Daily Open Source Infrastructure Report
25 March 2013

Top Stories

- DHS and ICS-CERT advised the energy, oil, water, and chemical industries to apply a patch to certain Siemens industrial control software that addresses a previously found vulnerability. – *Threatpost* (See item **1**)
- The brother of the Galleon Group founder found guilty of insider trading was indicted for allegedly being part of his brother's insider trading ring. – *New York Times* (See item **6**)
- Authorities issued a lock down of Marine Corps Base Quantico while searching for a marine that shot and killed two fellow marines. Officials lifted the lockdown after they found the suspect dead in an apparent suicide. – *CNN* (See item **18**)
- A report claimed a Washington, D.C. ambulance and 2 medic units were within a 4-mile radius of an officer that was struck and severely injured, but did not respond because fire stations failed to properly monitor for emergency calls. – *WRC 4 Washington D.C.* (See item **24**)

Fast Jump Menu

Energy Sector

1. *March 21, Threatpost* – (National) **DHS, ICS-CERT warn of Siemens HMI vulnerabilities.** DHS and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) advised the energy, oil, water, and chemical industries to use the newly patched Siemens industrial control software that addresses a previously found vulnerability.
   Source: http://threatpost.com/en_us/blogs/dhs-ics-cert-warn-siemens-hmi-vulnerabilities-032113

2. *March 19, WYTV 33 Youngstown* – (Ohio) **Colunbiana County well explosion caused by static electricity.** Officials reported a West Township oil well explosion that blew the cap the Atlas Energy well was caused by static electricity.
   Source: http://www.wytv.com/content/news/local/story/Columbiana-County-Well-Explosion-Caused-by-Static/rVYY9YwjC0aQ-B_1lVhYEg.cspx

[Return to top]

Chemical Industry Sector

See items **1** and **12**

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

3. *March 22, Denver Post* – (Colorado) **Cotter to brew uranium cocktail to clean tainted mine west of Denver.** The company that owns an abandoned uranium mine near Denver will use bioremediation to attempt to immobilize uranium in the water pumped from the mine. Currently, uranium-tainted water flows from the mine into a creek that feeds into Ralston Reservoir, where it has to undergo water treatment to be made safe to drink.
   Source: http://www.denverpost.com/environment/ci_22844964/cotter-brew-uranium-cocktail-clean-tainted-mine-west

4. *March 21, Associated Press* – (Illinois) **Unit 2 reactor shut down at Byron nuclear plant.** A cooling pump malfunction on the non-nuclear side of Byron Generating Station caused the Unit 2 reactor to be shut down.
   Source: http://www.news-gazette.com/news/politics-and-government/2013-03-21/unit-2-reactor-shut-down-byron-nuclear-plant.html

[Return to top]

Critical Manufacturing Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

Nothing to report

[Return to top]

Banking and Finance Sector

5. *March 22, Softpedia* – (International) **Website and mobile banking service of TD Bank disrupted by DDOS attack.** Canada-based Toronto-Dominion (TD) Bank experienced service interruptions to its Web site and mobile banking services caused by a distributed denial of service (DDoS) attack March 21.
   Source: http://news.softpedia.com/news/Website-and-Mobile-Banking-Service-of-TD-Bank-Disrupted-by-DDOS-Attack-339532.shtml

6. *March 21, New York Times* – (New York) **Brother of Galleon Group founder is indicted on insider trading charges.** The brother of the Galleon Group founder found guilty of insider trading was indicted for allegedly being part of his brother's insider trading ring.
   Source: http://dealbook.nytimes.com/2013/03/21/prosecutors-weigh-insider-trading-charges-against-raj-rajaratnams-brother/

7. *March 20, Santa Rosa Press Democrat* – (California) **FBI seeks 'Hoodie Bandit' suspected in Sonoma County bank robberies.** The FBI released photos of the suspect known as the "Hoodie Bandit", suspected of robbing three banks in Santa Rosa and Rohnert Park in February.
   Source:
   http://www.pressdemocrat.com/article/20130320/ARTICLES/130329955/1308/news?Title=FBI-seeks-Hoodie-Bandit-suspected-in-Sonoma-County-bank-robberies&tc=ar

[Return to top]

Transportation Sector

8. *March 21, U.S. Environmental Protection Agency* – (West Virginia) **West Virginia Department of Transportation settles alleged violations of underground storage tank regulations.** The West Virginia Department of Transportation (W.Va. DOT) agreed to pay $30,000 in a settlement with the U.S. Environnemental Protection Agency regarding alleged infractions of underground storage tank (UST) regulations at 10 facilities. W.Va. DOT will also improve Statewide UST monitoring procedures.
   Source:
   http://yosemite.epa.gov/opa/admpress.nsf/0/23F18A69747D50CF85257B350068BFEA

9. *March 21, Tampa Bay Times* – (Florida) **Traffic finally flows again after fiery**

collision on I-75. Two trucks collided and burst into flames causing damage to a 350 foot swath and backing up traffic for 10 miles on Interstate 75 near Wesley Chapel. Emergency crews spent several hours repairing the damage before reopening lanes.
Source: http://blogs.tampabay.com/news/publicsafety/accidents/two-trucks-collide-on-interstate-75-closing-southbound-lanes/2110372For additional stories, see items

[Return to top]

Agriculture and Food Sector

10. *March 22, Associated Press* – (Michigan) **Saginaw County herd quarantined, cow had bovine TB.** Authorities in Michigan confirmed a cow had bovine tuberculosis at a Saginaw County dairy farm and quarantined the herd to conduct further tests on all the animals.
Source: http://www.wnem.com/story/21765297/saginaw-county-herd-quarantined-cow-had-bovine-tb

[Return to top]

Water Sector

11. *March 21, Bangor Daily News* – (Maine) **Portland agrees to more than $53,000 in federal penalties for discharging sewage in waterways.** The city of Portland settled on a final penalty of $53,000 with the U.S. Environmental Protection for discharging untreated sewage into waterways for several years.
Source: http://bangordailynews.com/2013/03/21/news/portland/portland-agrees-to-more-than-53000-in-federal-penalties-for-discharging-sewage-in-waterways/

For additional stories, see items **1** and **3**

[Return to top]

Public Health and Healthcare Sector

12. *March 21, Southern California City News Service* – (California) **Norco: No injuries reported after chemical spill at medical center.** Patients and staff were evacuated from DaVita Dialysis in Norco after a chemical spill March 21. Hazmat crews worked to clean the area where the spillage occurred as patients were temporarily relocated.
Source: http://www.swrnn.com/2013/03/21/norco-no-inuries-reported-after-chemical-spill-at-medical-center/

13. *March 21, WZVN 7 Naples* – (Florida) **Children's medical records dumped.** Medical records of 13 children were found inside a dumpster behind the Health Care Network of Southwest Florida. The company stated they will notify the patients affected as well as re-evaluate their policies and retrain employees on the proper disposal of records.
Source: http://www.abc-7.com/story/21760378/nbc2-exclusive-childrens-medical-records-dumped#.UUxXyRzFVKA

14. *March 21, Norristown Times Herald* – (Pennsylvania) **Patient sets off fire alarm, threatens staff at Mercy Suburban Hospital, East Norriton.** A patient at Mercy Suburban Hospital in East Norriton was subdued after he set off a fire extinguisher and used a piece of wood to threaten nurses. The patient discharged the extinguisher, covering an entire floor with fumes, which led to the evacuation of a number of patients to other wings of the hospital.
Source: http://www.timesherald.com/article/20130321/NEWS/130329854/patient-sets-off-fire-alarm-threatens-staff-at-mercy-suburban-hospital-east-norriton-

[Return to top]

Government Facilities Sector

15. *March 22, Elkins Inter-Mountain; Upshur Bureau Chief* – (West Virginia) **Lewis County schools cleared after bomb threat.** Lewis County High School was evacuated and eventually dismissed after a March 21 bomb threat prompted by a student. It was the fourth such incident at an area school during the week of March 18.
Source: http://www.theintermountain.com/page/content.detail/id/560127/Lewis-County-schools-cleared-after-bomb-threat.html?nav=5014

16. *March 22, WTXL 27 Tallahassee* – (Florida) **Security breach in TCC's computer system.** Tallahassee Community College will notify roughly 3,300 individuals affected by an internal security breach when unauthorized access was obtained into their computer systems. College officials were informed of the breach by federal officers after a man was convicted of submitting false claims to the Internal Revenue Service.
Source: http://www.wtxl.com/news/local/tcc-computer-system-hacked/article_6083485a-92f3-11e2-b778-001a4bcf6878.html

17. *March 22, Columbus Dispatch* – (Ohio) **Jackson school board member guilty in threats.** A long-term member of the Jackson City Schools Board of Education was found guilty March 20 for sending threatening letters to several educators and other school-board members in the southeastern Ohio district in November and December 2009.
Source: http://www.dispatch.com/content/stories/local/2013/03/21/school-board-member-convicted.html

18. *March 22, CNN* – (Virginia) **'A long night' at marine base; 3 dead in shooting.** Authorities issued a lock down of the Marine Corps base in Quantico while searching for a marine that shot and killed two fellow marines on base. Officials lifted the lockdown after they found the marine in his room, dead from a self-inflicted gunshot wound.
Source: http://www.cnn.com/2013/03/22/us/virginia-quantico-shooting/index.html

19. *March 21, Myrtle Beach Sun News* – (South Carolina) **Horry County councilman threatened.** Police are investigating an emailed threat placed against a Horry County councilman warning him of being killed within 6 hours of receiving the email.
Source: http://www.myrtlebeachonline.com/2013/03/21/3394521/horry-county-

councilman-al-allen.html

20. *March 21, Information Week* – (National) **NASA tightens security in response to insider threat.** After an alleged National Aeronautics and Space Administration (NASA) intellectual property theft by a Chinese contractor, NASA is taking preventative steps and has shut down their technical reports database and imposed tighter restrictions on remote access to its computers, in addition to incorporating other security measures.
Source: http://www.informationweek.com/security/government/nasa-tightens-security-in-response-to-in/240151412

21. *March 21, Associated Press* – (North Carolina) **NC tobacco broker sentenced to 5 years for fraud.** A North Carolina tobacco broker involved in a massive scheme that involved dozens bilking the government-backed crop insurance program out of $100 million was sentenced to serve over 5 years in prison and repay $13 million.
Source: http://www.sfgate.com/news/crime/article/NC-tobacco-broker-sentenced-to-5-years-for-fraud-4374706.php

22. *March 21, Associated Press* – (Illinois) **Aurora University offers $25,000 reward after bomb threat.** After a March 20 bomb threat that cancelled classes and evacuated the campus of Aurora University, the president is offering a $25,000 reward for information in identifying and apprehending the individual responsible.
Source: http://www.sj-r.com/breaking/x609791143/Aurora-University-offers-25-000-reward-after-bomb-threat

23. *March 20, KMGH 7 Denver* – (Colorado) **1348-acre Galena Fire is now 100 percent contained.** Fire officials are working to clean up the remains of the Galena Fire that burned through 1,348 acres before reaching 100 percent containment March 20.
Source: http://www.thedenverchannel.com/news/front-range/fort-collins/1348-acre-galena-fire-is-now-100-percent-contained

[Return to top]

Emergency Services Sector

24. *March 21, WRC 4 Washington, D.C.* – (District of Columbia) **Report: 3 ambulances improperly out of service when D.C. police office was struck.** A March 21 report by the deputy mayor for public safety claimed a Washington, D.C. ambulance and 2 medic units were within a 4-mile radius of an officer that was struck and severely injured March 5, but did not respond to the scene. The report alleges the fire stations failed to properly monitor for emergency calls.
Source: http://www.nbcwashington.com/news/local/Report-3-Ambulances-Improperly-Out-of-Service-When-DC-Police-Officer-Was-Struck-199444121.html

[Return to top]

Information Technology Sector

25. *March 22, Softpedia* – (International) **Yahoo, LinkedIn, Twitter accounts vulnerable to session fixation attacks.** A security researcher identified a vulnerability that could allow cybercriminals to launch session fixation attacks and gain access to users' accounts.
Source: http://news.softpedia.com/news/Yahoo-LinkedIn-Twitter-Accounts-Vulnerable-to-Session-Fixation-Attacks-Video-339448.shtml

26. *March 22, IDG News Service* – (International) **Google Drive hit by three outages this week.** Google Drive experienced three service interruptions the week of March 18, preventing users from accessing files during the interruptions.
Source:
http://www.computerworld.com/s/article/9237831/Google_Drive_hit_by_three_outages_this_week

27. *March 22, Softpedia* – (International) **Security hole in control panels of UK registrars led to domain hijacking.** About 300 domains were stolen from U.K. registrar 123-Reg by attackers exploiting a vulnerability in the service's Web hosting control panel that allowed users with an account to access other accounts.
Source: http://news.softpedia.com/news/Security-Hole-in-Control-Panels-of-UK-Registrars-Led-to-Domain-Hijacking-339475.shtml

28. *March 22, Softpedia* – (International) **PyCon incident: Two people fired, DDOS attack launched against SendGrid site.** SendGrid's Web site was targeted by a distributed denial of service (DDoS) attack after an incident by a former employee at a conference drew the attention of social media users and a self-professed Anonymous group.
Source: http://news.softpedia.com/news/PyCon-Incident-Two-People-Fired-DDOS-Attack-Launched-Against-SendGrid-Site-339407.shtml

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at 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: https://www.it-isac.org

[Return to top]

Communications Sector

29. *March 21, Richmond Times-Dispatch*– (Virginia) **3 area TV stations experiencing antenna problem.** A March 6 problem with a shared antenna in the Richmond area left WCVW, WRIC, and WRLH television stations unavailable to some of their viewers. The problem affects those who receive their television "over-the-air" instead of through cable or satellite.
Source: http://www.timesdispatch.com/business/local/companies/area-tv-stations-

experiencing-antenna-problem/article_ebd285d1-40e0-5fc6-a19b-97dbf567fb68.html

30. *March 21, New Orleans Times-Picayune* – (Louisiana) **Super Bowl blackout report blames electric relay device, cites poor communication.** A March 21 report on the 2012 Super Bowl blackout blamed the outage on a mis-operation of a relay device that was part of an electric switchgear near the stadium. The device's settings were within recommended default settings but poor communication between the manufacturer and the stadium prevented the device's set-up to align with the stadium's specific fuse requirements.
Source: http://www.nola.com/business/index.ssf/2013/03/analysis_of_super_bowl_blackou.html

[Return to top]

Commercial Facilities Sector

31. *March 21, Buffalo News* – (New York) **Over $2,000 worth of copper pipe stolen in Newfane.** A vacant apartment building in Newfane had 250 feet of copper stolen from it, a March 21 building inspection revealed. The building was boarded up since fall 2010 and had copper stolen from both the garage and the home in the amount of more than $2,000.
Source: http://www.buffalonews.com/apps/pbcs.dll/article?AID=/20130321/CITYANDREGION/130329798/1003

32. *March 21, Palm Desert Patch* – (California) **Bomb scare at Palm Springs Art Museum prompts evacuation.** The Riverside County Sheriff's Hazardous Device team determined two packages left both inside and outside the Palm Springs Art Museum did not contain explosives. The museum reopened after about 4 hours.
Source: http://palmdesert.patch.com/articles/bomb-scare-at-palm-springs-art-museum-prompts-evacuation

[Return to top]

Dams Sector

Nothing to report

[Return to top]

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

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at 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 or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer