

UNCLASSIFIED



# NORTH DAKOTA HOMELAND SECURITY ANTI-TERRORISM SUMMARY



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

UNCLASSIFIED

# UNCLASSIFIED

## **NDSLIC DISCLAIMER**

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

## **QUICK LINKS**

[North Dakota](#)

[Regional](#)

[National](#)

[International](#)

[Banking and Finance Industry](#)

[Chemical and Hazardous Materials  
Sector](#)

[Commercial Facilities](#)

[Communications Sector](#)

[Critical Manufacturing](#)

[Defense Industrial Base Sector](#)

[Emergency Services](#)

[Energy](#)

[Food and Agriculture](#)

[Government Sector \(including  
Schools and Universities\)](#)

[Information Technology and  
Telecommunications](#)

[National Monuments and Icons](#)

[Postal and Shipping](#)

[Public Health](#)

[Transportation](#)

[Water and Dams](#)

[North Dakota Homeland Security  
Contacts](#)

UNCLASSIFIED

## **NORTH DAKOTA**

**Landslide moves Fargo road 13.5 feet, breaks water main.** Officials said Fargo, North Dakota's largest landslide in recent memory will cost at least \$100,000 to repair after it dislocated a section of road, broke a water main, and plugged a drainage ditch, the Forum of Fargo-Moorhead reported June 7. City employees became aware of the problem May 31 when the water pressure dropped in a north-side tower because of the water main break, the public works director said. Engineers found a section of 32nd Street North measuring more than 100 feet long had shifted 13.5 feet to the west, causing cracks in the gravel road and large ruts at each end. The road and an adjacent drain field had slid toward Legal Drain 10, pushing up the bottom of the drainage ditch and blocking the main channel. Engineers said it appeared the ground shifted under the weight of a stockpile of aggregate sitting along the street on the site of Border States Paving Inc.'s asphalt production plant. Engineers surveyed the drain to make sure water could still pass over the plugged section without flooding surrounding land and hired a contractor to clear the drain after Border States finished moving the aggregate away from the road to prevent more slumping. The drain was expected to be open by the weekend of June 9. All other repairs were expected to be complete in 4 to 6 weeks. Crews recapped the water main, for future development, at the point of breakage and will likely have to replace the entire section that shifted, they said. The damaged road was barricaded, temporarily cutting off access. Source: <http://www.inforum.com/event/article/id/363517/>

**Enbridge shuts key US Midwest oil line.** Enbridge shut down a key supply line for Canadian crude shipments to U.S. refineries June 6 but said the outage was expected to be short in duration and have little impact on deliveries. Enbridge, whose network of pipelines transports the majority of Canadian oil supplies to the United States, said Line 6A was expected to resume flows later in the day. The pipeline carries 609,000 barrels a day of Canadian and North Dakota crude to Griffith, Indiana, from Superior, Wisconsin. At Griffith, connected lines move the oil to other parts of the Midwest and into southern Ontario. Those regions were already oversupplied with crude, so refineries are not expected to face any shortages. Canadian crude prices, however, weakened as shippers already struggled with tight pipeline capacity to move oil out of western Canada. Source: <http://af.reuters.com/article/energyOilNews/idAFL1E8H6MMI20120606>

**Cool weather slows crop development in N. Dakota.** Cool conditions across North Dakota the week of May 28 slowed crop development, the Associated Press reported June 4. In its weekly crop report, the U.S. Department of Agriculture said frost was a concern for many parts of the State. The most adverse effects were felt in the northeastern and south-central parts of North Dakota. Statewide, there were 5.3 days of suitable fieldwork. Source: [http://www.cbsnews.com/8301-505245\\_162-57446983/cool-weather-slows-crop-development-in-n-dakota/](http://www.cbsnews.com/8301-505245_162-57446983/cool-weather-slows-crop-development-in-n-dakota/)

**Levee closed to pedestrian traffic, flood repairs under way.** The Williston Levee and the Williston Resource Office in North Dakota will be closed May 29 to August 15 for repairs, the Williston Herald reported. During the 2011 flood, the levee suffered significant damage and the

## UNCLASSIFIED

\$11.7 million project includes restoring the levee crest to an approximate elevation of 1862-1863 feet above sea level. The levee will be seeded for grass, returning it to pre-flood status and level of flood risk reduction. The access road will also be resurfaced during this period. The levee is a federally constructed flood control project designed to reduce the risk of flooding in low lying areas due to backwater from Lake Sakakawea, the reservoir for the Garrison Dam.

Source: [http://www.willistonherald.com/news/levee-closed-to-pedestrian-traffic-flood-repairs-under-way/article\\_3f55db7a-ab4f-11e1-9e5a-001a4bcf887a.html](http://www.willistonherald.com/news/levee-closed-to-pedestrian-traffic-flood-repairs-under-way/article_3f55db7a-ab4f-11e1-9e5a-001a4bcf887a.html)

### **REGIONAL**

**(Minnesota) Army Corps of Engineers to reopen Twin Cities locks, dams to commercial traffic Wednesday.** The U.S. Army Corps of Engineers reopened the three Minneapolis, Minnesota locks and dams to commercial traffic June 5, but the locks will remain closed to recreational boats. The Corps closed the locks to barges May 29 when flows on the Mississippi River exceeded 40,000 cubic feet per second (cfs). The locks were closed to recreational boats May 28 and will remain closed to recreational traffic until flows are below 30,000 cfs. The National Weather Service forecast indicated that may happen by June 10. Heavy rains the week of May 28 contributed to the increase in water. The Upper St. Anthony Falls and Lower St. Anthony Falls locks and dams are in downtown Minneapolis. Lock and Dam 1 is next to Minnehaha Park in Minneapolis. Source:

<http://www.therepublic.com/view/story/50935fdeef4491eb92f8e05d1a75026/MN--Minneapolis-Locks-Reopen>

**(Montana) Corps: Fort Peck Dam repair may cost more than \$225 million, but only \$46 million available.** Proposed repairs for Montana's Fort Peck Dam following epic flooding along the Missouri River in 2011 would cost more than \$225 million, according to cost estimates released May 30 by the U.S. Army Corps of Engineers. Corps officials acknowledged they are able to afford only \$46 million for damage assessments and repair work for now, mostly for the dam's spillway. Record snowfalls and massive spring rains in Wyoming and Montana in 2011 prompted the release of unprecedented volumes of water from the Corps' six Missouri River dams. The torrent damaged Fort Peck's spillway gates and eroded areas downstream from the dam, located at the top of the Missouri River system. The most expensive repairs outlined by the Corps' engineering consultants would bolster the spillway so it could handle releases of 265,000 cubic feet of water per second (cfs), which is more than four times the peak release of almost 66,000 cfs during 2011's flooding. The Fort Peck project manager said the proposed repairs are needed to ensure the spillway can be used to safely release water. The governor of Montana said the State would support any work that improves safety and storage capacity for the dam. Work on damage to the spillway gates already is underway. The \$245 million figure does not include any work that could be needed on a concrete drainage system beneath the spillway. Testing to determine whether that drainage system is working properly is planned for the week of September 4. As part of the testing, the Corps plans to release water at between 3,000 and 30,000 cfs at periodic intervals over 4 days. Source:

<http://www.therepublic.com/view/story/d7b301126517440a80ebb311f71eff5e/US--Fort-Peck-Dam>

UNCLASSIFIED

## UNCLASSIFIED

**(South Dakota) Corps says ‘anomaly’ found at Gavins Point.** The U.S. Army Corps of Engineers announced June 5 it found an “anomaly” under the apron at Gavins Point Dam near Yankton, South Dakota. The May 9 assessment, which used ground-penetrating radar (GPR), confirmed damage to the area under the spillway slab known as the “frost blanket.” The GPR also revealed an unidentified abnormality under the apron, which is the concrete found downstream of the gates that helps prevent erosion. Corps officials emphasized the dam was safe and structurally sound with no visible stress on the concrete. No restrictions were placed on the dam at this time, they said. The dam sustained releases of 160,000 cubic feet per second (cfs) for much of the 2011 summer. The Corps was conducting further research of the findings which could take 2 or more months. In addition, the Corps also announced June 5 an estimated \$10.5 million is needed for repairs to the dam. Source:

<http://www.yankton.net/articles/2012/06/06/community/doc4fced24559a31828008543.txt>

## **NATIONAL**

**(New Mexico) Sandia National Labs scientist arrested.** A Sandia National Labs scientist was arrested recently because he allegedly stole laboratory research and shared it with China, redOrbit reported June 6. He was accused of stealing research belonging to the United States that he claimed was his own original research that he shared with several Chinese universities. He went online to share the data with the country’s state-run schools. Sandia National Labs said he did not have access to classified national security information. The lab said the scientist was fired in April for removing a company-owned laptop from the facility. Sandia is known for its nuclear research, as well as the disposal of the U.S. nuclear weapons program’s hazardous waste. The company is a subsidiary of Lockheed Martin Corporation. Five years ago, the scientist started working on nanotechnology at a Sandia Labs research center that focuses on nanotechnology. He was indicted on five counts of federal program fraud, and one count of false statements, court papers said. Lab workers are not allowed to take any lab equipment on international trips without approval. Sandia released a statement June 4 saying it expects all employees to follow procedures. The scientist’s indictment in May was sealed until June 4, and he was arrested for the charges the weekend of June 2. He is scheduled to be arraigned on the charges June 12, and remains in federal custody. Source:

<http://www.redorbit.com/news/science/1112549346/sandia-national-labs-scientist-arrested/>

**Clean up from 2011 flooding continues.** The flooding along the Missouri and Mississippi Rivers in 2011 left many farmers struggling to recover. In 2012, many are still cleaning up the mess and working to restore cropland to productive levels seen before the flooding, Ag Professional reported June 5. The flooding caused many corn and soybean fields to become so damaged, that restoring the land will likely take multiple years. Some farmers have spent the past 9 months removing sand from fields and filling in holes gouged out by the flood. The sand is devastating to fields because it robs the soil of microbes that flourish in topsoil, which helps crops grow. Returning the soil to the previous levels of productivity can take time.

Compounding the problem of removing the sand is where to place it once it is removed from the land. The U.S. Army Corps of Engineers prohibits farmers from dumping the sand back into

UNCLASSIFIED

## UNCLASSIFIED

the river without a federal permit. As a result, much of it gets piled along the fields and is used to fill giant holes left by the water. Source: <http://www.agprofessional.com/news/Clean-up-from-2011-flooding-continues-157026465.html>

### **INTERNATIONAL**

**Sandbag thieves leave flood areas vulnerable.** Police in Victoria, Australia, were investigating the theft of sandbags from key locations around Lakes Entrance where residents were bracing for another king tide that could inundate properties June 7. The army and local residents spent the day sandbagging areas of the site which, together with nearby Loch Sport, Paynesville, and Raymond Island, was in danger again from floodwaters rushing from the high country to the coast. A state emergency service spokeswoman said sandbags were protecting critical infrastructure and properties from a predicted king tide June 6, but many people were seen stealing them overnight. The thefts were believed to have occurred at several locations around Lakes Entrance. There were fears the king tide June 6 could flood up to 400 homes, almost 50 properties at Metung, and more than 175 at Paynesville. The bureau of meteorology said major flood warnings were in place for the Mitchell and Snowy rivers. A moderate flood warning was issued for the Buchan, Macalister, and Thomson rivers, while minor flood warnings were issued for six other rivers. Source: <http://sl.farmonline.com.au/news/state/agribusiness-and-general/general/sandbag-thieves-leave-flood-areas-vulnerable/2582937.aspx>

**Iranian cell-phone carrier obtained banned US tech.** Interviews and documents show a fast-growing Iranian mobile-phone network managed to obtain sophisticated U.S. computer equipment despite sanctions that prohibit sales of American technology to Iran, Reuters reported June 4. MTN Irancell, a joint venture between MTN Group Ltd of South Africa and an Iranian government-controlled consortium, sourced equipment from Sun Microsystems Inc, Hewlett Packard Co, and Cisco Systems Inc, the documents and interviews show. MTN owns 49 percent of the joint venture but provided the initial funding. The procurement — through a network of tech companies in Iran and the Middle East — offers further evidence of the limitations of U.S. economic sanctions. The sanctions are intended to curb Iran's nuclear program, which Tehran maintains is peaceful. No U.S. company can sell goods or services to Iran unless it obtains special authorization. However, U.S. enforcement has focused on containing Iranian banks, terrorism, Iran's oil industry, and individuals and companies that Western capitals believe are involved in Tehran's nuclear development program. Source: <http://af.reuters.com/article/topNews/idAFJOE85401820120605>

### **BANKING AND FINANCE INDUSTRY**

**Tutorials teach cybercriminals how to avoid fraud detection systems.** Trusteer experts have come across tutorials in an underground hacking forum that detail how fraud detection systems set up by financial and e-commerce providers can be circumvented. The anti-fraud mechanisms usually fingerprint a device to identify signs of misuse. They collect data such as IP address, Web browser type and version, and operating system details. If too many orders from multiple user accounts are placed from one machine, alarm bells go off and the transactions are

UNCLASSIFIED

## UNCLASSIFIED

blocked. However, cybercriminals have found ways to bypass the system through use of virtual private networks (VPN) and proxy services that hide IP addresses. They are also shown how to make the system incorrectly read the fingerprints, making it believe different computers with different browsers and operating systems have been used. The software that performs the task is freely available for download and achieves its objectives by manipulating the information in the Web browser's User-Agent header. Source: <http://news.softpedia.com/news/Tutorials-Teach-Cybercriminals-How-to-Avoid-Fraud-Detection-Systems-274013.shtml>

**Restaurant chain reports card breach.** Penn Station Inc. confirmed 43 of its 235 U.S. restaurants may have been affected by a payments breach that exposed credit and debit details, BankInfoSecurity reported June 5. In a June 1 statement and list of frequently asked questions (FAQ) posted on Penn Station's Web site, the restaurant chain identified franchise locations in Illinois, Indiana, Kentucky, West Virginia, Michigan, Missouri, Ohio, Pennsylvania, and Tennessee that may have been affected. Penn Station's president said the company learned of the breach after a customer called to report his card had been compromised shortly after dining at one of Penn Station's franchised locations. Penn Station then contacted its processor, Heartland Payment Systems, and the U.S. Secret Service. Industry experts have suggested the breach is likely linked to either a processing hack or tampered point-of-sale devices. Debit and credit cards used during March and April may have been exposed. "Upon learning of the possibility of unauthorized access to credit and debit card information, all of the individual owners of the Penn Station restaurants changed the method for processing credit and debit card transactions," the FAQ states. Penn Station said only account holder names and card numbers were breached. Whether personal identification numbers or card verification codes were part of that information has not been clarified. Source: <http://www.bankinfosecurity.com/restaurant-chain-reports-card-breach-a-4826>

## **CHEMICAL AND HAZARDOUS MATERIALS SECTOR**

**EPA asks manufacturers of 18 chemicals to submit 'all relevant' risk information.** Chemical manufacturers that produce certain flame retardants, fragrances, and other chemicals are being asked to submit information relevant to risks the compounds pose to the Environmental Protection Agency (EPA) by August 31. Hazard data, exposure data, and other risk-relevant information developed by other organizations also may be submitted. The EPA released June 1 a list of 18 chemicals for which it plans to complete risk assessments in 2013 and 2014. It also asked interested parties to submit information, such as unpublished scientific studies not already available through the existing literature or information on uses and potential exposures, to the agency for the assessments. The EPA would use the risk analyses for regulatory or other actions the agency may conclude are needed to manage risks. The 18 chemicals were drawn from a list of 83 the agency released in March as candidates for risk assessment over the next several years. The EPA selected the chemicals because they have potential characteristics such as persistence in the environment, accumulation in the food chain, and harmfulness to human health or the environment. Source: <http://www.bna.com/epa-asks-manufacturers-n12884909812/>

UNCLASSIFIED

## UNCLASSIFIED

**Judge gives preliminary OK to herbicide settlement.** A federal judge in southern Illinois gave preliminary approval to a \$105 million settlement between Syngenta and community water systems in six States over the presence of one of the Swiss chemical maker's popular agricultural herbicides in drinking water. He ruled May 30 the deal in the nearly 8-year-old lawsuit over weed-killing atrazine appears to be a good compromise. The agreement could help reimburse nearly 2,000 community water systems that have had to filter the chemical from its drinking water or pay to test for it, the attorney behind the class-action lawsuit said. The lawsuit was pressed by community water systems from at least a half-dozen States — Illinois, Iowa, Indiana, Kansas, Missouri, and Ohio — that have sought to have the company reimburse them for filtering atrazine. As part of the deal, 1,887 community water systems serving more than 52 million Americans may be eligible to make a claim, the attorney said. With the judge's action, notice of the settlement will be sent to class members, with the judge to make a final determination October 22. Syngenta said it agreed to settle the matter "to end the business uncertainty" and avoid further legal costs. Under the settlement, the company will continue to sell atrazine to U.S. corn growers and denies any liability linked to the chemical, which Syngenta said is used in more than 60 countries and has been marketed in the United States since 1959. Research has shown runoff after rainstorms can wash the chemical — used for decades to kill grasses and broadleaf weeds — into streams and rivers, where it can enter drinking water supplies. Source: <http://www.businessweek.com/ap/2012-05/D9V3PI9O3.htm>

### **COMMERCIAL FACILITIES**

**Study: Storm surge from hurricanes threatens 4 million homes.** A survey of the nation's vulnerability to hurricane-driven storm-surge damage found that more than four million homes worth over \$700 billion are at risk along the Atlantic and Gulf Coasts, USA Today reported June 7. Storm surge — the massive mound of water that builds up and comes ashore as a hurricane moves over the ocean or Gulf of Mexico — is typically the most dangerous aspect of hurricanes. The report, released by research and consulting firm CoreLogic, found Florida is the state most prone to storm-surge damage, with about 1.4 million homes at risk, worth a total value of \$188 billion. Louisiana ranked second in total number properties at risk with nearly 500,000, while New York was second in total value of coastal properties possibly exposed at \$111 billion. At the city level, the New York City metro area contains the highest number of vulnerable properties and the highest exposure in total property value at risk. Source: <http://content.usatoday.com/communities/sciencefair/post/2012/06/storm-surge-hurricanes-corelogic-four-million-homes-at-risk/1?csp=34news#.T9DcQ1JgrNO>

### **COMMUNICATIONS SECTOR**

**(Colorado) Emergency radio system fails.** Severe weather briefly knocked the Colorado Statewide Digital Trunked Radio System offline the night of June 6. "It was a momentary glitch. It was a meteorological anomaly," a city radio technician said. Heavy rain and hail pounded Colorado Springs and Southern Colorado, two areas where radio towers are stationed that maintain the statewide frequency. The weather in those areas caused the frequency to go offline in Pueblo. The statewide frequency allows law enforcement and emergency responders

UNCLASSIFIED

## UNCLASSIFIED

to communicate on a single radio wave in the event of a large emergency. Source:

[http://www.chieftain.com/news/local/emergency-radio-system-fails/article\\_2c94f17c-b12d-11e1-a6c6-0019bb2963f4.html](http://www.chieftain.com/news/local/emergency-radio-system-fails/article_2c94f17c-b12d-11e1-a6c6-0019bb2963f4.html)

**Intelsat 19 satellite fails to deploy solar array.** The Intelsat IS-19 satellite launched May 31 has failed to deploy one of its two solar arrays, Intelsat announced June 1 — an anomaly that has affected other Space Systems/Loral (SS/L)-built satellites and is likely to have ripple effects on two others preparing for launch in the coming weeks. Luxembourg- and Washington, D.C.-based Intelsat, in its statement, said only that there was a “delay” in the deployment of one of the arrays. IS-19 is scheduled to replace Intelsat’s IS-8 at 166 degrees east, where in addition to taking on IS-8 customers, it will play a key role in Intelsat’s planned global network providing broadband communications to aeronautical and maritime customers. IS-8 has sufficient fuel to continue operating until late 2019, Intelsat said. Source:

[http://www.spacenews.com/satellite\\_telecom/120602-intelsat-19-satellite-fails-deploy-solar-array.html](http://www.spacenews.com/satellite_telecom/120602-intelsat-19-satellite-fails-deploy-solar-array.html)

**Text, don’t call when natural disaster strikes.** It is better to send text messages than to call when natural disasters strike and networks get congested, a senior U.S. official said May 31, also urging people to add battery-powered cell phone chargers to their storm emergency kits. The head of the Federal Emergency Management Agency (FEMA) told reporters that forecasts for a “normal” Atlantic hurricane season should not keep those in potentially affected areas from getting ready for storms that could make landfall. The U.S. government is working to extend its public alert warning system beyond radio and television to mobile networks, he said, noting that most new and upgraded cell phones have the capacity to receive such emergency notices. Households without fixed-line phones should be ready to charge cell phones during power cuts, the FEMA administrator said, also calling on families to make alternative communication plans for when wireless networks are congested. Source:

<http://www.reuters.com/article/2012/05/31/uk-usa-weather-storms-idUSLNE84U01D20120531>

**Opinion split on authority to shut down wireless in emergency.** In April, the Federal Communications Commission (FCC) issued a notice seeking public comments on whether the government and law enforcement should have unchecked authority to initiate a localized or citywide wireless service shutdown for public safety purposes. The 1-month period for filing public comments ended May 30. A review of the responses to the FCC requests over the past month shows that many support the idea of the government having the ability to quickly shut down wireless services, but only as a matter of last resort and only in an extreme emergency. The general manager of Bay Area Rapid Transit (BART) insisted that a temporary interruption of cell phone service is a necessary tool “under extreme circumstances where harm and destruction are imminent.” She noted, “For example, wireless devices may be used to detonate explosives.” Source:

[http://www.computerworld.com/s/article/9227650/Opinion\\_split\\_on\\_authority\\_to\\_shut\\_down\\_wireless\\_in\\_emergency](http://www.computerworld.com/s/article/9227650/Opinion_split_on_authority_to_shut_down_wireless_in_emergency)

UNCLASSIFIED

## **CRITICAL MANUFACTURING**

**NHTSA recall notice - Kia Borrego brake pedals.** Kia announced June 6 the recall of 21,912 model year 2009 Borrego vehicles manufactured from May 2, 2008 through January 20, 2009 equipped with non-adjustable brake pedals. Certain pedal mounts may have a fiberglass composition that allows them to break off in a collision where the impact has not immobilized the vehicle, which would then allow the vehicle to roll. If this occurs, the driver would need to stop the vehicle with the parking brake or experience a possible second impact, increasing the risk of personal injury. Kia will notify owners, and dealers will replace the brake pedal mount, free of charge. Source: [http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcld\\_ID=12V245000&summary=true&prod\\_id=451836&PrintVersion=YES](http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcld_ID=12V245000&summary=true&prod_id=451836&PrintVersion=YES)

## **DEFENSE/ INDUSTRY BASE SECTOR**

**Chipmaker denies inserting backdoor into silicon.** Chipmaker Microsemi denied suggestions it deliberately put a backdoor into ProASIC3 chips following the discovery of a weakness by a University of Cambridge researcher, PC Pro reported June 1. The denial follows speculation over the origins and purpose of a backdoor that could allow hackers to alter field programmable gate arrays used in military and other applications. Although Microsemi said it could neither confirm nor deny the details of the attack because the Cambridge researchers had not provided technical details necessary for a full investigation, it said “Microsemi can confirm that there is no designed feature that would enable the circumvention of the user security.” However, the Cambridge research team is sticking by its assertion that the backdoor remains a weakness and that only redesigned silicon would properly fix the problem. Source: <http://www.pcpro.co.uk/news/374962/chipmaker-denies-inserting-backdoor-into-silicon>

## **EMERGENCY SERVICES**

**(Florida) Woman tried to rob ambulance during medical call in suburban Lake Worth, officials say.** A woman was arrested June 4 in Lake Worth, Florida, after she allegedly entered an emergency vehicle while paramedics were on a medical call. According to a probable-cause arrest affidavit, a Palm Beach County Fire Rescue crew was at a call when the woman entered the ambulance. A firefighter said he went back to the ambulance to retrieve additional equipment when he saw the woman climbing into the passenger side front door. The firefighter instructed her to climb down and she refused, the affidavit said. The firefighter helped her down the steps of the ambulance and he then went to the back to get the equipment. She then followed him into the ambulance and refused to leave. The firefighter said he had to stay inside the ambulance for fear of theft or damage and was unable to return to assist the patient or his crew. The woman faces one count of burglarizing an emergency vehicle. Source: <http://www.palmbeachpost.com/news/news/crime-law/woman-tried-rob-ambulance-during-medical-call-subu/nPNTp/>

## UNCLASSIFIED

**(Arizona) Pentagon orders military-gear crackdown after Ariz. issues.** A spokesman for the Defense Logistics Agency (DLA) informed the Arizona Republic June 1 that new policies were being developed and a new accounting system would be employed to keep track of surplus military gear that law-enforcement agencies are able to requisition free. The newspaper had published a report detailing how the Pinal County Sheriff's Office, which has collected millions of dollars worth of surplus military equipment intended for law-enforcement use, has distributed vehicles and other gear to non-police agencies. The DLA spokesman said the agency's Law Enforcement Services Office is taking steps to clarify that police are not allowed to "loan" items to non-government fire departments and other agencies or enterprises that do not enforce laws. He also said the agency will monitor the sheriff's office to ensure it does not sell surplus military gear to enhance its budget in violation of federal rules. Source: <http://www.usatoday.com/news/military/story/2012-06-02/pentagon-military-gear/55347666/1>

## **ENERGY**

**NERC, utilities want more information sharing on cyber threats.** The head of the North American Electric Reliability Corp (NERC) and electric utility officials would like DHS to issue more security clearances to executives to improve their ability to address cyber threats to the power grid, speakers said June 4 at the Edison Electric Institute's annual meeting. The NERC president and CEO has top secret clearance from the government to view cybersecurity threats and attempts to hack the power grid, but additional NERC staff and utility officials should be able to see similar information. Because different agencies can be involved in gaining security clearance, NERC is working with the Department of Energy to speed up the process for top executives. Legislation is pending in Congress that would have utilities improve data sharing and cybersecurity protections. Source: <http://www.platts.com/RSSFeedDetailedNews/RSSFeed/ElectricPower/6354219>

**DOT: Trucks hauling sand, water for fracking not exempt from HOS rules.** Truck drivers hauling water and sand to oil and natural gas shale drilling sites in the United States do not qualify for a special oil-field service equipment exemption to extend their daily driving hours, Truckinginfo reported June 6. The rule clarification, or regulatory guidance, from the Department of Transportation (DOT) explains that time spent waiting while water and sand are unloaded at well sites counts toward the maximum 14 hours a day that a truck driver can work under hours of service rules. The guidance says the "waiting time" oil-field exemption in Sec. 395.1(d)(2), which allows these drivers to count waiting time as off-duty, is available only to operators of commercial motor vehicles that are specially constructed for use at oil and gas well sites, and for which the operators require extensive training in the operation of the complex equipment, in addition to driving the vehicle. The clarification says drivers of more typical commercial vehicles that haul water and sand in and out of these sites do not qualify for the exemption, "even if there have been some modifications to the vehicle to transport, load, or unload the materials, and the driver required some minimal additional training in the operation of the vehicle, such as running pumps or controlling the unloading and loading processes." Source: [http://www.truckinginfo.com/news/news-detail.asp?news\\_id=77153](http://www.truckinginfo.com/news/news-detail.asp?news_id=77153)

UNCLASSIFIED

## UNCLASSIFIED

**Nuclear, coal power face climate change risk: Study.** Warmer water and reduced river flows will cause more power disruptions for nuclear and coal-fired power plants in the United States and Europe in the future, scientists said, and lead to a rethink on how best to cool power stations in a hotter world. In a study published June 4, a team of European and U.S. scientists focused on projections of rising temperatures and lower river levels in summer and how these impacts would affect power plants dependent on river water for cooling. The authors predict coal and nuclear power generating capacity between 2031 and 2060 will decrease by between 4 and 16 percent in the United States and 6 to 19 percent in Europe due to lack of cooling water. The likelihood of extreme drops in power generation, either complete or almost-total shutdowns, was projected to almost triple. Thermoelectric power plants supply more than 90 percent of electricity in the United States and account for 40 percent of the nation's freshwater usage, said the study, published in the journal Nature Climate Change. Source: <http://www.reuters.com/article/2012/06/04/us-climate-water-energy-idUSBRE85304C20120604>

**EPA issues final rule for refinery flares, process heaters.** The U.S. Environmental Protection Agency (EPA) issued a final rule updating Clean Air Act standards for refinery flares and process heaters June 1. The new standards will reduce sulfur dioxide, nitrogen oxide, and volatile organic compound emissions while saving refiners about \$80 million per year, the EPA said. American Petroleum Institute and American Fuel & Petrochemical Manufacturers officials immediately disagreed. The EPA said the final rule, which was a response to petitions asking the agency to reconsider standards issued in 2008, provides greater compliance flexibility to refiners and ensures they can make routine operational requirements without triggering new requirements. It said the new standards rely on proven, widely used technologies to cut pollution from flares and process heaters. Source: <http://www.ogj.com/articles/2012/06/epa-issues-final-rule-for-refinery-flares-process-heaters.html>

## **FOOD AND AGRICULTURE**

**Drought dominates Corn Belt in La Nina's wake.** La Nina may be gone, but the persistent drought that plagued Texas in 2011 has now slowly expanded to other areas of the United States, Ag Professional reported June 8. A map of the country's midsection is now highlighted with a bright yellow in the U.S. Department of Agriculture's latest Drought Monitor, posing as a warning of a potential drought that could soon be tightening its grip on the region. Colorado, Kansas, Iowa, Illinois, Missouri, Oklahoma, and Texas are the latest to be covered by an overwhelming majority of land rated as abnormally dry to moderate drought. In the High Plains, less than 30 percent of the area is free from any drought or dryness, primarily in the Dakotas and Nebraska. A snow drought has turned into an extreme drought for areas of northwestern Colorado, and 100 percent of the State is in some state of abnormal dryness or drought. To the east, about 60 percent of Kansas is considered to be in a drought, compared to 32 percent the week of May 28. Long-term outlooks suggest little relief for most areas. In the Seasonal Drought Outlook, the drought is expected to persist or intensify over many areas to the west of the Mississippi River. Experts are also anticipating the drought to persist in Arkansas and Missouri,

UNCLASSIFIED

## UNCLASSIFIED

as well as parts of Illinois, Indiana, Kentucky, Tennessee, and Alabama. Source: <http://www.agprofessional.com/news/Drought-dominates-Corn-Belt-in-La-Ninas-wake-157897875.html>

**Multistate E. coli O145 outbreak confirmed in southern U.S.** The E. coli O145 outbreak that killed a toddler in New Orleans May 31 was connected to at least 11 illnesses across the southern United States, multiple State health departments confirmed with Food Safety News June 6. The Louisiana, Georgia, Alabama, Florida, and Tennessee State health departments said they are working with the U.S. Centers for Disease Control and Prevention (CDC) to investigate the outbreak. The CDC has not yet released other data related to the investigation, but a spokeswoman said States were in various stages of investigation. So far, health officials do not know the source of the contamination, but many said the vehicle was likely food. The confirmed cases are spread across the following States: Georgia (5 illnesses), Louisiana (2 ill and 1 dead), Alabama (2 illnesses), and Florida (1 illness). The confirmed outbreak illnesses appear to have begun in mid-April to early May. Source:

<http://www.foodsafetynews.com/2012/06/georgia-confirms-multi-state-e-coli-o145-outbreak-in-southern-us/>

**USDA plans to let chicken plants run faster with fewer inspectors.** As part of the U.S. President's push to streamline regulations on businesses, the U.S. Department of Agriculture (USDA) plans to let chicken slaughterhouses run production lines faster and with fewer federal inspectors, the Los Angeles Times reported June 6. Under the proposal, production lines would be allowed to move 25 percent faster, while the government would cut by as much as 75 percent the number of line inspectors eyeing chicken bodies for defects before the carcasses are packaged for consumption. The quicker conveyor belts also raise the prospects that plant workers who hang carcasses, clean, trim, and cut chickens at rapid speeds will be prone to more injuries as the pace is ratcheted up, labor groups said. The USDA estimated the proposal would eliminate as many as 800 inspector positions and save the federal government \$90 million over 3 years. Source: <http://www.latimes.com/business/la-fi-poultry-rules-20120606,0,3160691.story>

**Analysis: High U.S. corn prices warn of summer shortage.** From Ohio to Kansas, corn is selling at startlingly high prices, so high that they are signaling the United States will run short of corn the summer of 2012, Reuters reported June 4. If it does run short, the impact could be felt worldwide. Sales to export customers such as Mexico, Japan, South Korea, and China could take a hit as America grows 40 percent of the corn sold on the world market. Domestically, sky-high prices could have U.S. millers suspending operations. If corn for feed costs too much then milk, egg, and meat farmers could curtail production leading to higher food prices. Prices on the cash market, where processors and livestock feeders buy corn for use, have been unusually high for months. They are much higher than historically at this time. "Either farmers aren't selling or the corn isn't there," said a co-owner of Hollander-Feuerhaken, a Chicago brokerage and cash merchant. Even with strong basis, it was difficult to buy corn for domestic use, he said in late May. Source: <http://www.reuters.com/article/2012/06/04/us-corn-shortage-idUSBRE85316L20120604>

UNCLASSIFIED

## UNCLASSIFIED

**(Michigan) Michigan governor seeks federal disaster aid for crop losses.** Michigan's governor said June 1 he asked for federal disaster aid to help with crop losses estimated at \$223.5 million, caused by erratic weather, but an agriculture expert said Michigan farmers may not get a chance to apply for the assistance until fall. Summer-like temperatures in March, followed by frosts and freezes, led to some of the State's biggest losses in decades of cherries and other fruits. Usually, one fruit crop might be devastated, said a Michigan Farm Bureau Commodity and Marketing Department manager. However, the spring of 2012 all fruit crops were damaged except blueberries. Michigan's fruit industry is valued at more than \$190 million a year. The State will lose about 90 to 97 percent of its tart cherry crop, according to a letter the U.S. Senate Agriculture Committee chairwoman sent the week of May 28 to the Agriculture Secretary. Michigan produces three-fourths of the nation's tart cherries, used primarily in pies and other food products, and 20 percent of its sweet cherries. Source:

<http://www.detroitnews.com/article/20120602/BIZ/206020326#ixzz1wpKHIEOx>

**Government to expand E. coli testing in beef trimmings next week.** The government is expanding E. coli testing in some raw meat, a move expected to prevent more people from contracting the bacteria that can cause severe illness or death. Starting June 4, the meat industry will have to test beef trimmings for six new strains of E. coli that have been linked to a growing number of illnesses. Until now, the meat industry has been required to test for just one strain of the pathogen, known as E. coli O157:H7. That strain was identified after an outbreak at Jack in the Box fast-food restaurants killed four children. However, illnesses from that strain have decreased over the years while more people have been sickened by other strains found in foods such as lettuce and ground beef. The Agriculture Secretary said the change is needed to protect Americans from food-borne illnesses. The new tests will be conducted on beef trimmings — parts of the cow used to make ground beef — and expanded later to ground beef itself, and other cuts. In 2011, the agency collected nearly 2,700 samples for testing from meat processing plants nationwide. That number will not change, but each sample will now be tested for the six additional E. coli strains. Source:

[http://www.washingtonpost.com/politics/government-to-expand-e-coli-testing-in-beef-trimmings-next-week/2012/05/30/gJQAm57c2U\\_story.html](http://www.washingtonpost.com/politics/government-to-expand-e-coli-testing-in-beef-trimmings-next-week/2012/05/30/gJQAm57c2U_story.html)

**USDA survey shows fewer honeybee colony losses.** The U.S. Department of Agriculture said fewer honeybee colonies are being lost, suggesting bees' health may be improving. A survey made public May 31 shows about 22 percent of U.S. honeybee colonies were lost during the winter. That is a lower mortality than in the previous 5 years when colonies were decimated at a rate of about 30 percent a year. Bees are essential pollinators of about a third of the United States' food supply. Some of the devastation is attributed to colony collapse disorder, in which all the adult honey bees in a colony disappear or die. Prior to 2006, when the disorder was recognized, losses were about 15 percent a year from a variety of pests and diseases. Researchers said an unusually warm winter could have impacted colony survival. More than 5,500 beekeepers completed the survey. Source:

<http://www.sacbee.com/2012/05/31/4529721/usda-survey-shows-fewer-honeybee.html>

UNCLASSIFIED

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

**(California) F-16 intercepts small plane in U.S. President's air space.** An F-16 fighter intercepted a small private plane that entered restricted air space for the U.S. President's fundraising visit to Southern California June 6, according to a statement issued by North American Aerospace Command. The President was at the Beverly Hilton at the time of the plane's interception. It was intercepted northwest of Los Angeles and landed without incident at an airfield in Camarillo. Source: <http://www.google.com/hostednews/ap/article/ALeqM5gEcxhp7scwgYEFb3DNME8tAWU3hw?docId=b7029d6666794e7faf19592504ce29fa>

**(Illinois) Suspect held after powdery substance found in letter at DuPage courthouse.** Officials say they have in custody a person they believe sent a suspicious letter with a powdery substance to the DuPage County, Illinois courthouse June 5. A mail room clerk opened the letter and found a white substance inside. Deputies shut down the mail room and alerted the Wheaton Fire Department, which responded along with the FBI and a county hazardous materials team. An examination proved the powder to be harmless, according to the sheriff's office. Police have identified a suspect, who was turned over to the U.S. Marshal's office. The clerk was sent to the Central DuPage Hospital for a precautionary screening, police said. Source: [http://articles.chicagotribune.com/2012-06-05/news/chi-suspect-held-after-powdery-substance-found-in-letter-at-dupage-courthouse-20120605\\_1\\_powdery-substance-suspicious-letter-mail-room](http://articles.chicagotribune.com/2012-06-05/news/chi-suspect-held-after-powdery-substance-found-in-letter-at-dupage-courthouse-20120605_1_powdery-substance-suspicious-letter-mail-room)

**(California; Rhode Island) State of California site hacked, sensitive data leaked.** A hacker group calling itself "The Unknowns" breached the Web sites of the State of Rhode Island June 4 and the California Department of Forestry and Fire Protection June 5. The hackers made available screenshots to prove they gained access to the administrator panel, and published many usernames and clear text passwords. It appeared they dumped four credential sets that belong to one of the site's administrators, encrypted using MD5. Similar to other hacks, The Unknowns offer their information security "services" to the site's Webmaster. The Unknowns have also taken credit for breaching the sites of the U.S. Navy, the German federal government, and a couple of United Kingdom police servers. Source: <http://news.softpedia.com/news/State-of-California-Site-Hacked-Sensitive-Data-Leaked-273754.shtml>

## **INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**Criminals bypassing sophisticated device fingerprinting with basic tools.** Research from Trusteer shows device fingerprinting, which is used in fraud detection systems, might be a useless layer of protection after they discovered a manual for bypassing such features being circulated among online criminals. In it, the author explains how to bypass the layered protection found in several fingerprinting systems. The tutorial explains that the usage of commercial VPNs and proxy services will work to defeat the IP protections within the fingerprinting systems, and adds information on how to make sessions from a single system

## UNCLASSIFIED

appear as if they originate from different computers, operating systems, and browsers by altering the user agent headers. Source: <http://www.securityweek.com/criminals-bypassing-sophisticated-device-fingerprinting-basic-tools>

**Flame authors order infected computers to remove all traces of the malware.** The creators of the Flame cyber-espionage threat ordered infected computers still under their control to download and execute a component designed to remove all traces of the malware and prevent forensic analysis, security researchers from Symantec said June 6. Flame has a built-in feature called SUICIDE that can be used to uninstall the malware from infected computers. However, the week of May 28, Flame's creators decided to distribute a different self-removal module to infected computers that connected to servers still under their control, Symantec's security response team said. Even though it is similar in functionality to the SUICIDE feature — both being able to delete many files associated with the malware — the new module goes further. "It locates every [Flame] file on disk, removes it, and subsequently overwrites the disk with random characters to prevent anyone from obtaining information about the infection," the researchers said. "This component contains a routine to generate random characters to use in the overwriting operation. It tries to leave no traces of the infection behind." Source: [http://www.computerworld.com/s/article/9227876/Flame\\_authors\\_order\\_infected\\_computers\\_to\\_remove\\_all\\_traces\\_of\\_the\\_malware](http://www.computerworld.com/s/article/9227876/Flame_authors_order_infected_computers_to_remove_all_traces_of_the_malware)

**Fake Gmail Android application steals personal data.** Mobile security researchers from NQ Mobile intercepted a fake Gmail Android application dubbed DDSpy. The SMS based command and control feature of DDSpy is capable of uploading SMS messages, call logs, and vocal records to a remote server. The malware authors behind the fake Gmail Android application included a hard-coded e-mail address that can be easily changed using SMS messages. Moreover, the malicious application automatically starts recording outbound calls, or when instructed to do so over SMS. Source: <http://www.zdnet.com/blog/security/fake-gmail-android-application-steals-personal-data/12308>

**Siemens enhances security in post-Stuxnet SCADA world.** Stuxnet was not only a problem for Iran, but also for Siemens, whose process control systems were targeted in the attack that disrupted a nuclear facility in Iran. Since then, Siemens made several security moves in the wake of Stuxnet's discovery 2 years ago: most recently, new industrial control products that come with built-in security features. The president of the industry automation division for Siemens Industry Inc. said the new Simatic CP and Scalance communications processor products with firewall and virtual private network features help bolster security. Since Stuxnet, Siemens was ridiculed by various security researchers who discovered holes in the manufacturer's products, forcing Siemens to find security in a staid industry where air gaps traditionally were assumed enough to protect critical infrastructure. Source: <http://www.darkreading.com/advanced-threats/167901091/security/vulnerabilities/240001644/>

**Microsoft 'hardens' Windows Update from Flame penetration.** Microsoft "hardened" its Windows Update system after researchers discovered the Flame virus can infect PCs by offering

## UNCLASSIFIED

## UNCLASSIFIED

itself as an update masquerading as official Microsoft software. The worm infected computers in the Middle East and beyond for up to 2 years before being discovered by security experts in late May. Now, it emerged that the malware uses a skeleton-key-like certificate found in Microsoft's Terminal Services Licensing server to sign its malicious code and trick Windows machines into trusting and installing its executables. June 6, Microsoft said it was continuing to analyze Flame and repeated it would "evaluate additional hardening of both the Windows Update channel and our code signing certificate controls." It warned any customers who do not have their Windows Update software set to automatic configuration to install the latest patch immediately, which will thwart Flame's man-in-the-middle attack. Source:

[http://www.theregister.co.uk/2012/06/07/microsoft\\_combats\\_flame\\_with\\_additional\\_hardeni ng/](http://www.theregister.co.uk/2012/06/07/microsoft_combats_flame_with_additional_hardeni ng/)

**Google starts warning users of state-sponsored computer attacks.** Google unveiled a service that automatically displays a warning to users who may be the target of State-sponsored phishing or malware attacks. Company representatives did not indicate precisely what criteria is used to determine when a particular attack is sponsored by a government actor, because that information could be used to evade detection. They went on to say the company relies on "detailed analysis" and victim reports that "strongly suggest the involvement of states or groups that are state-sponsored." The warnings are being implemented after Google users were hit by several high-profile attacks that show evidence of being sponsored by governments in China and Iran. Source: <http://arstechnica.com/security/2012/06/google-state-sponsored-attack-warnings/>

**LinkedIn investigating reports of stolen passwords.** Business social network LinkedIn said it is investigating reports that more than 6 million passwords were stolen and leaked onto the Internet. Although LinkedIn did not confirm if any user data was hacked or leaked, researchers at Web security company Sophos said they confirmed a file posted online does contain, in part, LinkedIn password "hashes" — a way of encrypting or storing passwords in a different form. A consultant with Sophos recommended LinkedIn users change their passwords immediately. LinkedIn contains myriad information on its more than 160 million members, including potentially confidential information related to jobs being sought. Companies, recruiting services, and others have accounts alongside individuals who post resumes and other professional information. There is added concern that many people use the same password on multiple Web sites, so whoever stole the data could use the information to access Gmail, Amazon, PayPal, and other accounts, the Sophos consultant warned. LinkedIn referred repeated requests for comment to the company's Twitter feed, where it said its team was "looking into reports of stolen passwords." Two hours later, the company posted a second tweet saying it was still unable to confirm if a security breach occurred. A security researcher warned that LinkedIn users should be cautious about malicious e-mail generated around the incident. The concern is that users, after learning about the incident, would be tricked into following links in those e-mails. Instead of going to the real LinkedIn site to change a password, users would be directed to a scammer, who could then collect the information and use it for criminal activities. Source: <http://finance.yahoo.com/news/linkedin-investigating-reports-stolen-passwords-151609357.html>

UNCLASSIFIED

## UNCLASSIFIED

**Researchers reveal how Flame fakes Windows Update.** June 5, security researchers published detailed information about how the Flame cyber-espionage malware spreads through a network by exploiting Microsoft's Windows Update mechanism. Their examinations answered a question that puzzled researchers at Kaspersky Lab: How was Flame infecting fully-patched Windows 7 machines? Key to the phony Windows Update process was that the hackers located and exploited a flaw in the company's Terminal Services licensing certificate authority that allowed them to generate code-validating certificates "signed" by Microsoft. Armed with those fake certificates, the attackers could fool a Windows PC into accepting a file as an update from Microsoft when in reality it was nothing of the kind. Source:

[http://www.computerworld.com/s/article/9227736/Researchers\\_reveal\\_how\\_Flame\\_fakes\\_Windows\\_Update](http://www.computerworld.com/s/article/9227736/Researchers_reveal_how_Flame_fakes_Windows_Update)

**Hackers use social engineering to compromise CloudFlare CEO Gmail account.** Hackers were able to infiltrate the personal Gmail account of CloudFlare's CEO June 1, according to a post on the Web performance and security provider's blog. CloudFlare said the attack appeared to have begun in mid-May when an account request was sent to Gmail for the CEO's personal e-mail address. A week after it was initiated, the hacker convinced Google's account recovery systems to add a fraudulent recovery e-mail address to his personal Gmail account, and once it was added, the hacker reset his personal e-mail password. The hacker targeted a CloudFlare customer via the CEO's Google Apps administrative panel. The hacker was able to log into the customer's CloudFlare account and change DNS settings to temporarily redirect the site. CloudFlare has reset all customer API keys. This incident also illustrates weakness with the two-factor authentication on Google Apps. Google said it discovered a subtle flaw affecting the account recovery flow for some accounts. It has blocked that attack vector to prevent further abuse. Source: <http://www.thewhir.com/web-hosting-news/hackers-use-social-engineering-to-compromise-cloudflare-ceo-gmail-account>

**'Flame' spread via rogue Microsoft security certificates.** Analysis of the "Flame" code revealed rogue Microsoft security certificates were used to make the malware appear as if it was officially signed by Microsoft. Microsoft issued a security advisory June 3, revoked trust in the rogue certificates, and provided steps to help IT admins and users prevent attacks that rely on the spoofed Microsoft certificates. A post on the Microsoft Security Response Center blog stated, "We have discovered through our analysis that some components of the malware have been signed by certificates that allow software to appear as if it was produced by Microsoft." The Microsoft blog post explained that a vulnerability in an old cryptography algorithm is exploited by elements of Flame to make them appear as if they originated from Microsoft. Most systems around the world accept officially signed Microsoft code as safe by default, so the malware would enter unnoticed. Source:

[http://www.pcworld.com/businesscenter/article/256742/flame\\_spread\\_via\\_rogue\\_microsoft\\_security\\_certificates.html](http://www.pcworld.com/businesscenter/article/256742/flame_spread_via_rogue_microsoft_security_certificates.html)

**Browser feature can be abused to misrepresent download origin, researcher says.** Legitimate browser functionality can be abused to trick users into believing that a trusted Web site has

## UNCLASSIFIED

## UNCLASSIFIED

asked them to download a file, which is actually being served from a rogue server, a Google security engineer demonstrated May 29. The method removes the need for spoofed pages. His proof-of-concept attack begins with a button on a page that, when clicked, opens the official Flash Player download Web site in a second tab and switches the browser's focus to it. After a few seconds, the original page serves a file called flash11\_updater.exe from the researcher's server, which causes the browser to display a download dialog. However, because this happens while the active tab is the one with the official Flash Player Web site loaded into it and an adobe.com URL in the address bar, it appears as if the download was initiated by Adobe's Web site. "All the top three browsers are currently vulnerable to this attack," he said in a blog post. Source:

[http://www.pcworld.com/businesscenter/article/256610/browser\\_feature\\_can\\_be\\_abused\\_to\\_misrepresent\\_download\\_origin\\_researcher\\_says.html](http://www.pcworld.com/businesscenter/article/256610/browser_feature_can_be_abused_to_misrepresent_download_origin_researcher_says.html)

### **NATIONAL MONUMENTS AND ICONS**

**Forest Service chief acknowledges need to modernize fleet.** Although stating Lockheed P2V air tankers are safe, the chief of the U.S. Forest Service acknowledged the need to modernize the U.S. aerial firefighting fleet June 5 after two Idaho pilots aboard a P2V died in a crash June 3 while fighting a Utah fire, the same day another firefighting plane of the same vintage was forced to make a crash landing at Nevada's Minden-Tahoe Airport. The Government previously relied primarily on C-130s for firefighting efforts but slowly started adding P2Vs in the early 1990s, then began relying much more on the planes after two C-130 crashes in 2002. Also, a National Traffic Safety Board investigator arrived at the scene of the Utah crash and began scouring the 600-yard debris field for clues about why the plane went down. The investigator said authorities analyzing the crash will consider all potential causes, including weather, mechanical failure, and pilot error. The tanker was owned by Neptune Aviation. It was built in 1962, according to federal aviation records, but had been modified to fight fires and was among only a handful of air tankers available nationwide. The other P2V was owned by Minden Air Corp. in Minden, Nevada. Source: <http://www.firehouse.com/news/10725769/forest-service-chief-acknowledges-need-to-modernize-fleet>

### **POSTAL AND SHIPPING**

Nothing Significant to Report

### **PUBLIC HEALTH**

**Gonorrhea growing resistant to drugs, WHO warns.** June 6, the World Health Organization (WHO) urged governments and doctors to step up surveillance of antibiotic-resistant gonorrhea. The potentially dangerous disease that infects millions of people each year continues to grow resistant to drugs and could soon become untreatable. Scientists believe overuse or incorrect use of antibiotics, coupled with the gonorrhea bacteria's ability to adapt, means the disease is now close to becoming a super bug. "This organism has basically been developing resistance against every medication we've thrown at it," said a scientist in the

UNCLASSIFIED

## UNCLASSIFIED

WHO's department of sexually transmitted diseases. This includes a group of antibiotics called cephalosporins currently considered the last line of treatment. Resistance to cephalosporins was first reported in Japan, but more recently has also been detected in Britain, Australia, France, Sweden, and Norway. As these are all countries with well-developed health systems, it is likely cephalosporin-resistant strains are circulating undetected elsewhere. Therefore the Geneva-based agency wants countries not just to tighten their rules for antibiotic use, but also to improve their surveillance systems so the full extent of the problem can be determined.

Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2012/06/06/international/i000525D20.DTL>

### **TRANSPORTATION**

**(Washington) Copper theft causes railroad crossing to shut down.** A metal thief caused a malfunction at a heavily traveled Ocean Beach Highway railroad crossing the week of May 21 by stripping copper wire off the tracks, Longview, Washington police said June 1. A detective said no metal thieves in recent memory have targeted train tracks, and police are especially worried that future instances could cause a crash between a train and a car. Officers received a report May 24 that the railroad crossing arms in the 3100 block of Ocean Beach Highway had been down for more than 20 minutes, but no train could be seen, according to a court affidavit released June 1. A representative of Columbia & Cowlitz Railroad made a temporary repair of the equipment. However, because the source of the malfunction was unknown, the company also ordered train conductors to stop before the intersection, exit their trains and make sure the crossing was safe before proceeding. The damage to the tracks was estimated at about \$820. Source: [http://tdn.com/news/local/copper-theft-causes-railroad-crossing-to-shut-down/article\\_2742ebc4-ac7e-11e1-b7e7-001a4bcf887a.html#ixzz1wpU706fV](http://tdn.com/news/local/copper-theft-causes-railroad-crossing-to-shut-down/article_2742ebc4-ac7e-11e1-b7e7-001a4bcf887a.html#ixzz1wpU706fV)

### **WATER AND DAMS**

**New Wisconsin study on viruses in drinking water could have national impact.** A Wisconsin study that shows a connection between viruses in drinking water and human illness is likely to have a national impact and could eventually lead to federal rules requiring treatment of all public water systems, according to experts, the Wisconsin State Journal reported June 1. The research, published by the journal Environmental Health Perspectives, was conducted in 14 Wisconsin communities by two microbiologists with the U.S. Department of Agriculture's Agricultural Research Service. The 2-year study was among the first to closely link the presence of viruses in tap water to sickness in people drinking that water. At least 60 communities in Wisconsin do not treat drinking water with chlorine or ultraviolet light, both of which kill the contaminants, said the State Department of Natural Resources (DNR). The study found the source of viruses contaminating drinking water was likely wastewater coming from leaking sanitary sewers. The director of the DNR Bureau of Drinking Water and Groundwater said May 31 the study prompted the U.S. Environmental Protection Agency (EPA) to begin a nationwide sampling program that could result in a federal rule requiring treatment. The EPA-funded study showed that all 14 communities studied during the 2-year project had human viruses in their tap water. Of 1,204 samples, 24 percent were virus positive. The higher the virus concentration,

UNCLASSIFIED

## UNCLASSIFIED

the higher the rate of illness found in each community. During one part of the study, when norovirus was very common in one community's tap water, the proportion of illness in children younger than 5 years old attributable to their drinking water could have been as high as 63 percent. Source: [http://host.madison.com/news/local/health\\_med\\_fit/new-wisconsin-study-on-viruses-in-drinking-water-could-have/article\\_e8e5eefe-ab87-11e1-95bf-001a4bcf887a.html?comment\\_form=true](http://host.madison.com/news/local/health_med_fit/new-wisconsin-study-on-viruses-in-drinking-water-could-have/article_e8e5eefe-ab87-11e1-95bf-001a4bcf887a.html?comment_form=true)

## **HOMELAND SECURITY CONTACTS**

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

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

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

UNCLASSIFIED