

**UNCLASSIFIED**



# North Dakota Homeland Security Anti-Terrorism Summary



The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

**UNCLASSIFIED**

**NDSLIC DISCLAIMER**

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

**QUICK LINKS**

**North Dakota**

**Regional**

**National**

**International**

**Banking and Finance Industry**

**Chemical and Hazardous  
Materials Sector**

**Commercial Facilities**

**Communications Sector**

**Critical Manufacturing**

**Defense Industrial Base Sector**

**Emergency Services**

**Energy**

**Food and Agriculture**

**Government Sector (including  
Schools and Universities)**

**Information Technology and  
Telecommunications**

**National Monuments and Icons**

**Postal and Shipping**

**Public Health**

**Transportation**

**Water and Dams**

**North Dakota Homeland Security  
Contacts**

## NORTH DAKOTA

**ND power plant to unveil dried-coal technology.** The operator of North Dakota's biggest coal-fired power plant is touting — and attempting to sell — technology that it said improves efficiency and cuts pollution by drying and removing impurities from high-moisture coal. Great River, a supplier of electric power to rural cooperatives in Minnesota and Wisconsin, has worked for more than a decade developing the so-called DryFinishing process that uses waste heat from the factory to remove water from lignite, a low-quality but abundant coal in North Dakota. Great River got a \$13.5-million loan from the U.S. Energy Department and a \$647,000 state grant for the project, which went on line in December. The company will not disclose the project's overall cost. Lignite contains up to 40 percent water and the company's new process can cut the moisture content by a quarter. Drier coal creates more energy and lessens the amount of power needed to process and burn it, reducing emissions from factory stacks, he said. The process also removes some of the impurities such as sulfur and mercury found in low-grade coal, the company said. Source:

[http://www.forbes.com/feeds/ap/2010/06/02/business-us-drying-coal-north-dakota\\_7654959.html?boxes=Homepagebusinessnews](http://www.forbes.com/feeds/ap/2010/06/02/business-us-drying-coal-north-dakota_7654959.html?boxes=Homepagebusinessnews)

## REGIONAL

**(Minnesota) E. Coli outbreak tied to milk spreads.** A Minnesota investigation has found a fifth person who was sickened after drinking raw milk from a dairy farm near Gibbon. The state department of health reported June 3 that the people were sickened by E. coli bacteria after drinking raw milk from the Hartmann Dairy Farm. Four cases were reported the week of May 31. A toddler remains hospitalized but the other three have been discharged. The fifth case is a young child who was not hospitalized. The department said this week that the strain of E. coli involved has not been found in the state before. Furthermore, lab testing has also found E. coli in cheese from the farm. The state has prohibited movement of products off the farm. Source:

<http://www.foodmanufacturing.com/scripts/ShowPR~RID~15960.asp>

**(Minnesota) Metro nurses to strike June 10.** Representatives from the Minnesota Nurses Association announced Friday that 12,000 nurses will walk away from their jobs June 10 if they cannot reach a contract agreement with hospitals before then. If the strike occurs, it will begin at 7 a.m. that Thursday morning and end at 7 a.m. the following day. A nurse at St. John's Hospital, said nurses promised they would spend "any and/or every day until then" bargaining in order to avoid the strike. Among the contested parts of the contract, nurses are seeking a fixed nurse-to-patient ratio. Such a permanent system would improve patient outcome, nurses said. Nurses in the emergency room would be assigned no more than three patients at once. In intensive care units, it would be one patient per nurse. The hospitals said the proposed ratios are far too rigid and costly and suggest an alternative system in which the head nurse on each floor will make staffing decisions based upon the number and sickness of patients. A federal mediator will join bargaining teams from MNA and the 14 metro area hospitals when they return to the table Wednesday and Friday in hopes of reaching an

# UNCLASSIFIED

agreement before the planned strike. The strike announcement is the latest news since May 19, when nurses overwhelmingly voted to authorize the strike. Source:

<http://www.mndaily.com/2010/06/02/metro-nurses-strike-june-10>

**(Minnesota) NRC: Nuclear plant failed to evaluate flood risk.** Prairie Island Nuclear plant operators knew of the potential for flooding in the Red Wing, Minnesota plant's Unit 1 and Unit 2 turbine buildings, but failed to understand the implications on important safety-related equipment, according to a preliminary finding submitted to the plant Thursday by the U.S. Nuclear Regulatory Commission (NRC). The failure to identify and correct the potential safety issues in a timely manner is a significant human performance issue and cause for further review by the agency, according to NRC inspectors. Plant officials have 10 days to respond to the findings before the NRC decides whether to take enforcement action. "We're waiting now for their response," said a NRC spokesperson. The agency's preliminary findings are tied to a 2009 violation of low to moderate safety significance — called a "White finding" — involving the facility's failure to provide adequate protection of piping against natural events such as tornadoes and earthquakes. Later, when plant operators were evaluating piping in the turbine building for similar issues, they found that a rupture of piping caused by a natural event could result in the flooding of the building. At that time, they did not know what the extent or volume of that flooding would be, according to the Xcel Energy site vice president. Source: <http://www.republican-eagle.com/event/article/id/66927/>

## **NATIONAL**

**Scientists warn of unseen deepwater oil disaster.** Independent scientists and government officials say there is a disaster that can't be seen in the Gulf of Mexico's mysterious depths, the ruin of a world inhabited by enormous sperm whales and tiny, invisible plankton. Researchers have said they have found at least two massive underwater plumes of what appears to be oil, each hundreds of feet deep and stretching for miles. Yet the chief executive of BP PLC - which has for weeks downplayed everything from the amount of oil spewing into the Gulf to the environmental impact - said there is "no evidence" that huge amounts of oil are suspended undersea. BP's CEO said the oil naturally gravitates to the surface - and any oil below was just making its way up. However, researchers said the disaster in waters where light doesn't shine through could ripple across the food chain. On the surface, a 24-hour camera fixed on the spewing, blown-out well and the images of dead, oil-soaked birds have been evidence of the calamity. At least 20 million gallons of oil and possibly 43 million gallons have spilled since the Deepwater Horizon drilling rig exploded and sank in April. Source: [http://www.myfoxphoenix.com/dpp/news/national/apx\\_scientists\\_warn\\_unseen\\_deepwater\\_oil\\_disaster\\_06012010](http://www.myfoxphoenix.com/dpp/news/national/apx_scientists_warn_unseen_deepwater_oil_disaster_06012010)

## **INTERNATIONAL**

**Pakistan: Major released in Times Square terror probe.** A Pakistani military officer arrested and questioned in connection with the Times Square car-bomb investigation was set free and is not connected to the plot, Pakistani officials said, Tuesday. The major was released last week after he was questioned about his possible ties to the terror suspect accused in the attempt to bomb a major New York City commercial district. Pakistani authorities had said they suspected the major, but now say they do not believe the former military officer helped the suspected terrorist in the bombing attempt. A United States attorney declined comment late last week about any of the suspects in Pakistan —

UNCLASSIFIED

# UNCLASSIFIED

including the major — being questioned in connection with the Times Square terror plot. Investigators said they continue to examine who in Pakistan provided the suspect with bomb training as well as cash to try to carry out an attack in New York. Officials have said they suspect members of the Pakistani Taliban played a role. Several associates of the suspect remain in custody as Pakistan assists the U.S. in tracking possible accomplices. Source: <http://www.nbcnewyork.com/news/local-beat/Pakistan-Major-Released-in-Times-Square-Terror-Probe-95311809.html>

## **BANKING AND FINANCE INDUSTRY**

**Visa launches one-time passcode cards in Europe.** Visa has launched a payment card in Europe that contains a keypad and an eight-character display for showing a one-time passcode, an additional defense against potentially fraudulent Internet transactions. Visa's CodeSure also acts as a chip-and-PIN (personal identification number) card, where people enter into a terminal a four-digit pin that is confirmed by a microchip within the card during a face-to-face or cash machine transaction. Online transactions, however, are more susceptible to fraud as they do not use the PIN, often relying only on the details printed on the card. A hacker who has obtained details such as the card's number, expiration date and three-digit security code, may be able to make a purchase online. Visa and MasterCard have been pushing online merchants to implement the more stringent 3D Secure (3DS) system, also known as Verified by Visa or MasterCard SecureCode. The system requires a person to enter a password or portions of a password in a browser frame displayed during a transaction in order to complete an on-line purchase. But 3D Secure still uses a static password selected by a consumer and is vulnerable if someone mistakenly reveals their password through a phishing attack. The alphanumeric display and a keypad on Visa's CodeSure card overcome that vulnerability. During an e-commerce transaction, the customer would press the "Verified by Visa" button on the card and enter their PIN. If the PIN is correct, the card will generate an electronic one-time passcode that can be entered into the Verified by Visa frame. This one-time passcode is only valid for a very short period of time. If it were to be intercepted by a hacker, it would have to be used quickly before it expired.

Source:

[http://www.computerworld.com/s/article/9177663/Visa\\_launches\\_one\\_time\\_passcode\\_cards\\_in\\_Europe?taxonomyId=17](http://www.computerworld.com/s/article/9177663/Visa_launches_one_time_passcode_cards_in_Europe?taxonomyId=17)

**(Oregon) Scam Alert: fake "Umpqua Bank" phone calls demand personal info.** Scammers are targeting Umpqua Bank account holders with a new phone scam, starting with hundreds in Douglas County, Oregon. The Douglas County Sheriff's Office says hundreds of residents began receiving the phone calls over the Memorial Day weekend, starting on Saturday, May 29th, 2010. The calls were claiming to be from "Umpqua Bank." An automated message on the phone claims the customer's debit or credit card has been deactivated, asking customers to press one on their phone, then to enter in personal information. The Douglas County Sheriff's Office and Umpqua Bank say the phone calls are a scam. Scammers involved in this most recent phone fraud case ask for debit and credit card numbers, also Social Security card numbers and other information. Source:

<http://www.kmtr.com/news/local/story/Scam-Alert-fake-Umpqua-Bank-phone-calls-demand/ZbiCPMcQ90Or7lj9oxRI2Q.csp>

**Facebook used to find money mules.** Phishers are looking into different ways of reaching new recruits of cyber criminals by casting their nets onto social networking sites, creating special Facebook groups for their work-at-home scams, according to Kaspersky Lab. Far from a novel idea,

# UNCLASSIFIED

## UNCLASSIFIED

phishers have been using social networks for years to find new recruits. Now, the scammers have created Facebook groups specifically dedicated to the work-at-home scams that often serve as recruitment schemes for money mules. One such group has almost 225,000 members on Facebook, according to Kaspersky researchers. The criminals promise high earnings for minimal efforts: \$6,000 per month for only 18 hours of work per week. Job responsibilities often involve accepting deposits and wire transfers of thousands of dollars a day, then transferring the money to other accounts designated by the phishing gang. Although the money mule can make fast cash relatively easy, it is usually they who are most likely to be discovered, arrested and prosecuted. Sometimes, the money mules do not know what the end result of their activities is; all they know is they are transferring money from one account to another. Source:

<http://www.thenewnewinternet.com/2010/06/01/facebook-used-to-find-money-mules/>

**Phishing scam targets military credit unions.** U.S. Strategic Command officials are joining leading security software vendors in warning soldiers serving in the U.S. Armed Forces to be on high alert for a new phishing scam that targets customers at a pair of credit unions catering to servicemen and their families. The STRATCOM commander, is warning soldiers and their families that bogus Web sites imitating both USAA, a popular insurance and financial services firm catering to military families, and the Navy Federal Credit Union have successfully stolen the personal and banking data of an unknown number of customers. In a blog posting this week, Symantec officials said the phishing sites ask customers to fill in a form with their sensitive data to unlock what the corrupt Web page claims is a log-in error created by too many failed log-in attempts. This information includes Social Security numbers, credit card information, birth dates and mothers' maiden names. "The page also includes a fake CAPTCHA that accepts data irrespective of the number entered," Symantec's security team wrote. "When the sensitive information is entered, the phishing site states that the customer's password is unlocked for logging in. The page is then redirected to the legitimate site." Earlier this month, the Anti-Phishing Working Group (APWG) released a study that found that one phishing gang known as the "Avalanche" syndicate was responsible for more than two-thirds of the 126,000-plus phishing scams it unearthed in the last six months of 2009. Symantec said this latest attack comes from Web sites hosted on servers in Taiwan and variants of this particular phishing URL have been used to spoof other online brands, as well. Source:

<http://www.esecurityplanet.com/news/article.php/3884866/Phishing-Scam-Targets-Military-Credit-Unions.htm>

**Three Florida banks among five seized.** Three Florida banks, along with single banks in California and Nevada, were seized by the Federal Deposit Insurance Corporation (FDIC) Friday. The three Florida banks had assets of around \$1.5 billion and will cost the Deposit Insurance Fund (DIF) an estimated \$200 million. Altogether, the five banks had assets of around \$2 billion and will cost the DIF a little over \$300 million. In the first five months of 2010, the FDIC has seized 76 banks, 13 in Florida. Source:

<http://www.coosavalleynews.com/np85570.htm>

**FBI says 'Grandad Bandit' may be responsible for 21 bank holdups across the eastern U.S.** He may be old, but a man dubbed the "Granddad Bandit" is proving elusive. The FBI in St. Louis said an older man suspected of robbing a Regions Bank branch in St. Louis County May 18 is also suspected of 20 other bank robberies across the eastern and central United States. FBI officials plan a midday news conference Tuesday to discuss the case, including plans to launch a digital billboard campaign to help identify and capture the bandit. The FBI describes the suspect as tall, white, bald and heavy, 50 to 60

UNCLASSIFIED

# UNCLASSIFIED

years old. He is wanted in at least 10 states in addition to Missouri: Alabama, Arkansas, Georgia, Kansas, Florida, Michigan, New York, Oklahoma, Texas and Virginia. Source:

<http://www.fox4kc.com/news/sns-ap-mo--granddadbandit,0,4906092.story>

## **CHEMICAL AND HAZARDOUS MATERIALS SECTOR**

**Atomic waste gets ‘temporary’ home.** Three months after the U.S. canceled a plan to build a vast nuclear-waste repository in Nevada, the country’s ad hoc atomic-storage policy is becoming clear in places like Wiscasset, Maine. Wiscasset doesn’t even have a nuclear-energy plant anymore. The Maine Yankee facility was shuttered back in 1996 after developing problems too costly to fix, and the reactor was dismantled early this decade. What’s left is a bare field of 167 acres cleared and ready for development — except for one thing. Left behind are 64 enormous steel-and-concrete casks that hold 542 metric tons of radioactive waste. Seventeen feet tall and 150 tons apiece, the casks are protected by razor wire, cameras and a security force. Casks like these are the power industry’s biggest hot potatoes. Their presence at a defunct reactor site like Wiscasset’s underscores the intractability of the nuclear-waste problem confronting the power sector and the failure of U.S. policymakers to find a permanent solution. Meant for temporary storage next to energy plants, these containers are now serving as de facto indefinite repositories around America. Source:

[http://online.wsj.com/article/SB10001424052748704717004575269111331754570.html?mod=WSJ\\_hpp\\_MIDDLENexttoWhatsNewsThird](http://online.wsj.com/article/SB10001424052748704717004575269111331754570.html?mod=WSJ_hpp_MIDDLENexttoWhatsNewsThird)

**New anti-terrorism security measure developed for fertilizer dealers.** The Department of Homeland Security (DHS) has introduced a new security measure for chemical facilities and it could eventually directly impact producers. The new Personnel Surety program would apply to chemical facilities regulated under the Chemical Facility Anti-Terrorism Standards. That includes fertilizer manufacturers and agricultural retailers. The president of member services for the Fertilizer Institute, said agricultural producers are currently exempt from the program’s regulations but that is only temporary. She said DHS’s decisions could make a big difference given that it is not unusual for example, for producers to come to a facility to fill up the nurse tank with ammonia. “What we have tried to explain to DHS is that normally farmers do not load the tank themselves. An employee of the facility would load the tank. At that point we feel they should be considered escorted. Now on the other hand, if there is no employee there, would the facility be required to stop the producer from entering that area until somebody returns, or is a retailer going to have to tell his farmer customer that we are going to have to submit your name to the terrorist-creating database and have you cleared so that if you do come in and no one is there it doesn’t create a violation for us?” She said retailers do not like that approach. Source:

<http://www.aginfo.net/index.cfm/event/report/id/Northwest-Farm-and-Ranch-Report-16540>

**EPA moves to close key chemical safety loophole.** After years of allowing corporations to withhold vital safety information, the Environmental Protection Agency (EPA) screamed “stop” on Thursday. In the Federal Register, the agency said it will no longer permit the obstruction of safety evaluations by allowing firms to hide behind age-old claims of business secrecy. The EPA Administrator had told Congress earlier this year that the heavily lobbied for “confidential business information” protection was keeping the agency’s risk assessors from obtaining vital health and safety data on chemical substances awaiting approval. Thousands of chemicals were not properly evaluated because of the withheld information, she told lawmakers. The agency’s new stance has real-world implications. The

UNCLASSIFIED

# UNCLASSIFIED

EPA's move means that protection may no longer exist, at least within that agency. Other federal safety agencies, such as the Occupational Safety and Health Administration and the Food and Drug Administration, apparently still allow the corporate obfuscation. A careful legal interpretation of the long maligned but vital Toxic Substance Control Act (TSCA) convinced the agency that it could provide more valuable information to the public by identifying data where information may have been claimed and treated as confidential in the past but is not and was not in fact entitled to confidentiality under the TSCA. The EPA said it expects to begin reviews of confidentiality claims — both newly submitted and existing — August 25. Source:

<http://www.aolnews.com/nation/article/epa-moves-to-close-key-chemical-safety-loop-hole/19496225>

## **COMMERCIAL FACILITIES**

**Legally, many U.S. hotels lack fire sprinklers.** A fast-moving fire that killed four college students in a suburban Birmingham, Alabama motel illustrates a deadly problem facing travelers around the country: Many older hotels and motels can legally avoid installing sprinklers that stop blazes before they kill guests. Since a catastrophic fire killed 87 at the MGM Grand Hotel in Las Vegas in 1980, a national push to require sprinkler systems in new hotels and motels has helped bring fire deaths down significantly. Yet federal officials said an estimated 3,900 hotel and motel fires are reported to U.S. fire departments each year, causing on average 15 deaths, 150 injuries and \$76 million in property loss. The National Fire Protection Association (NFPA) said it is rare for a guest to die when a fire breaks out in a room with sprinklers, and that there hasn't been a documented fire in a sprinklered hotel that killed more than one person. While newer hotels must install sprinklers, older ones do not, and they take in travelers around the country. A study by the U.S. Fire Administration for 2005-2007 found that about 60 percent of hotels and motels reporting fires lacked sprinklers. The NFPA also found every single fire death from 2002 to 2005 was in a motel or hotel that lacked a sprinkler system. Source: <http://www.whec.com/news/stories/S1589999.shtml?cat=10036>

**(Michigan) Two stores called with bomb threat.** The Benton Township Police Department reported bomb scares at two businesses off Pipestone June 1. The Pri-Mart and Walmart received calls from a male saying he placed bombs near or in the businesses. Both places were called just before 11 a.m. Each place was evacuated while the Berrien County Bomb Squad searched the buildings. The Walmart had to close for two and a half hours before the all-clear was called. Source:

<http://www.wsjm.com/Updated--Two-Stores-Called-With-Bomb-Threats/7368781>

**(Ohio) Suspected bomb spurs evacuation of 60 apartments on Far West Side.** A call about a potentially suicidal woman turned into a bomb scare that prompted the evacuation of 60 apartment units on the Far West Side for six hours June 1. The situation at Saddlebrook Apartments off Roberts Road ended with no bomb being found and no charges being filed. Columbus police and fire received a call just after 3 p.m. that a woman at an apartment on Catalina Circle was suicidal. When the squad arrived, members saw what appeared to be dynamite. Police then evacuated the apartments. They also blocked off Roberts Road between Walcutt and Hilliard-Rome roads for some of the time. A school bus was stopped for about 20 minutes by the initial road shutdown. The scare turned out to be nothing. People were allowed back into their apartments at 9 p.m. Source:

[http://www.dispatch.com/live/content/local\\_news/stories/2010/06/02/suspected-bomb-spurs-evacuation-of-60-apartments.html?sid=101](http://www.dispatch.com/live/content/local_news/stories/2010/06/02/suspected-bomb-spurs-evacuation-of-60-apartments.html?sid=101)

UNCLASSIFIED

## **COMMUNICATIONS SECTOR**

**Dark side arises for phone apps.** As smartphones and the applications that run on them take off, businesses and consumers are beginning to confront a budding dark side of the wireless Web. Online stores run by Apple Inc., Google Inc. and others now offer more than 250,000 applications such as games and financial tools. The apps have been a key selling point for devices like Apple's iPhone. But concerns are growing among security researchers and government officials that efforts to keep out malicious software are not keeping up with the apps craze. In one incident, Google pulled dozens of unauthorized mobile-banking apps from its Android Market in December. The apps, priced at \$1.50, were made by a developer named "09Droid" and claimed to offer access to accounts at many of the world's banks. Google said it pulled the apps because they violated its trademark policy. The apps were more useless than malicious, but could have been updated to capture customers' banking credentials, said the chief executive of Lookout, a mobile security provider. "It is becoming easier for the bad guys to use the app stores," he said. Source:

<http://online.wsj.com/article/SB10001424052748703340904575284532175834088.html>

**US to work with India on National Broadband Plan.** The US has said that it would collaborate with India in evolving a National Broadband Plan. "We have initiated talks through the ICT joint working group last week in New Delhi. We have fixed a time-bound schedule to discuss things. The two sides will soon identify points of contacts for one-to-one interactions," the US Coordinator for International Communication and Information Policy, said. "The ICT working group, which used to meet periodically, could not meet because of elections here and in the US. "We have revived it last week and hope to follow it up six months later in December. These meetings would be held twice a year," he told Business Line. The group comprised top Government executives and representatives from businesses. "The Government set aside \$7-billion announced as part of the stimulus package for creating awareness about the benefits of broadband usage and the US Congress asked the Federal Communication Commission (FCC) to work for a national broadband plan. It came out with hundreds of recommendations. Source:

<http://www.thehindubusinessline.com/2010/06/01/stories/2010060151110800.htm>

**Does the Internet need a beat cop?** The Federal Communications Commission's (FCC) effort to reclassify a portion of broadband service ran into a major setback in the form of a cable-and telephone company-backed lobbying effort to get Congress to step in instead. Last week, House Democrats and Republicans warned the FCC in separate letters to halt its plan to reclassify broadband to exert more control over Internet access. Meanwhile, four key House Democrats announced plans to update the Communications Act with a new law. Reclassifying broadband "is not something that should be taken lightly and should not be done without additional direction from Congress," said a letter from 73 House Democrats to the FCC chairman. If last week was round three in the Title II fight, the round goes to incumbent Internet-service providers looking to head off common-carrier regulations applied to broadband. Title II refers to the Communications Act regulations for common-carrier services like legacy phone service, meant to ensure nondiscriminatory rates and practices in basic telecommunications service. Source: [http://www.multichannel.com/article/453202-Does\\_The\\_Internet\\_Need\\_A\\_Beat\\_Cop\\_.php](http://www.multichannel.com/article/453202-Does_The_Internet_Need_A_Beat_Cop_.php)

# UNCLASSIFIED

## **DEFENSE INDUSTRIAL BASE SECTOR**

**DDG 1000 could get new missile-defense radar.** The Pentagon's recent decision to eliminate half of a new radar system for the U.S. Navy's DDG 1000 Zumwalt-class destroyers - and delay the first of the ships by a year - are not, as many surmised, a result of cost growth or poor program performance. Instead, they are an effort to get a new, even more advanced and capable radar into the new ships. The new radar is the Air Missile Defense Radar (AMDR), a system currently in the early stages of development. The Navy plans to fit the radar, which will be designed from the start to handle ballistic missile defense, into new Flight III versions of its DDG 51-class destroyer. The first Flight III ship is to be ordered in 2016. Source: [http://nosint.blogspot.com/2010/06/ddg-1000-could-get-new-missile-defense.html?utm\\_source=feedburner&utm\\_medium=feed&utm\\_campaign=Feed:+blogspot/fqzx+\(N+aval+Open+Source+INTelligence\)](http://nosint.blogspot.com/2010/06/ddg-1000-could-get-new-missile-defense.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+blogspot/fqzx+(N+aval+Open+Source+INTelligence))

**Boeing GPS IIF-1 satellite sends first signals from space.** Boeing has acquired the first on-orbit signals from the Global Positioning System (GPS) IIF-1 satellite, the inaugural spacecraft in a 12-satellite constellation that the company is building for the U.S. Air Force. The signals indicate that the spacecraft bus is functioning normally and ready to begin orbital maneuvers and operational testing. A United Launch Alliance Delta IV rocket launched the GPS IIF-1 satellite May 27 from Cape Canaveral Air Force Station in Florida. The satellite separated from the rocket's upper stage, and a ground station on Diego Garcia in the Indian Ocean received the first signals from the newest member of the Air Force's GPS satellite constellation. The Air Force 19th Space Operations Squadron and Boeing's Mission Operations Support Center in El Segundo, Calif., confirmed that the satellite is healthy. GPS signals from the spacecraft payload will be turned on for test purposes in the coming weeks. GPS is the U.S. Department of Defense's largest satellite constellation, with 30 spacecraft on orbit. The GPS IIF satellites will provide more precise and powerful signals, a longer design life, and many other benefits to nearly 1 billion civilian and military users worldwide. Source: [http://www.gpsdaily.com/reports/Boeing\\_GPS\\_IIF\\_1\\_Satellite\\_Sends\\_First\\_Signals\\_From\\_Space\\_999.html](http://www.gpsdaily.com/reports/Boeing_GPS_IIF_1_Satellite_Sends_First_Signals_From_Space_999.html)

## **CRITICAL MANUFACTURING**

**2010 Ford Escape, Fusion & Mercury Milan recalled.** Ford is recalling certain Ford Escape, Ford Fusion and Mercury Milan vehicles from the 2010 model year. The company said that affected vehicles with automatic transmissions may not have the correct park rod guide retention pin, which could allow the vehicle to roll away while parked. Ford will notify owners and dealers will repair the vehicles free of charge. Owners may contact Ford at 1-866-436-7332 about Recall No. 10C12. Source: [http://www.consumeraffairs.com/recalls04/2010/ford\\_mercury.html](http://www.consumeraffairs.com/recalls04/2010/ford_mercury.html)

## **EMERGENCY SERVICES**

**USDA grants offer tornado sirens to small towns.** While Indiana's Department of Homeland Security (IDHS) directs grant money away from severe weather warning systems, Eyewitness News Investigates finds towns across Indiana could still tap into millions of dollars available for tornado sirens if they only knew the money was there. Another severe weather season has arrived in Indiana, and hundreds of thousands of Hoosiers live in towns where there are no tornado sirens. Despite

UNCLASSIFIED

# UNCLASSIFIED

millions of dollars available for warning sirens through state Homeland Security grants, small Indiana towns like Nashville and much bigger ones like Kokomo have not purchased any sirens to help warn residents about approaching storms, citing financial restraints that make warning sirens unaffordable. “There’s just not a lot of grant money out there for sirens,” said an emergency management director in Brown County, one of several Indiana counties without a single siren. Many local emergency management directors said the Indiana Department of Homeland Security never told them siren money is available, and state officials tell Eyewitness News the money is needed for other purposes – discouraging news to local communities that have tried unsuccessfully to get siren funding through IDHS. Source: <http://www.wthr.com/Global/story.asp?S=12561781>

## **ENERGY**

**(Alabama) Police charge pair in power-substation copper thefts.** A Decatur, Alabama, man risked electrocution to cut thousands of dollars worth of copper ground wires from power substations across Decatur, police said. Beginning in June 2009, fences surrounding Decatur Utilities and Joe Wheeler Electric Membership Corp. substations were cut and the copper stolen, said a Decatur police detective. The two utility companies filed more than 25 police reports over six months, he said. “Several other agencies throughout north Alabama were experiencing the same problem,” the police detective said. Huntsville police charged the criminals with multiple counts of second-degree theft as a result of a joint investigation between Decatur police and the Morgan County Sheriff’s Department, he said. Source: <http://www.decaturdaily.com/detail/61630.html>

**HM3 Energy lands USDA grant for biomass fuel research.** HM3 Energy announced June 2 it received a \$90,000 grant from the U.S. Department of Agriculture (USDA) to refine the process of turning forest and wood waste into an alternative fuel that can be burned cleanly in existing coal plants. Gresham-based HM3 Energy is using torrefaction — an oxygen-free, high-heat process — to convert biomass into dry and dense briquettes that can be used like coal. The USDA Small Business Innovation Research Phase I award will fund HM3’s refining of the process that will remove dirt, sand and rock from the biomass debris in order to produce clean-burning briquettes. The grant is likely to be followed by a Phase II award of \$750,000 or more to evolve the process into a demonstration phase. Source: [http://sustainablebusinessoregon.com/articles/2010/06/hm3\\_energy\\_lands\\_usda\\_grant\\_for\\_biomass\\_fuel\\_research.html](http://sustainablebusinessoregon.com/articles/2010/06/hm3_energy_lands_usda_grant_for_biomass_fuel_research.html)

**Cyberattacks seen as top threat to zap U.S. power grid.** Cyber attacks, pandemics and electromagnetic disturbances are the three top “high impact” risks to the U.S. and Canadian power-generation grids, according to a report from the North American Electric Reliability Corp. (NERC). “The specific concern with respect to these threats is the targeting of multiple key nodes in the system, if damaged, destroyed or interrupted in a coordinated fashion, could bring the system outside the protection provided by traditional planning and operating criteria,” states the report, “High-Impact, Low-Frequency Risk to the North American Bulk Power System.” The contents of the 118-page report are largely the result of closed-door discussions held since November by NERC (which plays a key role in setting security standards for the U.S. power grid), power providers and U.S. government officials. Source: <http://www.networkworld.com/news/2010/060210-nerc-cyberattack-power-grid.html?hpg1=bn>

# UNCLASSIFIED

# UNCLASSIFIED

**Energy transfer partners begins construction on Tiger pipeline.** Energy Transfer Partners, L.P. today announced that construction has begun on the approximately 175-mile Tiger Pipeline, an interstate natural gas pipeline to serve the Haynesville Shale and Bossier Sands producing regions in Louisiana and East Texas. The 42-inch diameter Tiger Pipeline will have an initial capacity of 2 billion cubic feet per day and is expected to be in service in the first quarter of 2011. Through a planned expansion project announced in February, and subject to FERC approval, the ultimate capacity of the Tiger Pipeline is expected to be 2.4 billion cubic feet per day, all of which is sold out under long-term contracts ranging from 10 to 15 years. Pending necessary regulatory approvals, the expansion is expected to be in service in the last half of 2011. Source:

[http://www.marketwatch.com/story/energy-transfer-partners-begins-construction-on-tiger-pipeline-2010-06-01?reflink=MW\\_news\\_stmp](http://www.marketwatch.com/story/energy-transfer-partners-begins-construction-on-tiger-pipeline-2010-06-01?reflink=MW_news_stmp)

## **FOOD AND AGRICULTURE**

**Ground beef E. coli recall amended.** Montclair Meat Co., Inc., of Montclair, California, announced June 3 that part of the approximately 53,000 pounds of ground beef the company recalled for potential E. coli contamination May 15 had been distributed to wholesalers, restaurants, institutions, and federal establishments for further processing. According to the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS), no illnesses have been reported in connection with the recalled ground beef products. The contamination was discovered during routine microbiological sampling. Products subject to recall include Various pound packages of "MONTCLAIR MEAT CO. GROUND BEEF" and "MONTCLAIR MEAT CO. ALL BEEF PATTIES." Source:

<http://www.foodsafetynews.com/2010/06/ground-beef-e-coli-recall-amended/>

**Raising food rivals fossil fuels in environmental damage.** Raising animals for food damages the environment as much as fossil fuel use, according to a new United Nations (UN) report. A panel of 27 experts with the UN Environment Program looked through previous UN reports to assess what economic activities generate the most pollution and use the most resources. Most of the data comes from the industrialized world. Not surprisingly, burning fossil fuels for transportation and electrical generation top the list for their contributions to climate change, acid rain and toxic pollution. But the report singles out food production as the other major factor driving environmental degradation. The report notes that raising livestock and clearing land for farms and ranches are significant greenhouse-gas emitters. Fertilizers and pesticides are the largest contributors to water pollution. And the world's insatiable appetite is depleting the planet's fisheries and using up land and fresh water at an alarming rate. The growing demand for meat and dairy products is putting particular strain on the environment. The report concludes, "A substantial reduction of impacts would only be possible with a substantial worldwide diet change, away from animal products." A former undersecretary at the U.S. Department of Agriculture, says that's going too far. "My reaction to the document is: we have problems. Let's do the research to try to fix the problems rather than changing the whole diet of the human race," he said. Source: <http://www1.voanews.com/english/news/environment/Raising-Food-Rivals-Fossil-Fuels-in-Environmental-Damage-95611189.html>

**New rust resistance genes added to common beans.** New cultivars of common bean developed by Agricultural Research Service (ARS) scientists and their university colleagues could shore up the legume crop's defenses against the fungal disease common bean rust. According to an ARS plant

UNCLASSIFIED

## UNCLASSIFIED

pathologist in Beltsville, Maryland., the new cultivars possess two or more genes for resistance to the rust fungi. Most of the cultivars also harbor Ur-11, which is considered the most effective rust-resistance gene in the world. The ARS and his colleagues at the University of Nebraska and Colorado State University resorted to this multi-gene strategy in response to the high diversity of strains of the bean rust pathogen. Lately, virulent new races of rust that have overcome the Ur-3 resistance gene appeared in Michigan and North Dakota. Until recently, this gene had been very effective in controlling rust in the United States, especially in North Dakota and Michigan, the country's largest bean-growing states. Now, Ur-3-protected varieties that once withstood the disease are succumbing to it, and there's concern the new races will spread to other Northern Plains states where common beans are grown, such as Colorado and Nebraska. Read more about this research and similar efforts to protect other legume crops in the May/June 2010 issue of Agricultural Research magazine. Source: <http://www.ars.usda.gov/is/pr/2010/100604.htm>

**(Washington) Study solves mystery of major wheat threat.** U.S. scientists say they have solved the mystery of why a pathogen threatening the world's wheat supply can be so adaptable, diverse and virulent. Researchers at the U.S. Department of Agriculture's Agricultural Research Service say they found it is because the fungus that causes the wheat disease called stripe rust can use sexual recombination to adapt to resistant varieties of wheat. A plant pathologist and two colleagues said they have shown for the first time that stripe rust, caused by *Puccinia striiformis*, is capable of sexually reproducing on the leaves of an alternate host called barberry, a common ornamental. The fungus also goes through asexual mutation. But sexual recombination offers an advantage because it promotes rapid reshuffling of virulence gene combinations and produces a genetic mix more likely to pass along traits that improve the chances for survival. Barberry (*Berberis* spp) is already controlled in areas where wheat is threatened by stem rust, caused by another fungal pathogen. But the ARS team said its findings are expected to lead to better control of barberry in areas like the Pacific Northwest, where lower temperatures during most of the wheat growing season make stripe rust a particular threat. The results of the study recently appeared in the journal *Phytopathology*. Source: [http://www.upi.com/Science\\_News/2010/06/01/Study-solves-mystery-of-major-wheat-threat/UPI-25031275427370/](http://www.upi.com/Science_News/2010/06/01/Study-solves-mystery-of-major-wheat-threat/UPI-25031275427370/)

**USDA detects antimicrobial-resistant genes.** Using an advanced genetic-screening technique, the U.S. Department of Agriculture's (USDA's) Agricultural Research Service scientists have detected — for the first time — over 700 genes that give microbes like *Salmonella* and *E. coli* the ability to resist antibiotics and other antimicrobial compounds. The new screening technique, called DNA microarray technology, allowed scientists to hone in on resistance genes in organisms that pose a threat to public health including: *Salmonella*, *E. coli*, *Campylobacter*, *Listeria*, and *Enterococcus*, among others. USDA scientists expressed worry over the findings, released last week. “Researchers are concerned that some of these organisms have acquired genetic resistance to the antibiotics used to kill them,” said the Agricultural Research Service (ARS), the main research arm of the agency, in a statement. “Finding the genes that confer resistance is an important step for scientists looking for new ways to control these organisms.” According to ARS, all genes identified in organisms are logged into GenBank, a gene database administered by the National Center for Biotechnology Information at the National Institutes of Health (NIH). This work was published in the scientific journal *Microbial Drug Resistance*. Source: <http://www.foodsafetynews.com/2010/06/usda-detects-over-700-antimicrobial-resistant-genes/>

UNCLASSIFIED

## UNCLASSIFIED

### **Organicgirl Produce announces baby spinach recall due to possible Salmonella contamination.**

Organicgirl Produce is recalling cases of baby spinach because of potential Salmonella contamination. The limited recall includes 336 cases of the 10 ounce packages of organicgirl Baby Spinach with a Use-By-Date of May 22 and Product Code 11A061167. The cases were sold in six states: Alabama, North Carolina, Oregon, Wisconsin, Arizona and California, according to a May 27 organic girl press release. At least one package of baby spinach was confirmed positive with Salmonella bacteria in a random sample test conducted by a third-party laboratory for the U.S. Food and Drug Administration. There have been no reported illnesses connected with the recall. organicgirl is asking consumers to discard organicgirl Baby Spinach with the matching Use-By-Date and Product Code. Retailers are being asked to remove the product from store shelves. Consumers with questions may call the organicgirl Produce consumer hotline at 831-758-7810, Monday – Friday, 8 a.m. – 5 p.m., Pacific Standard Time. Source:

[http://eatdrinkandbe.org/article/index.0528\\_fs\\_organicgirlspinach](http://eatdrinkandbe.org/article/index.0528_fs_organicgirlspinach)

**La. officials outline proposed seafood safety program.** Louisiana environmental officials sent a letter to British Petroleum May 29 outlining their plan for a long-term seafood safety plan. The officials included in the letter were the secretaries of the Louisiana departments of: wildlife and fisheries, health and hospitals, environmental quality, economic development and agriculture and forestry. In addition to sending a detailed proposal is for a 20-year, multi-agency initiative, the state also requested that BP make \$457 million available for implementation of the program. Source:

<http://www.wdsu.com/news/23734582/detail.html>

**Many protein drinks contaminated with heavy metals.** A Consumer Reports investigation found that many protein drinks could cause health problems over time if they are heavily consumed. Often used by body builders, protein drinks are made by mixing a powder with milk or water or juice. The investigation of 15 protein drinks done at an outside lab found either arsenic, cadmium, lead or mercury in each sample. Most of the tested products had low to moderate levels of contaminants. But three had levels high enough that if consumed three times a day, would exceed the maximum limits proposed by the government. The investigation also found some of these drinks could have excess protein, and most drinks didn't specify a maximum intake. Source:

<http://www.woai.com/content/health/story/Many-protein-drinks-contaminated-with-heavy-metals/j1oYwDRyDEClxqQaE7WjaQ.csp>

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

**Glitch highlights U.S. military reliance on GPS.** A problem that rendered as many as 10,000 U.S. military GPS receivers useless for days is a warning to safeguard a system that enemies would love to disrupt, a defense expert said. The Air Force has not said how many weapons, planes or other systems were affected or whether any were in use in Iraq or Afghanistan. But the problem, blamed on incompatible software, highlights the military's reliance on the Global Positioning System and the need to protect technology that has become essential for protecting troops, tracking vehicles and targeting weapons. "Everything that moves uses it," said the director of Globalsecurity.org, which tracks military and homeland security news. "It is so central to the American style of war that you just couldn't leave home without it." The problem occurred when new software was installed in ground control systems for GPS satellites on January 11, the Air Force said. Officials said between 8,000 and 10,000 receivers could have been affected, out of more than 800,000 in use across the military. One program still in development was interrupted but no weapon systems already in use were grounded

UNCLASSIFIED

# UNCLASSIFIED

as a result of the problem, the Air Force said. Source:

[http://www.msnbc.msn.com/id/37451462/ns/us\\_news-security/](http://www.msnbc.msn.com/id/37451462/ns/us_news-security/)

**(Missouri) Bomb squad examines suspicious package near courthouse.** A suspicious package kept the Bomb Squad with the Kansas City, Missouri Police busy Monday night. It turned out to be a suitcase full of garbage. Police responded to a call about a suspicious package around 9:30 p.m.. Someone reported a suitcase sitting on the sidewalk near the Jackson County Courthouse on 11th Street between Oak and McGee. The bomb squad X-rayed the suitcase to determine if they should diffuse it on the scene or take it to a secure facility. At that time, they learned that the suitcase was filled with trash. No one was hurt. Source: <http://www.fox4kc.com/news/wdaf-suspicious-package-bomb-squad-060110,0,23192.story>

## **INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**NSA leader urges cybersecurity protocols.** The commander of the newly created U.S. Cyber Command said Friday the nation needs precise rules of engagement that would set the standards for a quick counterattack to a serious breach of U.S. military or civilian data networks. It also would be helpful if there were international rules on how nations can respond to cyber attacks, he said. The commander took over the new command, which is primarily responsible for protecting the military's cyber networks, two weeks ago. He retains his duties as head of the National Security Agency, which conducts electronic surveillance of suspected adversaries and possible terrorists. During an appearance at the Center for Strategic and International Studies, he said his command is looking at current rules of engagement, how they conform to the laws and his responsibilities, and "how we can articulate those so the people know what to expect." He said there probably need to be two sets of rules of engagement, one to cover peacetime situations and another for war. He said the issue is complicated by the possibility that an adversary may use a neutral country's computers to launch the attack. In addition, there are differences between an attack on U.S. military systems and one against government or civilian networks. Source: [http://www.nextgov.com/nextgov/ng\\_20100603\\_4464.php](http://www.nextgov.com/nextgov/ng_20100603_4464.php)

**Don't click on 'Paramore n-a-k-ed photo leaked!' Facebook link.** Many Facebook users are being hit by further clickjacking attacks June 2, taking advantage of the social network's "Like" facility. The latest lure is a link which claims to point to a Web site containing a naked photo of the lead singer of the American rock band Paramore. Affected profiles can be identified by seeing that the Facebook user has apparently "liked" a link: The fact that the 21-year-old singer has been the subject of much Internet interest after a topless photo was leaked online, is only likely to fuel interest in the pictures promised by these links. Clicking on the links takes Facebook users to a third-party site which displays a message saying: Click here to continue if you are 18 years of age or above. The hackers have hidden an invisible button under the mouse pointer, so the mouse-press is hijacked wherever one clicks on the Web site. So when one clicks with the mouse, one is also secretly clicking on a button which tells Facebook that one 'likes' the Web page. This then gets published on the user's Facebook page, and shared with online friends, resulting in the link spreading virally. Source:

<http://www.sophos.com/blogs/gc/g/2010/06/02/click-paramore-naked-photo-leaked-facebook-link/>

**Botnets target websites with 'posers'.** Botnets increasingly are creating phony online accounts on legitimate websites and online communities in order to steal information from enterprises. This

UNCLASSIFIED

## UNCLASSIFIED

alternative form of targeted attack by botnets has become popular as botnet tools have made bots easier to purchase and exploit. A botnet expert and distinguished professor of computer science at Georgia Tech, says bots are showing up “en masse” to customer-facing websites — posing as people. “We are seeing tens of thousands of false registrations getting through existing defense-in-depth to get accounts on websites,” says the professor, who is also a member of the board of directors at Pramana and a co-founder of Damballa, both security firms that specialize in botnet mitigation. And these bots can walk off with data from those sites, either for competitive purposes or for selling the stolen information on the black market, according to new data from Pramana, a startup that spun off from Georgia Tech. “Instead of humans, bots are showing up en masse” on auction, social networking, and various other websites that require registration for participation or comments or webmail, he says. “If job listings are your valuable content, what if your competitors set bots to screen-scrape and take your content out the door? This screen-scraping is costing a lot of money and becoming way more prevalent.” Botnet operators are poking holes in CAPTCHA defenses. Pramana, which uses what it calls “HumanPresent” technology that looks at online activity in real-time in order to catch fraud before it occurs, saw 60 percent of bots crashing through CAPTCHAS and other defenses at one Fortune 100 client’s website. Source:

<http://www.darkreading.com/insiderthreat/security/attacks/showArticle.ihtml?articleID=225300009>

**Symantec warns of hike in World Cup spam.** Symantec has joined the chorus of voices warning users to brace for a surge in spam centered around the upcoming World Cup in South Africa. Unsolicited email using the tournament as a lure has risen by around 27 percent in the past month, according to new statistics posted on the security firm’s Net Threats 2010 site. Internet users were warned to expect a range of spam, including offers of counterfeit tickets, malware embedded in fake highlights videos and bogus FIFA product offers. Trend Micro observed similar trends last month, warning users of 419-style spam runs using the tournament as bait. Source:

<http://www.v3.co.uk/v3/news/2263999/symantec-warns-world-cup-spam>

**Google ditches Windows on security concerns.** Google is phasing out the internal use of Microsoft’s ubiquitous Windows operating system because of security concerns, according to several Google employees. The directive to move to other operating systems began in earnest in January, after Google’s Chinese operations were hacked, and could effectively end the use of Windows at Google, which employs more than 10,000 workers internationally. “We’re not doing any more Windows. It is a security effort,” said one Google employee. “Many people have been moved away from [Windows] PCs, mostly towards Mac OS, following the China hacking attacks,” said another. New hires are now given the option of using Apple’s Mac computers or PCs running the Linux operating system. “Linux is open source and we feel good about it,” said one employee. “Microsoft we don’t feel so good about.” In early January, some new hires were still being allowed to install Windows on their laptops, but it was not an option for their desktop computers. Google would not comment on its current policy. Windows is known for being more vulnerable to attacks by hackers and more susceptible to computer viruses than other operating systems. The greater number of attacks on Windows has much to do with its prevalence, which has made it a bigger target for attackers. Employees wanting to stay on Windows required clearance from “quite senior levels”, one employee said. “Getting a new Windows machine now requires CIO approval,” said another employee. Source:

<http://www.ft.com/cms/s/2/d2f3f04e-6ccf-11df-91c8-00144feab49a.html>

UNCLASSIFIED

## UNCLASSIFIED

**Mac spyware infiltrates popular download sites.** A spyware application that surreptitiously scans chat logs and hard drives of unsuspecting Mac users has found its way onto three of the more popular download sites, security researchers said Tuesday. Dubbed OSX/OpinionSpy, the spyware is distributed through software available on sites including Softpedia, MacUpdate, and VersionTracker, according to Intego, a provider of anti-virus software for Macs. The app isn't contained in the downloads themselves, but rather gets downloaded during the installation process, Intego said. A Windows version of the program has existed since at least 2008. Once installed, OpinionSpy scans files and folders on all attached hard drives and regularly sends data in encrypted form to several servers, according to Intego. It also injects code into the Safari, Firefox, and iChat applications and mines them for e-mail addresses, message headers, and other data. The program remains active even if the screensaver or other application that was originally downloaded is uninstalled. Source: [http://www.theregister.co.uk/2010/06/01/mac\\_spyware/](http://www.theregister.co.uk/2010/06/01/mac_spyware/)

**'Clickjacking' worm hits hundreds of thousands on Facebook.** A vulnerability on Facebook forced hundreds of thousands of users to endorse a series of Webp ages over the holiday weekend, making the social networking site the latest venue for an attack known as clickjacking. The exploit works by presenting people with friend profiles that recommend — or “Like,” in Facebook parlance — links with titles including “LOL This girl gets OWNED after a POLICE OFFICER reads her STATUS MESSAGE.” Those who click on the link see a page that's blank except for the words “Click here to continue.” Clicking anywhere on the page automatically forces the person to add the link to his list of Likes. Clickjacking is a term that describes attacks that allow malicious Web site publishers to control the links visitors click on. Virtually every browser that uses Adobe Flash is vulnerable, although many browsers come with safeguards that make exploitation harder. The Facebook worm that hit over the weekend superimposes an invisible Flash iframe over the entire page that links back to the victim's Facebook page. As a result, as long as the person is logged in, his profile automatically recommends the link to new friends as soon as the page is clicked on. Source: [http://www.theregister.co.uk/2010/06/01/facebook\\_clickjacking\\_worm/](http://www.theregister.co.uk/2010/06/01/facebook_clickjacking_worm/)

**House OKs cybersecurity reforms.** The House of Representatives has passed a bill that would update the federal government's cybersecurity requirements and create a permanent cybersecurity office within the White House, putting some long-sought reforms closer to passage. The reforms were passed as an amendment that made its way into the annual defense spending bill, the National Defense Authorization Act for Fiscal Year 2011. The defense authorization bill passed the House Friday by a 229-186 vote. Any differences would be reconciled in conference before the bill is sent to the President to sign. The most wide-ranging changes of the amendment, which combines legislation offered earlier this session by two Representatives, include creating a permanent National Office for Cyberspace and Office of the Federal Chief Technology Officer (CTO) within the White House, giving both the director of the National Office for Cyberspace and the federal CTO specific responsibilities, and adding new cybersecurity requirements for agencies in areas like acquisition, budgeting, and actually securing IT systems. Source: <http://darkreading.com/security/government/showArticle.ihtml?articleID=225200733>

## **NATIONAL MONUMENTS AND ICONS**

**(New Mexico) Rio Fire listed at 10 percent contained.** The Rio Fire, which is currently about six miles northwest of Jemez Springs, New Mexico and half a mile southwest of Fenton Lake State Park, has

UNCLASSIFIED

# UNCLASSIFIED

increased to 1,925 acres, but fire officials are listing the fire as 10 percent contained. The fire has been burning since June 1. No structures have been lost yet in the blaze, however the fire is threatening 83 structures currently. Air support continues to attempt to slow the fire by dropping water and retardant on the hot spots. Ground crews continue to strengthen and construct line along the west and north sides of the fire. Evacuations were put in order for people along FR 376, Fenton Lake State Park, the community of Seven Springs and the fish hatchery. Ten people were evacuated June 1. An evacuation center is set up at Jemez Valley High School gymnasium at 8501 Highway 4 near Jemez Pueblo. No one is staying at the evacuation center currently. Officials think the cause of the fire was an abandoned camp fire. Over the Memorial Day holiday, officials put out 17 abandoned campfires in the Jemez Ranger District alone. Source:

<http://www.krqe.com/dpp/news/environment/rio-fire-listed-at-10-percent-contained>

## **POSTAL AND SHIPPING**

**(Colorado) 2 In custody for “suspicious powder” hoax In Pueblo.** Streets in Pueblo were blocked off for hours May 27 after a suspicious substance was discovered. The white powder ended up being store brand sugar. Grand and 24th streets and a block radius in all directions were closed to traffic and all businesses and houses were evacuated for more than three hours. Witnesses say two men were acting suspicious around a mail dropbox and there was white powder found at the base of the dropbox and 20 feet west of it. One was pouring white powder into the mailbox wearing a gas mask, the other was videotaping the activity. According to sources from the Pueblo Police Department, one of them called police dispatch from a Sam’s Club in Pueblo to turn himself in. Officers picked him up and he is in custody. Another man was also arrested. Their car was found at a Sam’s Club on north end of Pueblo. That car is now in police custody. The FBI was also on scene because a US post office box is federal property. Source: <http://www.kktv.com/home/headlines/95045449.html>

## **PUBLIC HEALTH**

**New antibiotic proves safe and well tolerated.** The new antibiotic - PT1.2 - has been developed by Phico Therapeutics, initially to treat nasal infections of the bacterium *Staphylococcus aureus* including the ‘superbug’ MRSA. It is the first in a new class of antibacterial therapy forming Phico Therapeutics’s antibiotic platform technology called SASPject, which is specifically designed to combat the problem of drug resistance. “The completely new SASPject technology has the capability to revolutionise antibiotic therapy and human trials are a crucial milestone in product development,” explained the CEO of Phico Therapeutics. “Successful completion of this trial means that we have met the first milestone laid down by the Wellcome Trust as part of Phico’s Strategic Translation Award, and triggers drawdown of our second tranche of funds to cover the phase II trial.” Source:

<http://www.physorg.com/news194779751.html>

**(Texas) Substance prompts quarantine at VA hospital.** Four mailroom employees at the Audie L. Murphy Memorial Veterans Hospital were quarantined for more than an hour June 1 morning after a suspicious substance was found inside two envelopes. The substance was discovered about 10 a.m. and police and firefighters were called to investigate. A hazardous materials crew later determined the substance was not hazardous. Emergency vehicles left the hospital by 11:30 a.m. Patient care at the hospital was continued without interruption. Source:

UNCLASSIFIED

# UNCLASSIFIED

[http://www.mysanantonio.com/news/local\\_news/substance\\_prompts\\_quarantine\\_at\\_va\\_hospital\\_95328874.html](http://www.mysanantonio.com/news/local_news/substance_prompts_quarantine_at_va_hospital_95328874.html)

**(California) 1,300 San Diego nurses to strike over low staffing.** About 1,300 nurses in San Diego, California, are threatening to walk out of their jobs at the local UC hospitals next week. Nurses say they will go on strike because administrators refuse to address their concerns about inadequate staffing. California law requires hospitals to maintain strict nurse-to-patient ratios in all units around the clock. UC nurses say their departments are often short-staffed during breaks and at meal times. Nurses argue they cannot deliver good patient care under those conditions. UC officials say patient safety is a top priority, and maintain their hospitals obey the staffing law at all times. Source: <http://www.kpbs.org/news/2010/jun/01/1300-san-diego-nurses-set-strike-over-low-staffing/>

**PediaCare children's drugs recalled.** More children's medicines — four products sold under the PediaCare brand name — have been recalled. All four of the over-the-counter medications were made in Johnson & Johnson's troubled McNeil plant in Pennsylvania. Numerous problems at the plant, including drugs containing incorrect dosages and unsafe manufacturing conditions, led to the April 30 recall of popular child and infant versions of Tylenol, Motrin, Benadryl, and Zyrtec. The products recalled over the Memorial Day weekend are sold by Blacksmith Brands. They include: PediaCare Multi-Symptom Cold 4oz. (UPC # 3 0045-0556-05 9), PediaCare Long Acting Cough 4oz. (UPC# 3 0045-0465-04 7), PediaCare Decongestant 4oz. (UPC# 3 0045-0554-04 8), PediaCare Allergy and Cold 4oz. (UPC# 3 0045-0552-04 4) Although no injuries have been reported from use of these products, the manufacturer warns parents to stop using the drugs and to throw away any product they may have purchased. Source: <http://www.webmd.com/parenting/news/20100601/pediacare-childrens-drugs-recalled>

## **TRANSPORTATION**

**U.S. works with Middle East to bolster global aviation security.** The Department of Homeland Security (DHS) Secretary will travel to the United Arab Emirates (UAE) May 31-June 1. She will meet with her counterparts from the Middle East region and officials from the International Civil Aviation Organization (ICAO) to discuss ways to bolster global aviation security. This will be the fifth in a series of major international meetings hosted by ICAO member states in which the Secretary will participate to build consensus on strengthening global aviation security, and to identify specific steps that nations can take individually and collectively to protect all passengers. Prior to visiting UAE, the Secretary will travel to Saudi Arabia May 30-31 to meet with top Saudi officials about a variety of global security issues. She will discuss counter-terrorism, counter-radicalization and cooperation on critical infrastructure protection, and deliver remarks to students and businesswomen about the importance of opportunities in education, and the value of public service for women across the world. Source: [http://www.thegovmonitor.com/world\\_news/united\\_states/u-s-works-with-middle-east-to-bolster-global-aviation-security-32362.html](http://www.thegovmonitor.com/world_news/united_states/u-s-works-with-middle-east-to-bolster-global-aviation-security-32362.html)

**Despite fewer accidents, growing concern about air safety.** The skies over the United States have been remarkably safe in the last decade. On the surface, the numbers suggest the nation is doing a better job of keeping planes aloft. Not counting the four airliners lost to terrorism on September 11, 2001, the U.S. suffered only five fatal accidents from 2000-2009. In one of those accidents, a Southwest Airlines Boeing 737 slid off the runway at Chicago Midway Airport, hurting no one on

UNCLASSIFIED

## UNCLASSIFIED

board but killing a child when the plane struck a car. The most recent fatal accidents have involved small, commuter airlines. Previous decades have been much more deadly. In 1985, for example, there were five fatal airline accidents that year, killing 272 people. Though the numbers suggest improved safety, other data support the belief that the U.S. has been very lucky. Agence France-Presse (AFP) recently reported that the Federal Aviation Administration (FAA) has begun to review its air traffic control procedures after a startling number of near-misses in the last few months. "Over the last weeks there have been a number of instances where separation was lost between aircraft and in some cases there was a bit of a delay of notification that obviously caused some concern," an FAA spokesman told AFP. In other words, in several instances air traffic controllers have lost track of where planes are. In one of the most recent incidents, US Airways Flight 140, with 138 passengers on board, came within 100 feet vertically and .33 mile laterally, of a Boeing 747 cargo plane over Alaska. No one was injured but the two planes were well inside aircraft separation limits. Other close calls were reported in March at San Francisco International, and in Houston where there were two incidents involving Southwest Airlines jets. The FAA is currently investigating these incidents. The Wall Street Journal reports the agency is also very concerned by delays in reporting these near-collisions. While incidents are supposed to be reported within 24 hours, the FAA said it received some reports several days after the fact. Source:

[http://www.consumeraffairs.com/news04/2010/06/airline\\_safety.html](http://www.consumeraffairs.com/news04/2010/06/airline_safety.html)

## **WATER AND DAMS**

**(Texas) Bomb plot alert at Falcon Dam.** An alleged plot by a Mexican drug cartel to blow up a dam along the Texas border — and unleash billions of gallons of water into a region with millions of residents — sent American police, federal agents and local disaster officials scrambling last month to thwart such an attack, authorities confirmed Wednesday. Whether the cartel, which is known to have stolen bulk quantities of gunpowder and dynamite, could have taken down the five-mile-long Falcon Dam along the Rio Grande River may never be known. But it may have been derailed by a stepped-up presence by the Mexican military, acting in part on intelligence from the U.S. government, sources said. The warning was based on what the federal government contends were "serious and reliable sources" and prompted the Homeland Security Department to sound the alarm to first responders all along the South Texas-Mexico border. Mexico's Zeta cartel was planning to destroy the dam not to terrorize civilians, but to get back at its rival and former ally, the Gulf cartel, which controls smuggling routes from the reservoir to the Gulf of Mexico, the Zapata County sheriff and others familiar with the alleged plot said. Destroying the dam, however, also would have flooded large areas of agricultural land, as well as significant parts of a region with about 4 million border residents in Texas and Mexico. Besides the sheriff's agency, the U.S. Border Patrol, the Texas Department of Public Safety (DPS), and even game wardens, also responded. Citing security concerns, neither Homeland Security nor DPS commented. Source:

[http://www.mysanantonio.com/news/local\\_news/bomb\\_plot\\_alert\\_at\\_falcon\\_dam\\_95481059.html](http://www.mysanantonio.com/news/local_news/bomb_plot_alert_at_falcon_dam_95481059.html)

**EPA proposes new permit requirements for pesticide discharges.** The U.S. Environmental Protection Agency (EPA) is proposing a new permit requirement that would decrease the amount of pesticides discharged to U.S. waters. This action is in response to an April 9, 2009 court decision that found that pesticide discharges were pollutants, requiring a permit. The proposed permit, released for public comment and developed in collaboration with states, would require all operators to reduce pesticide discharges by using the lowest effective amount of pesticide, prevent leaks and spills, calibrate

UNCLASSIFIED

## UNCLASSIFIED

equipment and monitor for and report adverse incidents. Additional controls, such as integrated pest-management practices, are built into the permit for operators who exceed an annual treatment area threshold. "EPA believes this draft permit strikes a balance between using pesticides to control pests and protecting human health and water quality," said the assistant administrator for EPA's Office of Water. EPA estimates that the pesticide general permit will affect approximately 35,000 pesticide applicators nationally that perform approximately half a million pesticide applications annually. EPA is soliciting public comment on whether additional use patterns should be covered by this general permit. The agency plans to finalize the permit in December 2010. It will take effect April 9, 2011. Once finalized, the pesticide general permit will be used in states, territories, tribal lands, and federal facilities where EPA is the authorized permitting authority. In the remaining 44 states, states will issue the pesticide general permits. EPA has been working closely with these states to concurrently develop their permits. Source:

[http://www.watertechnonline.com/news.asp?N\\_ID=74212](http://www.watertechnonline.com/news.asp?N_ID=74212)

**The Ten Most Endangered Rivers of 2010.** There are tens of thousands of rivers and streams across the USA, and each year only ten make it on to the America's Most Endangered Rivers list. The 2010 list spotlights rivers facing a multitude of threats from New York to Iowa to California. The number one river on the list this year is the Upper Delaware River, where gas drilling threatens the drinking water supply for 17 million people in New York, New Jersey and Pennsylvania, according to American Rivers. A handful of other threats stand out this year. Mining puts West Virginia's Gauley and Oregon's Wild and Scenic Chetco at risk. New water supply dams threaten rivers like North Carolina's Little and Idaho's Teton. And outdated flood management imperils public safety and river health on Iowa's Cedar and California's Sacramento-San Joaquin, listed for the second year in a row. The 2010 report also features 22 endangered river success stories. The rankings are: 1) Upper Delaware River, Pennsylvania, New York; 2) Sacramento-San Joaquin River Delta, California; 3) Gauley River, West Virginia, 4) Little River, North Carolina; 5) Cedar River, Iowa; 6) Upper Colorado River, Colorado; 7) Chetco River, Oregon; 8) Teton River, Idaho; 9) Monongahela River, Pennsylvania, West Virginia; and 10) Coosa River, Alabama. Source: <http://www.americanrivers.org/newsroom/blog/ten-most-endangered-2010-6-2-2010.html>

**Household detergents, shampoos may form harmful substance in wastewater.** Scientists are reporting evidence that certain ingredients in shampoo, detergents, and other household cleaning agents may be a source of precursor materials for formation of a suspected cancer-causing contaminant in water supplies that receive water from sewage treatment plants. The study sheds new light on possible environmental sources of this poorly understood water contaminant, called NDMA, which is of ongoing concern to health officials. Their study is in ACS' Environmental Science & Technology, a semi-monthly journal. The lead scientist and his and colleagues note that scientists have known that NDMA and other nitrosamines can form in small amounts during the disinfection of wastewater and water with chloramine. Although nitrosamines are found in a wide variety of sources — including processed meats and tobacco smoke — scientists know little about their precursors in water. Past studies with cosmetics have found that substances called quaternary amines, which are also ingredients in household cleaning agents, may play a role in the formation of nitrosamines. Their laboratory research showed that when mixed with chloramine, some household cleaning products — including shampoo, dishwashing detergent, and laundry detergent — formed NDMA. The report notes that sewage treatment plants may remove some quaternary amines that form NDMA. However, quaternary amines are used in such large quantities that some still may persist and have a

UNCLASSIFIED

# UNCLASSIFIED

potentially harmful effect in the effluents from sewage treatment plants. Source:  
[http://www.eurekalert.org/pub\\_releases/2010-05/acs-hds052610.php](http://www.eurekalert.org/pub_releases/2010-05/acs-hds052610.php)

**NASA satellite to monitor water consumption.** National Aeronautics and Space Administration (NASA) engineers have begun building hardware for a new Landsat satellite instrument that will help monitor water consumption, according to a press release. This technology will be especially important in the U.S. West where precipitation is sparse and water rights are allocated, the release stated. The Thermal Infrared Sensor (TIRS), which will be built at the Goddard Space Flight Center in Greenbelt, Maryland, is a two-channel thermal imager, providing 100-meter spatial resolution across a 185-kilometer field-of-view. According to the release, TIRS will provide surface-temperature readings considered vital in a technique that resource managers in Idaho and other western states use to measure water use through “evapotranspiration,” a term which combines the evaporation of water into the atmosphere and the water vapor released by plants through respiration. Source:  
[http://watertechonline.com/news.asp?N\\_ID=74192](http://watertechonline.com/news.asp?N_ID=74192)

## **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(In ND only);** 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**