

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](#)

[Emergency Services](#)

[Regional](#)

[Energy](#)

[National](#)

[Food and Agriculture](#)

[International](#)

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

[Banking and Finance Industry](#)

[Information Technology and
Telecommunications](#)

[Chemical and Hazardous Materials
Sector](#)

[Public Health](#)

[Commercial Facilities](#)

[Transportation](#)

[Communications Sector](#)

[Water and Dams](#)

[Critical Manufacturing](#)

[North Dakota Homeland Security
Contacts](#)

[Defense Industrial Base Sector](#)

UNCLASSIFIED

UNCLASSIFIED

NORTH DAKOTA

(National) New federal rules are set for fracking. The U.S. Department of the Interior along with the U.S. President's administration released March 20 new federal regulations on hydraulic fracturing which include allowing government workers to inspect and validate concrete barriers that line fracking wells, and a requirement for companies to disclose the chemicals used during the fracturing process within 30 days of completing fracking operations, among other rules set to go into effect in June.

<http://www.nytimes.com/2015/03/21/us/politics/obama-administration-unveils-federal-fracking-regulations.html>

(North Dakota) 1 dead, 2 injured after icy roads in western N.D. lead to three accidents on I-94. A portion of eastbound Interstate 94 near Richardton was shut down for approximately 14 hours March 22 after the roadway was blocked by 3 accidents that were caused by icy road conditions.

<http://www.thedickinsonpress.com/news/local/3705660-1-dead-2-injured-after-icy-roads-western-nd-lead-three-accidents-i-94>

(North Dakota) Halliburton to close Minot facility. Officials at Halliburton reported March 24 that operations will be suspended at its Minot site and that the facility will be closed effective April 1 due to changing busineeds from consumers. <http://www.thedickinsonpress.com/news/north-dakota/3707037-halliburtonclose-minot-facility>

(North Dakota) Man arrested in fatal Bottineau County shooting. Bottineau County officials arrested a suspect in the March 24 shooting at the Turtle Mountain Pork hog farm near Landa that left two people dead. Area schools went into lockdown while authorities investigated the incident.

<http://www.wdaz.com/news/3706750-update-man-arrested-fatal-bottineau-county-shooting>

(North Dakota) Fargo police want access to business, residential cameras. A new program unveiled Tuesday allows residents and business owners here to give police access to their video cameras. Police say they'd like to use the footage to solve and deter crime. <http://www.inforum.com/news/crime/3707101-fargo-police-want-access-business-residential-cameras>

UNCLASSIFIED

UNCLASSIFIED

REGIONAL

(South Dakota) County officials reopen state Highway 11 near Corson. State Highway 11 from Interstate 90 to north of Corson was closed for several hours March 26 because the roadway was blocked by fire trucks and personnel that were battling a blaze at the site of a former grain elevator that started as a controlled burn and spread to an adjacent structure.

<http://www.mitchellrepublic.com/news/state/3708825-county-officials-reopen-state-highway-11-near-corson>

(Minnesota) 1 dead in Woodbury senior living fire. A March 27 fire at the Woodbury Senior Living apartments in Minnesota left 1 person dead and at least 2 others hospitalized while 71 residents were evacuated for nearly 4 hours. Officials worked to move 9 – 10 residents to other portions of the Woodbury Health Care Center after the fire caused extensive smoke and water damage to their apartments. <http://www.kare11.com/story/news/2015/03/27/1-dead-in-woodbury-senior-living-fire/70532132/>

NATIONAL

(National) DOE to look at separate disposal of defense, commercial nuclear waste. The U.S. President authorized the U.S. Department of Energy (DOE) to begin developing a national repository for high-level radioactive defense waste March 24, and the DOE announced plans to start with one or more temporary storage facilities for commercial waste at sites volunteered with State and community consent. http://www.tri-cityherald.com/2015/03/24/3477644_doe-to-look-at-separate-disposal.html

(Illinois) Two U.S. men arrested in plot to attack Illinois military base: Justice Department. The U.S. Department of Justice announced March 26 that a Chicago-area U.S. Army National Guard soldier and his cousin were arrested and charged for conspiring to support Islamic State (ISIS) in a plot which included an attack on an Illinois National Guard facility. Both men had met with an undercover FBI agent and discussed plans to attack the facility where the U.S. Army National Guard specialist was training. <http://www.msn.com/en-us/news/us/two-us-men-arrested-in-plot-to-attack-illinois-military-base-justice-department/ar-AAa3au4>

UNCLASSIFIED

UNCLASSIFIED

INTERNATIONAL

(International) Germanwings Crash Investigators Sorting Through Physical and Psychological Clues. As aviation experts in the French Alps piece together the shattered fragments of the Germanwings jetliner that crashed there on Tuesday, investigators here are engaged in a task that is at least as challenging: trying to understand what drove Andreas Lubitz, who was at the controls, to the apparent decision to fly the plane into a mountainside.

<http://www.nytimes.com/2015/03/30/world/europe/germanwings-plane-crash-pilot-andreas-lubitz.html?rref=world/europe&module=Ribbon&version=context®ion=Header&action=click&contentCollection=Europe&pgtype=article>

(International) Troops notified their names are on Islamic State kill list. A Pentagon spokesperson reported March 23 that U.S. military units notified members whose names and addresses were included on a “kill list” allegedly created by the Islamic State Hacking Division, who claim to be sympathizers of the Islamic State terrorist group. Officials stated that the personal information of former and current military personnel was pulled from publicly available sources and was not attributed to a data breach.

<http://www.usatoday.com/story/news/nation/2015/03/23/pentagon-response-islamic-state-kill-list/70335810/>

(International) U.S. offers \$3 million reward for alleged Russian cybercriminals. The U.S. Department of State announced rewards totaling \$3 million March 26 for information leading to the arrest or conviction of 2 Russian nationals believed to be key members in the Carder.su operation, in which participants created and trafficked identification documents and payment cards and perpetrated financial fraud and identity theft, causing losses of at least \$50 million. Thirty members involved in the operation have been convicted and 25 remaining are fugitives or pending trial. <http://www.securityweek.com/us-offers-3-million-reward-alleged-russian-cybercriminals>

BANKING AND FINANCE INDUSTRY

(International) Dridex banking malware dodges detection with run-on-close macros. Security researchers at Proofpoint discovered that the Dridex banking

UNCLASSIFIED

UNCLASSIFIED

malware is using run-on-close macros in infected Microsoft Office documents to avoid detection by malware sandboxes and antivirus software. The Dridex malware was previously linked to attacks targeting banking customers in the U.S., Canada, and the U.K. <http://www.securityweek.com/dridex-banking-malware-dodges-detection-run-close-macros>

(International) PayPal to pay \$7.7 million in U.S. Treasury sanctions case. PayPal agreed to pay \$7.7 million March 25 to settle U.S. Department of the Treasury charges for failing to adequately screen transactions for several years, resulting in 486 violations of sanctions programs against countries including Iran, Cuba, and Sudan, as well as for a specific Turkish national on the sanctions blacklist that had been tied to proliferators of weapons of mass destruction.

<http://www.reuters.com/article/2015/03/25/us-usa-treasury-ebay-idUSKBN0ML28620150325>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

(Texas) Cleanup underway after train hauling chemicals derails. Twelve cars of a Burlington Northern Santa Fe (BNSF) Railway train derailed near Valley Mills, Texas, March 21 causing about 7,000 gallons of dimethylformamide, an industrial solvent, to spill from a tanker car. A HAZMAT team worked to contain the spill, while crews removed the derailed cars and repaired damaged track and a bridge.

<http://www.kwtx.com/home/headlines/BREAKING-Train-297140101.html>

(California) Health advisory lifted after "release" at Dow Chemical plant in Pittsburg. Contra Costa County issued a Level 2 health advisory March 27 for Pittsburg and Antioch after an estimated several thousand pounds of chemicals were released into the air due to a machinery malfunction at the Dow Chemical facility in Pittsburg. No injuries were reported and the advisory was lifted almost 3 hours later. <http://www.nbcbayarea.com/news/local/Health-Advisory-Lifted-After-Release-at-Dow-Chemical-Plant-in-Pittsburg-297779241.html>

COMMERCIAL FACILITIES

(Florida) Bomb threat at Ocala Mall. The Paddock Mall in Ocala was closed for more than 3 hours March 24 after an individual phoned the police and claimed to have planted 6 bombs at the mall that he planned to detonate. The mall was

UNCLASSIFIED

UNCLASSIFIED

cleared to reopen after nothing suspicious was found.

<http://www.mygtn.tv/story/28599450/bomb-threat-at-ocala-mall>

(International) Vulnerability found in popular hotel routers. Cylance researchers discovered an authentication flaw in the firmware of several models of InnGate routers that are commonly used by hotels and convention centers that can be exploited to distribute malware to guests, monitor and record data sent over the network, and possibly gain access to a hotel's reservation and keycard system. The vulnerability was detected in 277 devices in 29 countries, including more than 100 devices located in the U.S. <http://www.scmagazine.com/vulnerability-discovered-in-inngate-routers/article/405708/>

COMMUNICATIONS SECTOR

(New Mexico) Hostage threat at Las Cruces radio station building a "false alarm". The Bravo Mic Communications building in Las Cruces which houses at least 2 radio stations and a marketing company was evacuated March 23 after a caller reportedly stated that he was armed and was going to take hostages inside the building. Authorities deemed the threat to be a false alarm and the building was cleared to reopen after about 4 hours. <http://www.kvia.com/news/1-person-in-standoff-with-police-at-las-cruces-radio-station-building/31974644>

CRITICAL MANUFACTURING

(International) Ford recalls over 220,000 vehicles in North America for three issues. Ford Motor Co., announced March 25 a recall for 194,484 model years 2011 – 2013 Ford Explorer SUVs and Police Interceptor utility vehicles in the U.S. for a spring issue that could cause doors to unlatch in a side-impact crash, and a recall for 1,586 model years 2013 – 2015 Lincoln MKT limo and hearse vehicles for a vacuum pump relay issue that could cause an underhood fire. The company also included 6,472 model years 2011 – 2013 F-Series Super Duty ambulance vehicles and a 6.7-liter diesel engine version from model years 2014 – 2015 in the recall due to an exhaust gas temperature sensor issue that could fail to detect a high temperature condition. <http://www.msn.com/en-us/news/us/ford-recalls-over-220000-vehicles-in-north-america-for-three-issues/ar-AA9YYKI>

UNCLASSIFIED

UNCLASSIFIED

DEFENSE/ INDUSTRY BASE SECTOR

(National) U.S., Lockheed fixing software glitch with GPS satellites. Lockheed Martin Corp announced that the company is working to resolve a technical error disclosed by the U.S. Air Force March 22 that involves the ground-based control system used to index some messages transmitted by global positioning system (GPS) IIF satellites built by Boeing Co. A “workaround” was put in place to avoid further errors while the company and the Air Force develop a full software correction for the flaw that had gone unnoticed since 2013.

<http://www.reuters.com/article/2015/03/23/usa-airforce-satellite-idUSL2N0W00EW20150323?feedType=RSS&feedName=everything&virtualBrandChannel=11563>

EMERGENCY SERVICES

(National) DHS issues draft guidance for disaster information sharing following earthquake exercise. DHS’ Science and Technology Directorate published draft guidance containing Essential Elements of Information (EIs) for information sharing in the event of an earthquake in Midwest and Southern States. The EIs were created based on lessons learned from a June 2014 planning exercise and instructs first responders on how to request and acquire mutual aid, among other recommendations. <http://www.fiercehomelandsecurity.com/story/dhs-issues-draft-guidance-disaster-information-sharing-following-earthquake/2015-03-23>

ENERGY

(International) Leaked full version of NanoCore RAT used to target energy companies. Security researchers at Symantec identified that approximately 40 percent of systems infected by the widely-available NanoCore remote access trojan (RAT) delivered by a malicious rich text format (RTF) or Microsoft Word file that exploits an old vulnerability in Windows Common Controls ActiveX component since January 2014 were in the U.S., while cyber-criminals have been employing the malware in targeted attacks on energy companies in Asia and the Middle East since March 6. <http://news.softpedia.com/news/Leaked-Full-Version-of-NanoCore-RAT-Used-to-Target-Energy-Companies-476606.shtml>

UNCLASSIFIED

UNCLASSIFIED

(West Virginia) Patriot Coal idles two mines in West Virginia. Patriot Coal announced March 23 that coal production at its Paint Creek Complex facility in West Virginia was idled effective March 22 due to a lesser demand for coal and high inventory levels. Coal production is scheduled to resume in 3 – 4 weeks while processing and shipping of coal to customers from stockpiles will continue.
<http://www.wkyt.com/wymt/home/headlines/Patriot-Coal-idles-two-mines-in-West-Virginia-297280981.html>

FOOD AND AGRICULTURE

(National) Twin City Foods, Inc. recalls frozen Cadia Organic Cut Spinach, Meijer Organics Chopped Spinach, Wild Harvest Organic Cut Leaf Spinach, and Wegmans Organic Just Picked Spinach because of possible health risk. The U.S. Food and Drug Administration announced March 24 that Twin City Foods, Inc., recalled Cadia Organic Cut Spinach, Meijer Organics Chopped Spinach, Wild Harvest Organic Cut Leaf Spinach, and Wegmans Organic Just Picked Spinach after Coastal Green Vegetable Company LLC, a supplier for the products, initiated a recall for bulk spinach due to possible *Listeria monocytogenes* contamination. The recalled products were distributed to warehouses in several States.
<http://www.fda.gov/Safety/Recalls/ucm439755.htm>

(Idaho) Agency: Monsanto to pay \$600K in fines for not reporting chemical releases at Idaho plant. Monsanto Co., entered into an agreement March 26 with the U.S. Environmental Protection Agency and the U.S. Department of Justice and agreed to pay \$600,000 in penalties to resolve charges that the company failed to report hundreds of uncontrolled releases of toxic chemicals at its Soda Springs facilities between 2006 and 2009.
<http://www.tribtown.com/view/story/b96261abeb57432d9ebf95692e78ab77/ID-Monsanto-Chemical-Releases>

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Vermont) Data breach reported by the Vermont Department of Labor. The Vermont Department of Labor released March 20 that a former employee intentionally obtained the names and Social Security numbers of at least 39 individuals from the department's unemployment database during regular work

UNCLASSIFIED

UNCLASSIFIED

duties February 24. Authorities seized the employee's personal computer devices and copies of documents as part of an ongoing investigation and found Social Security numbers for an additional 41 individuals in the former worker's possession. <http://www.vermontpressbureau.com/data-breach-reported-by-the-vermont-department-of-labor/>

(New Jersey) School district 'bitcoin hostage' situation continues; FBI, Homeland Security investigating. Swedesboro-Woolwich School District in New Jersey is investigating an attack on its computer network which caused them to postpone exams after discovering March 21 that their entire network was down when they received a ransom message requesting 500 bitcoins. The district restored encrypted files and is in the process of restoring its servers to remove the malware after email communications, online resources for an exam, Excel spreadsheets, and Adobe PDF files were breached as well.

http://www.nj.com/gloucester-county/index.ssf/2015/03/school_district_bitcoin_hostage_situation_continue.html

(Alaska) Fairbanks city website repaired after hackers attack. Officials reported March 25 that hackers took down the Fairbanks city government's Web site for about 4 hours March 24 and replaced it with a message from the group. The city announced that no information was accessed or breached in the attack.

http://www.newsminer.com/news/local_news/fairbanks-city-website-repaired-after-hackers-attack/article_44a5e7a8-d2c2-11e4-bf00-c32b132d5792.html

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

(International) New point-of-sale malware PoSeidon exfiltrates card data to Russian domains. Security researchers from Cisco Systems' Talos Security Intelligence and Research Group discovered that cybercriminals are using a new point-of-sale (PoS) malware family dubbed PoSeidon that infects systems via a binary file and uses a memory scraping technique to retrieve and clone Discover, American Express, MasterCard, and Visa card information before delivering it to command and control (C&C) servers in Russia. The malware contains routines to ensure persistence regardless of restart or user log-off.

<http://news.softpedia.com/news/New-Point-of-Sale-Malware-PoSeidon-Exfiltrates-Card-Data-to-Russian-Domains-476498.shtml>

UNCLASSIFIED

UNCLASSIFIED

(International) Over 15,000 vulnerabilities detected in 2014: Secunia. Secunia released its annual vulnerability review and found that 15,435 vulnerabilities across 3,870 applications from 500 vendors were discovered in 2014, 11 percent of which were considered highly critical while .3 percent were rated extremely critical. The report also states that over 60 percent of attacks occurred through remote networks making it the most common attack vector, among other trends. <http://www.securityweek.com/over-15000-vulnerabilities-detected-2014-secunia>

(International) Alleged hacker brought to N.J. on charges of large-scale identity theft. A Romanian national was extradited to the U.S. March 20 to face charges that he allegedly oversaw a large-scale computer hacking scheme in which he breached computer systems of retailers, medical offices, security companies, and individuals' online accounts to obtain several thousand user names, passwords, and payment card numbers from 2011 – 2014, including 10,000 credit and debit cards from one victim alone. http://www.nj.com/news/index.ssf/2015/03/alleged_hacker_brought_to_nj_on_charges_of_large-s.html

(International) Cisco Small Business IP phones vulnerable to eavesdropping. Cisco Systems confirmed that its Small Business SPA 300 and 500 series IP phones with firmware version 7.5.5 or older, contain flaws in authentication settings that could allow attackers to listen in on phone audio streams or make calls remotely by sending crafted extensible markup language (XML) requests to the affected device. The company is reportedly working on a patch to address the vulnerability. <http://www.net-security.org/secworld.php?id=18119>

(International) DDoS attackers distracting security teams with shorter attacks: Corero Networks. Corero Network Security reported in their quarterly trends and analysis report that 96 percent of distributed denial-of-service (DDoS) attacks against its customers in the fourth quarter of 2014 were less than 30 minutes in length and 79 percent used less than 5 gigabits per second (Gbps) of peak bandwidth, indicating that attacks were becoming more difficult to detect and were likely intended to partially saturate networks and distract security teams while leaving enough bandwidth for subsequent attacks to infiltrate networks and access sensitive information. <http://www.securityweek.com/ddos-attackers-distracting-security-teams-shorter-attacks-corero-networks>

UNCLASSIFIED

UNCLASSIFIED

(International) Half of all Android devices vulnerable to installer hijacking attacks. Security researchers at Palo Alto Networks discovered that a critical Android vulnerability discovered over a year ago and dubbed “Android Installer Hijacking”, can allow attackers to completely compromise devices by changing or replacing seemingly legitimate applications with malware during installation without users’ knowledge. The flaw affects all devices running Android versions 4.2 and earlier, and some running version 4.3. <http://www.net-security.org/secworld.php?id=18133>

PUBLIC HEALTH

(National) FDA approves Abiomed’s blood pump device. The U.S. Food and Drug Administration stated March 23 that it approved Abiomed Inc.’s Impella 2.5 System, a miniature blood pump system that can be used during angioplasty and stenting to maintain heart function and circulation during high-risk procedures. <http://www.reuters.com/article/2015/03/23/us-abiomed-fda-idUSKBN0MJ2D020150323>

(Indiana) Governor approves short-term needle exchange in HIV epidemic. The governor of Indiana declared a health emergency March 26 in southeastern Indiana after the Indiana State Department of Health recorded 79 HIV cases connected to intravenous drug use in Scott County. The governor also announced that the State would sanction a short-term needle-exchange program to last for 30 days to help address the epidemic. <http://www.indystar.com/story/news/politics/2015/03/25/gov-pence-visit-indiana-county-hiv-outbreak/70427432/>

TRANSPORTATION

(Colorado) Train derails in Weld County. A stretch of railroad tracks near Hudson, Colorado, suffered extensive damage and was closed indefinitely March 22 after at least 27 freight cars of a Burlington National Santa Fe Railway Co. (BNSF) train derailed and spilled an unspecified amount of coal. Crews used front-end loaders to clear the scene, and no environmental impact was reported. <http://www.9news.com/story/news/2015/03/22/train-derails-in-weld-county/25181437/>

UNCLASSIFIED

UNCLASSIFIED

(Louisiana) Officer shoots man who attacked TSA agents at New Orleans airport.

A man armed with a machete and wasp spray attacked several Transportation Security Administration (TSA) agents in Concourse B at the Louis Armstrong New Orleans International Airport March 20 before he was fatally shot by a law enforcement officer, while a TSA agent suffered non-life-threatening injuries when she was accidentally struck by the officer's gunfire. The concourse was secured while authorities investigated the incident and was scheduled to reopen March 21. <http://www.reuters.com/article/2015/03/21/us-usa-shooting-airport-idUSKBN0MH01S20150321>

WATER AND DAMS

(Vermont) Vermont city losing 600K-plus gallons of water daily in leak. Officials are investigating the source of a leak that is causing the loss of more than 600,000 gallons of water a day in Rutland, Vermont, and has been affecting customers' water pressure since March 21. The city's Public Works Commissioner reported that workers are inspecting valves, hydrants, and vacant buildings, and announced a plan to isolate and check 3 transmission lines running from a water plant into the city. <http://abcnews.go.com/US/wireStory/vermont-city-losing-600k-gallons-water-daily-leak-29892445>

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:

Darin Hanson, ND Division of Homeland Security dthanson@nd.gov, 701-328-8165

UNCLASSIFIED