Daily Open Source Infrastructure Report
21 January 2016

Top Stories

- The U.S. Department of the Treasury issued a warning January 19 advising taxpayers to be aware of callers impersonating Internal Revenue Service (IRS) agents and threatening victims to pay back-owed taxes. – *ABC News* (See item **3**)

- Authorities are investigating various threats of violence made via robocalls towards dozens of schools in six States January 19 which prompted evacuations, closures, and searches. – *Washington Post* (See item **15**)

- The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported that there was a surge in incidents involving U.S. critical infrastructure in fiscal year 2015, which brought the total count to 295 incidents. – *SecurityWeek* (See item **21**)

- A 4-alarm fire January 19 at a Center City, Pennsylvania apartment building prompted the response of 120 firefighters, an evacuation of 21 apartment units, and an evacuation of a surrounding apartment complex. – *WCAU 10 Philadelphia* (See item **23**)

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

See item **21**

Chemical Industry Sector

See item **21**

Nuclear Reactors, Materials, and Waste Sector

See item **21**

Critical Manufacturing Sector

See item **21**

Defense Industrial Base Sector

See item **21**

Financial Services Sector

1. *January 19, Canton Repository* – (Ohio) **Lake Twp. man pleads guilty in investment fraud case.** The owner of Lake Township-based Keystone Capital Management pleaded guilty January 19 to one count of wire fraud and two counts of money laundering charges after he reportedly ran a Ponzi scheme which defrauded 19 investors out of nearly $5.5 million between October 2009 and September 2013. The owner also used his client's money to pay personal and business expenses and promote and prolong his investment scheme, among other illegal actions.
Source: http://www.cantonrep.com/article/20160119/NEWS/160119215

2. *January 19, U.S. Securities and Exchange Commission* – (Colorado) **SEC: Alternative fund manager overcharged fees, misled investors.** The U.S. Securities and Exchange Commission announced January 19 that Equinox Fund Management LLC agreed to pay $400,000 in penalties, $600,000 in prejudgment interest, and $5.4 million in refunds to investors to settle allegations that the company overcharged management fees and misled investors by deviating from its valuation methodology for its future funds, The Frontier Fund (TFF) holdings.
Source: https://www.sec.gov/news/pressrelease/2016-11.html

3. *January 19, ABC News* – (National) **US Department of Treasury warns taxpayers about a 'frightening' fraud scam.** The U.S. Department of the Treasury issued a warning January 19 advising taxpayers to be aware of callers impersonating Internal Revenue Service (IRS) agents and threatening victims to pay back-owed taxes following reports that the Treasury Inspector General for Tax Administration (TIGTA) received 900,000 reports of fraudulent calls, resulting in over $26.5 million in victim losses since October 2013. TIGTA is urging people to hang up on the fraudulent

callers.
Source: http://abcnews.go.com/Business/us-department-treasury-warns-taxpayers-frightening-fraud-scam/story?id=36366276

For another story, see item **21**

Transportation Systems Sector

4. *January 20, KSFN 30 Fresno* – (California) **Hwy 41 closed near road 406 due to rockslide.** A 10-mile of Highway 41 from State Route 145 to Road 200 in Fresno remained closed indefinitely January 20 following a rockslide. Crews cleared the debris from the roadway and safety inspectors will evaluate the site.
Source: http://abc30.com/traffic/hwy-41-closed-near-road-406-due-to-rockslide/1165409/

5. *January 20, WREG 3 Memphis* – (Tennessee) **385 reopens after jackknifed truck is removed.** Westbound lanes of State Route 385 in Memphis were shut down for approximately 2 hours January 20 while crews removed a jackknifed semi-truck.
Source: http://wreg.com/2016/01/20/jackknifed-truck-shuts-down-part-of-385/

6. *January 19, KMBC 9 Kansas City* – (Missouri) **Crews clear wreck that snarled I-435 at Cookingham.** Southbound lanes of Interstate 435 in Kansas City, Missouri, were shut down for approximately 3 hours January 19 after a semi-truck slid off the interstate and began leaking hazardous materials.
Source: http://www.kmbc.com/news/accident-involving-tractor-trailer-closes-i435-at-cookingham/37517174

7. *January 19, San Francisco Chronicle* – (California) **North Berkeley BART station reopens after person killed by train.** Bay Area Rapid Transit's North Berkley Station was closed for 2 hours January 19 while officials investigated reports of a person being struck and killed along the tracks. The incident remains under investigation following the discovery of a body near the station.
Source: http://www.sfgate.com/bayarea/article/Report-of-intruder-on-tracks-closes-North-6769626.php

8. *January 19, KABC 7 Los Angeles* – (California) **Greyhound bus departs from LA, crashes in San Jose; 2 dead, 8 hospitalized.** A Greyhound Lines, Inc. bus crashed into safety barrels and flipped onto its side on U.S. 101 in San Jose January 19, killing 2 passengers and injuring at least 8 others.
Source: http://abc7.com/news/2-dead-18-injured-in-san-jose-bus-crash/1165086/

9. *January 19, WTVG 13 Toledo* – (Ohio) **OSHP: US 24 reopens after fatal accident.** Westbound lanes of U.S. 24 in Defiance, Ohio, were closed for 3 hours January 19 following a fatal accident involving 2 vehicles that left 1 person dead.
Source: http://www.13abc.com/home/headlines/Traffic-slow-on-US-24-in-Defiance-after-injury-accident-365818841.html

10. *January 19, KTRK 13 Houston* – (Texas) **Big rig wreck shut down southwest freeway for two hours in Stafford.** Southbound lanes of Highway 59 in Stafford, Texas, were shut down for 2 hours January 19 following an accident involving a semi-truck and at least 1 other vehicle that blocked all lanes.
Source: http://abc13.com/news/big-rig-wreck-shut-down-sw-freeway-for-hours/1164972/

For another story, see item **21**

Food and Agriculture Sector

11. *January 19, Associated Press* – (Indiana) **156K chickens added to list of poultry being euthanized.** The Indiana State Board of Animal Health reported January 19 that over 156,000 chickens will be euthanized, bringing the total number of birds euthanized to 400,000 following an investigation into the H7N8 virus outbreak at 10 affected commercial poultry farms.
Source: http://www.msn.com/en-us/news/us/156k-chickens-added-to-list-of-poultry-being-euthanized/ar-BBorjDO

12. *January 19, WVEC 13 Hampton* – (Virginia) **Plant fire breaks out in Surry County.** A January 19 fire at Edwards Virginia Smokehouse plant in Surry County closed the meat packaging plant indefinitely and prompted four fire departments to respond to the blaze. No injuries were reported and the cause of the blaze remains under investigation.
Source: http://www.13newsnow.com/story/news/2016/01/19/plant-fire-breaks-out-surry-county/79011002/

For another story, see item **21**

Water and Wastewater Systems Sector

See item **21**

Healthcare and Public Health Sector

See item **21**

Government Facilities Sector

13. *January 20, Detroit Free Press* – (Michigan) **Teacher sickouts close nearly all DPS schools.** Detroit Public Schools announced that 88 schools were closed January 20 due to teacher absences and sickouts which were organized to call attention to issues in classrooms and school buildings in the district.
Source: http://www.freep.com/story/news/local/michigan/wayne/2016/01/20/dps-teacher-sickouts/79046774/

14. *January 20, KUSA 9 Denver* – (Colorado) **4 schools closed due water outage.** Officials announced the indefinite closure of Welby Community School, McElwain

Elementary School, Monterey Community School, and Coronado Elementary School in Denver January 20 due to a water outage caused by a water main break.
Source: http://www.9news.com/story/news/education/2016/01/20/welby-community-school-closed-water-outage/79050468/

15. *January 19, Washington Post* – (National) **Police investigate threats against schools in six states.** Authorities are investigating various threats of violence made towards dozens of schools in Delaware, Maryland, New Jersey, Iowa, Pennsylvania, and Massachusetts January 19 which prompted evacuations, closures, and searches. No suspicious items were found and many of the threats were made via computer-generated robocalls.
Source: https://www.washingtonpost.com/local/education/police-investigate-threats-against-schools-in-six-states/2016/01/19/49ffdc92-bee2-11e5-9443-7074c3645405_story.html

16. *January 19, Springfield News-Sun* – (Ohio) **Carbon monoxide leak forces school closure.** Enon Elementary School in Ohio was closed January 19 due to a carbon monoxide leak from a boiler in the basement of the building. Classes were scheduled to resume January 20.
Source: http://www.springfieldnewssun.com/news/news/local-education/carbon-monoxide-leak-forces-school-closure/np7q2/

For another story, see item **21**

Emergency Services Sector

See item **21**

Information Technology Sector

17. *January 20, Softpedia* – (International) **Apple releases 28 security fixes for iOS, OS X and Safari.** Apple released 28 security patches for its iOS and Mac OS X operating systems (OS) and its Safari web browser through updated versions of OS X El Capitan 10.11.13, Safari 9.0.3, and OS X kernel that addressed critical vulnerabilities and allowed attackers to execute arbitrary code in the operating system's kernel and execute arbitrary code on the underlying operating system to trick a victim into accessing a malicious Web site.
Source: http://news.softpedia.com/news/apple-releases-28-security-fixes-for-ios-os-x-and-safari-499159.shtml

18. *January 20, Help Net Security* – (International) **Intel patches MiTM flaw in its Driver Update Utility.** Intel Corporation patched a remotely exploitable vulnerability in its Intel Driver Update Utility program that could have been exploited by attackers to conduct a man-in-the-middle (MiTM) attack to corrupt transferred data, leak information, and conduct arbitrary code execution.
Source: http://www.net-security.org/secworld.php?id=19349

19. *January 20, SecurityWeek* – (International) **Oracle released 248 security fixes.** Oracle released its Critical Patch Update (CPU) that fixed 248 vulnerabilities including authentication flaws and security issues in its Oracle Database, Java SE, and Oracle E-Business Suite, as well as other products. The company advised users to ensure all their products were updated to the newest versions to avoid exploitation.
Source: http://www.securityweek.com/oracle-releases-248-security-fixes

20. *January 20, The Register* – (International) **Cisco patches borked web box proxy hole.** Cisco released a patch fixing a vulnerability in its Web Security Appliance versions 8.5.3-055, 9.1.0-000, and 9.5.0-235 that allowed unauthenticated remote attackers to circumvent functionality that prevents proxied network traffic and bypass security restrictions due to improper handling of malformed Hypertext Transfer Protocol (HTTP) methods.
Source:
http://www.theregister.co.uk/2016/01/20/cisco_patches_borked_web_box_proxy_hole/

21. *January 20, SecurityWeek* – (International) **Critical infrastructure incidents increased in 2015: ICS-CERT.** The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported that there was an increase in incidents involving U.S. critical infrastructure in fiscal year 2015, increasing the total count to 295 incidences. Officials reported the increase was due to a spear-phishing campaign launched by an advanced persistent threat (APT) group against organizations in critical manufacturing, energy, transportation systems, government facilities, healthcare, and the communications sector, among other sectors.
Source: http://www.securityweek.com/critical-infrastructure-incidents-increased-2015-ics-cert

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: http://www.it-isac.org

Communications Sector

See Item **21**

Commercial Facilities Sector

22. *January 20, WABC 7 New York City* – (New Jersey) **4-alarm fire in Bayonne burns through 3 commercial, residential buildings.** Twenty people were displaced January 20 after a 4-alarm fire destroyed 12 apartment units, a restaurant, and a clock store in Bayonne, New Jersey, prompting fire crews to remain on site for several hours containing the incident.
Source: http://abc7ny.com/news/4-alarm-fire-burns-through-3-commercial-and-residential-buildings-in-bayonne/1165580/

23. *January 19, WCAU 10 Philadelphia* – (Pennsylvania) **Fire, now ice: Center City apartment fire.** A 4-alarm fire January 19 at a Center City, Pennsylvania apartment building prompted the evacuation of 21 apartment units and a surrounding apartment complex, and caused more than 120 firefighters to remain on site for over 2 hours containing the incident. Two firefighters sustained minor injuries and an investigation is ongoing to determine the cause of the blaze.
Source: http://www.nbcphiladelphia.com/news/local/Center-City-Apartment-Fire-Philadelphia-365830431.html

24. *January 19, KTXL 40 Sacramento* – (California) **Sacramento apartment fire injures 3, kills 2 dogs.** Sacramento Metro Fire Department reported that a January 19 apartment fire in the Arden area left 3 people injured and caused about $200,000 in damages.
Source: http://fox40.com/2016/01/19/sacramento-apartment-fire-injures-3-kills-2-dogs/

For another story, see item **21**

Dams Sector

See item **21**

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