



## Daily Open Source Infrastructure Report 11 October 2016

### Top Stories

- The governor of Florida reported October 7 that roughly 600,000 homes across the State were without power due to Hurricane Matthew. – *Reuters* (See item [1](#))
- Around 60 homes in Glen Rose, Texas, were evacuated October 6 after a semi-truck jackknifed and spilled 8,000 gallons of gasoline and diesel fuel on Highway 144. – *KTVT 11 Fort Worth* (See item [2](#))
- Six U.S. Army soldiers and two civilian co-conspirators were indicted October 5 for their roles in a more than \$1 million scheme where they stole and sold sensitive U.S. Army equipment from Fort Campbell in Hopkinsville, Kentucky, to anonymous Internet buyers in Russia, China, and other countries. – *U.S. Department of Justice* (See item [14](#))
- The owner of RASKO, a mall kiosk business, pleaded guilty October 6 to his role in a \$14 million immigration and money laundering scheme where he and co-conspirators recruited and sent over 140 foreign nationals to the U.S. to work at one of RASKO's locations from 2011 – 2016. – *U.S. Attorney's Office, Eastern District of Virginia* (See item [22](#))

---

### Fast Jump Menu

#### PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

#### SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

#### SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

#### FEDERAL and STATE

- [Government Facilities](#)
- [Emergency Services](#)

## Energy Sector

1. *October 7, Reuters* – (Florida) **Some 600,000 Florida homes without power due to hurricane: governor.** The governor of Florida reported October 7 that roughly 600,000 homes across the State were without power due to Hurricane Matthew and more outages were expected as the storm continues to move north along Florida's east coast.  
Source: <http://www.reuters.com/article/us-storm-matthew-power-idUSKCN1271J2>
2. *October 6, KTVT 11 Fort Worth* – (Texas) **18-wheeler crash & fuel spill causes evacuations in Glen Rose.** Around 60 homes in Glen Rose, Texas, were evacuated October 6 after a semi-truck jackknifed and spilled 8,000 gallons of gasoline and diesel fuel on Highway 144. HAZMAT crews responded to the scene to contain the fuel spill.  
Source: <http://dfw.cbslocal.com/2016/10/06/18-wheeler-crash-fuel-spill-causes-evacuations-in-glen-rose/>

## Chemical Industry Sector

3. *October 6, Hutchinson News* – (Kansas) **Three people in serious condition after chemical spill in Hesston.** A GVL Polymers, Inc. plant in Hesston, Kansas, was evacuated and closed until further notice October 6 following a spill involving an isocyanate product that sent six individuals to the hospital. Crews were working to clean up the chemical.  
Source: [http://www.hutchnews.com/news/courts\\_and\\_cops/updated-three-people-in-serious-condition-after-chemical-spill-in/article\\_6a27f4b6-2df7-56ab-89c8-4d6c3e29cab2.html](http://www.hutchnews.com/news/courts_and_cops/updated-three-people-in-serious-condition-after-chemical-spill-in/article_6a27f4b6-2df7-56ab-89c8-4d6c3e29cab2.html)

## Nuclear Reactors, Materials, and Waste Sector

Nothing to report

## Critical Manufacturing Sector

4. *October 6, U.S. Department of Labor* – (New Jersey) **New Jersey aluminum company continues to expose employees to machine hazards – resulting in working injuries, amputations.** The Occupational Safety and Health Administration cited Allstate Can Corporation with 1 willful and 4 serious safety violations September 16 after an investigation at the Parsippany, New Jersey facility revealed that the company failed to implement a hearing conservation program, failed to provide annual hearing tests for all employees exposed to high noise levels, and exposed employees to excessive noise in the production area, among other violations. Proposed penalties total \$104,220.  
Source:  
[https://www.osha.gov/pls/oshaweb/owadisp.show\\_document?p\\_table=NEWS\\_RELEASES&p\\_id=33267](https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=33267)

For another story, see item [3](#)

## Defense Industrial Base Sector

Nothing to report

## Financial Services Sector

5. *October 6, U.S. Attorney's Office, District of Massachusetts* – (National) **Boston man charged with identity theft in scheme to defraud retirement accounts.** A Boston resident was charged October 6 for his role in an identity theft scheme where he and a co-conspirator who worked as a customer service employee at Mercer, Inc. allegedly stole the personal information and bank account numbers from roughly 270 retirement accounts managed by Mercer, Inc. in order to withdraw money from the accounts from February 2014 – April 2014. The charges allege that the stolen retirement account information was used to load a prepaid card with almost \$20,000 in illicitly obtained funds, which the defendant used for personal expenses.  
Source: <https://www.justice.gov/usao-ma/pr/boston-man-charged-identity-theft-scheme-defraud-retirement-accounts>
6. *October 6, U.S. Attorney's Office, District of Maryland* – (Maryland; Washington, D.C.) **Federal indictment charges four conspirators in fraudulent credit card scheme.** Four individuals were charged October 6 for their roles in a fraudulent credit card scheme where the group allegedly stole the personal information of at least 33 victims in order to apply for and obtain credit cards, which were used to purchase merchandise and gift cards worth more than \$135,000 from October 2014 – July 2016.  
Source: <https://www.justice.gov/usao-md/pr/federal-indictment-charges-four-conspirators-fraudulent-credit-card-scheme>

## Transportation Systems Sector

7. *October 7, KTRK 13 Houston* – (Texas) **Driver slams into stalled vehicle, dies on Gulf Fwy.** Inbound lanes of the Gulf Freeway in Houston were closed for several hours October 6 – October 7 while crews worked to clear the wreckage from a two-vehicle crash that killed one person and injured five others.  
Source: <http://abc13.com/traffic/gulf-fwy-inbound-at-monroe-closed-after-deadly-crash/1543581/>
8. *October 6, WXIX 19 Newport* – (Kentucky) **AA Highway closed in Wilder after crash involving Rumpke truck.** AA Highway in Wilder, Kentucky, was shut down in both directions for several hours October 6, while crews worked to clear the wreckage from a three-vehicle crash that injured one person.  
Source: <http://www.fox19.com/story/33337205/aa-highway-shut-down-after-accident-involving-rumpke-truck>
9. *October 6, Orange County Register* – (California) **Motorcyclist dies in Ortega Highway crash near San Juan Capistrano.** A portion of Ortega Highway near San Juan Capistrano, California, was closed for about 2 hours October 6 following a collision involving a motorcycle that killed one person.

Source: <http://www.ocregister.com/articles/crash-731353-highway-traffic.html>

For additional stories, see items [2](#) and [11](#)

## **Food and Agriculture Sector**

10. *October 6, WFMZ 69 Allentown* – (Pennsylvania) **Firefighters from 3 counties battle barn blaze in Berks.** A three-alarm fire at a farm in Marion Township, Pennsylvania, October 5 – October 6 destroyed a barn housing dairy cows and critically injured two cows. The cause of the fire remains under investigation.

Source: <http://www.wfmz.com/news/news-regional-berks/firefighters-respond-to-marion-township-barn-fire/41987838>

For another story, see item [3](#)

## **Water and Wastewater Systems Sector**

11. *October 6, Great Falls Tribune; National Weather Service* – (Montana) **Heavy rains flooding northeastern Montana.** Residents from Hinsdale to Nashua in northeastern Montana were advised October 6 to move their livestock and equipment away from the floodplain and seek shelter elsewhere after 3 – 9 inches of rain and snowfall caused the Milk River and its tributaries to overflow, flooding lowlands and washing out roads in the region. Officials reported the heavy rainfall also caused a stock dam east of Highway 191 to break.

Source: <http://www.greatfallstribune.com/story/news/local/2016/10/06/heavy-rains-flooding-northeastern-montana/91671396/>

## **Healthcare and Public Health Sector**

12. *October 6, WJCL 22 Savannah* – (South Carolina) **Beaufort Memorial Hospital evacuating patients, closing emergency room.** Beaufort Memorial Hospital in Beaufort, South Carolina, began evacuating approximately 70 patients and closed its emergency room October 6 in preparation of Hurricane Matthew.

Source: <http://www.wjcl.com/article/beaufort-memorial-hospital-evacuating-patients-closing-emergency-room/4965274>

## **Government Facilities Sector**

13. *October 7, KRDO 13 Colorado Springs* – (Colorado) **Beulah Hill Fire now 75% contained, 5,232 acres burned.** Crews reached 75 percent containment October 6 of the 5,232-acre Beulah Hill Fire burning in Pueblo County, Colorado, prompting officials to lift evacuation orders for residents from 3R Road, south of Highway 78, and the Signal Mountain subdivision. The fire destroyed 8 homes and 16 outbuildings.

Source: <http://www.krdo.com/news/pueblo/beulah-hill-fire-now-75-contained-5232-acres-burned/108229155>

14. *October 6, U.S. Department of Justice* – (International) **Six Fort Campbell soldiers and two others charged with stealing and selling sensitive military equipment.** Six U.S. Army soldiers and two civilian co-conspirators were indicted October 5 for their roles in a more than \$1 million scheme where the group stole sensitive U.S. Army equipment from Fort Campbell in Hopkinsville, Kentucky, and sold it to anonymous Internet buyers in Russia, China, Kazakhstan, and Mexico, among other countries. Source: <https://www.justice.gov/opa/pr/six-fort-campbell-soldiers-and-two-others-charged-stealing-and-selling-sensitive-military>

## **Emergency Services Sector**

Nothing to report

## **Information Technology Sector**

15. *October 7, SecurityWeek* – (International) **VMware patches directory traversal flaw in Horizon View.** VMware released versions 7.0.1, 6.2.3, and 5.3.7 of its Horizon View products for Microsoft Windows after a security researcher, dubbed “BrukOut” discovered the products were plagued with a flaw that could allow a remote attacker to carry out a directory traversal attack on the Horizon View Connection Server to access sensitive information. Source: <http://www.securityweek.com/vmware-patches-directory-traversal-flaw-horizon-view>
16. *October 7, SecurityWeek* – (International) **X.Org library flaws allow privilege escalation, DoS attacks.** The X.Org Foundation released patches addressing more than a dozen vulnerabilities in its client libraries, including an out-of-bounds memory read or write error flaw in libX11 versions 1.6.3 and earlier, an integer overflow issue on 32-bit systems in libXfixes versions 5.0.2 and earlier, and a denial-of-service (DoS) condition via out of boundary memory access or endless loops in XRecord versions 1.2.2 and earlier, among other vulnerabilities. X.Org reported most of the flaws exist because the client libraries trust the server to send correct protocol data and do not consider that the values could cause an overflow or other issues. Source: <http://www.securityweek.com/xorg-library-flaws-allow-privilege-escalation-dos-attacks>
17. *October 6, SecurityWeek* – (International) **Cerber ransomware can now kill database processes.** Security researchers from BleepingComputer discovered a new variant of the Cerber ransomware family is able to kill many database processes before the encryption process begins by using a close\_process directive in the configuration file in order to encrypt the processes’ data files. The researchers also found Cerber switched to a four-character randomly generated extension and started scrambling the name of the encryption file, making it more difficult for victims to recover their data. Source: <http://www.securityweek.com/cerber-ransomware-can-now-kill-database-processes>

For another story, see item [20](#)

## Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

### Communications Sector

Nothing to report

### Commercial Facilities Sector

18. *October 6, WBRZ 2 Baton Rouge* – (Louisiana) **4 injured in apartment complex fire off of Essen Lane.** A 2-alarm fire at the Cobblestone apartment complex in Baton Rouge, Louisiana, October 6 destroyed 18 units, displaced 36 families, sent 3 people to an area hospital, and damaged 3 nearby buildings. The cause of the fire remains under investigation.  
Source: <http://www.wbrz.com/news/4-injured-in-apartment-complex-fire-off-of-essen-lane/>
19. *October 6, WITI 6 Milwaukee* – (Wisconsin) **“It was crazy:” Walmart store near Miller Park Way in West Milwaukee evacuated after bomb threats.** Authorities are investigating a series of five bomb threats that prompted a 2-hour evacuation of the Walmart store in West Milwaukee, Wisconsin, October 6.  
Source: <http://fox6now.com/2016/10/06/developing-walmart-store-near-miller-park-way-in-west-milwaukee-evacuated-after-bomb-threat/>
20. *October 6, Softpedia* – (International) **FastPOS malware abuses Windows Mailslots to steal POS data.** Trend Micro security researchers reported a point-of-sale (PoS) malware, dubbed FastPOS received updates and now uses a modular design with separate components, memory scrapper and keylogger, designed to infect Microsoft Windows computers running 32-bit and 64-bit systems, making the malware more efficient and more difficult to detect. The malware was spotted abusing Mailslots, a Windows mechanism used to store inter-process communications (IPC) in the computer’s random access memory (RAM) in order to avoid creating permanent files.  
Source: <http://news.softpedia.com/news/fastpos-malware-abuses-windows-mailslots-to-steal-pos-data-509006.shtml>
21. *October 6, San Francisco Bay City News* – (California) **Firefighters clean up small radioactive spill that prompted evacuations in Antioch.** Around 50 apartment units in about 8 apartment complexes in Antioch, California, were evacuated for roughly 3 hours October 6 after a radioactive material spilled at a construction site when a truck ran over a piece of equipment that contained cesium and americium. No injuries were reported and HAZMAT crews cleaned up the radioactive material.  
Source: <http://www.nbcbayarea.com/news/local/Contra-Costa-Fire-Investigate->

[Hazmat-Situation-at-Antioch-Construction-Site-396177381.html](#)

22. *October 6, U.S. Attorney's Office, Eastern District of Virginia* – (International) **Israeli owner of mall kiosk business pleads guilty to immigration and money laundering charges.** An Israeli national and owner of RASKO, a mall kiosk business, pleaded guilty October 6 to his role in a \$14 million immigration and money laundering scheme where he and co-conspirators identified, recruited, and sent over 140 foreign nationals to the U.S. to work at one of RASKO's locations in Virginia, Georgia, Pennsylvania, or New Jersey in violation of their visitor visa status from 2011 – 2016. The charges state the business owner routed several million dollars in sales proceeds to Israeli bank accounts that he controlled and spent the money on scheme-related expenses. Source: <https://www.justice.gov/usao-edva/pr/israeli-owner-mall-kiosk-businesses-pleads-guilty-immigration-and-money-laundering>

For another story, see item [3](#)

## **Dams Sector**

See item [11](#)



**Department of Homeland Security (DHS)**  
**DHS Daily Open Source Infrastructure Report Contact Information**

**About the reports** - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

**Contact Information**

Content and Suggestions:	Send mail to <a href="mailto:cikr.productfeedback@hq.dhs.gov">cikr.productfeedback@hq.dhs.gov</a> or contact the DHS Daily Report Team at (703) 942-8590
Subscribe to the Distribution List:	Visit the <a href="#">DHS Daily Open Source Infrastructure Report</a> and follow instructions to <a href="#">Get e-mail updates when this information changes</a> .
Removal from Distribution List:	Send mail to <a href="mailto:support@govdelivery.com">support@govdelivery.com</a> .

---

**Contact DHS**

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at [nicc@hq.dhs.gov](mailto:nicc@hq.dhs.gov) or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at [soc@us-cert.gov](mailto:soc@us-cert.gov) or visit their Web page at [www.us-cert.gov](http://www.us-cert.gov).

**Department of Homeland Security Disclaimer**

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.