

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

Study to determine floods' impact on river channel. Local entities in North Dakota are partnering with state and federal agencies to study Missouri River channel patterns to predict what the river may do after the 2011 flood, the Bismarck Tribune reported March 8. A water resource engineer for the Water Commission, said the 3-year \$1.08 million geomorphic study is broken down into channel changes, erosion, sediment buildup, and impacts on water levels. It focuses on an area from south of Garrison Dam to the Oahe Delta, she said. The goals of the project include determining channel changes and flood impacts, and assessing ice jam risks and sediment, and the impacts of wood debris and standing trees. The manager said local entities should find the project useful for planning and zoning, and deciding where building should and should not occur. The changes may impact the city's wastewater treatment and water treatment plants, the Bismarck city administrator said. The costs are being shared by the U.S. Army Corps of Engineers, U.S. Geological Survey, the State Water Commission, state Health Department, state Game and Fish Department, state Transportation Department, the cities of Bismarck and Mandan, and Burleigh and Morton counties or their water districts. Source: http://bismarcktribune.com/news/local/study-to-determine-floods-impact-on-river-channel/article_88a57002-6968-11e1-95cc-0019bb2963f4.html

51.9 million for flood repairs to Garrison Dam. A senator from North Dakota said March 7 an additional \$700 million in disaster aid was approved for the U.S. Army Corps of Engineers for flood mitigation efforts on the Missouri River. Nearly \$52 million was targeted for repairs to the Garrison Dam and levees in Williston, he said. In addition to repairs at the Garrison Dam, projects include repairs to the Williston levee, river bank stabilization with repairs at the Hoge Island area, and work to address sandbar concerns near the mouth of the Heart River. According to a Corps project sheet, work on the dam includes 21 assessment and repair items estimated to cost \$51.9 million. The sheet listed —significant actions that include repairs to the spillway gates, concrete spillway slabs, west abutment walls, and flood control tunnel repairs. The Corps also listed dredging an area upstream of the spillway to restore full capacity, a survey of the spillway channel, spillway dredging, and repairs to the west Tailrace road. Source: http://bismarcktribune.com/news/state-and-regional/million-for-flood-repairs-to-garrison-dam/article_205d8224-68a4-11e1-8655-001871e3ce6c.html

REGIONAL

(Midwest) Gavins Point Dam releases near. Releases of water from Gavins Point Dam near Yankton, South Dakota, will increase incrementally beginning in mid-March for the Missouri River navigation season. The U.S. Army Corps of Engineers said March 6 full-service flows will be provided for barge traffic and other downstream uses during at least the first half of the navigation season. The higher flows are scheduled for March 23 at Sioux City, Iowa, March 25 at Omaha, Nebraska, March 26 at Nebraska City, Nebraska, March 28 at Kansas City, Missouri, and April 1 at the river's mouth near St. Louis. The river's reservoir system enters the spring runoff season well-prepared to capture spring runoff, with slightly more than its full capacity of flood control storage available, said the water management chief in Omaha. The mild winter allowed

UNCLASSIFIED

the Corps to make higher-than-normal releases throughout the winter. The runoff forecast above Sioux City in 2012 is 26.1 million acre-feet, slightly above the normal of 24.8 million acre-feet. Source: <http://www.omaha.com/article/20120306/NEWS01/703079959>

(Minnesota) State's 2 nuclear plants will get post-Fukushima upgrades. The owner of Minnesota's two nuclear power plants said it is preparing to spend \$20 million to \$50 million on safety upgrades and studies based on the lessons of the nuclear catastrophe in Japan a year ago this month. Xcel Energy is buying more diesel pumps and portable generators that could be quickly deployed at its Monticello and Red Wing Prairie Island plants if all backup electricity went out, as it did at Japan's Fukushima Daiichi plant. Some critics question whether the actions are sufficient, pointing with skepticism to the purchase of off-the-shelf pumps and backup generators, rather than more expensive equipment designed for nuclear plants. The chief nuclear officer for the Minneapolis-based utility, who is also a member of the industry's post-Fukushima steering committee, said in an interview that Xcel's safety costs could climb as high as \$250 million if the utility is required to purchase nuclear-qualified equipment and take other costly steps such as building earthquake-proof off-site buildings to store and protect it. Source: <http://www.startribune.com/local/west/141381543.html?page=1&c=y>

NATIONAL

Grief, resilience after storms rip through states, killing 39. With dozens dead and scores of buildings reduced to rubble, residents of the Midwest and South March 4 were assessing the damage that a series of vicious twisters left behind March 2 and 3, CNN reported. By the time the powerful storm system faded, 39 were dead: 21 in Kentucky, 13 in Indiana, 3 in Ohio, and 1 each in Alabama and Georgia. Tall, once-sturdy trees littered the ground. Bright yellow school buses lay smashed into buildings. Garbage bins and wooden beams, which had flown through the air, resurfaced hundreds of yards away. The tornado outbreak began March 2 and extended into March 3, affecting millions of people from Indiana to Georgia. The National Weather Service has confirmed that at least 42 tornadoes swept across 10 states March 2. More than 400 National Guard troops were deployed in Kentucky, while 250 more were dispatched in Indiana, according to officials. Two tornadoes hit Henryville, Indiana, destroying a school complex that housed multiple schools, as well as most homes and businesses in the town. In addition to the dead, hospitals continued to treat scores suffering from major trauma to minor injuries related to sudden ferocious spurts of high winds, powerful hail, and drenching rains. Source: http://www.cnn.com/2012/03/04/us/severe-weather/index.html?hpt=us_c1

INTERNATIONAL

Frankfurters recalled in Canada due to Listeria concern. The Canadian Food Inspection Agency and Glatt's Kosher Meat Products of Montreal, Quebec, Canada, are warning the public not to consume certain Glatt's brand Beef Frankfurters Jumbo BBQ because they may be contaminated with *Listeria monocytogenes*, Food Safety News reported March 3. The recalled product, Glatt's brand Beef Frankfurters Jumbo BBQ, is sold in 375-gram packages. The frankfurters were distributed in Ontario and Quebec. Source:

UNCLASSIFIED

UNCLASSIFIED

<http://www.foodsafetynews.com/2012/03/frankfurters-recalled-in-canada-due-to-listeria-concern/>

Toronto sees sharp increase in salmonellosis. Over the past decade, the Canadian city of Toronto, Ontario, has averaged about 70 cases of Salmonella infection during the first 2 months of the year, Food Safety News reported March 4. In 2012, as of February 28, 114 cases of salmonellosis were confirmed in the city. In a news release, Toronto Public Health (TPH) attributed much of the sharp increase to three known clusters of illness: a large catered event February 11 that resulted in transmission of *S. typhimurium* to numerous attendees who continue to report illness; an outbreak, still under investigation by Public Health Ontario, of a less common species of Salmonella (*S. heidelberg*) across the region; and an uptick of *S. enteritidis* (the most common strain of Salmonella reported in Toronto) linked to recent travel to Cuba. Because of this general increase in circulating Salmonella infection, TPH has warned that there is higher chance of person-to-person transmission. Source:

<http://www.foodsafetynews.com/2012/03/toronto-sees-sharp-increase-in-salmonellosis/>

BANKING AND FINANCE INDUSTRY

Federal court in Illinois shuts down nationwide 'Employee Benefit Plan' tax scheme. A federal court in Illinois permanently barred two women and four companies from operating an alleged scheme to help high-income individuals attempt to avoid income taxes by funneling money through purported employee benefit plans, the Justice Department announced March 6. According to the government complaint, the defendants claimed to promote and operate plans that provide insurance benefits to participating companies' employees, when in fact the scheme was simply a mechanism for the firms' owners to receive tax-free or tax-deferred income for personal use. In the most recent version of the scheme, each participant's company made supposedly tax deductible payments to a purported benefit plan. The contributions were then allegedly transferred to an account within a company based in the Caribbean island of Anguilla, in which they were invested until the owner terminated the program and received the assets. The complaint alleged participants from across the country have transferred at least \$239 million as part of the scheme, and that total contributions may exceed \$300 million. Source: <http://www.justice.gov/tax/2012/txdv12290.htm>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Expert panel: 10-mile evacuation zone may not be adequate for some nuclear power plants. The United States should customize emergency plans for each of the nation's 65 nuclear power plants, a change that in some cases could expand the standard 10-mile evacuation zone in place for more than 3 decades, an expert panel recommended in a report that was to be released March 9. That's one of the lessons to emerge in a 40-page report set to be released 3 days before the 1-year anniversary of Japan's nuclear disaster from a committee that examined the incident for the American Nuclear Society. The panel included a former chairman of the Nuclear Regulatory Commission, a fellow at a Department of Energy laboratory, and seven other nuclear scientists. The report concluded U.S. nuclear power oversight is adequate to protect

UNCLASSIFIED

UNCLASSIFIED

public health and safety but that emergency zones —should not be based on arbitrary mileage designations. Under rules in force since 1978, communities near nuclear plants must prepare federally reviewed evacuation plans for those living within 10 miles of the facility. Source: <http://www.duluthnewtribune.com/event/apArticle/id/D9TC7HM80/>

NRC examining potential impact on nuclear plant safety from upstream dam failure. The Nuclear Regulatory Commission (NRC) announced March 7 that it started a formal evaluation of potential generic safety implications for dam failures upstream of U.S. commercial nuclear power plants. The NRC began examining this issue after inspection findings at two plants, and recently completed an initial screening assessment. While this screening did not identify any immediate safety concerns, inspections or other reviews at individual plants led to those plants taking appropriate actions regarding flooding scenarios. Based on the screening, the NRC staff recommended that flooding from upstream dam failure be further evaluated as part of implementing recommendations from the agency's Japan Near-Term Task Force. Source: <http://www.power-eng.com/news/2012/03/07/nrc-examining-potential-impact-on-nuclear-plant-safety-from-upstream-dam-failure.html>

EPA targets chemicals. Seven chemicals or categories of substances will undergo risk assessment by the Environmental Protection Agency (EPA), the agency announced March 1. The move could lead to their regulation under the Toxic Substances Control Act (TSCA). As justification, the agency cited the substances' potential to harm human health and widespread human exposure to them. One of the chemicals, HHCb, is used as a fragrance in consumer products. Three more compounds are solvents. Also, the EPA will conduct risk assessments of long-chain chlorinated paraffins and medium-chain chlorinated paraffins. Both are used in industrial cutting fluids, commercial paints, adhesives, sealants, and caulks. Other categories slated for risk assessment are antimony and antimony compounds, which are used in a variety of commercial applications, such as flame retardants. The seven chemicals or categories of substances are among 83 commercial chemicals EPA has selected for further review and potential regulation. Source: <http://cen.acs.org/articles/90/web/2012/03/EPA-Targets-Chemicals.html>

CSB develops policy on employee participation in investigations. The U.S. Chemical Safety Board (CSB) announced March 7 it has developed a new policy on employee participation in investigations the Board hopes will enhance the vital role played by plant workers in determining root causes of incidents and promoting facility safety. The policy, approved unanimously, followed a 2011 CSB roundtable involving accident victims, family members, and worker representatives. The new policy essentially states that employees and their representatives have similar rights in CSB accident investigations as they do during Occupational Safety and Health Administration inspections. The CSB is an independent federal agency charged with investigating serious chemical accidents. The agency's board members are appointed by the U.S. President and confirmed by the Senate. The Board does not issue citations or fines but does make safety recommendations. Source: <http://www.csb.gov/newsroom/detail.aspx?nid=404>

UNCLASSIFIED

COMMERCIAL FACILITIES

(New York) Police: House has enough explosives to ‘blow up the entire block’. Police investigating a marijuana scent at a Long Island, New York home discovered an arsenal of guns, grenades, and bomb-making material that would have been enough to —blow up the entire block, NBC New York reported. Police officers went to the home in Woodmere after an alarm went off March 7 and found a man there without identification. A Nassau County police inspector said responding officers saw a semi-automatic handgun and two military-style grenades as soon as they opened the door. Police took the man into custody and evacuated about 20 homes on the block as a precaution while they searched the rest of the home. During their search, police discovered a massive cache of weapons, including 100 handguns, 20 rifles, 15 pipe bombs, 15 handmade grenades, and 50 pounds of bomb-making material, police said. In addition to the weapons, police found a marijuana greenhouse as well as a pit in the backyard with a wire that extended into the house. Police believe the man used the pit to test explosives. The home is owned by the man’s parents, who live in Florida during the winter. Police said they were not sure the parents knew the man was living in the house. Authorities said they do not know of any motive the man had for developing the arsenal or what he planned to do with it. Source: <http://usnews.msnbc.msn.com/news/2012/03/07/10602365-police-house-has-enough-explosives-to-blow-up-the-entire-block>

Sony hackers stole \$253M worth of music files. Hackers who breached Sony’s networks in 2011 also stole more than 50,000 music files, including previously unreleased tracks, Wired reported March 5. The lost music was estimated to be worth around \$253 million, according to the Daily Mail. Sony discovered the theft within weeks of its occurrence, but kept the news under wraps. Sony recently acknowledged the breach to the BBC. The company discovered the hack through routine monitoring of social networking sites, fan sites, and hacker forums. Sony still possesses copies of all the music, and the breach did not affect its ability to release albums and individual songs that were taken by the hackers. Source: <http://www.wired.com/threatlevel/2012/03/sony-music-hack/>

COMMUNICATIONS SECTOR

Judge extends DNS Changer deadline as malware cleanup progresses. March 5, a federal judge extended an operation that will keep hundreds of thousands of users infected with the “DNS Changer” malware connected to the Internet until they can clean their machines. Meanwhile, Internet Identity (IID), which is monitoring the cleanup efforts, said March 6 it had seen a “dramatic” decrease in the number of computers infected with DNS Changer. DNS Changer, which at its peak infected more than 4 million Windows PCs and Macs worldwide, was the target of a major takedown led by the U.S. Department of Justice in November 2011. The malware hijacked users’ clicks by modifying domain name system (DNS) settings to send URL requests to the criminals’ own servers, a tactic that shunted victims to hacker-created sites that resembled the real domains. As part of the “Operation Ghost Click” takedown and accompanying arrests of 6 Estonian men, the FBI seized more than 100 command-and-control servers hosted at U.S. data centers. To replace those servers, a federal judge approved a plan

UNCLASSIFIED

where substitute DNS servers were deployed by the Internet Systems Consortium, the non-profit group that maintains the popular BIND DNS open-source software. Without the server substitutions, DNS Changer-infected systems would have been immediately severed from the Internet. March 5, a U.S. district court judge extended the deadline for shutting down the replacement servers by 4 months, from March 8 to July 9, 2012. Two weeks ago, authorities argued that victims needed more time to wipe DNS Changer from computers before their connections were cut off. Source:

http://www.computerworld.com/s/article/9224926/Judge_extends_DNS_Changer_deadline_a_s_malware_cleanup_progresses?taxonomyId=17

Researchers find vulnerabilities in satellite TV and DVB Systems. A Polish security researcher discovered flaws in digital satellite TV set-top-boxes and Digital Video Broadcasting (DVB) chipsets, which he will present at the Hack in the Box (HITB) conference in Amsterdam May 21-25. His findings reveal a large number of digital satellite TV platforms worldwide are exposed to malicious operations due to weaknesses that exist not only in the software and the hardware of these devices but also because of the services supplied by many vendors. The expert wants to demonstrate that digital satellite TV set-top-boxes are exposed to hacking and malware infection with no user interaction required. His research shows that malware can be leveraged by a hacker to gain access over the Internet to the encrypted satellite TV programs paid by an unsuspecting user. "It will be the first ever discovery and disclosure of real malware threats in the context of the digital satellite TV platform," he said. "And this will also be the first ever successful attack documented against digital satellite set-top-box equipment implementing Conax Conditional Access System with advanced cryptographic pairing function." The Conax Conditional Access System was implemented worldwide for protecting paid content against illegal sharing and distribution. Source: <http://news.softpedia.com/news/Researchers-Find-Vulnerabilities-in-Satelite-TV-and-DVB-Systems-257232.shtml>

CRITICAL MANUFACTURING

Toyota recalls over 681,000 vehicles in U.S. Toyota Motor Corp announced March 7 the recall of more than 681,000 cars and trucks in the U.S. market to address potential problems. The Japanese automaker said it will recall about 495,000 Tacoma pickup trucks from model years 2005 to 2009 to replace a part in the steering wheel. Toyota will replace the steering wheel spiral cable assembly because friction may occur over time involving that part, which may result in the driver's side airbag being deactivated and not deploying in an accident. It is also recalling about 70,500 Camry mid-sized cars and 116,000 Venza crossover vehicles from model years 2009 to 2011 to replace a stop lamp switch. Silicon grease during assembly may lead to increased electrical resistance that can cause the vehicle not to start or the shift lever not to move from the —park position, Toyota said. Source:

<http://www.msnbc.msn.com/id/46657176/ns/business-autos/#.T1jSankhJUS>

Chrysler recalls 210,000 Jeep Liberty SUVs. Chrysler announced March 7 the recall of nearly 210,000 Jeep Liberty sport utility vehicles from model years 2004 and 2005 due to potential problems resulting from excessive corrosion that could lead to a loss of control by the driver.

UNCLASSIFIED

UNCLASSIFIED

Some may be equipped with rear lower control arms that can fracture due to corrosion caused by road salt used in certain states, according to documents filed with the National Highway Traffic Safety Administration. The recall is expected to begin by the end of April. Source: <http://bottomline.msnbc.msn.com/news/2012/03/07/10600266-chrysler-recalls-210000-jeep-liberty-suvs>

NHTSA recall notice - Nissan Quest engine software. Nissan announced March 5 the recall of 23,531 model year 2011-2012 Nissan Quest vehicles. Due to software programming, while driving at slow speeds or idling on a decline with a quarter tank of fuel or less, there may be an insufficient supply of fuel to the engine. As a result, the engine may stall. Vehicle stalling could increase the risk of a crash. Nissan will notify owners, and dealers will reprogram the fuel pump control module. The safety recall is expected to begin during March. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcld_ID=12V076000&summary=true&prod_id=1246770&PrintVersion=YES

NHTSA recall notice - Gabriel and Partsmaster strut assemblies for the Ford Focus. Ride Control announced March 5 the recall of 10,006 Readymount strut assemblies under the Gabriel name and privately branded Partsmaster name. The strut assemblies were sold as aftermarket service equipment for use on model year 2000-2005 Ford Focus vehicles. The assemblies were produced with an incorrect nut that does not contain a flange. The absence of the nut can allow the Readymount assembly to pull apart the top mount. If the assembly separates during installation, it could result in injury to the installer. If the assembly separates while the vehicle is in motion, it could result in damage to the vehicle and possibly result in a crash. Ride Control will notify owners and will repair or replace affected parts. The safety recall is expected to begin during March. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcld_ID=12E007000&summary=true&prod_id=1436778&PrintVersion=YES

NHTSA recall notice - Daimler Trucks Freightliner, Sterling, and Western Star fuel line systems. Daimler Trucks announced March 5 the recall of 103,437 model year 2006-2013 Freightliner, Sterling, and Western Star vehicles equipped with Detroit Diesel EPA07, EPA10, DD13, and DD15/16 engines. The pump to rail high pressure fuel line support system used on the engines is sensitive to assembly torque and may be damaged during service work. As a result of other repairs, the line supports may loosen, potentially leading to fuel line cracking and a fuel leak. A fuel leak could create a road hazard, increasing the risk of a crash. A fuel leak in the presence of an ignition source can also result in a fire. Daimler Trucks will notify owners, and the fuel line support system will be replaced by service facilities. The recall is expected to begin during March. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcld_ID=12V074000&summary=true&prod_id=1438781&PrintVersion=YES

UNCLASSIFIED

DEFENSE/ INDUSTRY BASE SECTOR

U.S. Export Enforcement Coordination Center opens. The U.S. Presidential administration has opened a new Export Enforcement Coordination Center (E2C2), one of four steps in its export control reform agenda, Defense News reported March 8. DHS will administer the new center. It has a leadership team that includes officials from DHS, the FBI, and the Commerce Department. The plan is to increase information sharing and coordination between law enforcement and intelligence officials to better track and prosecute violations of U.S. export controls laws. The center, which will eventually have 30 individuals working for it, officially opened March 7. Participating organizations include DHS, the Office of the Director of National Intelligence, and the departments of Justice, Commerce, State, Treasury, Defense, and Energy. There will also be representation from agencies including the FBI, the Commerce Department's Bureau of Industry and Security, U.S. Customs and Border Protection, Defense Criminal Investigative Service, the National Nuclear Security Administration, and the Defense Security Service. The administration has also created the Information Triage Unit (ITU), which will be housed within Commerce. Another multiagency organization, the ITU was established to collect information and intelligence from across the government to help licensing agencies make more informed decisions, a senior government official said. Source:

<http://www.defensenews.com/article/20120308/DEFREG02/303080001/U-S-Export-Enforcement-Coordination-Center-Opens?odyssey=tab|topnews|text|FRONTPAGE>

Ex-Marine accused of selling sensitive military equipment on eBay. A retired U.S. Marine was arrested and arraigned March 4 on four counts of attempting to sell sensitive military laser light filters on eBay and ship them overseas, authorities said. He pleaded not guilty. The man, from Rosamond, California, is charged with 4 counts of making false statements on customs forms in his attempts to ship more than 100 laser light interference filters abroad between December 2009 and February 2010. A U.S. attorney spokesman said an undercover investigation led authorities to the man. He worked in the Marine Aviation Supply Office as a staff sergeant at Edwards Air Force Base in California until his retirement in December 2011. An assistant U.S. attorney confirmed the alleged wrongdoing occurred during his time in uniform. Authorities opened a probe after receiving a tip about the sale of the filters on eBay. The indictment said the man falsely stated his packages contained camera lenses, filters, and other equipment, when in reality they contained the laser light filters. Officials said the sophisticated lights cannot legally be exported without a license from the State Department. The filters, which protect optics inside night vision goggles from being damaged by lasers, are considered so sensitive the military requires they be destroyed after use. The man faces a maximum sentence of 20 years in prison, as well as a maximum \$1 million fine. He is due back in court March 26. Source:

<http://latimesblogs.latimes.com/lanow/2012/03/ex-marine-accused-ebay.html>

F-22 oxygen problems still a mystery. The U.S. Air Force Scientific Advisory Board (SAB) announced it could find no cause for the hypoxia suffered by F-22 pilots from the lack of oxygen in the cockpit, the Panama City News Herald reported March 4. The advisory board was asked to investigate the oxygen systems in the F-22 after months of problems with both the main and backup oxygen systems. "The SAB did look at the oxygen system and was not able to find a

UNCLASSIFIED

single cause related to the oxygen system,” said an Air Force spokesman. He went on to say improvements were made to the oxygen system. He also said the health effects of pilots will be monitored. The SAB, an independent board working under the direction of the Air Force, looked at numerous reported problems regarding the oxygen system. The full SAB report is slated for release in May or June, the spokesman confirmed. Source:

<http://www.news Herald.com/articles/panama-100902-problems-city.html>

EMERGENCY SERVICES

Drug shortages for paramedics forces review. Alarmed by drug shortages that could affect the lifesaving efforts of paramedics, a medical board that oversees emergency medical services in southern Nevada is exploring the possible use of alternative medications, which would require the re-education of rescue personnel, the Las Vegas Review-Journal reported March 8. The board also voted March 7 to extend the expiration dates on eight critical drugs, giving them a longer shelf life if new supplies are slow in coming. Stressing that ambulances remain well-equipped with the drugs long in use by first responders, the chairman of the medical advisory board of the Southern Nevada Health District said it is being proactive in dealing with a national problem that is affecting both hospitals and emergency medical services. Though the Food and Drug Administration requires manufacturers to conduct studies to determine the stability and shelf life of their products and to label them accordingly, medical advisory boards can legally extend their expiration dates in the interest of public health. Only recently, at a February conference of emergency physicians in Dallas, has it come to light that the problem could extend to paramedics. Source: <http://www.lvrj.com/news/drug-shortages-have-medical-board-looking-for-alternatives-142005293.html>

Anonymous defaces police equipment supplier site, releases Symantec code. For the second time the week of March 5, hackers associated with the Anonymous hacking collective took down a Web site in retaliation for the arrests of several of their prominent members. The latest victim was New York Ironworks, a supplier of police equipment and tactical gear based in New York City. The company’s main Web page was defaced with a message from AntiSec, a group affiliated with Anonymous, one of whose members was arrested the week of March 5. The message expressed support for those who were arrested and anger at fellow hacker “Sabu” whose cooperation with the FBI contributed to the recent arrests. It included a brief diatribe against the FBI, a promise of more hacks March 9, and a 1-minute clip of the final moments of the movie the Fight Club. Also posted on the defaced site was what appeared to be hundreds of usernames and passwords as well as evidence purporting to show that the hackers had gained root access to the server hosting the Web site. Meanwhile, AntiSec members also released source code to Symantec’s Norton Antivirus 2006 software in apparent tribute to those who were recently arrested. A 1.07GB file that is apparently the source code was published on Pastebin March 8. Source:

http://www.computerworld.com/s/article/9225043/Anonymous_defaces_police_equipment_supplier_site_releases_Symantec_code?taxonomyId=17

UNCLASSIFIED

UNCLASSIFIED

FBI says Irish police misstep led to leak of sensitive conference call by hackers. An Irish police officer's e-mail blunder led to the leak of a sensitive conference call between the FBI and Scotland Yard, U.S. law enforcement said March 6. An indictment unsealed in a New York court alleges a teenager linked to the Lulz Security group of hackers was able to eavesdrop on the call after an unnamed officer with Ireland's national police force forwarded a work message to his unsecure personal e-mail account. The e-mail, which apparently originated from an individual with the FBI, invited dozens of law enforcement officers from across Europe and the United States to coordinate efforts against LulzSec and its amorphous umbrella group, Anonymous. The FBI's indictment said a man intercepted the e-mail and used the information in it to access and secretly record the January 17 call, which hackers subsequently broadcast across the Internet. The indictment said the man was charged with one count of computer hacking conspiracy, and one count of intentionally disclosing an unlawfully intercepted wire communication. Source: http://www.washingtonpost.com/world/europe/fbi-says-irish-police-misstep-led-to-leak-of-sensitive-conference-call-by-hackers/2012/03/06/gIQATDy9uR_story.html

ENERGY

(West Virginia) Thieves target coal mine; reward offered for information. Thieves stole \$20,000 worth of equipment from a coal mine in Boone County, West Virginia, March 7; a problem authorities claim is becoming common in the area. Miners are frequently being prevented from working because of stolen equipment. State police said thieves are finding their way around security, stealing equipment and then selling it for bargain prices. It is an effort that troopers believe is leading to more illegal activity. The investigation into the recent theft is ongoing. Source:

[http://www.wsaz.com/news/headlines/Thieves Target Coal Mine Reward Offered for Information_141817753.html](http://www.wsaz.com/news/headlines/Thieves_Target_Coal_Mine_Reward_Offered_for_Information_141817753.html)

(Wisconsin) WE Energy substation victim of copper theft. A WE Energies substation in Rubicon, Wisconsin, was the victim of copper wire theft five times in 2 weeks, the Beaver Dam Daily Citizen reported March 6. The Dodge County Sheriffs Department, working in cooperation with WE Energies, agreed to conduct surveillance of the site. March 5, authorities saw two men in the act of stealing and were able to take one person into custody after he hid in a recycling dumpster. The man was held on suspicion of theft, possession of burglary tools, criminal damage to property, and criminal trespass. It was unclear exactly how much copper was stolen or how much damage was caused as a result of the burglaries. Source:

http://www.wiscnews.com/bdc/news/local/article_3c07ae46-6755-11e1-a8b4-001871e3ce6c.html

FOOD AND AGRICULTURE

Allergen alert: Spring rolls with fish and soy. The Canadian Food Inspection Agency (CFIA) and Gold Phoenix Asian Food are warning people with allergies to fish or soy not to eat certain Gold Phoenix Asian Food brand Spring Rolls and Sauce products distributed in British Columbia, Food

UNCLASSIFIED

UNCLASSIFIED

Safety News reported March 9. The recalled products contain fish and soy, which are not listed on the label. The recall is for: Crispy Vegetable & Yam Spring Rolls & Sauce and Vietnamese Crispy Spring Rolls & Sauce. Source: <http://www.foodsafetynews.com/2012/03/allergen-alert-spring-rolls-with-fish-and-soy/>

(California) Imported candies with too much lead. Three candies are being recalled after tests conducted by the California Department of Public Health (CDPH) found they exceed California standards for lead, Food Safety News reported March 6. The recalled candies are: Chef's Pride Rewadi Candy imported from Pakistan; Shah's Deer Brand Revdi (Sesame Candy) imported from India; and Shah's Deer Brand Revdi (Gud) (Sesame Candy) imported from India. Chef's Pride Rewadi Candy was distributed by R&R Importers in Montclair, California. The two Shah's Deer Brand candies were distributed by Shah Distributors in Gardena, California. Recent chemical analysis by CDPH showed Chef's Pride Rewadi Candy, Shah's Deer Brand Revdi (Sesame Candy), and Shah's Deer Brand Revdi (Gud) (Sesame Candy) contained as much as 0.12, 0.40, and 0.35 parts per million of lead, respectively. California considers candies with lead levels in excess of 0.10 parts per million to be contaminated. Source: <http://www.foodsafetynews.com/2012/03/california-recall-for-candies-with-too-much-lead/>

Tyson Foodservice pizza topping recalled. Tyson Prepared Foods of South Hutchinson, Kansas, is recalling about 12,060 pounds of pizza topping because the packaging identifies an ingredient as beef, but it actually is pork, Food Safety News reported March 6. Additionally, the pork contains soy, a potential allergen, which is not listed on the label. The discrepancies were reported by a product purchaser. The recalled products were produced January 12 and were sold to food-service institutions nationwide via a distributor. The product is intended for use in restaurants or institutional food operations; it is not sold in retail grocery stores. Source: <http://www.foodsafetynews.com/2012/03/foodservice-pizza-topping-recalled/>

High levels of resistant bacteria on meat (again). A new report is out from the federal collaboration that monitors antibiotic resistance in animals, retail meat, and people, and the news is not good, Wired reported March 3. The full title is the 2010 Retail Meat Report from the National Antimicrobial Resistance Monitoring System. The report was issued by the Food and Drug Administration. It reports the results of testing on 5,280 meat samples collected in 2010 in California, Colorado, Connecticut, Georgia, Maryland, Minnesota, New Mexico, New York, Oregon, Tennessee, and Pennsylvania. The report — which is broken down first by food-borne organism and then by meat type — notes a number of instances where either the percentage of bacteria that are antibiotic resistant, or the complexity of the resistance, is rising. Source: <http://www.wired.com/wiredscience/2012/03/resistant-bacteria-meat/>

U.S. offers food safety alerts on Twitter, state by state. The U.S. Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) has launched Twitter accounts for specific states that can share news of recalls on poultry, meat, and other food products for those specific regions, Mashable reported March 5. "These new Twitter feeds provide yet another mechanism for us to provide consumers with critical updates and relevant information they need to protect their families from foodborne illness," the USDA Under Secretary for Food

UNCLASSIFIED

UNCLASSIFIED

Safety said. “The immediacy of information-sharing through social media is unparalleled, and we believe these timely, targeted updates will better protect public health.” Every state will now have its own Twitter alert handle using the state’s two-letter abbreviation followed by “_FSISAlert.” Previously FSIS alerts were issued through press releases and one main Twitter account, @USDAFoodSafety. The state-specific feeds will help consumers more easily identify which recalls are relevant to them. Source: [http://mashable.com/2012/03/05/food-safety-alerts-twitter/?utm_source=pulseneews&utm_medium=referral&utm_campaign=Feed:+Mashable+\(Mashable\)](http://mashable.com/2012/03/05/food-safety-alerts-twitter/?utm_source=pulseneews&utm_medium=referral&utm_campaign=Feed:+Mashable+(Mashable))

(Nebraska; Wyoming) Animal feed recalled, effect on horses feared. Western Feed LLC is voluntarily recalling two lots of its Kountry Buffet 14 percent feed because it may contain monensin sodium, which is potentially fatal for horses, the Morrill, Nebraska company said March 3. Monensin sodium, or Rumensin, is a medication used for some livestock and poultry. However, it can be fatal to horses if fed at sufficiently high levels, Western Feed said in a statement posted on the Food and Drug Administration Web site. Western Feed received a report of some horses that died from eating the feed. The feed was distributed December 2 to December 15, 2011, to retailers in Nebraska and Wyoming. Source: <http://www.reuters.com/article/2012/03/03/us-recall-horsefeed-idUSTRE8220JG20120303>

Allergen alert: ‘Gluten free’ candy with wheat. Jelly Belly Candy Co. of Fairfield, California, recalled Peter Rabbit Deluxe Easter Mix “Gluten Free” candies because the malted milk balls may contain wheat, Food Safety News reported March 5. The recall is for 2.7-ounce bags. The candy assortment was distributed nationwide. Source: <http://www.foodsafetynews.com/2012/03/allergen-alert-gluten-free-candy-with-wheat/>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Alabama) Pipe bomb diffused at Winston County Courthouse. The Winston County, Alabama Courthouse was abuzz with activity March 8 after an active pipe bomb was discovered, the sheriff told WBRC 6 Birmingham. In an investigator’s room, a theft victim was identifying his stolen tool box, when they opened up the tool box and discovered the bomb. Winston County authorities called in Alcohol, Tobacco, Firearms, and Explosives agents and the Jefferson County Bomb Squad to diffuse the bomb. They were successful in disarming it. The sheriff said the tool box was seized after authorities busted a theft ring during a raid earlier the week of March 5 at the Natural Bridge Motel. Source: <http://northwestal.myfoxal.com/news/news/107612-pipe-bomb-diffused-winston-county-courthouse>

FBI investigates suspicious letters delivered to schools, businesses in D.C., 6 states. Two more suspicious letters with powder were delivered in Washington, D.C., March 8, one at Amidon Bowen Elementary and one at Bibiana restaurant. Oyster-Adams Bilingual School evacuated after suspicious letters were found. FBI agents and local law enforcement agencies were

UNCLASSIFIED

UNCLASSIFIED

investigating possible links between about 20 suspicious letters delivered in Washington, D.C., Texas, Alabama, Massachusetts, Rhode Island, Connecticut, and New York City. The six letters discovered in Washington, D.C. appear to be linked and all of them were tested and are not hazardous, officials said. Bibiana became the third Italian restaurant in Washington D.C. to receive a suspicious mailing with white powder inside. HAZMAT crews removed the letter for testing. March 8, another school received an alarming delivery. Office personnel found an envelope containing white powder at Amidon Bowen Elementary. The envelope was found before students arrived at school. The Washington, D.C. Department of Health and Oyster Adams Bilingual School were evacuated March 7. Before that, two other Italian restaurants were evacuated the week of March 5. A woman on a stretcher was taken out of the Department of Health after a letter containing white powder was found. Just hours before that, the Oyster Adams Bilingual School was evacuated when another letter was found. It contained flour and children returned to school about an hour later. Several schools in the Dallas area, a middle school in Connecticut, an art museum in New York City, a bank in Birmingham, Alabama, and schools in Massachusetts and Rhode Island all received similar letters. Law enforcement sources said, the letters are not addressed to anyone in particular. "We'll investigate who is responsible, because we can't have this type of drain on our federal, state, and local authorities and not to mention the panic it causes the community," said the Chief of the Enfield, Connecticut Police. Source: <http://www.wjla.com/articles/2012/03/fbi-investigates-suspicious-letters-delivered-to-schools-businesses-in-d-c-6-states-73553.html>

(Massachusetts) 2 arrested after allegedly plotting shooting at former high school over Facebook. Two Massachusetts men were arrested March 5 after allegedly discussing on Facebook how they would carry out a Columbine-style shooting at their former high school, Fox News reported. Both were arrested following an investigation by police and school officials. Both face charges of threatened use of a dangerous weapon at Attleboro High School in Attleboro, Massachusetts. According to police, a current student at the high school saw the alleged discussion between the two men on Facebook and contacted school officials, who immediately notified police. The alleged discussion took place on the individual Facebook pages of the former students. A specific target was not mentioned in the discussions, and school officials do not believe that anyone at the school was in imminent danger. Source: <http://www.foxnews.com/us/2012/03/06/2-arrested-after-allegedly-plotting-shooting-at-former-high-school-over/>

(Oklahoma) Dramatic shootout outside Tulsa courthouse. A man was arrested March 7 after he opened fire outside the Tulsa County Courthouse in Tulsa, Oklahoma, wounding a deputy and a bystander before being wounded himself, police said. The gunman was in critical condition after being shot by police. Police said the man walked into the plaza outside the courthouse and Tulsa City-County Library and began firing into the air. He then sat on a cement bench at the plaza, according to KJRH 2 Tulsa. Three deputies reportedly arrived moments later and exchanged fire with the suspect. One deputy was shot in the hand. The deputy is in serious condition with non-life-threatening injuries. Deputies fired five rounds at the suspect, striking him in the face and body. He was taken into surgery and was in critical condition as of March 7. It is not clear if a bullet from the gunman or from police struck the bystander, who is in fair

UNCLASSIFIED

UNCLASSIFIED

condition. A police spokesman said the suspect was considered to be in police custody, but had not been formally charged. The courthouse was set to be open as usual March 8. The Tulsa World reported that a wedding ceremony had just taken place in the plaza when the gunfire erupted. Source: <http://usnews.msnbc.msn.com/news/2012/03/08/10608473-dramatic-shootout-outside-tulsa-courthouse>

IG faults Energy Department for not fully implementing HSPD-12. Despite 7 years of effort and \$15 million spent, the Department of Energy (DOE) has not fully implemented the physical and logical access controls required under Homeland Security Presidential Directive-12 (HSPD-12), according to a new report from the DOE inspector general (IG), Federal Computer Week reported March 5. The agency has also not issued HSPD-12 credentials to many of the 40,000 contractor personnel at its 5 field sites, the report said. Two of the field sites, Oak Ridge National Laboratory and the East Tennessee Technology Park, were partially done, and three others had not started yet. Under HSPD-12, federal agencies were required to establish credentialing systems for workers and contractors for access to buildings, computers and equipment. The IG also said four of the field sites failed to provide credentials to contractors who do not hold security clearances, which is contrary to the directive. All together, about 11,000 individuals without security clearances who require routine access to work sites for at least 6 months had not been issued credentials as required, the IG wrote in the report. He faulted the department for not providing effective guidance. Source: <http://fcw.com/articles/2012/03/05/ig-faults-energy-department-for-not-fully-implementing-hspd12.aspx>

(Colorado) Guns OK'd on campus. The Colorado Supreme Court ruled March 5 that students and employees with concealed-weapon permits can carry handguns on University of Colorado campuses, overturning a ban by the school's regents. Gun-rights advocates had challenged the university policy that was adopted in 1994, arguing the university's governing board had superseded state gun laws. The justices agreed, noting that the state's concealed-carry law, passed by the state legislature, trumped the university's policy. Source: <http://www.theprovince.com/news/Guns+campus/6256727/story.html>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

How Anonymous plans to use DNS as a weapon. After engaging in a recent rash of attacks in retaliation for the takedown of file-sharing site Megaupload, the Anonymous's denial of service tools have not been as active. Disappointed with the current denial of service tools at their disposal, members of Anonymous are working to develop a next-generation attack tool that will, among other options, use the Domain Name System (DNS) itself as a weapon. The scale and stealthiness of the technique, called DNS amplification, is its main draw for Anonymous. DNS amplification hijacks an integral part of the Internet's global address book, turning a relatively small stream of requests from attacking machines into a torrent of data sent to the target machines. Source: <http://arstechnica.com/business/news/2012/03/how-anonymous-plans-to-use-dns-as-a-weapon.ars>

UNCLASSIFIED

UNCLASSIFIED

Scareware demands ransom after making files and folders invisible. Bitdefender came across a piece of scareware that makes victims believe something may have happened to all the files and folders stored on their computers. The user is then requested to pay \$80 for a tool that allegedly addresses the problem. Identified as Trojan.HiddenFilesFraud.A, the rogue disk repair utility starts operating by informing the user of certain issues that affect the computer. Since many users are accustomed to fake antivirus, this malicious application is programmed to make everything look more realistic. It changes the attributes of all files and folders, setting them as Hidden, so the user may believe everything was deleted from the hard drive. Certain key shortcuts are also disabled to induce more panic. Also, the worm that downloads HiddenFilesFraud.A, Win32.Brontok.AP@mm, ensures the files' attributes cannot be modified from Windows Explorer back to their original state. After displaying the numerous —errors that affect the system, the scareware advertises a repair utility that costs \$80. However, the so-called utility does absolutely nothing. Brontok.AP@mm, the element responsible for installing Trojan.HiddenFilesFraud.A, quickly copies itself on removable media drives to ensure it spreads without difficulty from one computer to another. Source:

<http://news.softpedia.com/news/Scareware-Demands-Ransom-After-Making-Files-and-Folders-Invisible-257383.shtml>

Chinese tech firms fingered for military collaboration. The People's Liberation Army is actively arming and developing its soldiers with advanced information warfare capabilities which would represent a —genuine risk to U.S. military operations in the event of a conflict, a new report alleges. Contractor Northrop Grumman's report for the U.S. government on the cyber threat posed by China was released March 8. The contractor asserts the People's Republic believes information warfare and computer network operations are a vital part of any military operation and are integrating them with traditional components under a framework known as —information confrontation. It argues the Chinese military is constantly evaluating U.S. command and control infrastructure and will therefore likely —target these system with both electronic countermeasures weapons and network attack and exploitation tools in the event of a conflict. The report also warns that joint ventures of the Symantec Huawei type could lead to a risk of intellectual property theft and long-term erosion of competitiveness for Western firms. The close relationship between China's large multinational telecoms and hardware-makers and the PLA also creates a potential for state-sponsored or directed attacks against the supply chain for equipment used by military, government, and private industry, the report warns. Source: http://www.theregister.co.uk/2012/03/08/northrop_grumman_china_pla/

2 in 3 Android anti-malware scanners not up to the job. Two-thirds of Android anti-malware scanners failed to protect against a range of malware in independent tests. AV-Test put 41 different virus scanners for Android through their paces. Almost two-thirds of these scanners are not yet suitable for use as reliable products, identifying less than 65 percent of the 618 types of malware tested. Packages that detected more than 90 percent of the Android malware thrown at them included Droid security software from Avast, Dr Web, F-Secure, Ikarus, Kaspersky, Zoner, and Lookout. Products that picked up more than 65 but less than 90 percent of Android malware included applications from established desktop companies (AVG, Bitdefender, ESET, Norton/Symantec, QuickHeal, Trend Micro, Vipre/GFI and Webroot) and

UNCLASSIFIED

UNCLASSIFIED

many mobile specialists (AegisLab and Super Security). Android security products from Bullguard, Comodo, G Data, McAfee, NetQin, and Total Defense fell into the third range (detection of between 40 to 65 percent). AV-Test said these products generally provided reliable malware protection against a few families, but fell down elsewhere — probably due to inadequate mobile malware sample collection. A fourth group of Android security products provided detection rates of less than 40 percent — essentially completely unreliable. These products — none of which came from recognized security vendors — generally failed to react even when smartphone users opened the well-known Android Trojan, much less detecting anything wrong during a regular scan. Source:

http://www.theregister.co.uk/2012/03/07/android_anti_malware_tests/

Anonymous takes down security firm's website, vows to fight on after arrests. Hackers claiming to belong to the Anonymous hacking collective defaced Panda Security's PandaLabs Web site March 7 in apparent response to the arrests of five hackers March 6 in the United Kingdom and the United States. In a defiant message posted on PandaLabs' hacked homepage, Anonymous taunted the former LulzSec leader Sabu for helping the FBI nab the hackers and vowed to carry on its hactivist campaign regardless of the setback. They also posted what appeared to be log-in credentials of numerous Panda Labs employees. They noted the attack on the security firm's site was in retaliation for Panda's alleged role in helping law enforcement crack down on members of the collective. According to a statement, a Panda Security spokeswoman said the hackers obtained access to a Panda Security Web server hosted outside of Panda's internal network. This server was used only for marketing campaigns and to host company blogs, it said. "Neither the main website www.pandasecurity.com nor www.cloudantivirus.com were affected in the attack," the statement said. "The attack did not breach Panda Security's internal network and neither source code, update servers nor customer data was accessed. The only information accessed was related to marketing campaigns such as landing pages and some obsolete credentials, including supposed credentials for employees that have not been working at Panda for over five years," the company said. Source:

http://www.computerworld.com/s/article/9224958/Anonymous_takes_down_security_firm_s_website_vows_to_fight_on_after_arrests?taxonomyid=17

6 charged with hacking; LulzSec founder reportedly helping Feds. Six computer hackers associated with groups including Anonymous, LulzSec, and AntiSec were arrested and charged in New York in connection with a series of attacks on computers used by the entertainment industry, credit card companies, intelligence firms, and an Irish political party, U.S. officials announced March 6. One of the six, known by his computer name of "Sabu," pleaded guilty previously and was said by officials to be working with the government against his former colleagues. He was described by officials as one of the founders of LulzSec, an offshoot of the antigovernment hacking group Anonymous. LulzSec planned and executed attacks around the world against targets the group saw as favoring established business and government institutions. Sabu pleaded guilty August 15, 2011 to 12 counts connected to computer hacking and other crimes against Fox Broadcasting, Sony Pictures, and the Public Broadcasting Service, according to the FBI and the U.S. attorney's office for the Southern District of New York. Source:

UNCLASSIFIED

UNCLASSIFIED

<http://www.chicagotribune.com/news/nationworld/la-na-nn-lulzsec-hackers-charged-20120306,0,6670874.story>

1200,000 webpages compromised to lead visitors to fake AV sites. In the past several months, mass infections were not uncommon, and now security experts believe they found another one. Websense found 30,000 unique Web sites are currently compromised to redirect visitors to sites that promote fake antivirus software. A total of 200,000 Web pages, part of the 30,000 sites, are compromised, with the campaign apparently designed to target mostly sites hosted by the WordPress content management system. After multiple redirects, victims are taken to a Web site that performs a fake scan, pointing out many infections and threats. The scan is designed to appear as if it takes place in a Windows Explorer window, but in reality it is simply a Web page designed to fool users. When the scan is complete, the user is urged to install an antivirus tool. However, the antivirus tool is a trojan that once installed provides complete control of the infected machine. More than 85 percent of the compromised sites are located in the United States. The injected code is usually placed before the tag. Web site administrators who suspect their sites may be compromised should check their code for the malicious script. According to researchers, if one of the Web pages displays the code, then most likely the entire site is compromised and each page should be thoroughly checked and cleaned. Source: <http://news.softpedia.com/news/200-000-Webpages-Compromised-to-Lead-Visitors-to-Fake-AV-Sites-256874.shtml>

4 high severity vulnerabilities fixed in Chrome Stable 17.0.963.65. Google released a new variant of Chrome Stable 17 to address important vulnerabilities that may have affected the safety of users. Chrome Stable 17.0.963.65 addresses 14 high-severity flaws that include use-after-free issues in the v8 element wrapper, in SVG value handling, in SVG document handling, in SVG use handling, in multi-column handling, in quote handling, in flexbox with floats, in class attribute handling, in table section handling, and with SVG animation elements. Other security holes include an out-of-bounds read in text handling, bad casts in anonymous block splitting and in-line box handling, and a buffer overflow in the Skia drawing library. Source: <http://news.softpedia.com/news/14-High-Severity-Vulnerabilities-Fixed-in-Chrome-Stable-17-0-963-65-256594.shtml>

NATIONAL MONUMENTS AND ICONS

Wildfires: Aerial firefighting fleet insufficient, chief says. With another potentially devastating wildfire season on the horizon, the U.S. Forest Service chief told Congress March 6 the agency's diminished and aging fleet of firefighting air tankers is insufficient to combat the nation's increasingly severe fires. Air tankers are a central component of the Forest Service's firefighting operations, particularly in Inland Southern California, where communities like Lake Arrowhead, Idyllwild, and Big Bear are surrounded by rugged terrain and are accessible by only a few roads. However, the number of air tankers at the agency's disposal has fallen from 43 to 11 in the last 12 years as airworthiness issues grounded many of the decades-old aircraft. A proposal contains a request for \$24 million to help modernize the agency's aerial firefighting fleet, and the Forest Service is moving forward to acquire more tankers. However, it is unclear when

UNCLASSIFIED

UNCLASSIFIED

additional aircraft would be available. The fleet has dwindled while fire seasons have grown longer and more destructive, a trend attributed in part to climate change. Wildfires scorched more than 8 million acres in 2011, placing it among the 5 worst years over at least a half-century. Source: <http://www.pe.com/local-news/politics/ben-goad-headlines/20120306-wildfires-aerial-firefighting-fleet-insufficient-chief-says.ece>

POSTAL AND SHIPPING

PUBLIC HEALTH

CDC: ‘Superbug’ transmitted outside hospitals. Many patients infected by the deadly superbug *Clostridium difficile* (*C. difficile*), long thought to be contracted mainly during hospital stays, are already exposed when they are admitted to the hospital, U.S. infectious disease experts said March 6. Rates of *C. difficile*, the most common hospital-based infection in the United States, continue to climb. A new study from the U.S. Centers for Disease Control and Prevention (CDC) found half of the cases of *C. difficile* reported by hospitals were present at the time a patient was admitted or within the first 3 days of admission, suggesting they were already infected when they entered the hospital. *C. difficile* is linked to more than 14,000 U.S. deaths each year, according to the CDC. The infections just in hospitals add an extra \$1 billion a year in health system costs. While *C. difficile* has long been thought to be a hospital problem, the new CDC report suggests patients can be exposed to *C. difficile* in many healthcare settings. Hospital stays involving *C. difficile* infections as the primary diagnosis more than tripled between 2000 and 2009, fueled in part by more deadly strains of the drug-resistant bacteria. Source: <http://www.foxnews.com/health/2012/03/07/cdc-superbug-transmitted-outside-hospitals/>

New report calls for enhanced security to safeguard protected health information. With the release March 5 of “The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security,” health care organizations now have a new method to evaluate the “at risk” value of protected health information (PHI) that will enable them to make a business case for appropriate investments to better protect it. This report was created through the PHI Project. Source:

http://www.ansi.org/news_publications/news_story.aspx?menuid=7&articleid=3173

TRANSPORTATION

(Washington, D.C.) Metro knew of brake problems for years, transit officials say. Washington Metro Transit Authority (Metro) in Washington, D.C., knew for 6 years that some of its rail cars have brake parts that fail sooner than expected, transit officials said March 8. The failure was found in some of the agency’s newest rail cars in 2006. Most of the defective parts have been replaced, but 184 cars with similar parts are in service, according to Metro. The transit authority plans to begin replacing the parts — known as “brake disc hubs” — in the summer. In January and December 2011, brake parts fell from trains in two incidents. The December 2011 incident, which occurred during morning rush hour, shut down service along the downtown

UNCLASSIFIED

UNCLASSIFIED

core of the Orange and Blue lines for hours. The Metro chief executive said the system has suffered from a lack of funding and lax maintenance for years. The transit authority is amid a six-year, \$5 billion capital program to implement recommendations from the National Transportation Safety Board, refurbish stations and replace deteriorating equipment. Source: http://www.washingtonpost.com/local/trafficandcommuting/metro-board-member-says-agency-knew-of-brake-problems-for-years/2012/03/08/gIQAip0NzR_story.html

WATER AND DAMS

Dam emergency plans could be improved, say auditors. An Interior Department inspector general review of emergency action plans at seven large dams in the western United States finds room for improvement, Fierce Homeland Security reported March 5. In a report dated February 27, auditors examined emergency preparedness at five “national critical infrastructure” dams and two “major mission critical” dams. Destruction or failure of either type of dam would be devastating to the public. Bureau of Reclamation personnel at all seven dams had in place emergency action plans, auditors say, but all lacked documentation. Auditors acknowledge none of the documentation they say should be undertaken is a requirement of bureau policy, but say it is important nonetheless. Corrective actions learned as a result of exercises were not always entered into the Dam Safety Information System, and some after-action reports did not include recommendations at all. One national critical infrastructure dam had not conducted a tabletop emergency exercise since August 2007, auditors also found. Bureau policy requires that one be conducted once every 3 years; the report notes dam personnel subsequently held an exercise. However, bureau policy for training is also unclear, auditors say. The training requirement “broadly encompasses all dam operating personnel, even those individuals having only minor or indirect roles during emergency operations at the dam.” The bureau is updating and rewriting the training requirements, the report adds. Source: http://www.fiercehomelandsecurity.com/story/dam-emergency-plans-could-be-improved-say-auditors/2012-03-05?utm_medium=rss&utm_source=rss

(Louisiana) Corps of Engineers liable for levee failures. A federal appeals court upheld a judge’s landmark ruling March 2, that the U.S. Army Corps of Engineers is liable for property owners’ claims, saying the shoddy work on a shipping channel caused billions of dollars in damage in New Orleans from Hurricane Katrina’s storm surge. A three-judge panel from the 5th U.S. Circuit Court of Appeals rejected the federal government’s argument it is entitled to immunity from lawsuits blaming Katrina’s flood damage on the Corps’ operation and maintenance of the Mississippi River–Gulf Outlet, a New Orleans navigation channel. The federal government asked the 5th Circuit to reverse a 2009 decision by a U.S. District Judge, who ruled flooding in St. Bernard Parish and New Orleans’ Lower 9th Ward from the 2005 storm was a man-made disaster created by Corps negligence. The judge awarded nearly \$720,000 in damages to five plaintiffs who sued. The Corps has also received roughly 500,000 administrative claims that could become fodder for similar suits. Source: <http://www.sunherald.com/2012/03/03/3793742/corps-of-engineers-liable-for.html>

UNCLASSIFIED

UNCLASSIFIED

NORTH DAKOTA HOMELAND SECURITY CONTACTS

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

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

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168

UNCLASSIFIED