspx>

**FCC move to disable stolen smartphones won't stop government data thieves.** A new nationwide system for shutting off stolen smartphones announced April 10 might stop scammers from reselling government devices, but it would not necessarily protect the sensitive data inside, some information security experts said. The wireless industry agreed to, within 6 months, block service on portable electronics when users report them to police as stolen, a Federal Communications Commission (FCC) chairman and law enforcement officials said April 10. The companies also are working to create, within 18 months, a single database containing the identification numbers of stolen devices worldwide so that thieves cannot swap carriers to avoid detection. The Veterans Affairs Department, the largest federal agency, reported that only 55 percent of its portable electronics inventory — including smartphones, tablets, and laptops — was protected with a standard encryption format called Federal Information Processing Standards 140-2; NASA ranked at the bottom with a 41 percent protection rate; and DHS, reported 75 percent of its devices were encrypted. Most agencies reported encrypting at least 80 percent of their mobile devices, including 100 percent fully encrypted inventories at the State and Treasury departments, and the General Services Administration and Social Security Administration. AT&T, T-Mobile, Verizon, and Sprint, the carriers that cover 90 percent of U.S. subscribers, have committed to participate in the phone-disabling database, FCC officials said. Source: [http://www.nextgov.com/nextgov/ng\\_20120410\\_5674.php](http://www.nextgov.com/nextgov/ng_20120410_5674.php)

**State-sponsored cyber spies want your Facebook status, researchers say.** According to security researchers, Facebook frequently takes flack for privacy invasions, but the next controversial byproduct of the social network may be cyber espionage, Nextgov reported April 9. Status updates on Facebook posted by friends and family of government officials or the officials' own unencrypted Facebook activities can be used to gather intelligence such as U.S. troop movements, said the security strategy director for cybersecurity firm Imperva. While data brokers profit by collating social communications for advertisers, spies and hackers on government payrolls can profit by parsing the same information. Government-sponsored hackers and spies may use tactics such as eavesdropping on a Facebook member's activities through unencrypted Wi-Fi connections. Facebook uses a secure connection to read users' log-in credentials but all other data is sent back and forth in an unprotected format. Responding to this potential vulnerability, Facebook in January allowed users to opt into a setting that secures

UNCLASSIFIED

## UNCLASSIFIED

all Facebook activities. Imperva recommends users enable that option. Source:

[http://www.nextgov.com/nextgov/ng\\_20120409\\_3435.php](http://www.nextgov.com/nextgov/ng_20120409_3435.php)

**(Georgia) 2 suspects plead guilty in Georgia militia plot.** Two Georgia men pleaded guilty to conspiring to get an unregistered explosive and an illegal gun silencer in what prosecutors describe as a plot to attack government targets. The suspected ringleader of the group and another man entered their pleas April 10 in federal court in Gainesville, about 55 miles northeast of Atlanta. They could face up to 5 years in prison and a \$250,000 fine. They also agreed to cooperate with authorities. They are among four men arrested in November 2011. Source: [http://www.wgme.com/template/inews\\_wire/wires.national/3242bd64-www.wgme.com.shtml](http://www.wgme.com/template/inews_wire/wires.national/3242bd64-www.wgme.com.shtml)

**(Pennsylvania) Pitt empties 3 more buildings for afternoon bomb threat.** University of Pittsburgh officials ordered the evacuations of Heinz Chapel, Panther Central, and Victoria Hall after another bomb threat, the Pittsburgh Tribune-Review reported April 9. The threat was received about a half hour after officials cleared the University Club due to a threat and hours after an early-morning threat led to the evacuations of Amos Hall, Bruce Hall, Brackenridge Hall, and Panther Hall. In all, the university received 4 threats against 12 buildings April 9. Officials used social media outlets as well as the university's emergency notification system to send out alerts. The threats are just the most recent in a string of several dozen that have disrupted classes at the university in recent weeks. The university announced new security measures April 8 that include limiting access to a building that has been cleared of a threat to one entrance and requiring everyone to show a university ID to enter. The region's Joint Terrorism Task Force is investigating the threats. Source: [http://www.pittsburghlive.com/x/pittsburghtrib/news/breaking/s\\_790519.html](http://www.pittsburghlive.com/x/pittsburghtrib/news/breaking/s_790519.html)

## **INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**New fake anti-virus shakes down frightened file-sharers.** Security researchers discovered a strain of fake anti-virus software that tries to intimidate supposed file-sharers into paying for worthless software. SFX Fake AV, first detected by antivirus scanner firm Malwarebytes, blends the features of scareware with those more associated with ransomware trojans. The malware stops any legitimate antivirus package from running on compromised PCs. This particular strain of malware also stops Process Explorer and prevents browsers from loading — tactics designed to force users to complete the “input credit card details” screen and pay money for the scamware. The app also falsely tells victims they are going to be sued for breaching anti-piracy legislation, claiming it detected torrent links on PCs. It offers to get around this problem by activating an “anonymous data transfer protocol” for torrent links, another inducement aimed at persuading users into paying for the worthless security app. This latter feature differentiates the malware from strains of scareware seen in the past, which demand money after supposedly detecting “offensive materials” on PCs. The malware also performs a fake scan that classifies Windows Registry Editor as a pornography tool. The vice president of research at Malwarebytes said: “SFX Fake AV is morphing at a relatively fast rate, so it is something that signature-based vendors will have to watch out for as there will be an increasing number of variants in the wild.

UNCLASSIFIED

## UNCLASSIFIED

Also, the use of Dropbox as a delivery mechanism is something that the industry is going to have to take into account and protect against, as it is an emerging trend.” Source:

[http://www.theregister.co.uk/2012/04/13/scareware\\_ransomware\\_hybrid/](http://www.theregister.co.uk/2012/04/13/scareware_ransomware_hybrid/)

**Apple delivers Flashback malware hunter-killer.** Two days after Apple promised to decontaminate Macs infested with the Flashback malware, the company delivered. The newest Mac OS X Java update issued April 12 includes a tool that will “remove the most common variants of the Flashback malware,” Apple’s advisory read. April 10, Apple for the first time acknowledged the Flashback malware campaign that exploited a Java vulnerability to infect hundreds of thousands of Macs. At the same time, Apple pledged to craft a detect-and-delete tool that would scrub compromised machines of the attack code. The April 12 update also disables automatic execution of Java applets in the Java browser plug-in; the exploit used by Flashback to infect Macs was hidden inside a malicious Java applet hosted on compromised Web sites. One of the reasons Flashback was able to infect so many Macs was because the Java plug-in automatically ran the offered applet. Apple’s move is a step toward disabling Java, the advice most security experts suggest to users. Source:

[http://www.computerworld.com/s/article/9226175/Apple\\_delivers\\_Flashback\\_malware\\_hunter\\_killer](http://www.computerworld.com/s/article/9226175/Apple_delivers_Flashback_malware_hunter_killer)

**Fake account verification email phishes for Google credentials.** Google users are being targeted with e-mails purportedly coming from the Google Team confirming a bogus recovery e-mail update. Hosted on a compromised Web site, the destination is a page made to look like Gmail’s login page, set up to harvest the users’ login credentials for their Gmail, and consequently, for all their other Google accounts. Source: <http://www.net-security.org/secworld.php?id=12725>

**Trojanized Angry Birds offered for download.** The extreme popularity of Rovio’s Angry Birds mobile game has made it and its special editions ideal for luring unsuspecting users into downloading malware. A trojanized version of the latest addition — Angry Birds Space — has recently recently been spotted by Sophos researchers being offered on a number of unofficial Android app stores. Users who download it may not even realize that they have downloaded a malicious app, as the packet appears to be a fully-functional version of the game, and the name and the icon of the app correspond with the ones used by the legitimate app. However, the bundled GingerBreak exploit works in the background to gain root access to the device and to use it to download and install additional malware from a remote Web site. The compromised device is then at the mercy of the criminals behind the malware and is now effectively part of a botnet. The criminals can force the device to download any additional packet they want or make the browser go to any Web page they choose. Source: [http://www.net-security.org/malware\\_news.php?id=2066&utm](http://www.net-security.org/malware_news.php?id=2066&utm)

**No permissions Android application can harvest, export device data.** April 9, a researcher was able to demonstrate Android applications without permissions can still access files used by other applications, including which applications are installed and a list of any readable files used by those applications. That capability could be used to identify applications that have weak

UNCLASSIFIED

## UNCLASSIFIED

permissions vulnerabilities and exploit those, he warned. He unveiled a proof of concept Android application, dubbed “NoPermissions” that works with Android phones running version 4.0.3 and 2.3.5 of the operating system. Among the data he found on his own Android phone were certificates from his mobile Open VPN application. Not only could an attacker take advantage of the lack of strict permissions to collect data, he wrote, they could also export it from the phone without permissions. The URI ACTION-VIEW Intent network access call is supported without permissions, which will open a browser on the Android device. An attacker could then pass data to the browser in the form of a URI with GET parameters to pass it to an Internet accessible server or device using successive browser calls. Source:

[http://threatpost.com/en\\_us/blogs/no-permissions-android-application-can-harvest-export-device-data-041012](http://threatpost.com/en_us/blogs/no-permissions-android-application-can-harvest-export-device-data-041012)

**Malware-infected flash cards shipped out with HP switches.** HP sent out a warning to customers after the vendor found it inadvertently shipped virus-laden compact flash cards with its networking kit. The unnamed malware appeared on flash cards that came bundled with HP ProCurve 5400zl switches. The flash card would not have any effect on the switch itself but “reuse of an infected compact flash card in a personal computer could result in a compromise of that system’s integrity,” HP warned in a bulletin issued April 10. It is unclear how the unknown malware got onto the Flash cards that come bundled with the 10 Gbps-capable line of LAN switches, but an infected computer somewhere in the manufacturing process — possible in a factory run by a third-party supplier — is the most obvious suspect. Source:

[http://www.theregister.co.uk/2012/04/11/hp\\_ships\\_malware\\_cards\\_with\\_switches\\_oops/](http://www.theregister.co.uk/2012/04/11/hp_ships_malware_cards_with_switches_oops/)

**Apple promises Flashback malware killer.** April 10, Apple for the first time publicly acknowledged a malware campaign that has infected an estimated 600,000 Macs, and said it would release a free tool to disinfect users’ machines. Although Flashback has circulated since September 2011, it was only in March that the newest variant began infecting Macs using an exploit of a Java bug Oracle patched in mid-February. Apple maintains its own version of Java for Mac OS X, and is responsible for producing security updates. It issued a Java update April 3 that quashed the bug Flashback has been using to infect Macs. In the 7 weeks between Oracle’s and Apple’s updates, hackers responsible for Flashback managed to insert their software — designed for, among other things, password theft — onto an estimated 2 percent of all Macs. Apple said it was working with Internet service providers to “disable [the Flashback] command and control network,” referring to the practice of asking hosting firms to pull hacker-operated command-and-control servers off the Internet so infected computers cannot receive further orders. The company promised to issue a special tool to “detect and remove the Flashback malware.” Apple did not set a timetable for its release. Source:

[http://www.computerworld.com/s/article/9226084/Apple\\_promises\\_Flashback\\_malware\\_killer?source=rss\\_security&utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed:computerworld/s/feed/topic/17+\(Computerworld+Security+News\)&utm\\_content=Google+Reader](http://www.computerworld.com/s/article/9226084/Apple_promises_Flashback_malware_killer?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_content=Google+Reader)

**Rise of ‘forever day’ bugs in industrial systems threatens critical infrastructure.** The number of security holes that remain unpatched in software used to control refineries, factories, and other

## UNCLASSIFIED

## UNCLASSIFIED

critical infrastructure is growing. These holes are becoming so common that security researchers have coined the term “forever days” to refer to the unfixed vulnerabilities, Ars Technica reported April 9. The latest forever day vulnerability was disclosed in robotics software marketed by ABB, a maker of industrial control systems for utilities and factories. According to an advisory issued the week of April 2 by the U.S. Cyber Emergency Response Team, the flaw in ABB WebWare Server will not be fixed even though it provides the means to remotely execute malicious code on computers that run the application. “Because these are legacy products nearing the end of their life cycle, ABB does not intend to patch these vulnerable components,” the advisory stated. The notice said the development of a working exploit would require only a medium skill level on the part of the attacker. Forever day is a play on “zero day,” a phrase used to classify vulnerabilities that come under attack before the responsible manufacturer has issued a patch. Also called iDays, or “infinite days” by some researchers, forever days refer to bugs that never get fixed — even when they are acknowledged by the company that developed the software. In some cases, rather than issuing a patch that plugs the hole, the software maker simply adds advice to user manuals showing how to work around the threat. Source: <http://arstechnica.com/business/news/2012/04/rise-of-ics-forever-day-vulnerabilities-threaten-critical-infrastructure.ars>

**Anonymous blamed for attacks on technology group websites.** Two technology trade associations said they were targeted by the hacker-activist group Anonymous as it singled out supporters of proposed legislation to improve U.S. cybersecurity. Anonymous claimed credit for denial-of-service assaults on the TechAmerica and USTelecom Web sites, according to the associations representing companies including IBM, Apple, and AT&T. Such offensives typically involve flooding a Web site with traffic, causing it to crash. The organizations said the attacks amount to reprisal for supporting the legislation, among cybersecurity bills under consideration by Congress, designed to encourage companies and government agencies to voluntarily share information about cyber threats. Users could not connect to the Web site for USTelecom, which represents telephone companies led by AT&T, Verizon, and CenturyLink, starting April 8 and the site was “up and down” April 9 as technicians worked to restore service, said a spokeswoman. The Web site of TechAmerica, whose members include IBM, Microsoft, and Apple, was not loading April 9. The attack began April 8 and the association was working April 9 to get the site back up, a TechAmerica spokeswoman said. The trade groups support cybersecurity legislation introduced by the chairman and ranking member of the House Intelligence Committee. Source: <http://www.bloomberg.com/news/2012-04-09/anonymous-blamed-for-attacks-on-ustelecom-group-websites.html>

**Web attacks use smart redirection to evade URL security scanners.** Antivirus vendor ESET has come across new Web-based malware attacks that try to evade URL security scanners by checking for mouse cursor movement, ESET researchers said in a blog post April 6. The new drive-by download attacks were spotted in the Russian Web space and do not require user interaction to infect computers with malware. Rogue JavaScript code is being added to local JS files that get loaded in the “head” section of every HTML page. The code injected into these JavaScript files loads a different JS file from an external location but only if mouse cursor movement is detected. The purpose of the mouse movement detection is to filter out URL

UNCLASSIFIED

## UNCLASSIFIED

scanners and Web crawlers used by security companies or search engines to detect infected sites. If the check determines the request came from a human, the external JavaScript code injects an iframe into the original HTML page, which then loads attack code from an installation of the Nuclear Pack exploit toolkit. In this case, it attempts to exploit the CVE-2012-0507 Java vulnerability and the CVE-2010-0188 Adobe Reader vulnerability. Source:

[http://www.computerworld.com/s/article/9225957/Web\\_attacks\\_use\\_smart\\_redirection\\_to\\_e\\_vade\\_URL\\_security\\_scanners](http://www.computerworld.com/s/article/9225957/Web_attacks_use_smart_redirection_to_e_vade_URL_security_scanners)

**New security flaws detected in mobile devices.** Findings of two recent examinations of mobile devices highlight how designers of smartphones and tablet PCs failed to fully account for security and privacy implications. In one study, security firm Cryptography Research showed how it is possible to eavesdrop on any smartphone or tablet PC as it is being used to make a purchase, conduct online banking, or access a company's virtual private network. Cryptography Research is "working with one of the major smartphone and tablet companies right now to put countermeasures in," Cryptography Research's chief technology officer said. No known actual attacks have occurred, he said. In another demonstration, researchers at McAfee highlighted several ways to remotely hack into Apple iOS. McAfee's research team remotely activated microphones on a variety of test devices and recorded conversations taking place nearby. They also showed that it is possible to steal secret keys and passwords, and pilfer sensitive data. "This can be done with absolutely no indication to the device user," says McAfee's principal security architect. Source: <http://www.usatoday.com/tech/news/story/2012-04-08/smartphone-security-flaw/54122468/1>

## **NATIONAL MONUMENTS AND ICONS**

**(Virginia) Wildfires burning 20,000 acres in national forest areas.** Crews fighting major southwest Virginia wildfires were battling blazes that, collectively, reached historic proportions — and led officials to close some surrounding areas to the public April 13. "Right now, when you look at the entire George Washington National Forest, we have 20,000 acres on fire," said a head ranger for the Warm Springs and James River district of the George Washington and Jefferson National Forests. The three largest fires near the Roanoke area — at Alleghany Tunnels, Rich Hole, and Barbours Creek — all grew significantly between April 11 and 12. Of the three major fires in the area, the only one threatening buildings was the fire in the Barbours Creek Wilderness. Four residences northeast of the fire had been secured, and the Potts Mountain Jeep Trail and Pines Campground were closed. Source:

<http://m.roanoke.com/mapp/story.aspx?arcID=307420>

**(Florida) Spreading smoke causes Jacksonville officials to issue air quality advisory.** Firefighters were still trying to contain 6 of 20 wildfires burning in Northeast Florida, with other fires likely to erupt in the coming days because of extremely dry conditions and no rainfall expected for at least a week, fire and weather officials said April 9. The biggest fire resulted from a lightning strike that has burned nearly 12,000 acres of mostly forest land at the Columbia-Baker county line. That fire, which is about 30 percent contained, caused heavy smoke to drift into the Jacksonville area as winds shifted from when the fire first started the

UNCLASSIFIED

## UNCLASSIFIED

week of April 2, said a meteorologist with the National Weather Service. The second biggest fire — 450 acres, 90 percent contained — was burning in Putnam County. That is known as the 8 mile fire, south of Grebe Street and 1 mile west of Florida 19. Two fires of 100 to 150 acres were attacked by local firefighters and state forestry crews in Clay County. Those fires are on Crowl Road off U.S. 17 — 50 percent contained — and Beauty Bush Lane — 95 percent contained. Source: <http://jacksonville.com/news/crime/2012-04-09/story/6-wildfires-still-not-contained-first-coast-smoke-over-jacksonville>

### **POSTAL AND SHIPPING**

**(Florida) Woman injured after acid bomb explodes in mailbox.** A Davie, Florida woman was injured April 11 after some sort of explosive went off in her mailbox. She told police she was home the night of April 10 when she heard a loud “boom”. She said she did not think anything about it. It was when she left her home April 11 that she noticed the door to her mailbox was hanging from the opening. When she reached inside, she told police her hand touched a plastic bottle and she experienced a burning sensation. She called police to report it and was treated for minor injuries by Davie Fire Rescue. Police suspect the material inside the bottle and the mailbox was some sort of acid. A police captain said since the incident involved a mailbox they are looking into possible federal charges of deploying a destructive device. Source: <http://miami.cbslocal.com/2012/04/11/woman-injured-after-acid-bomb-explodes-in-mail-box/>

**(Massachusetts) Minnesota man charged with hacking into Marlborough server.** A man was charged April 6 in federal court with hacking a protected Marlborough, Massachusetts company’s server and obtaining personal information of his co-workers, according to U.S. Immigration and Customs Enforcement (ICE). According to court documents, between May 3 and June 6, 2011, the man launched a “brute force attack” against the servers of Workscape Inc., a Marlborough company. Workscape hosted an employee benefits site for employees of FedEx Ground. The man, himself a FedEx Ground employee, allegedly created a computer program to hack into the Workscape system and obtain personal information about other FedEx Ground employees, including their names, addresses, and Social Security numbers. Based on information obtained during the investigation, it appears that he never used or released this information, according to the ICE. If convicted, the man faces a year in prison and a \$100,000 fine. Source: <http://www.metrowestdailynews.com/news/x168224807/Minnesota-man-charged-with-hacking-into-Marlborough-server>

### **PUBLIC HEALTH**

**Painkiller prescriptions grow nearly 200 percent since 1991.** Painkiller abuse in the United States has exploded along with skyrocketing prescriptions and sales, top national health officials told a crowd of hundreds at the National Rx Drug Abuse Summit April 11. Even well-meaning doctors and dentists are fueling the epidemic of prescription drug abuse by prescribing narcotics too often and for too long, officials said. The director of the National Institute on Drug Abuse at the National Institutes of Health cited statistics showing prescriptions for opiate-based painkillers dispensed by retail pharmacies rose from 76 million in

UNCLASSIFIED

## UNCLASSIFIED

1991 to 219 million in 2011. Kentucky is one of the hardest-hit states, with about 1,000 deaths a year attributed to prescription-drug overdoses — more deaths than in traffic accidents. The director said dentists and emergency medicine physicians were the chief prescribers of painkillers to patients 5 to 29 years old, and high prescribers should consider alternatives, particularly for this vulnerable group. She also said education on pain management is sorely lacking in medical schools, which offer an average of 7 hours, compared with 75 hours in U.S. veterinary schools. A principal deputy director at the U.S. Centers for Disease Control and Prevention said opioid overdose death rates have risen in lockstep with sales. In 2010, enough prescription painkillers were prescribed to medicate every American adult every day for a month. Source: <http://www.courier-journal.com/article/20120411/NEWS01/304110095/Painkiller-prescriptions-grow-n>

**Animal antibiotics: FDA asks drug companies to limit overuse amid health concerns.** April 11, the U.S. Food and Drug Administration (FDA) called on drug companies to help limit the use of antibiotics in farm animals, a decades-old practice that scientists say contributed to a surge in dangerous, drug-resistant bacteria. Antibiotic drugs like penicillin are routinely mixed with animal feed and water to help livestock, pigs, and chickens put on weight and stay healthy in crowded feeding lots. Scientists warned such use leads to the growth of antibiotic-resistant germs that can be passed on to humans. Under the new FDA guidelines, the agency recommends antibiotics be used “judiciously,” or only when necessary to keep animals healthy. It also wants to require a veterinarian to prescribe the drugs. They can currently be purchased over-the-counter by farmers. The draft recommendations by the FDA are not binding, and the agency is asking drug manufacturers’ to voluntarily put the proposed limits in place. Drug companies would need to adjust the labeling of their antibiotics to remove so-called production uses of the drugs. Production uses include increased weight gain and accelerated growth, which helps farmers save money by reducing feed costs. The FDA hopes drugmakers will phase out language promoting non-medical uses within 3 years. Source: [http://www.huffingtonpost.com/2012/04/11/animal-antibiotics-fda-livestock\\_n\\_1417655.html?ref=food&ir=Food](http://www.huffingtonpost.com/2012/04/11/animal-antibiotics-fda-livestock_n_1417655.html?ref=food&ir=Food)

**(Utah) Utah: Medical records breach more extensive.** Health officials in Utah said hackers who downloaded thousands of medical files from state computers stole far more personal information than originally thought. The Utah Department of Health said April 6 that nearly 182,000 recipients of Medicaid and the Children’s Health Insurance Program had their personal information stolen. The department estimates more than 25,000 Social Security numbers were compromised. Agency officials originally thought the hackers stole 24,000 Medicaid claims. Officials said the attack started the week of March 26 and likely came from eastern Europe. The information was on a new server that had security tools installed improperly. Source: <http://www.businessweek.com/ap/2012-04/D9TVKSM00.htm>

**(Arizona) Arizona health officials warn public about Norovirus.** Seven clusters of Norovirus found in assisted-living homes for seniors have authorities in southern Arizona warning the public about the sometimes fatal flu-like illness, the Associated Press reported April 9. The Pima County Health Department is warning the public to use extra caution around the elderly and

UNCLASSIFIED

## UNCLASSIFIED

children, who are more susceptible to Norovirus. The department is investigating the clusters of found in assisted-living facilities in the area. They say Norovirus is not uncommon in such homes, but that it is rare to see so many different clusters at the same time. Source:

<http://www.abc15.com/dpp/news/state/arizona-health-officials-warn-public-about-norovirus>

### **TRANSPORTATION**

**Analysis of 15 failed terrorist plots against surface transportation provides insight into tactics, weapons, and more.** The Mineta Transportation Institute, April 10, released a research report, *Carnage Interrupted: An Analysis of Fifteen Terrorist Plots Against Public Surface*

Transportation, which examines several factors in 13 plots that authorities uncovered and foiled before attacks could be carried out. It also presents an additional two cases in which terrorists attempted to carry out attacks that failed. The reports analyzed plots from 1997-2012, primarily in the United States and the United Kingdom because they have been frequent targets. The report describes each plot in terms of the terrorists' plan, motivation, objective, target selection, tactics and weapons, reconnaissance, timing, security measures in place at the target, and how the plot was disrupted. A principal investigator noted that four of the plots involved chemical or biological substances. "It seems highly likely that the plotters in these cases had in mind the 1995 sarin attack in Tokyo," he said. "By mid-decade the poison fad was over." He said train and bus bombings in Madrid and London that killed many people led terrorists by the end of the decade to shift to multiple bombs as the attack prototype. The free report is available for download from [transweb.sjsu.edu/project/2979.html](http://transweb.sjsu.edu/project/2979.html). Source:

<http://www.marketwatch.com/story/analysis-of-15-failed-terrorist-plots-against-surface-transportation-provides-insight-into-tactics-weapons-and-more-2012-04-10>

**Korean Airlines jetliner diverted to Canadian military base after bomb threat.** A Korean Airlines Boeing 777 en route from Vancouver, Canada, to Seoul, South Korea, was diverted to a nearby Canadian military base after the airline's U.S. call center received a bomb threat. Authorities continued to search the aircraft early April 11 and the Royal Canadian Mounted Police (RCMP) said nothing suspicious had yet been found. Korean Airlines said in a statement the call center received the threat April 10 about 25 minutes after take-off from Vancouver International Airport. Airline officials said the aircraft with 149 passengers then turned around. A Canadian spokeswoman for The North American Aerospace Defense Command, said two U.S. F-15 fighter jets from Portland, Oregon, escorted the plane to Canada's Comox air base on Vancouver Island, 113 miles outside Vancouver. The passengers and crew stayed overnight in the area while officials did a detailed search of the plane's luggage April 10, a RCMP inspector said. The inspector said the same Korean Airlines flight out of Vancouver faced a similar threat April 9, and the all-clear was given after a 2-hour search. Source:

<http://www.startribune.com/nation/146959355.html>

### **WATER AND DAMS**

(Florida) **Security system overhaul slated at Boynton Beach water treatment plants.** The security system at the two water treatment plants in Boynton Beach, Florida, will receive

UNCLASSIFIED

## UNCLASSIFIED

improvements to their security television and access system, WPTV 5 West Palm Beach reported April 6. The improvements come after a former city employee was charged with stealing city tools from the site and pawning them for \$1,000. The employee was arrested and is facing charges. The Palm Beach County Inspector General's Office investigated city policies after the arrest and the city's vice mayor said they are following the federal Bio-Terrorism Response Act which requires the upgrades. About 90,000 of the residents in the Boynton Beach area receive water from the two plants. Source:

[http://www.wptv.com/dpp/news/region\\_s\\_palm\\_beach\\_county/boynton\\_beach/security-system-overhaul-slated-at-boynton-beach-water-treatment-plants](http://www.wptv.com/dpp/news/region_s_palm_beach_county/boynton_beach/security-system-overhaul-slated-at-boynton-beach-water-treatment-plants)

### **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