

**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. If you have any comments to improve this summary or local information you would like to see in the summary please send the information to; [kihagel@nd.gov](mailto:kihagel@nd.gov)

**UNCLASSIFIED**

**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**

**NORTH DAKOTA**

(North Dakota; Minnesota) **Collin Peterson: Dams may be part of solution.** A U.S. Representative, D-Minnesota, said Tuesday he's pleased Fargo-Moorhead officials picked a North Dakota diversion as their locally preferred flood protection plan. But he said it will be a "heavy lift" to get the local and federal funding necessary to build it. In meetings with Clay County and Moorhead officials, he advocated a multi-pronged approach to making sure a diversion gets built. He said that includes working on water retention projects that will reduce the negative effects a Red River diversion would have on downstream communities, including several in northwest Minnesota. He said Department of Agriculture dollars could be accessed to accomplish some of the work. In addition to building dams, he said the use of drain tiles by rural landowners could be another factor in reducing downstream impacts of a diversion. In decades past, using underground pipes to drain water from farmland was perceived as causing problems, he said. Source: <http://www.inforum.com/event/article/id/274621/>

# UNCLASSIFIED

**Power cooperatives make headway in restoring services.** Linemen by the hundreds continued working around the clock Tuesday to restore electric power to rural North Dakotans. But the damage is severe and the area affected is extensive. "It could be the end of the month before we get everything done," the co-manager of Mor-Gran-Sou Electric Cooperative said. Mor-Gran-Sou, which serves Morton, Grant, and Sioux counties, lost about 8,000 power poles in the April 2 storm and between 400 and 450 miles of power lines. Crews from Minnesota, Kansas, and Wisconsin have been called in to help. The city of Flasher is using a larger generator as its source of power. The issue with the Flasher area is transmission lines. Most of the residents in New Salem had power but the area surrounding the town was still blacked out. Roughrider Electric in Oliver County lost about 500 power poles in the storm. At Capital Electric Cooperative, a spokesman estimated there are still 200 to 300 customers without power; an additional 45 linemen from Idaho are on the job and he hopes power will be fully restored by early next week. At McLean Electric, a spokesman said there are still about 75 without service in scattered areas near Underwood, Riverdale, and south of Mercer. He said the co-op lost about 150 power poles and have called in crews from Verendrye Electric, hoping to have service fully restored by the week's end. It could be several months until permanent repairs are completed once power is restored, he said. Source: [http://www.bismarcktribune.com/news/state-and-regional/article\\_26b51952-41fa-11df-b747-001cc4c03286.html](http://www.bismarcktribune.com/news/state-and-regional/article_26b51952-41fa-11df-b747-001cc4c03286.html)

**North Dakota firm recalls whole beef head products that contain prohibited materials.** North American Bison Co-Op, a New Rockford, North Dakota establishment, is recalling approximately 25,000 pounds of whole beef heads containing tongues that may not have had the tonsils completely removed, which is not compliant with regulations that require the removal of tonsils from cattle of all ages, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced today. Tonsils are considered a specified risk material (SRM) and must be removed from cattle of all ages in accordance with FSIS regulations. SRMs are tissues that are known to contain the infective agent in cattle infected with Bovine Spongiform Encephalopathy (BSE), as well as materials that are closely associated with these potentially infective tissues. Therefore, FSIS prohibits SRMs from use as human food to minimize potential human exposure to the BSE agent. The recalled products were produced between June 25, 2009, and February 19, 2010. These products were shipped to distribution centers in Maryland, Michigan, and Minnesota for further sale. The problem was discovered during FSIS inspection activities at the establishment. Source: [http://www.fsis.usda.gov/News & Events/Recall\\_023\\_2010\\_Release/index.asp](http://www.fsis.usda.gov/News & Events/Recall_023_2010_Release/index.asp)

## **REGIONAL**

**(Minnesota) Chemical leak closed industrial park in Elk River.** A minor chemical leak caused Industrial Circle in Elk River, Minnesota, to close at 3:30 p.m. Tuesday, April 6 and reopen the following morning at 5:30. The Elk River Fire chief said the original call came in to the department at approximately 3:30 p.m. from a delivery person, who noticed the odor of a leak while dropping off a cylinder at Gradient Technology. At the time it was unknown what type of chemicals were in the canisters, so the immediate concern was to evacuate nearby businesses. The shipping company that called in the leak had delivered a shipment of eight cylinders to the business. Seven of those, each filled with six different chemicals, were leaking. A metro regional chemical assistance team was called in to meter the area and the leaks were determined to not be dangerous to the general public. However, some of the chemicals did have flammable characteristics, he said, and a noxious odor, so the department wanted to make sure the chemicals had fully dissipated. The chemical assistance

UNCLASSIFIED

## UNCLASSIFIED

team and the fire department worked together to bring the cylinders out of the building and in to the parking lot. Gradient Technology called in a contract company to clean up the spill. All of the chemicals were neutralized and disposed of, he said. The contract company, Bay West, showed up at 1:50 a.m. and finished up shortly after 5 a.m. The Elk River Fire Department also stayed on scene until 5. No area residential streets were closed. Source: <http://erstarnews.com/content/view/11856/94/>

**(Minnesota) Stillwater / Restaurant warns of credit breach.** More than a dozen people who visited Mad Copper Saloon & Eatery in downtown Stillwater, Minnesota, in the past few weeks may have had their credit card information stolen by a thief who apparently obtained the numbers via an unsecured router. "Somehow, the security of our network got breached. We have corrected the problem, and we sincerely apologize to anyone who has had a problem," the restaurant's owner said on April 6. He advised patrons to check their credit card statements, and if they find anything suspicious, to cancel the card and call the police. The restaurant owner said he learned last week of the thefts — which affected 12 to 15 customers — and immediately brought in a computer specialist to secure the router. He said he has heard from customers that their credit card information was used at Walmart stores in California. Source:

[http://www.twincities.com/ci\\_14832825?source=most\\_email&nclick\\_check=1](http://www.twincities.com/ci_14832825?source=most_email&nclick_check=1)

**(Minnesota) Eighth-grader terrifies students with handgun.** Authorities say they expect an eighth-grader will be charged with multiple felonies after terrorizing two classes at Hastings Middle School with a loaded handgun. School officials say the 14-year-old boy burst into a science class Monday and pointed the gun at the teacher and at students, who were too stunned to leave their seats. The boy then moved on to another classroom and broke a window to unlock the door and gain entry. He again pointed the loaded gun at students in the class, but fled without firing any shots. School officials say a police liaison officer caught up with the student as he ran out of the building and tackled him. Officers from Hastings and Dakota County arrested the boy and took him to juvenile detention. Source: <http://www.duluthnewtribune.com/event/apArticle/id/D9ETIRUG1/>

**(Montana) Residents get break from levee mandate.** Some 1,200 Great Falls and Vaughn residents living along the Sun River have received a reprieve from a looming deadline requiring their levees to be certified or face floodplain status on new federal maps, a U.S. senator said Monday. The Federal Emergency Management Agency (FEMA) is requiring new digital flood maps. As part of that process, levees had to be inspected and certified by April 28. Neither levee district has had the levees certified. The senator said Monday that U.S. Homeland Security Secretary agreed to cancel the April 28 deadline and send a FEMA certification team made up of national and regional staff to Great Falls to help determine the next steps in the flood re-mapping process. The Secretary also was agreeable to the senator's request to find a longer term solution to the levee certification and flood map issue. Missing the deadline would result in de-accreditation, with the properties being shown as located in the floodplain on the new maps requiring higher insurance rates and lowering property values. Residents of the levees districts said the Army Corps of Engineers would not certify the levees and that they could not afford to hire a private company. Source:

<http://www.greatfalls Tribune.com/article/20100406/NEWS01/4060312>

**(Montana) Missoula 911 dispatcher reported refinery explosion as joke.** Missoula County, Montana, authorities are investigating after a 911 dispatcher apparently broadcast a false report of an

UNCLASSIFIED

# UNCLASSIFIED

explosion last week as an April Fool's Day prank. The request for an emergency response came over the airwaves shortly after 8:30 a.m. on April 1, and the dispatcher told local fire and medical emergency services to respond to the Conoco bulk plant in Missoula for a large fire or explosion. The sheriff said the radio call was immediately followed by a request for cancellation. The Missoula County attorney has asked the sheriff's department to investigate and determine if a criminal offense occurred. The emergency services director said his department would make a personnel decision after interviewing the employees who were there during the prank. He did not know whether emergency crews responded to the false report. Source: [http://www.billingsgazette.com/news/state-and-regional/montana/article\\_5d93e3c8-4177-11df-bb40-001cc4c002e0.html](http://www.billingsgazette.com/news/state-and-regional/montana/article_5d93e3c8-4177-11df-bb40-001cc4c002e0.html)

**(Wyoming) Local restaurants hit with credit card scam.** Four local restaurants were targets over the weekend of a credit card scam. Cheyenne Police say the Pie Lady, Olive Garden, Golden House and Cloud Nine received calls from a man requesting receipt information, like credit card numbers. The man used an alias and claimed to be a detective with the Cheyenne Police Department. None of the restaurants gave any information to the caller. But, without a suspect in custody, Cheyenne Police are worried other restaurants may be targeted. Source: <http://www.kgwn.tv/story.aspx?ID=3888&Cat=2>

## **NATIONAL**

**(West Virginia) 25 confirmed dead in Montcoal mine explosion.** Officials at the site of a Monday afternoon explosion at Massey Energy's Performance Coal Co. in Montcoal in western Raleigh County, West Virginia, confirmed early Tuesday that 25 miners died in the blast. At a 2 a.m. press briefing, a Mine Safety and Health Administration (MSHA) administrator said rescue teams were pulled from the mine due to conditions inside. At that time four miners remained unaccounted for and two were receiving treatment at area hospitals. Concentrations of methane and carbon monoxide that rescue crews detected in the mine "were to the point that they were risking their own lives," he said. Rescue efforts will resume as soon as conditions permit. Officials also plan to drill bore holes from the surface into the mine to help ventilate it and to collect samples. That process will take some time because a road will have to be dozed to the site where the hole will be drilled, he said. The incident at Massey Energy's Performance Upper Big Branch Mine occurred shortly after 3 p.m. Monday. A nine-man crew was exiting the mine when there was an apparent explosion. Out of the nine miners on the man trip, seven were killed instantly. Officials said they believed the missing miners may be as far back as 8,000 feet from mine portal. Authorities are hoping the trapped miners made it to one of the mine's refuge chambers, which can provide 90 hours of oxygen. Those chambers will hold up to 36 people and have food and water available. Source: <http://www.register-herald.com/todaysfrontpage/x552031616/Massey-Energy-reports-explosion-at-W-Va-mine>

## **INTERNATIONAL**

**Qaeda group threatens to attack World Cup.** The North African terror group al Qaeda in the Islamic Maghreb has threatened to attack this summer's World Cup games in South Africa. "How amazing could the match United States vs. Britain be when broadcasted live on air at a stadium packed with spectators when the sound of an explosion rumbles through the stands, the whole stadium is turned upside down and the number of dead bodies are in their dozens and hundreds, Allah willing," read a statement the group published in a recent issue of the Jihadi online magazine Mushtaqun Lel Jannah

UNCLASSIFIED

## UNCLASSIFIED

(Longing to Paradise). In addition to the U.S. and U.K. teams, the teams representing France, Germany, and Italy are also on the group's list of targets. The group said they would use some undetectable explosive that will be able to circumvent security checkpoints at the games. The statement appeared to directly challenge FIFA's president. "All the security checks and X-ray machines that America will be sending after reading this article would not be capable of detecting how those explosives made it into the stadium and that for a simple reason that we will be announcing in due course," the statement says. Source: [http://www.cbsnews.com/8301-503543\\_162-20001940-503543.html](http://www.cbsnews.com/8301-503543_162-20001940-503543.html)

**Researchers trace data theft to intruders in China.** Turning the tables on a China-based computer espionage gang, Canadian and U.S. computer security researchers have monitored a spying operation for the past eight months, observing while the intruders pilfered classified and restricted documents from the highest levels of the Indian Defense Ministry. In a report issued Monday night, the researchers, based at the Munk School of Global Affairs at the University of Toronto, provide a detailed account of how a spy operation it called the Shadow Network systematically hacked into personal computers in government offices on several continents. The Canadian researchers stressed that while the new spy ring focused primarily on India, there were clear international ramifications. One researcher noted that civilians working for NATO and the reconstruction mission in Afghanistan usually traveled through India and that Indian government computers that issued visas had been compromised in both Kandahar and Kabul in Afghanistan. "That is an operations security issue for both NATO and the International Security Assistance Force," said the researcher, who is also chief executive of the SecDev Group, a Canadian computer security consulting and research firm. Source: <http://www.nytimes.com/2010/04/06/science/06cyber.html?pagewanted=1>

## **BANKING AND FINANCE INDUSTRY**

**(Arizona) Police: Bank robber threatened tellers with explosives.** A 72-year-old man has been arrested after police say he robbed a Compass Bank located inside an Albertson's supermarket in Prescott. Prescott Police say that he entered the bank, showed tellers a handgun, and claimed he had put explosives in the store Thursday afternoon. He robbed two tellers of an undisclosed amount of cash, as well as some personal money, according to police. He was taken into custody immediately after he exited the bank. The store was evacuated and searched for explosives, but nothing was found. He is being held at the Yavapai County Jail on three counts of armed robbery, two counts of aggravated assault, and two counts of kidnapping. He is being held on a \$500,000 bond pending his next court appearance. Source: <http://www.myfoxphoenix.com/dpp/news/crime/bank-robber-explosives-4-8-2010>

**(Texas) White powder mailed to west Houston office.** Almost 150 people were evacuated from a building in west Houston after a mysterious white powder was found in a letter received at one of the offices. Houston firefighters arrived at approximately 2 p.m. Thursday to the Wallis State Bank building on Town and Country Lane after learning of the opened letter in the mailroom in the Tax Masters, Inc. office. A Houston Fire Department spokesman said that 20 people who were in the mailroom when the powdery substance was discovered were escorted out of the office and isolated. Investigators, including U.S. Postal Service officials, are trying to identify the substance, but tests so far have not yielded any positive results for toxic contamination. Source:

UNCLASSIFIED

# UNCLASSIFIED

<http://www.myfoxboston.com/dpp/news/local/100408-white-powder-mailed-to-west-houston-office>

**Visa warns of key logger increase.** Visa has warned its customers to be aware of the increased risk posed by key-logging trojans. The credit-card company claimed in recent weeks it had seen a rise in this technique, which obtains information from victims through software that captures and records their keystrokes. The particular malware affecting Visa payment systems sends payment card data to a fixed IP address or e-mail that the hacker can then access and use as he or she sees fit. "In these instances, the hacker is able to install key logger malware on the point of sale (POS) system due to insecure remote access and poor network configuration," Visa stated. It admitted that key loggers can be difficult to detect, but it has developed a list of security measures for retailers using the system. These include removing unnecessary remote access, implementing a secure-network configuration, regularly observing which software is installed and ensuring anti-virus programs are kept up-to-date. Source: <http://www.itpro.co.uk/622108/visa-warns-of-key-logger-increase>

**Customers sue Countrywide Financial over theft and sale of personal data.** Customers of Countrywide Financial have filed a class-action lawsuit over the 2008 data breach that enabled company insiders to steal and sell their personal information. According to a Courthouse News Service report, the class-action lawsuit on behalf of 16 plaintiffs seeks \$20 million in damages, plus punitive damages. The data theft, originally attributed to a single employee working over a two-year-period, exposed data on tens of thousands of customer records. The lawsuit alleges that Countrywide Financial employees stole and sold "tens of thousands, or millions" of customers' personal financial information, according to the news report. The suit claims the defendants do not dispute that customers' private financial information was disseminated. It seeks to find out "whether the dissemination was intended as a plan or scheme, or was intentional; [and] whether any of the defendants was simply aiding and abetting, rather than an architect of the plan to disseminate the personal information." Source:

[http://www.darkreading.com/database\\_security/security/privacy/showArticle.jhtml?articleID=224201969](http://www.darkreading.com/database_security/security/privacy/showArticle.jhtml?articleID=224201969)

**SEC proposes revised rules for asset-backed securities.** In response to problems exposed by the financial crisis, the Securities and Exchange Commission on April 8 proposed comprehensive changes to the rules governing offers, sale and reporting with respect to asset-backed securities. The proposed revisions are intended to improve investor protection and increase transparency and efficiency in the public and private markets for asset-backed securities. Under current rules, asset-backed securities may be registered on a Form S-3 registration statement and later offered "off the shelf" if the securities are rated investment grade by a nationally recognized statistical-rating organization. In recognition that investors may have unduly relied on ratings, the proposed rules would eliminate the credit-rating requirement. The SEC is proposing to revise Regulation AB, which currently requires disclosure of material, aggregate information about the composition and characteristics of asset pools, to provide additional disclosure requirements for asset-backed security offerings. For each loan or asset in the asset pool, the SEC is proposing to require disclosure of specified data relating to the terms of the asset, obligor characteristics, and underwriting of the asset. Such data would be provided in a machine-readable, standardized format. Issuers would be required to provide the asset-level data or grouped account data at the time of securitization, when new

UNCLASSIFIED

# UNCLASSIFIED

assets are added to the pool underlying the securities, and on an ongoing basis. Source:

<http://www.hedgeco.net/blogs/2010/04/08/sec-proposes-revised-rules-for-asset-backed-securities/>

**Javelin report: ATM attacks growing in sophistication.** ATM attacks have shifted from basic skimming into attacks on ATM software and ATM networks, fraudulent mobile alerts, and account takeover via stolen information and call centers, according to a report released on April 6 by Javelin Strategy & Research. Traditional skimming is being replaced by more sophisticated attacks as criminals have become more organized and global, said an analyst at the Pleasanton, California-based research firm and author of the report. “Now what we’re seeing is use of malware inside the ATMs or somewhere along the ATM network that takes the same data and gives it to the criminals.” For example, there have been ATM attacks in which apparent maintenance crews opened up ATMs and installed malware on the machines, he said. Early last year, Diebold Inc. issued a security update for its Windows-based ATMs after criminals attacked a number of them in Russia and installed malware designed to steal sensitive data. In other cases, such as in the RBS WorldPay heist, criminals target the backend, where the ATM interfaces with other networks at a financial institution, the analyst said. “Someone can gain access through administrative privileges to encrypted PIN data, then use a laptop computer to reverse the encryption on the PINs,” he said. Source:

[http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185\\_gci1508178,00.html](http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1508178,00.html)

## **CHEMICAL AND HAZARDOUS MATERIALS SECTOR**

**EPA proposes adding more chemicals to Toxics Release Inventory List.** The U.S. Environmental Protection Agency (EPA) is proposing to add 16 chemicals to the Toxics Release Inventory (TRI) list of reportable chemicals, the first expansion of the program in more than a decade. Established as part of the Emergency Planning and Community Right to Know Act (EPCRA), TRI is a public EPA database that contains information on toxic chemical releases and waste-management activities reported annually by certain industries as well as federal facilities. EPA has concluded, based on a review of available studies, that these chemicals could cause human cancer. The purpose of the expansion is to inform the public about chemical releases in their communities and to provide the government with information for research and regulation development. Four of the new chemicals are proposed to be added under the polycyclic aromatic compounds category. This category includes chemicals that are persistent, bioaccumulative, toxic and are likely to remain in the environment for a very long time. The chemicals are not readily destroyed and may build up or accumulate in body tissue. The TRI, established as part of the EPCRA of 1986, contains information on nearly 650 chemicals and chemical groups from about 22,000 industrial facilities. EPA will accept public comments on the proposal for 60 days after it appears in the Federal Register. Source:

<http://yosemite.epa.gov/opa/admpress.nsf/d0cf6618525a9efb85257359003fb69d/f6a45e8e44dbef13852576fd005f7555!OpenDocument>

## **COMMERCIAL FACILITIES**

**(California) Downtown Calexico declared unsafe from 7.2 earthquake.** Calexico’s city manager says the earthquake-damaged business district is unsafe and should remain closed until the weekend so repairs can be made. He says business owners are pressuring him to remove the police tape and allow stores to reopen. The City Council is expected to decide on the matter Tuesday night. He says

UNCLASSIFIED

# UNCLASSIFIED

historic buildings with badly damaged facades pose a danger. Calexico was the U.S. city hit hardest by the 7.2-magnitude quake centered in Mexico's Baja California peninsula, where two people died. In downtown Calexico, glass, building cracks, and rubble are everywhere following Sunday's quake. The city manager says much of downtown was built about 100 years ago and the older buildings fared worse than those constructed more recently. Some businesses are beginning to re-open, while dozens more are still tagged too dangerous. Retro-fitting them will be costly, ranging into the tens of millions. In nearby El Centro, a shaky apartment foundation had residents still fearful for their lives. "El Centro's main street has a lot of structural damage with fallen brick, busted storefront windows, and garbage everywhere. The hospital set up a triage outside with numerous people coming in with broken bones," said a captain with the Salvation Army in El Centro. San Diego 6 reports the Sheraton Harbor Island hotel in San Diego was evacuated due to earthquake damage that includes cracked floors. Guests also reported room doors sticking after the quake. A San Diego Fire-Rescue spokesman says a structural engineer has determined the building itself is not compromised, but floors 7-12 in the center and north towers are red tagged and closed because exit doors are jammed. There are some reports of cracked buildings in San Diego's North Park and broken windows at the San Diego Sports Arena. Source: [http://www.sandiego6.com/news/local/story/Downtown-Calexico-Declared-Unsafe-from-7-2/9xFciod8t0S3\\_HvjOz7skA.csp](http://www.sandiego6.com/news/local/story/Downtown-Calexico-Declared-Unsafe-from-7-2/9xFciod8t0S3_HvjOz7skA.csp)

## **COMMUNICATIONS SECTOR**

**FCC may tweak broadband plan after Comcast ruling.** Despite a recent ruling that said the Federal Communications Commission did not have the right to interfere in Comcast's network management issues, the agency is pushing ahead with its national broadband plan, though there might be some tweaks. "The Comcast/BitTorrent opinion has no effect at all on most of the plan," the general counsel for the FCC wrote. "Many of the recommendations for the FCC itself involve matters over which the commission has an 'express statutory delegation of authority.' These include critical projects such as making spectrum available for broadband uses, improving the efficiency of wireless systems, bolstering the use of broadband in schools, improving coordination with Native American governments to promote broadband, collecting better broadband data, unleashing competition and innovation in smart video devices, and developing common standards for public safety networks." Those thoughts were echoed by the FCC chairman, who acknowledged that the court's decision "may affect a significant number of important plan recommendations." That includes: strengthening public safety communications; cyber security; consumer protection, including transparency and disclosure; and consumer privacy. Source: <http://www.pcmag.com/article2/0,2817,2362444,00.asp>

**(Hawaii) Vandals leave hundreds in Waipahu with no phone or Internet service.** 1,100 Hawaiian Telcom customers in Waipahu were cut off from telephone and internet service Sunday. "Sunday night we learned that two of our cables in the Waipahu area had been cut in several places," said a Hawaiian Telcom spokesperson. The target was a pole on Waipahu Depot Street. No copper was taken. Hawaiian Telcom says the vandalism of their poles is uncommon. Crews have been working around the clock to get customers back online since Sunday. So far at least 500 customers have had their service restored, but the job could take a while. Some who have been re-connected to the Internet say they are still experiencing some problems. There is no timeline when service will be restored. Hawaiian Telcom says it has filed a police report. Source: <http://www.khon2.com/news/local/story/Vandals-Leave-Hundreds-in-Waipahu-with-No-Phone/yQfuOL4m3UuE1YBkq1ZxUQ.csp>

UNCLASSIFIED

# UNCLASSIFIED

**(District of Columbia) FCC evacuated for bomb threat.** FCC headquarters was evacuated Wednesday morning due to a bomb threat, a source within the commission confirmed. Speculation regarding the threat emerged as events were canceled. Notification went out around 11:20 a.m. that a CLS round table had been canceled. Further speculation sped through various Twitter feeds, though nothing initially appeared on the FCC's Web site nor its own Twitter page. The source within the Portals said some meetings were held on the grass before staff was dispatched. "Several buildings cascaded into the threat warning," the source said. Details about the nature and timing of the threat were unavailable, though the source said staff was out for about two hours — the "longest ever," and that bomb-sniffing dogs were dispatched. E-mail releases from the commission resumed mid-afternoon. Source: <http://www.televisionbroadcast.com/article/98014>

**Congress pressing FCC on FM in cell phones.** The FCC chairman has been busy lately signing letters to Members of Congress who have written to him and the Homeland Security Secretary urging them to require inclusion of FM tuners in cell phones so that they are capable of receiving Emergency Alert System notifications. On April 2, the FCC released 61 letters that the chairman had sent in reply to those Members of Congress. The chairman carefully avoided taking any position on the issue, but noted that the FCC in December initiated a 28-month period during which the mobile phone companies must develop a commercial Mobile Service Alert System (CMAS). He noted that the FCC's standards for CMAS do "not require or prohibit the use of Alert-FM" or similar FM radio-based technologies for the cell companies' emergency alerting system. Source: <http://www.rbr.com/media-news/washington-beat/23042.html>

**(California) Calif gov declares state of emergency after earthquake.** The governor of California declared a state of emergency Monday after a powerful earthquake centered in Mexico left severe damage in southern California. A 7.2 magnitude earthquake centered in Baja California on Mexico's west coast Sunday killed two people and knocked out power and telephone services and damaged buildings there. The temblor also disrupted telephone communications, buckled roads, broke water mains, and damaged critical water storage facilities across the border in Imperial County, California, the governor said. The Mexican government-owned power company Comision Federal de Electricidad said it was restoring power to customers after the quake, although the utility did not say how many were without electricity. Two transmission lines between Mexicali and Tijuana on the northern border suffered outages and there were problems at 27 substations, 11 of which have since been brought back online, according to the company. Mexico's biggest fixed-line telephone company, Telefonos de Mexico, sent crews out to repair damaged fiber optic lines, although the company did not say how many people were without phone service. State oil monopoly Petroleos Mexicanos, or Pemex, said gasoline supplies were flowing into Baja California after a temporary power outage at a distribution center, and that fuel supplies there were sufficient to meet demand. Sempra Energy, which owns power and natural gas facilities on both sides of the border, said none of its facilities in Mexico or southern California were seriously damaged. Source: <http://www.nasdaq.com/aspx/stock-market-news-story.aspx?storyid=201004052105dowjonesdjonline000206&title=calif-gov-declares-state-of-emergency-after-earthquake>

# UNCLASSIFIED

## **DEFENSE INDUSTRIAL BASE SECTOR**

**Aerojet tests missile in -65 degree conditions.** Military aircraft at high altitude can experience extremely cold temperatures, which is not a problem for a new rocket-motor technology developed by Lockheed Martin and Aerojet, a part of Rancho Cordova, California -based GenCorp. The two companies announced that their motor for a Joint Air-to-Ground Missile program succeeded in operating down to -65 degrees. Testing was performed in Camden, Arkansas. Source:

[http://nosint.blogspot.com/2010/04/aerojet-tests-missile-in-65-degree.html?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed:+blogspot/fqzx+\(N+aval+Open+Source+INTelligence\)&utm\\_content=Google+Reader](http://nosint.blogspot.com/2010/04/aerojet-tests-missile-in-65-degree.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+blogspot/fqzx+(N+aval+Open+Source+INTelligence)&utm_content=Google+Reader)

**Report: Defense contractors battle 'relentless' online assaults.** Foreign nations are increasingly exploiting the Internet, including social-network sites, to conduct industrial espionage against Defense Department contractors, according to a new government report. "United States defense-related technologies and information are under attack each day, every hour and from multiple sources," said the Defense Security Service (DSS). DSS oversees security at 13,000 contractor facilities. "The attack is pervasive, relentless and unfortunately, at times, successful." Released March 30, the report reviews 2008 events. The study found that attacks came from nations considered unfriendly and friendly. E-mail messages requesting price quotes and system information were the preferred method to attempt to steal U.S.-technology data. Users also sent multiple e-mail requests for the same information to different individuals working for the same contractor. Hackers from East Asia and the Pacific region focused their attention on information systems, accounting for 29 percent of suspicious-contact reports turned in to the DSS. More than a third of the attacks (36 percent) coming from European countries — including Russia and NATO allies — tried to obtain information on aeronautical systems and 12 percent targeted information-technology data. Foreign attempts to obtain information on unmanned aerial vehicles have become so prevalent that a special section of the report is devoted to them. Source:

[http://www.nextgov.com/nextgov/ng\\_20100405\\_4562.php?oref=rss](http://www.nextgov.com/nextgov/ng_20100405_4562.php?oref=rss)

## **CRITICAL MANUFACTURING**

**Mazda, GM put in 'smart pedals' to reassure buyers.** Automakers believe Toyota's struggles with unintended-acceleration claims have made auto buyers so nervous that even companies not bedeviled by such claims feel compelled to announce remedies anyway. General Motors, for example, said Monday it will put brake-throttle override technology, also known as "smart pedals," into all its vehicles by the end of 2012, even though GM pedals are involved in relatively few safety complaints to the government. GM already has an internal requirement for brakes to be able to stop a vehicle with an open throttle from highway speed, even without a system that overrides a stuck throttle. Mazda confirmed Monday that it, too, will introduce brake-throttle override on the Mazda2 subcompact on sale this summer, and will have it on all models by the end of the 2011 model year. Brake-throttle overrides sense when both the throttle's open and the brakes are being applied hard. The systems then use a vehicle's traction control and other electronics to cut engine power to ensure the brakes will prevail. Source: [http://www.usatoday.com/money/autos/2010-04-06-brakes06\\_ST\\_N.htm](http://www.usatoday.com/money/autos/2010-04-06-brakes06_ST_N.htm)

# UNCLASSIFIED

**Toyota hid pedal defect in violation of U.S. law, LaHood says.** Toyota Motor Corporation “knowingly hid a dangerous defect” that caused its vehicles to accelerate unexpectedly, the U.S. said, for the first time accusing the world’s largest automaker of breaking the law. The U.S. Transportation Secretary proposed a record civil penalty of \$16.4 million, the most the government can impose. The fine recommended yesterday escalates the confrontation between Toyota and the Secretary, who initially praised the carmaker for its handling of recalls the company attributed to faulty accelerator pedals. The fine was announced the week after Toyota reported U.S. sales rose 41 percent in March, signaling the company may be recovering from global recalls of more than 8 million vehicles. Toyota waited at least four months before telling U.S. regulators that gas pedals might stick, the Secretary said in a statement yesterday. Companies have five business days to report safety defects, the Transportation Department said. Source: <http://www.businessweek.com/news/2010-04-06/toyota-hid-pedal-defect-in-violation-of-u-s-law-lahood-says.html>

## **EMERGENCY SERVICES**

**(New York) Breathing problems persist in September 11 rescuers.** Rescue workers who responded to the World Trade Center attacks on September 11, 2001 continued to have diminished lung capacity seven years after the attack, researchers reported on Wednesday. Breathing problems among New York Fire Department employees, caused by dust, smoke, and other toxic chemicals, became apparent one year after the twin towers collapsed. Their lung capacity typically diminished as if they had aged 12 years. Doctors had hoped their lungs would gradually rebound, as they often do from routine smoke exposure. But over the next six years, their lungs continued to worsen, said a doctor of the Albert Einstein College of Medicine in New York, who led the study. Firefighters who had never smoked tobacco lost about 25 milliliters of lung volume annually. Emergency medical services personnel lost about 40 milliliters, the researchers reported in the New England Journal of Medicine. The city has been conducting lung capacity tests on its rescue personnel since 1997. Before September 11, very few firefighters scored below normal for their age on the test. Years later, 13 percent did. Among emergency medical services workers, 11 percent had below-normal results before the collapse of the twin towers; seven years later, 23 percent scored low. The study also compared rescue workers who were at the scene initially and those who showed up a day or more later, and found that the early responders suffered the most. Source: <http://www.reuters.com/article/idUSTRE6365V420100408>

**(New York) Crime rate spurs shift in NYPD resources away from anti-terror patrols.** The recent crime spike in some city neighborhoods has prompted a shift in NYPD resources. The mayor says a number of police patrols from the counter-terrorism Critical Response Vehicle program will be transferred back to their home boroughs to aid police operating in high crime neighborhoods. The cars in the program had been contributed from across the police department’s 76 precincts, and were part of an anti-terror team that regularly patrolled a number of potential terror targets — including Times Square and Madison Square Garden. The move was made in part to reduce the city’s rising crime rate. Nearly two weeks ago, the New York Police Department’s CompStat program said the city had seen a 22 percent increase in recorded murders. The NYPD also released a statement today saying the Critical Response Vehicles “are periodically used for conventional crime suppression.” The police department added that instead of devoting all 67 cars in the program to counter terrorism patrols, “eight of them will patrol in parts of Queens and Brooklyn that have

UNCLASSIFIED

# UNCLASSIFIED

experienced crime increases.” Source: <http://www.1010wins.com/Rising-Crime-Rates-Prompt-Shift-in-NYPD-Resources/6734300>

## **ENERGY**

**(North Carolina) Thieves cut copper wire from poles.** Copper wire was cut and stolen from 30 Duke Energy power poles Wednesday along Shue Road and Miller Chapel Road in Salisbury. The theft was reported to have occurred between 8 a.m. and 1 p.m. The cost to replace the wire was estimated at \$3,000. According to a Rowan County sheriff’s deputy, the wire was cut about as high as a person can reach, so the thief cut away all that was possible without using a ladder. The sheriff’s office is conducting an investigation. As of Friday morning, no one had been charged or arrested in connection with the crime. Source: <http://www.salisburypost.com/News/040910-WEB-Duke-Energy-copper>

**(Georgia) Thieves take wire from utility poles.** For the second time in less than a week, thieves made off with copper wire from a county sewage treatment plant under construction off Bailey Street in Southeastern Clarke County, Georgia, Athens-Clarke police said. The thieves used machinery at the site to remove some of the wire that workers recently had installed on utility poles, police said. The wire, stolen between 8 a.m. April 2 and 8 a.m. April 5, is owned by the Georgia Power Co. and was valued at \$4,000, according to police. More Georgia Power wire, valued at \$1,680, went missing from the construction site between March 30 and March 31, police said. Source: [http://www.onlineathens.com/stories/040710/cop\\_602803005.shtml](http://www.onlineathens.com/stories/040710/cop_602803005.shtml)

**DOE pitches \$10M for energy cybersecurity.** The Energy Department has finally announced details of the grant it will award for setting up a National Electric Sector Cyber Security Organization, which will be the major authority charged with protecting the electricity grid. The grant is worth around \$10 million and potential applicants have less than a month — until April 30 — to pull their applications together. The National Energy Technology Laboratory is managing the process for DOE. The department first made the announcement about the new organization at the beginning of this year. The idea is to have it develop and establish safeguards for emerging technologies such as the smart grid, which will use IT to tie intelligent meters and other devices together to give a better way of managing power demand and supply. Source: <http://fcw.com/blogs/quick-study/2010/04/energy-grid-cybersecurity-grants.aspx>

**(Texas) ‘Cyber attack’ aimed at Texas electricity provider.** A Houston, Texas, news station uncovered details about a so-called “cyber attack” on one of Texas’ largest electricity providers. A confidential e-mail obtained by Local 2 explains a “single IP address in China” tried 4,800 times to log in to the Lower Colorado River Authority’s computer system. In the e-mail, the Electricity Reliability Council of Texas reports all login attempts failed and went on to term the incident a “suspected sabotage event.” The e-mail explained the FBI had been notified. According to its Web site, the LCRA provides electricity to more than a million Texans in rural cities and towns. When contacted by Local 2, officials with the LCRA would “neither confirm, nor deny” the incident or the contents of the e-mail. Officials with the FBI’s Houston office also declined to comment. Source: <http://www.click2houston.com/news/23046216/detail.html>

UNCLASSIFIED

## **FOOD AND AGRICULTURE**

**(Florida) USDA confirms new citrus disease in Florida.** The U.S. Department of Agriculture's Animal and Plant Health Inspection Service (APHIS) on April 8 confirmed the presence of *Guignardia citricarpa*, or citrus black spot, in Collier County, Florida. "This detection demonstrates the effective and collaborative nature of the citrus health response program," said a deputy administrator for APHIS' plant protection and quarantine. "It has not only provided the infrastructure upon which we made this early detection but also the framework for APHIS' regulatory response. "We are working in collaboration with the Florida Department of Agriculture and Consumer Services, the University of Florida's Citrus Research and Education Center and the citrus industry to limit the spread and impact of this disease through swift regulatory actions, education and informed compliance." A fungal disease marked by dark, speckled spots or blotches on the rinds of fruit, citrus black spot is an economically significant citrus disease. It causes early fruit drop, reduces crop yield, and renders the highly blemished fruit unmarketable. While all commercial citrus cultivars are susceptible to citrus black spot, the most vulnerable are lemon and late-maturing citrus varieties like Valencia. Source: [http://www.aphis.usda.gov/newsroom/content/2010/04/fla\\_citrus\\_disease.shtml](http://www.aphis.usda.gov/newsroom/content/2010/04/fla_citrus_disease.shtml)

**Report finds significant weakness in FDA Food Inspections.** There are "significant weaknesses" in the U.S. Food and Drug Administration's (FDA) program to inspect domestic food facilities, according to a new federal report. The report said the FDA needs to increase the number of domestic food inspections to keep up with food-borne outbreaks. "The findings demonstrate that more needs to be done to protect public health and to ensure that FDA has the necessary tools to prevent outbreaks of food-borne illness," a Health and Human Services inspector general said. The report indicated that more than 300,000 Americans are hospitalized and roughly 5,000 die annually after consuming contaminated foods and beverages. The report suggested that the FDA may need to request more authority from Congress to gain access to records from more companies. It noted that food facilities with a history of serious violations have, at times, refused to give the FDA access. "This might impede FDA's ability to determine the most appropriate action to take to ensure compliance with applicable laws and regulations," the report stated. A bill that would give the FDA more powers, including the authority to force companies to recall products, has been stalled in the Senate. Source: <http://www.lloyds.com/CmsPhoenix/DowJonesArticle.aspx?id=453126>

**Honey laundering bust highlights sticky problem.** In recent years honey has made federal investigators think of smuggling rings. And as the latest bust underscores, despite the investigators' efforts, it may be all but impossible to keep the tainted Chinese honey at the center of the problem off U.S. store shelves. The arrest occurred last week at Los Angeles International Airport, where federal officials nabbed a man as he deplaned from Taiwan. Federal investigators are trying to crack down on illegally-imported Chinese honey, for financial and safety reasons. The accused man was arrested for allegedly conspiring to illegally import honey that was deliberately mislabeled to avoid U.S. anti-dumping duties, according to statements in the criminal charges filed by the U.S. attorney for the Northern District of Illinois and a special agent in charge of the U.S. Immigration and Customs Enforcement operation in Chicago. The suspect is the president of Blue Action Enterprise Inc., a California-based honey import company, and also heads several similar companies, including 7 Tiger Enterprises Inc., Honey World Enterprise Inc. and Kashaka USA Inc., the court papers said. The charges against him allege his involvement in 96 shipments of Chinese honey falsely declared as

## UNCLASSIFIED

originating in South Korea, Taiwan, and Thailand. He is also one of scores of people on both sides of the Pacific playing the name-change game with what adds up to millions of pounds of honey. Their schemes involve an intricate shuffle of shipping papers and labels meant to conceal the origin of honey transported in green-painted 55-gallon drums or 250-gallon plastic carboys — thereby avoiding stiff taxes and safety inspections. The money is in the form of the protective tariffs or taxes placed on foreign products that intentionally undercut domestic prices. It was in 2001 that the U.S. Commerce Department imposed honey taxes against China whose extremely low-cost honey was flooding the market and threatening the survival of U.S. beekeepers. Source:

<http://www.aolnews.com/nation/article/honey-laundering-bust-highlights-sticky-problem/19429121>

**(Washington; Oregon) Washington food company recalls cheese product because of Listeria risk.**

Del Bueno of Grandview, Washington, is recalling all size packages of Queso Fresco Fresh Cheese because it has the potential to be contaminated with *Listeria monocytogenes*, an organism which can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. Although healthy individuals may suffer only short-term symptoms such as high fever, severe headache, stiffness, nausea, abdominal pain and diarrhea, *Listeria* infection can cause miscarriages and stillbirths among pregnant women. Queso Fresco Fresh Cheese was distributed to retail markets in Washington and one in Hermiston, Oregon. The cheese is packaged in round clear plastic packages, and is marked on the back with a code date; all codes up to and including May 30, 2010, are being recalled. Washington State Department of Agriculture has linked one illness to the cheese. The recall is the result of a routine sampling program by Washington State Department of Agriculture which revealed that the cheese is contaminated with *Listeria*. The company has notified its customers and has pulled the product from retail stores. Del Bueno is working with FDA to conduct the recall. Source:

<http://www.reliableplant.com/Read/23860/Washington-food-company-listeria>

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

**(Washington) Bomb left at Spokane federal building.** Authorities are investigating the March 28 discovery of an improvised explosive device next to the Thomas S. Foley U.S. Courthouse in downtown Spokane, Washington. The public was not alerted to the bomb until the Spokesman-Review newspaper inquired about it on April 7. A spokesman for the U.S. Attorney's office said the device was located late in the evening of March 28. He said the public was not notified because they did not want to compromise the investigation. No arrests have been made, and he would not provide other details. Source: [http://www.seattlepi.com/local/6420ap\\_wa\\_explosive\\_device\\_spokane.html](http://www.seattlepi.com/local/6420ap_wa_explosive_device_spokane.html)

**(Tennessee; District of Columbia) FBI investigates Cohen.** Inside his Memphis office, A Democratic Congressman shows hate mail he's received on his Blackberry containing threats for criticizing the Tea Party movement. The congressman says he has received at least three e-mails, "When you take the action of three, sick individuals who suggested that I should be burned on a cross and/or my throat slit, this doesn't reflect well on the Tea Party." One e-mail says, "It would be nice to read someone had cut your (expletive) throat." Another e-mail reads, "If our tea parties had hoods, we would burn your (expletive) on a cross on the White House front lawn." The comments were sparked

UNCLASSIFIED

## UNCLASSIFIED

by an interview the congressman did during the week of March 29 to April 2. The congressman said, "I did not suggest, although some people have taken it, that all Tea Party people are out to do harm to others, as the Ku Klux Klan did. I said they were without robes and hoods, which means they were not the Klan." The congressman said his remarks were motivated by incidents at a Washington, D.C. rally last month. Source: <http://www.wreg.com/news/wreg-cohen-threats-story,0,3491966.story>

**Many U.S. government agencies have been attacked, survey says.** IT workers in the U.S. federal government say their systems are already under attack, and they do not expect the situation to get better in coming months. According to a survey published today by Clarus Research Group and Lumension, nearly three-quarters of federal IT decision-makers who work in national defense and security departments or agencies say the possibility is "high" for a cyberattack by a foreign nation in the next year. One-third of these respondents say they have already experienced such a cyberattack within the past year. Forty-two percent of respondents believe the U.S. government's ability to prevent or handle these attacks is only fair or poor. Sixty-four percent of respondents identified the increasing sophistication and growth in volume of cyberattacks as the No. 1 IT security risk. Only 6 percent of respondents rated the federal government's overall ability to handle possible cyberattacks as "excellent," the survey says. Difficulty integrating multiple technologies, aligning IT needs with department objectives, and complying with requirements were identified as the greatest challenges in managing IT security operations. The majority of respondents said they felt more confident in their level of IT security today than they did a year ago. Source: [http://www.darkreading.com/vulnerability\\_management/security/government/showArticle.jhtml?articleID=224201585](http://www.darkreading.com/vulnerability_management/security/government/showArticle.jhtml?articleID=224201585)

**(Washington) Yakima man arrested for threatening Senator Patty Murray.** A Yakima man has been charged with threatening to kill a democratic Senator over her support for health care reform. Court documents say federal agents arrested the suspect in Yakima Tuesday. The FBI said the Senator's office in Seattle reported the threats, which were left on voice mail from a blocked telephone number. Agents said they traced the calls to the suspect's home near Yakima. A KGMI legal analyst said the threats are not protected as free speech. "This is clearly a case of malicious speech that I think crosses the line into criminal behavior," said the legal analyst. "Typically when you see someone who's acting in this fashion, you have to wonder if they're okay — if they're mentally okay." The Senator's office told the FBI that it had been receiving harassing messages from the caller for months, but they became more threatening as congress was voting on health care legislation. Excerpts of the expletive-laced messages transcribed in court documents show the caller saying he wanted to kill the Senator, and it would "just take one piece of lead." Source: <http://kgmi.com/Yakima-Man-Arrested-For-Threatening-Senator-Patty-/6749521>

**(Missouri) Bomb threat closes Kansas City federal courthouse.** Authorities say the federal courthouse in Kansas City is reopening after a suspicious package flagged as explosive was found to contain nothing but phone books. The courthouse was evacuated and employees were sent home Monday morning after a package was found near an entrance for prisoners. A note on the package said the contents would explode. The U.S. Marshal for the Western District of Missouri says bomb and arson detectives investigated the package that contained only phone books. The marshal says the courthouse will reopen this afternoon. He says no one has claimed responsibility for the bomb threat and that authorities have no suspects. The Bureau of Alcohol, Tobacco, Firearms and Explosives and

UNCLASSIFIED

# UNCLASSIFIED

the FBI will investigate. Source:

<http://www.google.com/hostednews/ap/article/ALeqM5ieyaRSnMFVUH-p3rtygEmUB7eObAD9ET1NHG0>

## **INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

### **Identity Thieves Filed For \$4 Million In Tax Refunds Using Names Of Living And Dead**

A group of sophisticated identity thieves managed to steal more than \$4 million by filing bogus tax returns using the names and Social Security numbers of other people, many of them deceased, according to a 74-count indictment unsealed in Arizona Thursday. The thieves operated their scheme for at least three years from January 2005 to April 2008, allegedly filing more than 1,900 fraudulent tax returns involving about \$4 million in refunds directed to more than 170 bank accounts. Full Article: <http://www.wired.com/threatlevel/2010/04/fake-tax-returns/>

**1-in-10 Windows PCs still vulnerable to Conficker worm.** More than a year after doomsday reports hinted that the Conficker worm would bring down the Internet, one-in-10 Windows PCs still have not been patched to plug the hole the worm wriggles through, new data shows. And 25 of every 1,000 systems are currently infected with the worm. According to Qualys, a security risk and compliance management provider, about 10 percent of the hundreds of thousands of Windows systems it monitors for customers have not yet applied Microsoft's MS08-067 security update. MS08-067, an out-of-band release that shipped in October 2008, patched a bug in the service Windows uses to connect to file and print servers. Source:

[http://www.computerworld.com/s/article/9174998/1\\_in\\_10\\_Windows\\_PCs\\_still\\_vulnerable\\_to\\_Conficker\\_worm](http://www.computerworld.com/s/article/9174998/1_in_10_Windows_PCs_still_vulnerable_to_Conficker_worm)

**Researcher details new class of cross-site scripting attack.** A new type of cross-site scripting (XSS) attack that exploits commonly used network administration tools could be putting users' data at risk, a researcher says. The lead security research engineer at nCircle on April 2 published a white paper outlining a new category of attack called "meta-information XSS" (miXSS), which works differently than other forms of the popular attack method — and could be difficult to detect. "Think about those network administration utilities that so many webmasters and SMB administrators rely on — tools that perform a whois lookup, resolve DNS records, or simply query the headers of a Web server," the white paper states. "They're taking the meta-information provided by various services and displaying it within the rendered Website. "These Web-based services introduce a class of XSS that can't be captured by the current categories." He explains that there are three current types of XSS attacks: reflected, persistent, and DOM-based. MiXSS has aspects of both reflected and persistent attacks, but does not fall into either category, the engineer explains. "It is valid user input provided to a service," he says. "The service then utilizes the user-provided data to gather data and display it for the user. It is in this data that the cross-site scripting occurs." Source:

[http://www.darkreading.com/vulnerability\\_management/security/app-security/showArticle.ihtml?articleID=224201569&subSection=Application+Security](http://www.darkreading.com/vulnerability_management/security/app-security/showArticle.ihtml?articleID=224201569&subSection=Application+Security)

**Adobe considers changes to mitigate PDF attack.** Adobe Systems is considering modifying its PDF applications to counter a way to run arbitrary code on Windows computers by embedding it in a malicious PDF file. Recently, a security researcher detailed a way to run executable code using a different launch command even though PDF applications from Adobe and Foxit do not allow

UNCLASSIFIED

## UNCLASSIFIED

embedded executables to directly run. The attack requires some social engineering. Adobe's Reader and Acrobat products do display a warning that only trusted executables should be opened, but the security researcher showed how it was possible to modify part of the warning message in order to persuade a user to open the file. The company is considering modifications to the programs. Source: <http://www.infoworld.com/d/security-central/adobe-considers-changes-mitigate-pdf-attack-723>

**Police cuff 70 eBay fraud suspects.** Romanian police have arrested 70 suspected cybercrooks, thought to be members of three gangs which allegedly used compromised eBay accounts to run scams. The alleged fraudsters obtained login credentials using phishing scams before using these trusted profiles to tout auctions for non-existent luxury goods (luxury cars, Rolex watches and even a recreational aircraft). Buyers handed over the loot but never received any goods in return. The 800 victims of the scam are estimated to have suffered a total of \$800,000 in losses since 2006. Victims were located across Western Europe, Scandinavia, the US, Canada and New Zealand. Complaints from the victims led to a joint FBI and Romanian Directorate for Investigating Organized Crime and Terrorism (DIICOT) investigation culminating in the execution of 101 search warrants and multiple arrests across Romania on April 6. Source: [http://www.theregister.co.uk/2010/04/07/romania\\_cybercrime\\_bust/](http://www.theregister.co.uk/2010/04/07/romania_cybercrime_bust/)

**Under protected corporate secrets.** Enterprises are investing heavily in compliance and protection against accidental leaks of custodial data (such as customer information), but under-investing in protection against theft of far more valuable corporate secrets, according to a global survey by Forrester Consulting. Nearly 90 percent of surveyed enterprises agreed that compliance with PCI-DSS, data privacy laws, data breach regulations, and existing data security policies is the primary driver of their data security programs. Significant percentages of enterprise budgets (39 percent) are devoted to compliance-related data security programs. But secrets comprise 62 percent of the overall information portfolio's total value while compliance-related custodial data comprises just 38 percent, a much smaller proportion. This strongly suggests that investments are over weighed toward compliance. The survey found that while organizations focus on data security incidents related to accidental loss, information theft by employees or trusted outsiders is more costly. For example, based on responses received in the survey, employee theft of sensitive information is 10 times costlier than accidental loss on a per-incident basis: hundreds of thousands of dollars versus tens of thousands. Source: <http://www.net-security.org/secworld.php?id=9104>

**Symantec warns cloud computing security approaches need to catch up to adoption.** A survey of IT professionals has painted a troubling picture of enterprise approaches to cloud computing security. According to the survey, which was done by Symantec and the Ponemon Institute, many organizations are not doing their due diligence when it comes to adopting cloud technology—a situation that may partly be due to ad hoc delegation of responsibilities. Among the findings: Few companies are taking proactive steps to protect sensitive business and customer data when they use cloud services. Less than 10 percent of those surveyed said their organizations performed any kind of product vetting or employee training to make sure cloud computing resources met security requirements before cloud applications were deployed. In addition, just 30 percent of the 637 respondents said they evaluate cloud vendors prior to deploying their products, and most (65 percent) rely on word-of-mouth to do so. Fifty-three percent rely on assurances from the vendor. However, only 23 percent require proof of security compliance such as with regulation SAS 70. Source: <http://www.eweek.com/c/a/Security/Symantec-Cloud-Computing-Security-Approaches-Need-to-Catch-up-to-Adoption-252954/>

UNCLASSIFIED

## NATIONAL MONUMENTS AND ICONS

**(Maryland; West Virginia; District of Columbia) Flooding damage at Chesapeake and Ohio Canal National Historical Park nears \$3 million.** Flood waters that raged along the Chesapeake and Ohio Canal National Historical Park caused nearly \$3 million in damage, according to updated estimates from park officials. As reported late last month, damage included two breaches of the canal's towpath near Harpers Ferry, which now have temporary bridges over them, and general scouring of the towpath surface, said the deputy supervisor. Causing the damage was a combination of heavy rains and melt from the winter's record-breaking snowstorms. Together they pushed the Potomac River over its banks. While still considered a moderate flood, these waters were the highest the area had seen since 1996, he added. A road is now being built near Lock 5 to provide access to the broken inlet lock. A gate was broken at Lock 2 as well, and a debris field needs clearing near the Monocacy Aqueduct. The deputy supervisor expects repairs to last into the summer. Source: <http://www.nationalparkstraveler.com/2010/04/flooding-damage-chesapeake-and-ohio-canal-national-historical-park-nears-3-million5672>

**(New Hampshire) Police believe they know origin of Odiorne Park bomb.** Police reported that they now know the origin of the April 5 bomb found in Odiorne Park (N.H.) The key to the discovery of the stainless steel pipe with a screw-on cap and a quarter at both ends of the pipe, was a tip from Seacoast Crime Stoppers and a combined investigation by Rye Police, New Hampshire State Police, the Bureau of Alcohol, Tobacco, and Firearms and the FBI. "Based on the information we have and the agencies that assisted us in investigating we're confident we have concluded who made the device and how it was made," the police chief said. "We're confident there was only one person involved and we'll be moving forward appropriately." He added that although the department believes the source of the device is known there are still questions as to how it came to be in the park. Forensic evidence suggests the device is between four months one year old. the police chief praised the public in coming forward with information that assisted the departments in the investigation. Source: <http://www.seacoastonline.com/articles/20100408-NEWS-100409836>

**(New Hampshire) Device found at Rye state park was pipe bomb.** A suspicious device found near a well-traveled portion of Odiorne State Park on Sunday contained potentially explosive materials, according to the police chief. He confirmed on Monday that a preliminary examination by the New Hampshire State Police Explosives Disposal Unit shows the device found late Sunday morning appears to be a pipe bomb. Local officers have checked Odiorne State Park for additional similar devices and say they have not found any, but urge residents to call police if they find any suspicious pipe or package in the ocean-side park. The chief said the device was "chrome" colored and appeared to be a pipe with caps on both ends. The pipe was located on the other side of stonewall that separates a walking trail from a rocky beach. "It was in the immediate area of where the public does walk," he said. He also said the device shows no signs of having washed up on the beach. The investigation is ongoing. Source: [http://www.fosters.com/apps/pbcs.dll/article?AID=/20100406/GJNEWS\\_01/704069927/-1/FOSNEWS](http://www.fosters.com/apps/pbcs.dll/article?AID=/20100406/GJNEWS_01/704069927/-1/FOSNEWS)

**(Virginia) Blue Ridge Parkway shooting suspect arrested.** After receiving a tip Wednesday, local and federal authorities patiently pulled surveillance beginning at 4 a.m. on the Stuarts Draft, Virginia

## UNCLASSIFIED

home of a man suspected of shooting two people earlier this week on the Blue Ridge Parkway. Nearly 12 hours later, a 56-year-old man was arrested without incident. The man is suspected of shooting a 27-year-old Charlottesville man and an 18-year-old Palmyra woman. An Augusta County sheriff said the victims were at the Rock Point Overlook on Monday night watching the sunset when they were both shot in the back with a single shotgun blast. The male victim, who has muscular dystrophy, also was struck on the side of his face. He tumbled an estimated 150 feet down the overlook after being shot. After reportedly firing the first shot, the suspect got out of his burgundy Kia Sephia, but was immediately met by the female victim. Despite being shot, she tried to wrestle the shotgun away. After a fight, she managed to escape after flagging down a man and his wife who happened upon the scene in their car. On Wednesday, the female victim was listed in fair condition. The male victim is in critical condition. Source: <http://www.newsleader.com/article/20100408/NEWS01/4080319>

**(Virginia) FBI joins manhunt after 3 shot on Blue Ridge Parkway.** A Virginia State Police spokeswoman said a state trooper was injured during the rescue of shooting victims Monday night on the Blue Ridge Parkway. The trooper slipped and fell on steep terrain and suffered minor injuries, she said. State police continue to provide resources Tuesday, but the Augusta County Sheriff's Office is leading the shooting investigation, authorities said. A Public Information Officer for the National Park Service confirmed Tuesday morning that the FBI has joined local and state authorities in the search for a suspect in relation to the Monday parkway shootings. "I know that there was a double shooting — one male and one female," she confirmed, but added, "I am not sure of the exact time line of the events that occurred." The incident occurred around mile post 10 at the Rock Point Overlook on the Blue Ridge Parkway. The road between mile markers 0-13 remains closed. There was no information available on a possible third victim or the suspect. Source: [http://www2.newsadvance.com/lna/news/local/article/three\\_people\\_reported\\_shot\\_on\\_blue\\_ridge\\_parkway/25799/](http://www2.newsadvance.com/lna/news/local/article/three_people_reported_shot_on_blue_ridge_parkway/25799/)

## **POSTAL AND SHIPPING**

**(Connecticut) Building secured after 'suspicious substance' found at Redding Church Tuesday.** An investigation continues of a "suspicious substance" that was received in the mail at Sacred Heart Church in Georgetown Tuesday, according to the police chief. The building where the mail was received is "next-door to the church" and has been secured, said the police chief. He confirmed that two people were treated at the scene with decontamination equipment and brought to Danbury Hospital but "show no symptoms" of exposure. Emergency officials were not able to elaborate late Tuesday on what type of substance had been found at the church. A statement released Tuesday by the police chief however said that "at this time, there is no danger to the surrounding community." He added that local, state and federal agencies were investigating the incident. Source: <http://www.newstimes.com/news/article/Building-secured-after-suspicious-substance-438430.php>

**(Ohio) Suspicious odor from envelope prompts evacuation of Ohio state offices in Columbus.** Authorities say a suspicious odor from an envelope mailed to an Ohio agency caused the evacuation of a seven-story Columbus office building. A fire department spokesman says nine people complained of eye and nose irritation, but their symptoms cleared once they got fresh air. Hundreds of workers waited outside for about 90 minutes Wednesday morning as emergency crews investigated. When the envelope was opened in an office of the Ohio Department of Job and Family Services workers complained of a peppery, toner-like smell. The envelope contained a claim that he said was sent by a

UNCLASSIFIED

## UNCLASSIFIED

“reputable company.” He says there was no powder inside, as initially reported. The envelope will be examined by city health officials. Source: <http://www.fox8.com/news/sns-ap-oh--buildingevacuated,0,842908.story>

**(California) SB County building evacuated after white substance is found in mail.** Sheriff’s deputies evacuated 150 people from a county building Wednesday morning after an employee opening mail discovered an envelope with a white substance inside. An employee at the Department of Aging and Adult Services at 686 E. Mill St. was opening mail shortly before 9 a.m. when the substance was found. “They discovered a white substance inside. They quickly alerted the authorities,” said the San Bernardino County sheriff’s spokeswoman. Deputies evacuated about 150 employees and cordoned off the department where the letter was found. She said she did not know what the letter contains. Employees showed no signs of illness. Source: [http://www.sbsun.com/news/ci\\_14836243](http://www.sbsun.com/news/ci_14836243)

**(Texas) Wheelchair-bound man arrested for pipe bomb incidents.** An arrest has been made in the case of pipe bombs and Molotov-cocktail-type incendiary devices that have been found around East Texas for the past two months, a federal official close to the case told CBS 19’s news partner, the Tyler Paper, Wednesday morning. The arrest comes in the wake of another device being found at the Tanglewood Shopping Center in Tyler at Loop 323 and Fifth Street shortly after 11 a.m. Wednesday. At 11:40 a.m. CDT, Pointe North Drive in Tyler was blocked off, and a bomb squad headed down the road. Officials told the Tyler Paper a van parked at that location may have as many as five bombs inside. More than 30 devices have been found in the last two months in mailboxes, in front of businesses, and along rural roads in East Texas. Federal and local authorities were at the Tanglewood Shopping Center Wednesday morning. The device was found in a U.S. Postal Service blue mailbox in the shopping center parking lot. The Bureau of Alcohol, Tobacco, Firearms and Explosives was on the scene, and had a robot activated to remove the device. The shopping center parking lot, as well as the parking lot of an adjacent Burger King restaurant, was closed off. Cars parked in the shopping center parking lot were being moved. Source: <http://www.cbs19.tv/Global/story.asp?S=12270224>

**(Texas) White powder letters received by two schools in the Garland Independent School District.** A Special Agent in Charge (SAC) is requesting the public’s assistance in identifying the person or persons responsible for sending two letters containing a white powder substance to the Ethridge School in Garland, Texas, and John Armstrong school in Sachse, Texas. Earlier this morning, two schools within the Garland Independent School District received letters, through the U.S. Mail, containing white powder. The Garland Police and Fire Department, along with the Sachse Police Department, the U.S. Postal Inspection Service, and the FBI responded to the scene. Initial field testing indicated the substance within the envelopes was not toxic and there was no threat to anyone’s health or safety. Further laboratory testing is being done in an effort to identify the substance within the envelopes. One school district employee at Ethridge School, who had been exposed to the white powder, was taken to a local hospital as precautionary measure. The sending of threatening or hoax letters containing a white powder substance is a violation of Title 18, Section 844 (e) and is punishable for up to 10 years in prison and a \$250,000 fine for each letter sent. Source: <http://dallas.fbi.gov/pressrel/pressrel10/dl040610.htm>

**(Texas) Powder forces evacuation of part of Texas airport.** Authorities have evacuated about 30 people from the administrative offices of the San Antonio International Airport after the discovery of an envelope containing white powder. Officials say airport employees found the envelope in the mail

UNCLASSIFIED

## UNCLASSIFIED

around 2:30 p.m. Monday. An airport spokesman told the San Antonio Express News that the incident did not affect passengers or flights. A spokesman for the San Antonio fire department said firefighters trained to handle hazardous materials were at the airport. The department's hazardous materials team was not sent to the scene. The offices overlook the check-in level of the airport. No injuries were reported. Source:

<http://www.dallasnews.com/sharedcontent/APStories/stories/D9ET8TGO0.html>

**(Washington) Post Office evacuated following peculiar incident.** City prosecutors are still trying to determine if charges will be filed against the 50-year-old Woodinville salesman who backed up his SUV in front of the Woodinville Post Office, apparently locked himself out of his vehicle, triggered a misting device on the vehicle's roof that sprayed a mysterious fluid toward the front door and walked away on Thursday. The fluid, it turns out, was water. But the bizarre incident evacuated the post office for three hours and set off a full-blown hazardous materials response from the Woodinville Fire & Life Safety District. "It's our responsibility to assume the worst-case scenario," the WFLSD community services spokesman said. The spokesman said a service call came in at 12:26 p.m. for a vehicle "leaking some sort of fluid" toward the front door of the post office right next door to the fire house. "When we arrived we saw an SUV backed into a parking stall with a contraption on its roof containing a generator, an air compressor and a spraying device," he said. "Every 10 seconds or so it would spray a puff of mist, and evidently it was hitting customers coming in and out of the post office." The call came in from the Woodinville Postmaster, who was alerted to the disturbance by customers, made an announcement to locate the driver of the vehicle, and evacuated the federal building when she received no public response. "We cordoned off the area and set up our HAZMAT team to identify the fluid and pretty quickly determined it was distilled water," the spokesman said. Source: [http://www.nwnews.com/index.php?option=com\\_content&view=article&id=1118:post-office-evacuated-following-peculiar-incident&catid=34:news&Itemid=72](http://www.nwnews.com/index.php?option=com_content&view=article&id=1118:post-office-evacuated-following-peculiar-incident&catid=34:news&Itemid=72)

## PUBLIC HEALTH

**(North Carolina) Fake nurse arrested, charged with stealing drugs from WFU Baptist Medical Center.** A woman who worked as a nurse at Wake Forest University Baptist Medical Center in North Carolina was not actually a nurse and now faces criminal charges, according to a spokesperson for the State Bureau of Investigation. The woman was investigated by the SBI's Drug Diversion Unit. She was arrested Monday at the Wake County Magistrate's Office after she turned herself in to the SBI, according to the N.C. Department of Justice public information officer. She said the woman worked under a false name at Wake Forest Baptist Medical Center. A media relations manager at Wake Forest University Baptist Medical Center said the woman worked at the hospital for three months. The woman was charged with embezzlement of a controlled substance by an employee of an employee of a registrant, which is a felony. Source:

<http://www.digtriad.com/news/local/story.aspx?storyid=140168&catid=57>

**(Washington) Police respond to bomb threat at UWMC.** University police responded Monday morning to a bomb scare at the UW Medical Center (UWMC), the second bomb scare at a campus building in two days. According to the UW Police Department (UWPD), an anonymous caller contacted UWMC security claiming that there was a bomb in the area around the medical center. Security personnel at the UWMC contacted the UWPD, who sent officers and an explosive-sniffing K-

## UNCLASSIFIED

## UNCLASSIFIED

9 unit. After searching the building and the surrounding area, officers found no trace of any explosive device. An e-mail distributed to UWMC staff stressed that the situation was under control but that if any staff member saw something suspicious, he or she should contact the medical center's director of public safety. On Sunday, an anonymous caller reported a bomb in a specific apartment in Stevens Court, another incident in which no explosives were found. While UWPD officers responded to the report, checking the suspicious apartment as well as the surrounding area, the UWPD did not send a K-9 unit, because they did not believe the report to be credible, partly because the caller was giggling, said the UWPD commander. There are no suspects for either incident at this time, and the calls remain under investigation. Source: <http://dailyuw.com/2010/4/7/police-respond-bomb-threat-uwmc/>

**(North Carolina) Police subdue armed man outside VA Medical Center.** Police officers subdued an armed man outside the Charles George VA Medical Center in Asheville the night of April 1, authorities said. VA officers responded to a report around 11:45 p.m. of a man sitting in his car with a shotgun, the hospital's spokesman said. He said police repeatedly asked the man to put down the weapon and get out of his car, which was parked outside the emergency department. The man got out of the car, still holding the weapon, and turned toward one of the officers. Police fired two shots at the suspect but did not hit him. Three officers then rushed the suspect and got him on the ground. He was handcuffed without further incident. The man was being held April 2 at the hospital for medical observation. Asheville police, the FBI, the U.S. Attorney's Office, and the VA Office of the Inspector General were notified of the incident. Source: <http://www.citizen-times.com/article/20100402/NEWS01/100402013/1007/COLUMNISTS>

**H1N1 outbreaks in US, abroad carefully monitored.** As the deadly H1N1 flu is making a comeback in places around the world, including in the southwest United States – Georgia in particular, which has been hit particularly hard – authorities are wondering whether these new outbreaks of the influenza virus represent a worrisome “third wave,” a new mutation, or whether something else is in play that's responsible. Alabama and North Carolina also have reported outbreaks, Centers for Disease Control and Prevention (CDC) officials reported in their latest update on the spread of the virus. CDC warned Georgians to get vaccinated for the H1N1 flu. Georgia has one of the lowest rates of vaccination among its population, which some experts believe is likely contributing to the increase in new infections there. Local activity has also been reported in Arkansas, Louisiana, Mississippi, Tennessee, Virginia, Hawaii, New Mexico and Puerto Rico. Across the world in Malaysia, new A H1N1 clusters have been detected throughout the country, putting the country's Health Ministry on high alert. The World Health Organization (WHO) reported that the H1N1 pandemic influenza remains the most prominent influenza virus circulating around the world and that the virus remains active in parts of the tropical zones of Asia, the Americas, and Africa. Source: <http://www.hstoday.us/content/view/12796/149/>

**Healthcare industry overlooks critical gaps in data security.** As the healthcare industry prepares for a major shift to electronic health records (EHRs) over the next several years, a new bi-annual report provides data that shows that providers are still having difficulty adequately securing patient data in a rapidly changing landscape. The 2010 HIMSS Analytics Report: Security of Patient Data indicates that healthcare organizations are actively taking steps to ensure that patient data is secure. However, these efforts appear to be more reactive than proactive, as hospitals dedicate more resources toward

## UNCLASSIFIED

# UNCLASSIFIED

breach response vs. breach prevention through risk management activities. “The results of the latest study are bittersweet to say the least,” said the chief operating officer for Kroll Fraud Solutions. “On one hand, healthcare organizations are demonstrating increased awareness of the state of patient data security as a result of heightened regulatory activity and increased compliance. On the other, organizations are so afraid of being labeled ‘noncompliant’ that they overlook the bigger elephant in the room, the still-present risk and escalating costs associated with a data breach. We need to shift the industry focus from a ‘check the box’ mentality around compliance to a more comprehensive, sustained look at data security.” Source: <http://www.net-security.org/secworld.php?id=9102>

## **TRANSPORTATION**

**U.S. trains, buses ‘vulnerable’ to terror attack, Lieberman warns.** A U.S. Senator warned Sunday that America’s trains, subways, and buses are “vulnerable” to the kinds of terror attacks that have struck London, Madrid, and most recently Moscow, and said more needs to be done to protect U.S. riders. As the Department of Homeland Security rolls out new security measures for screening suspicious passengers flying into the United States, the chairman of the Senate Homeland Security Committee said the federal government should be paying a lot more attention to security on the ground. “The threat is real to non-aviation transportation. All you’ve got to do is look around the world,” the Senator said, listing the numerous cities that have had their rail and bus lines bombed over the past decade. “These are targets and we know that.” The Senator said the federal government is working with state and local officials to improve transportation security at places other than U.S. airports but that the work is far from finished. Major U.S. transit systems like Washington, D.C.’s Metro and the New York subway have stepped up security in the wake of the Moscow bombings. The U.S. President, speaking on NBC’s “Today” show this past week, called the threat of terror attacks on ground mass transit in the United States a “significant concern,” but said his Administration is trying to guard against it. Source: <http://www.foxnews.com/politics/2010/04/04/trains-buses-vulnerable-terror-attack-lieberman-warns/>

**FAA error-reporting program reveals hazards, yields fixes.** A new error-reporting program in the nation’s air-traffic system is revealing thousands of previously unknown hazards such as dangerous runway crossings and unreported midair problems. In the year and a half since the Federal Aviation Administration (FAA) kicked off the program — which guarantees employees immunity in exchange for honest accounts of all but the most serious lapses — the agency has been deluged by more than 14,000 reports, according to agency records reviewed by USA TODAY. The reports, which had not been widely released until now, have allowed the FAA to make numerous fixes to festering problems, such as improving signage at critical runway intersections, the agency says. It has also opened a window into what was widely suspected but could never be documented: that far more planes are sent on errant and potentially dangerous tracks than were ever officially reported. Source: <http://abcnews.go.com/Travel/faa-error-reporting-program-reveals-hazards-yields-fixes/story?id=10285215>

**(Mississippi) Airport vandals cause damage, concern.** The Corinth-Alcorn airport sees from a dozen or so planes a day, to just a few, but a growing problem has people here concerned for the safety of all of them, and people who live nearby. The runway at Corinth-Alcorn airport is the busiest in Northeast Mississippi outside Tupelo, but recent vandalism has managers here concerned. Someone has been breaking into the airport property, and stealing or damaging the colored lights the line the

UNCLASSIFIED

# UNCLASSIFIED

runway. "It marks the runways, the taxiways and at night time it is an absolute necessity to have that lighting," said the airport manager. Those lights tell pilots where to takeoff and land, and where to go once they get on the ground. The fixtures can cost hundreds, while the colored lenses can cost about \$50. Vandals have broken the fence line in several places, sometimes, even driving onto the airport property in four-wheelers. That leaves openings in the airports secure perimeter and that could present an invitation to many unwanted guests. "We've on rare occasions seen deer inside the airfield and a couple of times we had some cattle on the field," said the airport manager. Source: <http://www.wreg.com/news/wreg-airport-vandals,0,28712.story>

## **WATER AND DAMS**

**(Michigan) Dam to be removed from Pigeon River.** The owners of a much-troubled dam on the Pigeon River in northern lower Michigan have agreed to remove the structure and return the river to its natural state in settlement of environmental damage claims over a 2008 dam failure. Golden Lotus Inc., which owns Song of the Morning yoga retreat where the impoundment is located, also will pay \$150,000 to the state Department of Natural Resources and Environment to compensate for the investigation and cleanup related to the dam failure. The June 2008 break in the dam was the third such event in the last 50 years, each time resulting in the release of massive loads of sediment and devastation to the downstream fishery. Source:

<http://www.freep.com/article/20100406/NEWS06/100406062/1008/NEWS06/Dam-to-be-removed-from-Pigeon-River>

**(Rhode Island) Blue Pond Dam collapse one of few in R.I.** A 200-year old, earthen dam in Rhode Island gave way after record rainfall, March 30. The Blue Pond Dam was built in the 1800s, creating a pond that powered a succession of textile mills and created work for residents of the village of Rockville in Hopkinton. The waters of Blue Pond sliced through it like a knife cutting cake, unleashing an estimated 179 million gallons of water — 2.3 million cubic feet — on a rampage through Hopkinton. The blast of water hurtled through the woods, destroying about 2,000 feet of a local road that led to the pond. The Hopkinton Public Works director said it took about 500 tons of gravel to get it back to where it could support emergency vehicles. It washed out the small bridge that carried Route 3 over Canonchet Brook, a loss that forced state Department of Transportation officials to use Route 95 between Exits 1 and 2 as a detour. Farther downstream, water blew out culverts and flood control structures near the Lindhbrook Country Club, before flowing through Woodville and hitting the Wood River, where it swamped two bridges and left one, the Woodville Road Bridge, impassable. The Wood River sent what had been Blue Pond down to the Pawcatuck River and into Chapman Pond, possibly contributing to the surge that flooded Chapman Pond so much that it closed parts of Route 91. "Every piece of road damage was because of it," he said of the effect the dam break had in town. "Twelve feet of water just disappeared overnight. This would have been spectacular to see."

Source: [http://www.projo.com/news/content/FLOOD\\_DAMS\\_04-08-10\\_8K11F4D\\_v26.3a57a53.html](http://www.projo.com/news/content/FLOOD_DAMS_04-08-10_8K11F4D_v26.3a57a53.html)

**(California) Long Beach seawall 'in imminent danger of collapse'.** Portions of the sea walls protecting Naples Island in Long Beach from the ocean are "in imminent danger of collapse" and could send homes sliding into the water if not replaced soon, officials said Monday. The assessment came in a recent verbal report that an engineer and city staff gave to a councilman, whose district includes Naples. On Tuesday at a special study session, Long Beach officials will consider spending up to \$9.5 million to rebuild the most severely damaged sections of the concrete sea walls. The fear is that if

UNCLASSIFIED

# UNCLASSIFIED

some of the sea walls buckle or crumble, oceanfront properties could fall into the water. The city has long known about the deterioration of the neighborhood's sea walls, first built in the 1923 to protect properties from dredged canals. The 20-foot-deep structures were rebuilt after being damaged by the 1933 earthquake. Workers have been repairing salt water corrosion and maintaining the walls annually, but the councilman said they are getting too old to justify continuing to patch them up. One alternative, according to a report the council will hear Tuesday, is to spend \$1 million reinforcing the most damaged portions, extending their life by another five to 10 years. Within the next 10 to 25 years, the city will need to replace all the neighborhood's sea walls, at a cost of \$60 million. Source: <http://latimesblogs.latimes.com/lanow/2010/04/long-beach-sea-walls-in-eminent-danger-of-collapse.html>

## **NORTH DAKOTA HOMELAND SECURITY CONTACTS**

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **Fusion Center (24/7):** 866-885-8295; email: [ndslic@nd.gov](mailto:ndslic@nd.gov) ; FAX: 701-328-8175

**State Radio:** 800-472-2121 **Bureau of Criminal Investigation:** 701-328-5500 **Highway Patrol:** 701-328-2455

**US Attorney's Office Intel Analyst:** 701-297-7400 **Bismarck FBI:** 701-223-4875 **Fargo FBI:** 701-232-7241

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

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



UNCLASSIFIED

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**

**UNCLASSIFIED**