

UNCLASSIFIED



NORTH DAKOTA HOMELAND SECURITY ANIT-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

Garrison Dam spillway use being reassessed. U.S. Army Corps of Engineers officials tested the Garrison Dam's emergency spillway in North Dakota again June 2, and they will decide whether it needs minor repairs. The spillway gates were opened June 1 for the first time in more than 50 years. But the spillway was later shut off because water flows caused some spraying at the spillway's edge. The Corps project manager said the spraying happened because the concrete surface was uneven at the base of the spillway. A Corps spokeswoman said some spillway gates were reopened June 2, and they are letting out 5,000 cubic feet of water per second. She said the gates stayed open all night, and things will be re-evaluated early June 3. The project manager said the glitch will not affect the dam's water release schedule. Source:

<http://www.jamestownsun.com/event/apArticle/id/D9NJVKDG1/>

Radio tower collapses as butte shifts. Two local radio stations went off the air the evening of June 1 when their broadcasting tower northeast of Dickinson, North Dakota collapsed after the ground beneath it shifted, a Clear Channel Radio business manager said. KCAD and KZRZ will be back on the air when a temporary tower is in place, he said. The incident is believed to have been caused by saturated soil, the business manager noted. Parts of the tower landed on a nearby transmitter building, causing minor damage. The tower is not salvageable, since it broke into several parts on its way down, he said. A new communications tower is being erected amongst the others on the butte. The hope is that the new communications tower will be up by the end of June. Source: <http://www.thedickinsonpress.com/event/article/id/48273/>

Train cars go off tracks near Minot; no injuries. About half a dozen cars of a BNSF Railway freight train went off the tracks west of Minot, North Dakota June 2. The Ward County Sheriff told KCJB radio that no one was hurt and no hazardous materials were involved. He said the cars tipped shortly before 5 a.m. at a spot where the track had shifted. There was no immediate word on when the tracks might reopen. Source:

<http://www.newstimes.com/default/article/Train-cars-go-off-tracks-near-Minot-no-injuries-1406530.php>

Army corps continues repairs on Williston Levy. A special meeting was held May 31 to discuss a boil in the levy at the headwaters of Lake Sakakawea — an area in the levee that could potentially bring the water up and cause the ground to erode. The U.S. Army Corps of Engineers worked June 1 to fix the levee but ran into a few difficulties. The Corps of Engineers is working around the clock to fix a levy to keep it from flooding Williston, North Dakota. A corps official said they had an interruption in the contract because there were people walking in between the trucks and trucking. In order to avoid these interruptions, the Corps is not allowing traffic from East Dakota Parkway near their office, to the water treatment plant. They are also not allowing joggers or fisherman at the levy. The official said the corps will continue to remove debris around pressure relief wells. Wells relieve pressure from within the earth's surface next to the levy, so water can bleed off and flow. Source:

http://www.kfyrtv.com/News_Stories.asp?news=49560

UNCLASSIFIED

WDAY TV, AM radio equipment damaged. After Memorial Day storms brought station programming to a halt for WDAY TV and WDAY-AM 970 radio, engineers are assessing damage. WDAY Channel 6 news went down May 30, and when a generator could not keep the equipment cool enough, programming was shut down. While regular programming resumed May 31, Xcel Energy restored power to the station about 4:50 p.m. Although there was no direct damage to the building or the station, the WDAY operations manager said the temperature will take its toll on the equipment. Even though no permanent damage was sustained to the news station, storms damaged all three WDAY-AM 970 radio towers. Source: <http://www.inforum.com/event/article/id/321817/group/News/>

Levees going up to protect South Dakota cities. Crews raced approaching floodwaters May 31 to complete emergency levees aimed at protecting South Dakota's capital city, and two other towns as the swollen Missouri River rolled downstream from the Northern Plains. Meanwhile, the mayor of Minot, North Dakota, ordered a quarter of the city's residents to evacuate areas along the flooding Souris River. He said the evacuation affects about 10,000 people who live along a 4-mile stretch of the Souris, which has risen with rain, snowmelt and discharges from Lake Darling. The mayor said residents are expected to be out of their homes by the night of June 1, in part to give construction crews room to raise and reinforce earthen dikes in the area. Residents of Dakota Dunes in southeastern South Dakota, below the final dam on the Missouri River, have been told to move their possessions to higher ground and be ready to leave their homes by June 2, a day before releases from the dams are set to increase again. The U.S. Army Corps of Engineers is increasing releases from the six dams on the Missouri to drain water from record rains of up to 8 inches that fell in eastern Montana and Wyoming and western North Dakota and South Dakota in the past 2 weeks. Heavy runoff from melting snow in the northern Rocky Mountains is expected to add to the problem soon. In North Dakota, more than 7 miles of levees were being built in Bismarck, and another 3.5 miles were going up across the river in Mandan. Source: <http://www.cbsnews.com/stories/2011/05/31/ap/business/main20067774.shtml>

Garrison Dam release update. The U.S. Army Corp of Engineer's announced May 28 that releases from the Garrison Dam in North Dakota would come quicker than previously announced. On May 30, the release was still 85,000 cubic feet per second (cfs). Now, instead of June 10 for the next release, it is been moved up to June 4. The release will be 90,000 cfs. Then 95,000 cfs June 6, and 100,000 June 7. An official with the Corp said they still plan a release of 105,000 cfs, but that date has not yet been determined. Source: <http://www.kxnet.com/getArticle.asp?ArticleId=782320>

Snowmelt, rain worsen flooding in northern Plains. Historic flooding in the Missouri River basin spurred voluntary evacuations in North Dakota May 30, while in Montana emergency workers ferried food and water to a town cut off by flood waters. The measures came as states in the northern Rockies and northern Plains plan for displacement of thousands and scramble to build levees in an expanding fight against river overflows predicted to worsen in coming weeks. Rains in the region May 30 intensified threats already posed by melting of record snows in the Rockies, prompting federal water managers to increase controlled spills from mainstem

UNCLASSIFIED

UNCLASSIFIED

reservoirs into the Upper Missouri River from Montana to states downstream. The record releases are designed to ease pressure on six dams and prevent uncontrolled flooding that would place hundreds of thousands of people at risk, officials said. Authorities on May 30 continued to deny rumors that the Fort Peck Dam in northeastern Montana had failed. Source: <http://www.reuters.com/article/2011/05/31/us-usa-flooding-plains-idUSTRE74U01920110531>

REGIONAL

(South Dakota; Montana) S. Dakota residents evacuate ahead of dam releases. Flood-threatened neighborhoods in Pierre, South Dakota, and its sister city Fort Pierre across the swollen Missouri River largely emptied June 2 as residents heeded calls to leave for higher ground ahead of the planned release of water from upstream dams. Most of the approximately 3,000 people living in low-lying areas of Pierre and Fort Pierre had left their homes. No one was ordered to leave home ahead of the planned June 3 dam releases, but it appeared few were willing to take their chances. Water releases from the Oahe Dam were expected to increase slightly starting early June 3 and gradually rise until June 7, when water levels were projected to crest 4 feet higher, or about 2 feet below the levee top. A similar release schedule was planned starting June 4 at Gavin's Point Dam upstream of Dakota Dunes, where the water level is expected to eventually rise another seven feet by June 14, again cresting about 2 feet below the tops of levees. In Montana, which has been dealing with widespread flooding from heavy rains in the past couple of weeks, federal officials started ramping up water releases June 2 from Fort Peck Dam. Officials warned dozens of residents downstream their homes could flood when the peak is released in the next 2 weeks. Source: <http://www.timesunion.com/news/article/S-Dakota-residents-evacuate-ahead-of-dam-releases-1406130.php>

(Montana) Gov. Schweitzer asks president to declare major disaster in Montana after flooding. The Montana governor asked the president June 1 to declare a major disaster in the flooded state, as a break in the weather allowed residents to dry out and prepare for another round of high water that could arrive in the coming weeks. The flood-soaked Crow Indian Reservation and counties across Montana were moving to make repairs after up to 8 inches of rain fell in some places last week, causing widespread flooding and hitting central and eastern Montana particularly hard. Hard-hit Big Horn County was preparing for more problems by ordering 50,000 sandbags. Officials on the Crow reservation planned to use about 10,000 of those bags to protect septic operations and other important areas. Many of the reservation's facilities were damaged by floodwater that forced hundreds of people to evacuate their homes last week. The reservation's septic facility was not operating and residents were advised to boil tap water before drinking it. Source: <http://www.therepublic.com/view/story/c131ddb440f44438839472e14ebe86c5/MT--Montana-Flooding/>

(Montana; Wyoming) Rockslide closes major park road. A rockslide temporarily closed the road between Mammoth Hot Springs and Tower Junction in Yellowstone National Park, the park said

UNCLASSIFIED

UNCLASSIFIED

in a press release May 28. Rocks and debris were discovered early that morning, covering a section of road at the entrance to Blacktail Plateau Drive, about eight miles east of Mammoth Hot Springs. The road is not expected to reopen to travel May 29. The press release said that park managers remained concerned about the threat posed by a large amount of loose rock and dirt above the roadway, which could easily dislodge and fall. Engineers with the Federal Highway Administration were being brought in to assess the condition of the road. Barricades have been set-up on both sides of the slide area. The road is currently open for emergency travel only. It is unknown when the road may be safe to reopen to travel by area residents, visitors, and park employees. The cause of the early morning rockslide is unknown. The road closure temporarily cuts off the communities of Cooke City and Silver Gate from most of the park. The road between Tower and Canyon has not opened for the summer, so that travel route is not affected. Residents and visitors can travel between Cooke City and Cody, Wyo., over Wyoming 296, the Chief Joseph Scenic Highway. Source:

http://www.bozemandailychronicle.com/news/article_24ca8408-8973-11e0-acc4-001cc4c002e0.html

(Montana) Floods halt phone service in Mont. cities as rain continues, snowmelt looms; SD town on alert. Flooding disrupted emergency phone service across a broad swath of eastern Montana May 30 as areas of the state remained inundated and downstream communities prepared for the worst. In southeast South Dakota, residents of the small town of Dakota Dunes were told to be ready to leave their homes by May 29 — and prepare to be gone awhile — as the Missouri River continued to rise. Knox County emergency manager told the Norfolk Daily News that Nebraska Highway 12, which connects Lazy River Acres with Niobrara and Verdel, could be flooded over soon. In Montana, flooding near Hardin on May 29 brought down telephone equipment that handles 911 and long-distance calls for Glendive, Miles City, Sidney, Fairview, Colstrip, Forsyth, Wibaux, and Terry. Emergency calls were rerouted until full service was restored at about 11 a.m. May 30, Qwest spokeswoman said. Source:

http://www.washingtonpost.com/national/soaked-montana-gets-more-rain-downstream-states-prepare-for-reservoir-releases/2011/05/30/AGlpugEH_story.html

NATIONAL

2 Iraqis indicted on terrorism charges in Kentucky. The Justice Department announced May 31 the indictment of two Iraqis currently living in Kentucky on terrorism charges that included an alleged plot to deliver explosives and Stinger missiles for use against Americans abroad. The two men were arrested in Kentucky May 25, and a federal grand jury in Bowling Green returned the 23-count indictment the May 24. Each faces life in prison if convicted of the charges. One of the men has been under investigation since September 2009. Over the last 8 years, officials say, he allegedly has supported efforts to kill U.S. forces in Iraq, first with improvised explosive devices and more recently by attempting to aid Iraqi insurgents with financial support and weapons, including rocket-propelled grenade launchers and Stinger missiles. Source:

<http://www.chicagotribune.com/news/nationworld/sc-dc-0601-kentucky-terrorists-20110531,0,5708529.story>

UNCLASSIFIED

INTERNATIONAL

IMF taking steps against possible hacking threat. The International Monetary Fund (IMF) has taken steps to combat a possible cyber attack from hacking group Anonymous Operations, a spokesman said June 1. Website Zero Hedge on June 1 had a post linking to an Anonymous Operations Twitter account that suggested hackers would target the IMF's website in relation to the fund's work with Greece. The IMF is one of several key negotiators trying to work with the struggling European nation as it seeks to restructure a bailout package and its debt obligations. In statements previously attributed to the group, the hacking collective has blamed the IMF and Greek government for the conditions of fund aid to the country. In a May 25 statement cited by Zero Hedge and attributed to Anonymous, the group said —the people of Greece have been left with no other option than to take to the streets in a peaceful revolution against the economic tyrants that are the IMF. Source:

<http://www.marketwatch.com/story/imf-taking-steps-against-possible-hacking-threat-2011-06-01>

Death toll rises to 13 in E.coli outbreak. The health authorities in Europe stepped up efforts May 30 to halt a deadly outbreak of a virulent form of E. coli bacteria in cucumbers as a dispute broke out between Spain and Germany over the source of the illness. The effects of the outbreak were being felt as far away as the United States, where two people who had recently been traveling in Germany, and a third person, had fallen sick with the illness, the European Commission said. The federal and state authorities in Germany — where effects are by far most severe — said the death toll climbed to 13 by May 30, from 10 May 29, in one of the largest outbreaks its kind reported worldwide. Hundreds of people have been struck down across the European Union with symptoms such as bloody diarrhea and stomach cramps. Vegetables were pulled from shelves in many countries, though no official Continent-wide bans were announced. Health policy and disease control mainly remain in the hands of national governments. German authorities the week of May 23 had identified fresh Spanish cucumbers from Malaga and Almeria as one of the possible sources for the outbreak. Source:

<http://www.nytimes.com/2011/05/31/world/europe/31iht-ecoli31.html? r=1>

BANKING AND FINANCE INDUSTRY

SEC employee misled fellow investors: watchdog. A Securities and Exchange Commission (SEC) employee invested in a company accused of preying on deaf people, and misled fellow investors into thinking their money was safe despite a SEC probe. The SEC Inspector General (IG) recommended disciplinary action, including possible dismissal of the employee, according to a roundup of his recent and pending investigations sent to the U.S. Congress May 31. The IG's office received a tip in February from a regional senior official who said a Washington, D.C.-based employee invested in an investment company that was the subject of an active

UNCLASSIFIED

investigation. The tipster accused the employee of “providing false, misleading and nonpublic information” to other investors, telling them the company was legitimate, and that they would “be receiving considerable sums of money from their investments.” The IG’s report did not mention the names of the employee or the company, but court records from these dates point to Imperia Invest IBC, an Internet-based investment company that allegedly targeted deaf investors and others by raising more than \$7 million from them without delivering a single payment. A federal judge in Utah later ordered the firm to pay \$15.2 million in disgorgement and prejudgment interest. The IG said the SEC employee later admitted to communicating with investors and was placed on administrative leave. Source:

<http://www.reuters.com/article/2011/05/31/us-sec-kotz-idUSTRE74U6FB20110531>

Former Nasdaq executive Donald Johnson pleads guilty to fraud for insider trading. A federal crackdown on insider trading has nabbed a former executive of the Nasdaq Stock Market who pleaded guilty May 27 to one count of securities fraud for trading on confidential information about companies listed on the Nasdaq. The man placed illegal trades from his computer at Nasdaq offices in New York, using an online brokerage account in his wife’s name, the Securities and Exchange Commission (SEC) said. From 2006 to 2009, he reaped more than \$755,000 in illegal profits, the SEC said. From his perch at Nasdaq’s “market intelligence desk,” the man received advance word of market-moving corporate developments such as changes in company leadership, earnings reports and the fact that a drug for hypertension had won approval from the U.S. Food and Drug Administration, the government said. He used the information to place secret trades, sometimes betting stocks would rise and other times betting they would fall, the government said. Source: http://www.washingtonpost.com/business/economy/former-nasdaq-executive-pleads-guilty-to-fraud/2011/05/26/AGjUeGCH_story.html

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

(Pennsylvania) Another ‘scam’ at Limerick nuclear plant. For the second time the week of May 30, one of the two reactors at the Limerick Generating Station in Pennsylvania experienced an unscheduled shutdown. Unit 1 experienced an automatic “scram” at about 10:15 a.m. June 3, according to a spokesperson for the Nuclear Regulatory Commission (NRC). “There were no complications during the shutdown, safety systems responded as expected, and the cooldown of the reactor is proceeding safely,” he said via e-mail. “Workers were performing testing on plant instrumentation when the Unit 1 turbine tripped offline, automatically shutting down the reactor,” the senior manager of communications with Exelon Nuclear said. Both said the precise cause of the shutdown was still under investigation. Unit 2, which just returned to service June 2, was operating at 93 percent power June 3, the company said in a press release. The company said that there is no risk to the public, and that there were no injuries associated with the shutdown. Source: <http://perkiomenville.patch.com/articles/another-scram-at-limerick-nuclear-plant>

U.S. runs short of gas used in detecting nuclear material. The United States is running out of a rare gas that is crucial for detecting smuggled nuclear weapons materials, according to a new

UNCLASSIFIED

UNCLASSIFIED

Congressional audit. The gas, helium-3, is a byproduct of the nuclear weapons program, but as the number of nuclear weapons has declined, so has the supply of the gas. From 2003 to 2009, the Energy Department's (DOE) Isotope Program was selling the gas at a rate of about 30,000 liters per year, while the DOE's National Nuclear Security Administration (NNSA) was producing only 8,000 to 10,000 liters, the Government Accountability Office (GAO) found. Yet, as the supply was shrinking, the DHS spent \$230 million to develop the detection technology that required helium-3. As a result, government scientists and contractors are now racing to find or develop a new detection technology. The GAO report said the NNSA, which gathers the gas from old nuclear weapons, never told the Isotope Program about the slowing rate of helium-3 production. That is in part because it was secret information that could be used to calculate the size of weapon stockpiles. For its part, the Isotope Program calculated demand for the gas not in a scientific way, but instead on the basis of how many commercial companies called to inquire each year about helium-3 supplies. The House science committee's Subcommittee on Investigations and Oversight, which was asked to study the problem after it was detected in 2008, planned to release the report the week of May 30. Source:

http://www.nytimes.com/2011/05/29/us/29helium.html?_r=1

Wider U.S. nuclear evacuation zone unneeded, official says. The United States should not widen the minimum evacuation zone around nuclear plants to 50 miles from 10 miles, said a member of the U.S. Nuclear Regulatory Commission May 26. It is "unreasonable" to require the wider zone just because U.S. citizens were urged to stay 50 miles from a nuclear plant damaged by an earthquake and tsunami in Japan, he said at a conference in Washington. U.S. officials made a decision on the evacuation zone in Japan based on incomplete information, he said. The 10-mile "emergency planning zone" around U.S. nuclear plants can be expanded during an accident if the situation worsens, he said. Source: <http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2011/05/26/bloomberg1376-LLTHA76S972R01-6FUGMVNEONPS7D1GOP9JQ4L03S.DTL>

'Tornado Alley' reactor not fully twister-proof. The closest nuclear power plant to tornado-ravaged Joplin, Missouri, was singled out weeks before the storm for being vulnerable to twisters. Inspections triggered by Japan's nuclear crisis found that some emergency equipment and storage sites at the Wolf Creek nuclear plant near Burlington, Kansas might not survive a tornado. Specifically, plant operators and federal inspectors said Wolf Creek did not secure equipment and vehicles needed to fight fires, retrieve fuel for emergency generators, and resupply water to keep nuclear fuel cool as it is being moved. Wolf Creek, until recently, was one of three nuclear plants placed on a federal watch list in March for safety-related issues. A former nuclear plant engineer who now works on nuclear safety for the advocacy group Union of Concerned Scientists, said the equipment that a tornado could disable is the "backup of backups," but that potential should raise concern nonetheless. Already this year, tornadoes have knocked out power to nuclear power plants in Alabama and Virginia, exposing vulnerabilities. Wolf Creek's location in Tornado Alley means it was designed to handle the maximum tornadoes possible for the United States, with wind speeds up to 360 miles per hour, and a maximum rotational speed of 290 miles per hour. But its fire truck, for example, is parked in a sheet-metal building "not protected from seismic or severe weather events," according to

UNCLASSIFIED

UNCLASSIFIED

the Nuclear Regulatory Commission (NRC) inspection conducted after the Japanese disaster.

Source: <http://www.npr.org/templates/story/story.php?storyId=136694610>

COMMERCIAL FACILITIES

(Oklahoma) Gunman dead, one injured in shooting at Tulsa shopping center. The gunman is dead after shooting a victim at a Tulsa Hills Shopping center hair salon June 2 in Tulsa, Oklahoma. The suspect was found dead inside SportClips. A female victim was taken to an area hospital in serious condition. Police were called to the scene at about 3:30 p.m. after a report of shots fired. When they arrived, they were able to speak with the victim, a 29-year-old female. The woman told police that the shooter came into the SportClips and shot her in the neck, then shot himself. The victim was taken by ambulance to a Tulsa hospital in serious condition. Court records show a protective order was filed against the suspect June 1. The female victim was listed in serious condition. Source: <http://www.ktul.com/story/14829449/shooting-reported-at-south-tulsa-fast-food-restaurant>

COMMUNICATIONS SECTOR

Nothing Significant to Report

CRITICAL MANUFACTURING

Model helicopters, sewing machines, baby hats on recall listing. Janome America Inc. of Mahwah, New Jersey is recalling Elna Sewing Machines sold nationwide from September 2010 to April 2011. The wires inside the sewing machine can short circuit, posing a risk of fire. This recall involves the Elna eXcellence 740 sewing machine. The machine is white and navy with a digital touch panel. "Elna" and "eXcellence 740" are printed on the front of the machine. Consumers should immediately unplug and stop using the machine, and return it to the store where it was purchased for a free repair. For more information, contact Janome at (800) 631-0183 or visit the firms Web site at www.elnausa.com. Source: <http://businessclarksville.com/2011/06/02/model-helicopters-sewing-machines-baby-hats-on-recall-listing/>

Toyota recalls 106,000 Prius cars. Toyota recalled 106,000 first-generation Prius hybrid cars globally June 1 for faulty steering caused by a nut that may come loose. The single minor accident suspected of being related to the problem was reported in the United States, according to Toyota Motor Corp. The latest recall from Toyota affects 52,000 Prius cars sold from 2001 through 2003 in the United States, a company spokesman said. Toyota said loose nuts in the electric-power steering can cause the vehicle, if operated over a long time, to steer with too much force. Source:

UNCLASSIFIED

UNCLASSIFIED

<http://www.google.com/hostednews/ap/article/ALeqM5g4iQVLL2swxQXp9gQdsNsygr3L4g?docid=85be044b5e2d493fa0a1352445452587>

DEFENSE/ INDUSTRY BASE SECTOR

Chinese execs plead to attempting to export military-grade microchips. Two Chinese aerospace executives have pleaded guilty in U.S. court to attempting to violate the U.S. arms embargo against China by purchasing thousands of military-grade microchips. The U.S. attorney for the Eastern District of Virginia said the guilty pleas June 1 from the two Chinese executives represent the latest in a series of prosecutions targeting both traditional espionage and economic espionage efforts from Beijing. The executives were targets of an undercover operation after an unidentified Virginia company tipped off authorities that a Chinese firm, Beijing Starcreates, was trying to buy radiation-hardened microchips that work in outer space and are typically used in military systems. In their plea, the executives admitted trying to use a straw buyer to purchase the chips. Source:

<http://www.nbcwashington.com/news/local/Chinese-Execs-Plead-to-Attempting-to-Export-Military-Grade-Microchips-122974518.html>

Second defense contractor L-3 ‘actively targeted’ with RSA SecurID hacks. An executive at L-3 Communications warned employees in April that hackers were targeting the company using inside information on the SecurID keyfob system freshly stolen from an acknowledged breach at RSA Security. “L-3 Communications has been actively targeted with penetration attacks leveraging the compromised information,” read an April 6 e-mail from an executive at L-3’s Stratus Group to the group’s 5,000 workers, one of whom shared the contents with Wired on condition of anonymity. It is not clear from the e-mail whether the hackers were successful in their attack, or how L-3 determined SecurID was involved. An L-3 spokeswoman declined comment in April, except to say: “Protecting our network is a top priority and we have a robust set of protocols in place to ensure sensitive information is safeguarded. We have gotten to the bottom of the issue.” Source: <http://www.wired.com/threatlevel/2011/05/l-3/>

Lockheed Martin suffers massive cyberattack. A major online attack was launched earlier in May against the networks of Lockheed Martin, the largest defense contractor in the United States. Lockheed Martin released a statement May 28 confirming the attack, which it described as “significant and tenacious.” The company said its information security team “detected the attack almost immediately and took aggressive actions to protect all systems and data.” As a result, the company said, “our systems remain secure; no customer, program, or employee personal data has been compromised.” Hackers reportedly exploited Lockheed’s VPN access system, which allows employees to log in remotely by using their RSA SecurID hardware tokens. Attackers apparently possessed the seeds — factory-encoded random keys — used by at least some of Lockheed’s SecurID hardware fobs, as well as serial numbers and the underlying algorithm used to secure the devices. Source:

<http://www.informationweek.com/news/government/security/229700151>

UNCLASSIFIED

UNCLASSIFIED

(Gulf of Mexico) U.S. Navy rejects new radar ship. A new ship intended to carry a ballistic missile tracking radar failed its acceptance trials earlier in May and will need repairs before it can enter service, the U.S. Navy said May 26. The Howard O. Lorenzen (T-AGM 25), built by VT Halter Marine at Moss Point, Mississippi, is a 12,000-ton, 534-foot-long ship intended to carry the Cobra Judy Replacement (CJR) radar, a key sensor used in treaty monitoring and verification for ballistic missile issues. Built under an initial \$199 million contract awarded in 2006, the ship has been under construction at VT Halter's yard since August 2008, when delivery was scheduled for June 2010. The Navy's Board of Inspection and Survey (INSURV) conducted acceptance trials in the Gulf of Mexico during the week of May 9, according to the Naval Sea Systems Command (NAVSEA) in Washington. The trial "was reported as unsatisfactory", NAVSEA said. The failed grade was due to three major discrepancies — thrust bearing temperature, and steering, and anchor demonstrations. Three of 15 graded areas — electrical, damage control, and aviation — were also graded unsatisfactory. Source: <http://www.defensenews.com/story.php?i=6638463&c=AME&s=SEA>

EMERGENCY SERVICES

(Missouri) Kansas man charged with setting fire to an Ozark County fire department and breaking in to fire chief's home. A man from Shawnee, Kansas has been arrested in connection with a fire and home break-in in Ozark County, Missouri, KSPR 33 Springfield reported May 31. The fire at the Timber Knob Fire Department and break-in at a home near Pontiac resulted in more than \$200,000 in damages, according to the chief deputy. After a 1-month investigation, warrants were obtained for the arrest of the 28-year-old, who is charged with stealing, first and second degree burglary, arson, and armed criminal action. His cash-only bond has been set at \$200,000. Authorities said he had worked for the fire chief at one time, and was also attempting to purchase some firearms from her. The chief deputy for Ozark County said he anticipated additional arrests. Source: <http://www.kspr.com/news/local/kspr-kansas-man-charged-with-setting-fire-at-ozark-county-fire-department-20110531,0,1094345.story>

ENERGY

Nothing Significant to Report

FOOD AND AGRICULTURE

(Colorado) 2 Colorado deaths linked to Listeria infection. Colorado health officials said June 2 that two deaths in Denver were linked to a Listeria infection since May 20. Colorado Department of Public Health and Environment epidemiologists and Denver Public Health and Denver Environmental Health are investigating three reported cases. All three involved people of Hispanic/Latino heritage. A male in his 30s and a female in her 60s died from the infection.

UNCLASSIFIED

UNCLASSIFIED

On average, Colorado has about 10 cases of listeriosis per year. The investigation is ongoing and the source of the current outbreak is unknown. Consumption of food contaminated with *Listeria monocytogenes* can cause listeriosis, an uncommon but potentially fatal infection.

Source: <http://www.thedenverchannel.com/education/28116292/detail.html>

(Oklahoma) Okla. company recalls chicken, ham products. Allison's Gourmet Kitchens, a Moore, Oklahoma-based food company, recalled almost 23,000 pounds of chicken and ham products due to mislabeling. The U.S. Department of Agriculture said the recall was made because the packaging does not list the ingredients potassium sorbate and/or sodium benzoate. The affected products were sold between April 15 and May 18. The chicken salad was sold in Illinois, Kansas, Louisiana, Missouri, Nebraska, North Carolina, Pennsylvania, Texas, and Virginia. The ham salad was distributed in Texas. The use-by dates on the packages range from May 27, 2011 to June 29, 2011. The agency said the labeling problem was discovered during a routine review. Source: <http://www.chron.com/disp/story.mpl/ap/tx/7592915.html>

Chinese agency says European E. coli is new strain; Russia sets ban. Scientists at the Beijing Genomic Institute said the outbreak of infection in Germany from an *E. coli* strain that has swept across Europe was caused by a new —super-toxic *E. coli* strain, though the U.S. Centers for Disease Control and Prevention (CDC) said the strain has been seen before. The CDC said the strain is very rare and added that while it is not aware of any cases reported in the United States, it is aware of a few reports of the strain from other countries. Britain's Health Protection Agency has said that the strain suspected in the outbreak is —rare and —seldom seen in the U.K. The outbreak is responsible for 15 deaths in Germany and one in Sweden, and has sickened more than 1,000 people in at least 10 countries, according to the World Health Organization. The European Food Safety Alert Network initially said enterohemorrhagic *Escherichia coli*, a strain of *E. coli* that causes hemorrhaging in the intestines, was found in organic cucumbers originating from Spain, packaged in Germany and distributed to countries including Austria, the Czech Republic, Denmark, Germany, Hungary, Luxembourg, and Spain. But authorities are saying the source has not been pinpointed. Source: http://www.cnn.com/2011/WORLD/europe/06/02/europe.e.coli/index.html?hpt=hp_t2

U.S. increases food inspections after deadly E.coli outbreak in Europe. Tainted vegetables are believed to have claimed the lives of 16 people and sickened more than 1,000 in Europe. U.S. health officials are inspecting cucumbers and other produce from Spain after European governments believe an *E. coli* outbreak that originated in Germany was first linked to contaminated cucumbers from Spain. While the exact source has still not been determined, vegetables have been known to carry *E.coli* bacteria since they are grown with fertilizer using cow manure. "Due to the information received about the outbreak in Germany, FDA (Food and Drug Administration) is flagging shipments of cucumbers, tomatoes and lettuce from Spain for further inspection," a FDA spokesman said. The agency heightened calls for inspection the week of May 23, specifically produce from Spain as more information became available about the exact cause of the outbreak. The FDA said cucumbers from Spain are not imported to the United State on a large scale this time of year. However, it is still not clear if the cucumbers are

UNCLASSIFIED

UNCLASSIFIED

the cause of the outbreak in Europe. Source: <http://www.examiner.com/healthy-trends-in-atlanta/u-s-increases-food-inspections-after-deadly-e-coli-outbreak-europe>

(Illinois) FDA: Tiny Greens grew outbreak salmonella strain. The strain of Salmonella that sickened 94 people in 16 states and the District of Columbia in November and December of 2010 appears to have originated at a sprouts farm in Urbana, Illinois. Tiny Greens Organic Farm was hit with a May 5 warning letter from the U.S. Food and Drug Administration that discloses results of the environmental sampling that public health authorities completed during the outbreak. The FDA said it linked a Salmonella enteric serotype from the outbreak “to sprouts grown in your facility.” The agency said one sample collected from a compost pile outside Tiny Greens was found to have a Pulse Field Gel Electrophoresis (PFGE) result (DNA “fingerprinting”) indistinguishable from the outbreak strain. Also implicated in the outbreak was Jimmy John’s fast food restaurant chain, which was a large purchaser of Tiny Greens sprouts. The multistate outbreak led Tiny Greens to recall its Alfalfa and Spicy Sprouts, although the owner said at the time there was nothing more than a “statistical association” to his product. Source: <http://www.foodsafetynews.com/2011/06/tiny-greens-was-growing-the-outbreak-salmonella-strain/>

(Michigan) Ground beef recalled in Southern Michigan. Irish Hills Meat Company of Tipton, Michigan, recalled about 900 pounds of ground beef products that may have been contaminated with E. coli O157:H7, the U.S. Department of Agriculture’s (USDA) Food Safety and Inspection Service (FSIS) said May 31. The ground beef was shipped to restaurants in Southern Michigan. The problem was discovered through routine FSIS monitoring that confirmed a positive result for E. coli O157:H7. The recalled ground beef was packed in 10-pound clear polybags, with the establishment number “EST. 10014” inside the USDA mark of inspection, and then packaged in boxes that contain 3-5 bags. The production dates May 23 and May 26 are stamped on the boxes. Source: <http://www.foodsafetynews.com/2011/06/ground-beef-recalled-in-southern-michigan/>

Outbreak: Secondary exposures make up about half of all confirmed equine herpes virus cases, veterinary officials report. Of the 47 cases of equine herpesvirus (EHV-1) now confirmed across 9 Western states, 14 were contracted through secondary or tertiary exposure, veterinary officials report. Another 28 cases of equine herpesvirus myeloencephalopathy (EHM), the neurologic form of the disease, have been reported — 25 from direct exposure during the recent National Cutting Horse Association competition in Ogden, Utah. The U.S. Department of Agriculture (USDA) Animal and Plant Health Inspection Services (APHIS) now places the total number of EHV-1/EHM cases at 75. Eleven of those horses died or were euthanized. More than 400 horses in 19 states were exposed at the Utah event, and another 1,635 are at risk of secondary or tertiary exposure, APHIS said in its May 26 update on the outbreak. Although the incubation period for EHV-1 is 2 to 14 days, Washington’s state veterinarian said the virus can shed for up to 28 days. Source: <http://veterinarynews.dvm360.com/dvm/Veterinary+Equine/Outbreak-New-equine-herpes-virus-cases-emerge/ArticleStandard/Article/detail/724806?contextCategoryId=378>

UNCLASSIFIED

UNCLASSIFIED

Salmonella outbreak from backyard poultry. A least 25 people in 11 states have become sick from human Salmonella serotype Altona after handling their backyard chicks and ducklings, according to the U.S. Centers for Disease Control and Prevention (CDC). The CDC said a traceback investigation implicates a national mail-order hatchery, Feed Store Chain A, which supplies poultry for people raising flocks at home for fresh eggs, as the source. Seven people have been infected with the outbreak strain of Salmonella in Ohio; four in North Carolina; three in Kentucky; two in Maryland, Pennsylvania, and Tennessee; and one in Indiana, Minnesota, New York, Vermont, and Virginia, the CDC said. Laboratory testing in May confirmed Salmonella Altona bacteria matching the outbreak strain in three samples collected from a chick and the yard of an ill person's household in Ohio, as well as from three samples collected from chick and duckling displays at two locations of Feed Store Chain A in North Carolina. Onset of their illnesses was between February 25 and April 25, 2011. The case patients range in age from less than 1 year old to 84 years old; the median age is 8 years. Among the 21 patients with available information, 8 (38 percent) were so sick they had to be hospitalized. Source:

<http://www.foodsafetynews.com/2011/05/salmonella-outbreak-from-backyard-poultry/>

(Oregon; Washington) Listeria spurs shutdown of Oregon sprout firm. At the behest of the U.S. Food and Drug Administration (FDA), government attorneys persuaded the U.S. District Court for Oregon to issue a permanent injunction against Shanghai Company Inc., a bean sprout firm in Portland, Oregon, and its owners. The order, signed in May, shuts down the sprout business unless and until the defendants can bring it back into compliance with food safety rules, entirely to FDA's satisfaction. The federal court ordered everyone associated with Shanghai to "cease, directly or indirectly, receiving, processing, manufacturing, preparing, packaging, holding, and distributing any article of food" at the existing site, or any other location. The owners and anyone working with Shangha are enjoined from doing anything that would cause food to be considered adulterated, under the law, and from putting adulterated food into interstate commerce. Listeria contamination of its ready-to-eat bean sprouts and inside its facility has been the most serious problem. The Portland business was getting seeds from Jilin, China, then growing and distributing sprouts to retailers in Oregon and Washington. Its most recent recall, issued November 24, 2010, was of mung bean sprouts in clear 9 oz. and 5 lb. bags found to be contaminated with Listeria. Source:

<http://www.foodsafetynews.com/2011/05/listeria-problem-prompts-shutdown-of-portlands-shanghai-co/>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

Massive Gmail phishing attack hits top U.S. officials. Hundreds of personal Gmail accounts, including those of some senior U.S. government officials, were hacked as a result of a massive phishing scheme originating from China, Google said June 1. The account hijackings were a result of stolen passwords, likely by malware installed on victims' computers or through victims' responses to e-mails from malicious hackers posing as trusted sources. That type of hack is

UNCLASSIFIED

UNCLASSIFIED

known as phishing. Gmail's security systems themselves were not compromised, Google said. The company believes the phishing attack emanated from Jinan, China. In addition to the U.S. government personnel, other targets included South Korean government officials and federal workers of several other Asian countries, Chinese political activists, military personnel, and journalists. After the most recent cyber attack, a Chinese official insisted June 2 that his government takes the attacks seriously. A spokesman from Google declined to comment on how the company obtained the information about the most recent hack. Public information, user reports, and a third-party hacking blog called Contagio was used to determine the scope, targets, and source of the attack. Source:

http://money.cnn.com/2011/06/01/technology/gmail_hack/index.htm?hpt=hp_t2

(California) S.F.: Federal courthouse evacuated because of suspicious package. A police bomb squad is investigating a suspicious package discovered at the federal courthouse at Mission and Seventh streets in San Francisco, California June 1. The package was reported at about 11:30 a.m. in a basement area where packages come in and are X-rayed, a police officer said. One package was deemed suspicious, and the Federal Protective Service, which provides security at the courthouse, asked the Police Department's bomb squad to respond, he said. The basement and first floor of the building were evacuated, and people on the other floors were told to shelter in place, he said. Source: http://www.mercurynews.com/breaking-news/ci_18184359?nclick_check=1

New England states coordinate cyber-security response planning. A number of states are tightening the coordination between IT professionals in government and industry to minimize the potential impact of a disruption to computerized systems. Rhode Island, Massachusetts, and New Hampshire are coordinating plans for responding to interruptions in services due to cyberattacks or natural disasters that disrupt computer systems that facilitate critical services. In 2009, Rhode Island officials met with representatives from hospitals, financial institutions, colleges, universities, the military, cable, and communications industries, and utilities to identify who the stakeholders were, and who could contribute resources to a cyber-disruption response team. The plan describes a fairly straightforward implementation of Emergency Support Function (ESF) 2 under the National Response Framework. The response team, which is still being formed, will likely be made up of 8 to 12 members, organized under the Rhode Island State Police, who will be responsible for restoring critical IT systems. Cyber-disruption teams are also being established in Massachusetts and New Hampshire as well as the Providence and Boston UASI regions. The teams will have personnel from IT, emergency management, public safety and service providers who can advise an incident commander about restoring or maintaining critical infrastructure under ESF-2. Source:

<http://www.emergencymgmt.com/disaster/New-England-States-Cyber-Security-Response-Planning-052511.html>

UNCLASSIFIED

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Hotmail and Yahoo users also victims of targeted attacks. Web mail users at Yahoo and Hotmail have been hit with the same kind of targeted attacks that were disclosed earlier the week of May 30 by Google, according to security software vendor Trend Micro. Trend Micro described two similar attacks against Yahoo Mail and Windows Live Hotmail in a blog post, published June 2. “It’s an ongoing issue for more than just Gmail,” a senior threat researcher with Trend Micro said. He believes Facebook accounts have also been used to spread similar attacks. Google made headlines June 1 after revealing several hundred Gmail users — including government officials, activists, and journalists — had been the victims of targeted spearphishing attacks. Google mentioned phishing on June 1, but the criminals have been using other attacks too. In March, Google said hackers were taking advantage of a flaw in Microsoft’s Windows software to launch politically motivated hacks against activists. Corporate networks have been under attack for years, but hackers now see personal Web mail accounts as a way to get information that can help them sneak into computers that would otherwise be locked down. Source: <http://www.csoonline.com/article/683451/hotmail-and-yahoo-users-also-victims-of-targeted-attacks>

Facebook video scam puts malware on Mac and Windows. Facebook seems unable to stop scammers from circulating malicious Web links that install fake antivirus software on victims’ computers. The scam was spotted May 31 by antivirus vendor Sophos. At that time the criminals behind it were luring victims into installing the software by offering links purportedly to a video of the disgraced former International Monetary Fund Managing Director and a hotel maid. The scam switched June 1 and the link was supposed to be an X-rated video of two female celebrities. In both cases there is no such video. People who click on the link are sent to a Web site that tries to install the fake antivirus software. The scam is slightly different, depending on whether the victim is using a Mac or a PC. On the PC, the site tells victims that they need to install the latest version of Adobe Flash Player to watch the video. But the software they install is actually the fake antivirus program. On the Mac, there is a pop-up window that looks like a security warning. When victims click to —fix the security problems, they end up installing the fake software. The same type of software, MacGuard or MacDefender, has recently been plaguing Mac users. Source: http://www.computerworld.com/s/article/9217229/Facebook_video_scam_puts_malware_on_Mac_and_Windows

Spammers using domain parking services to bypass anti-spam filters. Security experts are warning that spammers are increasingly taking advantage of domain parking services offered by registrars in an attempt to circumvent reputation-based anti-spam products and conceal their sites. Symantec.cloud’s senior software engineer explained in a blog post that parking services are usually used by registrants to reserve a domain for future use to mitigate the risk of cyber squatting, or to monetize a particular domain through online advertising. However, his team recently noticed “a large domain parking service being abused by spammers on a massive scale.” “Each domain hosted on the service contains an open redirect script, allowing spammers to redirect to any URL of their choice,” he said. “Since the redirect does not affect the parking

UNCLASSIFIED

page, and domains parked on domain parking services are typically not used for any other purpose, it is unlikely that the domain owners will notice when their domains are inevitably added to anti-spam block lists.” The researcher warned that such strategies could help spammers escape detection by some anti-spam products, especially given that many of the domains have been registered for years and are therefore seen as more likely to have a good reputation. Source: <http://www.v3.co.uk/v3-uk/news/2074224/spammers-domain-parking-services-bypass-anti-spam-filters>

Google faces new round of Android malware. For the second time in 3 months, Google pulled dozens of malware-infected smartphone apps from the Android Market. The 34 apps were pulled over the weekend of May 28 and 29, and May 31 by Google after security researchers notified the company. As in the March episode, when Google removed more than 50 apps, the newest round consisted of pirated legitimate programs that had been modified with malicious code and then re-released to the Android Market under false names. However, there was an important difference to this campaign, said the CTO of Lookout, a firm that specializes in mobile security. “These apps have the ability to fire up a page on the Android Market,” he said, adding that the hackers can send commands to the smartphone telling it what market page to display. He speculated that the attackers intended the new feature as a way to dupe users into downloading additional rogue apps that would have malicious functions, just as when a hijacked PC is told to retrieve more malware. “They seem to have been designed to encourage people to install additional payloads,” he said. He said it was impossible to deduce hacker intent from the malicious apps’ code, but he believed the criminals took the new path because social engineered attacks — those that rely on tricking victims into installing malware rather than depending on an exploited vulnerability — are more difficult to defend against. Source: http://www.computerworld.com/s/article/9217178/Google_faces_new_round_of_Android_malware

HP expands recall of notebook computer batteries due to fire hazard. Hewlett-Packard Company, of Palo Alto, California, issued a recall May 27 for about 162,000 additional lithium-ion batteries used in HP and Compaq notebook computers (54,000 and 70,000 batteries were previously recalled in May 2010 and May 2009, respectively). The recalled lithium-ion batteries can overheat and rupture, posing fire and burn hazards to consumers. Since the May 2010 recall expansion, HP has received 40 additional reports of batteries that overheated and ruptured, resulting in 7 burn injuries, 1 smoke inhalation injury, and 36 instances of property damage. The batteries were sold at computer and electronics stores nationwide, hp.com, and hpshopping.com from July 2007 through July 2008. Source: <http://www.cpsc.gov/cpsc/pub/prerel/prhtml11/11234.html>

Critical vulnerability in open source Eucalyptus clouds. Researchers at Ruhr-University Bochum have discovered a critical vulnerability in Eucalyptus, an open source implementation of the Amazon EC2 cloud APIs. An attacker can, with access to network traffic, intercept Eucalyptus SOAP commands and modify them or issue their own arbitrary commands. To do this, the attacker must only copy the signature from an XML packet sent by Eucalyptus to the user. As Eucalyptus did not properly validate SOAP requests, the attacker could use their own copy in

UNCLASSIFIED

UNCLASSIFIED

commands sent to the SOAP interface and have them executed as the authenticated user. All versions up to and including 2.0.2 are vulnerable; a fixed version, 2.0.3, is available to download. Ubuntu's Eucalyptus-based Ubuntu Enterprise Cloud (UEC) is also vulnerable; updates for Ubuntu 10.04 LTS, 10.10 and 11.04 are already available in Canonical's repositories. Eucalyptus said the changes made to close the holes may lead to some existing tools failing to work as the system will interpret them as a replay attack if they issue commands too rapidly. Source: <http://www.h-online.com/security/news/item/Critical-vulnerability-in-open-source-Eucalyptus-clouds-1252593.html>

New scareware campaign uses fake Firefox security alerts. Security researchers from Sophos warn of a new scareware campaign that directs Firefox users to rogue pages mimicking security alerts normally issued by the browser. Firefox leverages Google's Safe Browsing API to prevent users from visiting Web sites flagged as malicious. The service aggregates data from various third-party sources and Google's own specialized crawlers. When a rogue page is opened in Firefox, the browser displays a security alert saying the request has been blocked and providing the user several options. According to Sophos, the people behind this scareware distribution campaign have cloned the page and modified it to appear as if a computer scan is also performed and infections are found. "Mozilla Firefox recommends you to install proper software to protect your computer," the phishing page says and presents a "Start Protection" button. Clicking it will prompt people to download and install a rogue antivirus application designed to scare them into buying a license to allegedly clean the fictitious infections. The scam is browser-aware and will direct Internet Explorer users to a different page mimicking a classic Explorer window. Source: <http://news.softpedia.com/news/New-Scareware-Campaign-Uses-Fake-Firefox-Security-Alerts-203305.shtml>

Pharma spam campaign distributes fake Apple AppStore emails. Security researchers from Finnish antivirus vendor F-Secure warn about a wave of pharma spam e-mails masquerading as official communications from Apple's AppStore. The e-mails bear a subject of "ID:[random number] Apple AppStore Order Cancellation" and come with spoofed headers to appear as if they from an AppStore@apple(dot)com address. The messages were created using a real Apple AppStore e-mails template, but all links inside have been replaced with ones leading to rogue online pharmacies. There are two links, one on the random ID number and one on "order information." The e-mails are designed to make recipients ask themselves questions like why was his order canceled or why was there an order in the first place. In both cases, users will likely click on the links to obtain more information, only to find themselves taken to a rogue pharmacy Web site selling prescription drugs. Source: <http://news.softpedia.com/news/Pharma-Spam-Campaign-Distributes-Fake-Apple-AppStore-Emails-202746.shtml>

NATIONAL MONUMENTS AND ICONS

(Arizona) **Arizona wildfires prompt evacuation orders.** Authorities have ordered issued a mandatory evacuation order for two communities in southeastern Arizona near the Horseshoe

UNCLASSIFIED

UNCLASSIFIED

Two wildfire. The Cochise County Sheriff's office issued the evacuation for the Paradise and East Whitetail Canyon June 2. Officials said winds pushed the fire over a northeast perimeter and across Rock Creek Canyon. The Chiricahua National Monument was closed June 2. The fire has burned about 135 square miles and containment has dropped down to 50 percent. About 800 firefighters were battling the 86,000-acre wildfire. The U.S. Forest Service said crews were working to contain the northeast perimeter of the fire, and protect structures in evacuated communities. Meanwhile, another wildfire threatened evacuations in Alpine, in the Apache National Forest. Residents were told to prepare to evacuate because of a wildfire southwest of the community. Residents and guests in cabins and ranches surrounding Alpine already have left, but fire officials did not know how many. The Wallow fire has burned 40,500 acres across dried out forest land in eastern Arizona, and is being fanned by strong winds. It was at zero containment. Fire officials said Alpine residents could be asked to leave within 12 to 24 hours. Alpine is home to about 250 people, though not all live there year-round. Source: <http://www.cbsnews.com/stories/2011/06/02/national/main20068548.shtml>

POSTAL AND SHIPPING

(California) White powder shuts down Ferndale post office. A package and delivery bag with white powder that caused the Ferndale, California post office to close its doors for roughly an hour in the morning May 26 was determined to be a broken bottle of penicillin, according to hazardous materials investigators. They were called to the post office at about 9:45 a.m., said the coordinator for the Humboldt-Del Norte Hazardous Materials Response Team. Investigators found a broken glass bottle with a broken label alongside the white substance, he said. Firefighters with the Ferndale Fire Department visited the package's recipient who was able to show them another bottle identical to the broken bottle. "(It was) a bottle of penicillin that had broken in transit and leaked through the package, and ... penicillin, once [the] water evaporates ... turns back to powder form" he said, adding a local veterinarian was able to verify that the substance was penicillin. The post office reopened around 10:15 a.m. Source: http://www.times-standard.com/ci_18146546

PUBLIC HEALTH

(Arizona) Study: Faulty pharmacy alert systems missing risky drug interactions. The computer systems used by pharmacies to flag potentially dangerous drug combinations before a prescription is filled often are flawed, according to a University of Arizona study published in the Journal of the American Pharmacists Association, the Arizona Republic reports. From December 2008 to November 2009, the researchers tracked activities at 64 independent, chain-operated, and hospital pharmacies in Arizona. Researchers tested the pharmacy computer systems using a fictional patient who was taking a regimen of 18 drugs primarily for cardiovascular problems. Thirteen of the drugs the patient requested were considered "clinically significant" — meaning they likely are harmful when paired with another drug on the

UNCLASSIFIED

UNCLASSIFIED

patient's regimen. The researchers used a "pass/fail" system to indicate whether the various pharmacy computer systems were able to identify the fictional patient's medication regimen as potentially harmful. Only 28 of the 64 pharmacies identified the dangerous drug interactions. According to the Arizona Republic, there are a number of potential theories explaining why more drug interactions are not flagged, including: outdated systems; pharmacies' turning off some alert settings to cut back on being overwhelmed by alerts; and inconsistencies in the drug databases on which the systems rely to generate alerts. Source:

<http://www.ihealthbeat.org/articles/2011/6/1/study-faulty-pharmacy-alert-systems-missing-risky-drug-interactions.aspx>

Mobile phones in hospitals pose pathogen threat, researchers say. Wireless phones are seen as a perilous health risk by researchers who say the number of dangerous multi-drug resistant organisms on patients' and their visitors' mobile devices greatly exceed the number found on healthcare providers' devices in one studied hospital. In a report published in the June issue of the American Journal of Infection Control, Turkish researchers who examined pathogens on cell phones at the 800-bed University Turgut Ozal Medical Center in Turkey suggest their findings have important implications for hospitals in the United States. The researchers took swab samples from 133 mobile phones they obtained from patients, companions, and visitors and 67 from healthcare workers, and ran cultures on bacteria collected from the keypads, microphones, and ear parts of each device. Nearly 40 percent of the phones collected from patients and their visitors, versus 20.6 percent of those collected from healthcare workers, showed presence of pathogenic bacteria. "Furthermore (a) higher number of multi-drug resistant pathogens were present on the mobile phones of (the) patients' group (including family members and patients' companions)," the researchers added. Source:

<http://www.healthleadersmedia.com/content/TEC-266803/Mobile-Phones-May-Pose-MRSA-Threat>

(Georgia) Atlanta hospital notifies nearly 700 patients about TB exposure. Nearly 700 patients and 100 employees at Emory University Hospital in Atlanta, Georgia have been exposed to tuberculosis (TB) after coming in contact with a hospital employee carrying the disease, a hospital spokesman said May 26. The Georgia Department of Community Health and the hospital have identified 680 patients who were exposed to TB between November and February, a hospital spokesman said. Patients will begin getting tested for TB the week of May 30, he said. To date, no patients or employees have reported symptoms, he said. The hospital and the department began notifying people about the exposure this month, after an Emory employee was diagnosed in April with the infectious disease, he said. The employee did not know he had TB when he came in contact with employees and patients, the hospital said. The hospital took extra precautions by contacting patients who were in the hospital for 90 days before the day the employee is known to have developed the disease, he said. All hospital employees are screened for the disease and must receive screenings each year, it added. A hospital statement did not say whether the employee who developed TB had been screened. Source: <http://edition.cnn.com/2011/HEALTH/05/26/georgia.tuberculosis.scare/>

UNCLASSIFIED

TRANSPORTATION

(California) Pipe bomb found near Salinas river bridge. A pipe bomb, found by a California Department of Fish and Game warden near the Salinas River bridge in Salinas, California forced the closure of Blanco and Reservation Road May 30. The Monterey County Sheriff's Office said the warden found the explosive device while walking along the Salinas River, patrolling for hunting and fishing violations. The warden discovered what appeared to be a pipe bomb along the waters edge and notified the sheriff's office and roped off the area for safety. The county's bomb squad arrived on-scene in about 15 minutes. The 7-inch bomb was made of galvanized steel. It measured 1.5 inches in diameter with an externally threaded-end capped pipe. Officers rendered it safe with remote disruption tools. The California Highway Patrol assisted the squad by closing Blanco Road between Cooper Road and Reservation Road for about 15 minutes. Officers spent a few hours searching the river bed looking for any evidence. The remnants of the device were collected for analysis. Source:

<http://www.kionrightnow.com/story/14751529/possible-explosive-device-near-salinas-river>

(New York) Final JFK terror plot suspect convicted. The last suspect in a scheme to blow up jet fuel tanks at New York's John F. Kennedy International Airport in Queens has been convicted of participating in the failed plot. The man was convicted May 26 of several conspiracy counts. Two other people were convicted in 2010 of conspiracy charges and are serving life in prison. A fourth pleaded guilty to providing material support and was sentenced to 15 years. The man's case was separated from the others after he fell ill. Prosecutors argued the men wanted to kill thousands of people and cripple the American economy by using explosives to blow up the fuel tanks and the underground pipelines that run through an adjacent Queens neighborhood. Defense attorneys argued the case was created by government intervention. The man, an imam from Trinidad, faces life in prison. Source: <http://newyork.cbslocal.com/2011/05/27/final-jfk-terror-plot-suspect-convicted/>

WATER AND DAMS

(Michigan) 2.6 billion gallons of sewage dumped into Lake St. Clair. About 2.3 billion gallons of sewage was dumped into Lake St. Clair and other local waterways in Michigan due to the recent heavy rains, forcing the continued closure of three local beaches. Metro Beach in Harrison Township and the two St. Clair Shores beaches — at Memorial Park and Blossom Heath — are off-limits because of high E. coli bacteria levels. The Macomb County Health Department is now reporting that the heavy rains which commenced May 25 on caused sewer systems to overflow in 15 different locations along the lakeshore, the Clinton River and the river's tributaries. Of the total pollution discharged, at least 2 million gallons consisted of raw sewage. The volume of untreated sewage that was spewed into the waterways starting May 25 could rise dramatically once all the figures are in. At the George W. Kuhn Drain in Madison Heights (formerly the Twelve Towns Drain), Oakland County officials sent 1.6 billion gallons of treated sewage gushing into the Red Run Drain over a 54-hour period on May 25-27. Officials said the discharges are

UNCLASSIFIED

necessary to prevent sewer backups that would flood thousands of home basements. As of June 1, the county has experienced 3.6 billion gallons of pollution discharges in 2011. Source: <http://www.dailytribune.com/articles/2011/06/01/news/doc4de6c9f1a3499027023942.txt?viewmode=fullstory>

NORTH DAKOTA HOMELAND SECURITY CONTACTS

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

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

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

UNCLASSIFIED