Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

OVER-THE-ROAD-BUS INTELLIGENCE AWARENESS DAILY (OTRBIAD) REPORT

November 7, 2024

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (CISR) MONTH

Transportation Systems Sector

Moving millions of people and goods across the country daily, the Transportation Systems Sector provides critical lifeline services for communities, supports national defense, and facilitates response and recovery operations. The Sector consists of seven key subsectors or modes: Mass Transit and Passenger Rail, Highway and Motor Carrier, Freight Rail, Maritime Transportation Systems, Pipeline Systems, Aviation, and Postal and Shipping. The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector Risk Management Agencies for the Transportation Systems Sector. This vast network of public and private critical infrastructure owners and operators, the infrastructure and services they manage, and the extensive interdependencies among the transportation modes and other sectors are exposed to myriad of threats and risks, necessitating coordinated planning and investments to manage all hazards efficiently and effectively.
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructuresectors/transportation-systems-sector

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

Raleigh Police Investigating After 6 Rush-Hour Shootings Into Cars On Interstate 40
The News & Observer, 11/6/2024

[Raleigh, North Carolina] Raleigh police are investigating after six separate shootings into cars during morning rush hour along Interstate 40. Deputy Chief Rico Boyce said the first incident was reported Monday near the Chapel Hill Road exit when a woman suffered a non-life-threatening gunshot wound to her leg. Later that day, police responded to a second call from a victim reporting a single gunshot to their vehicle while traveling near the Buck Jones Road exit; that person was not injured, Boyce said during a news conference Wednesday.
https://www.newsobserver.com/news/local/crime/article295158999.html#storylink=cpy

ANALYST COMMENTARY: During a press conference on 6 November 2024, the Raleigh Police Department warned that an unknown gunman had been shooting at random passenger vehicles along a four mile stretch of Interstate-40 (I-40) in the Raleigh, North Carolina area. According to the Raleigh

Police Department, on 4 November 2024, two cars near Chapel Hill Road were struck by gunfire around 6:30 a.m. during the morning commute hours and one woman was shot in the leg during the incidents, which also resulted in a vehicle crash. On 6 November, four more vehicles were reportedly struck by gunfire between 5:00 a.m. and 6:30 a.m. during the morning commute hours on nearby I-40, though no injuries were reported. The Raleigh Police Department has said they believe the incidents are all related, and that the perpetrator is using a handgun. It is unclear if the perpetrator is shooting from another vehicle, or if they are positioned near the road. On 7 November, a seventh car was struck by gunfire near I-40 at approximately 8:50 a.m., though it is unclear at this time if this incident is related to the other six. The Raleigh Police Department is working with the North Carolina State Highway Patrol, the Wake County Sheriff's Office, and the Cary Police Department to investigate the shootings, and no suspect or motive has been identified thus far. In response to the incidents, law enforcement have asked commuters to come forward if they may have any dash cam videos from the times of the shootings, and additional law enforcement patrols are being conducted along I-40.

Train Derailment Spills Hundreds Of Gallons Of Diesel Into Columbia River Near Tri-Cities
The Olympian, 11/6/2024

[Wallula, Washington] Four refrigerated train cars derailed early Wednesday morning near Wallula, spilling an estimated 660 gallons of diesel fuel onto the riverbank and into the Columbia River. The Union Pacific train cars carrying frozen vegetables tipped over onto the bank of the river at 3:20 a.m. about 15 miles south of Pasco. The diesel was used to power the refrigeration. A cleanup contractor for the train company set out booms around a sheen of diesel stretching along the river near the eastern shoreline. The Washington state Department of Ecology was notified at 4 a.m. but initial reports were that there had not been a spill. Ecology sent out responders after being notified that there was diesel in the river about 6:30 a.m. Ecology will continue to monitor the spill, which will be cleaned up by the Union Pacific contractor, said Stephanie May, communications manager for the Eastern Regional Office of the Department of Ecology.
https://www.theolympian.com/news/state/washington/article295158879.html#storylink=cpy

Some Subway Trains Delayed As NYPD Search For Suspect After Man Shot On Upper West Side
ABC 7, 11/7/2024

[Manhattan, New York] Police are searching throughout a subway station for a suspect after a man was shot on the Upper West Side on Thursday morning. It happened just before 9:30 a.m. at 69th Street and Columbus Avenue. The 47-year-old victim was shot in the leg and shoulder by another man who fled down 69th Street toward Central Park. Police believe the suspect ran into the subway at 72nd Street and Central Park West and they were looking for him in a tunnel north of the station. Some passengers had to be evacuated and A/B/C/D trains were delayed in both directions while the NYPD conducts the investigation. https://abc7ny.com/post/uws-shooting-police-searching-suspect-after-man-shot-leg-upper-west-side-nyc/15522357/

Wildfire Tears Through Southern California Community After Burning Dozens Of Homes
1010 WINS, 11/7/2024

[Camarillo, California] A fast-moving wildfire fueled by heavy winds was tearing through a community northwest of Los Angeles for a second day Thursday after destroying dozens of homes and forcing thousands of residents to flee when it exploded in size in only a few hours. The Mountain Fire prompted evacuation orders Wednesday for more than 10,000 people as it threatened 3,500 structures in suburban communities, ranches and agricultural areas around Camarillo, California Gov. Gavin Newsom said in a statement. The fire was at 0% containment late Wednesday, according to the Ventura County Fire Department. The National Weather Service said a red flag warning, which indicates conditions for high fire danger, would remain in effect until 6 p.m.
https://www.audacy.com/1010wins/news/national/wildfire-tears-through-southern-california-community-after-burning-dozens-of-homes

ANALYST COMMENTARY: At approximately 9:00 a.m. on 6 November 2024, a wildfire, since dubbed the Mountain Fire, broke out in Ventura County northwest of Los Angeles, California. Due to winds in excess of 40 miles per hour, coupled with dry conditions, the fire grew from 25 acres to 1,000 acres by 10:00 a.m. Over 800 firefighters have been sent to battle the wildfire, 10,000 people are under evacuation orders, and 3,500 structures are threatened. Several structures have been burned and multiple fire and smoke related injuries have also been reported. Multiple roads near the scene of the fire have been closed down for emergency traffic, and authorities have warned drivers in the area to be watch for emergency vehicles. It is unclear what started the fire. As of 7 a.m. on 7 November, the fire has reportedly grown to 14,500 acres and is zero percent contained. For wildfires, percent contained measures how much of the wildfire perimeter is still burning freely, and how much of it is "hemmed in," or prevented from expanding outward by either firefighting efforts or terrain features like rock faces and lakes. To achieve containment, firefighters often need to move quickly along the anticipated perimeter of the fire and create firebreaks by thinning vegetation and creating a boundary of mineral soil, which is soil that will not burn because it is mostly devoid of plant matter. Firefighting aircraft, tanker trucks, and other flame-retardant delivery systems are often used to dampen areas around the perimeter, which slows the movement of the fire towards the perimeter and buys firefighters on the ground time to clear vegetation and create firebreaks.

TERRORISM & EXTREMISM

Man With Blowtorch, Manifesto Arrested At Capitol Visitor Center: Officials
FOX 5, 11/5/2024

[Washington D.C.] The U.S. Capitol Police arrested a man who smelled like fuel and was carrying a torch and flare gun at the Capitol Visitor Center in D.C. According to officers, the man was stopped during their screening process at the Capitol Visitor Center. Officers say the center is closed for tours for the day,

while the investigation continues. The suspect has been described as an adult white man in his late 20s. Officers tracked the suspect's earlier movements and located his vehicle at 9th and Maryland Avenue, NE. Senior congressional correspondent for FOX News Chad Pergram reports the suspect had a 25-page manifesto and drove all night from Michigan to the Capitol. https://www.fox5ny.com/news/man-arrested-possession-torch-flare-gun-capitol-visitor-center-dc

Santa Fe Springs Man Sentenced To Prison For Submitting Fake Online Tips Claiming Others Planned Attacks On Military Facilities
Department of Justice, 11/5/2024

[Los Angeles, California] A Santa Fe Springs man has been sentenced to 12 months and one day in federal prison for reporting eight online tips to the United States Department of Defense (DOD) falsely claiming that certain women were about to perpetrate mass-casualty attacks at U.S. military facilities in Los Angeles and Orange counties, the Justice Department announced today. Daniel Sandoval, 29, was sentenced Monday by United States District Judge Stephen V. Wilson. Sandoval pleaded guilty on February 12 to one count of false information and hoaxes. According to his plea agreement, on March 21, 2021, Sandoval knowingly provided an online tip to the DOD reporting system that falsely stated that a woman – identified in court documents as "S.C." – was planning to detonate bombs in a "mass attack" at a U.S. Navy weapons facility located in Seal Beach. According to Sandoval's tip, the attack would involve "blowing up military vehicles stationed there and civilian personnel vehicles." https://www.justice.gov/usao-cdca/pr/santa-fe-springs-man-sentenced-prison-submitting-fake-online-tips-claiming-others

SECURITY & SAFETY AWARENESS

Gridlock Guy: Big Rig Crashes Clear Far More Quickly With GDOT's TRIP Program
The Atlanta Journal-Constitution, 11/3/2024

[Georgia] Georgia's Department of Transportation founded the Highway Emergency Response Operators (HERO) program about one year before the 1996 Olympics. Anticipating the rush of traffic, GDOT wanted to create a network to clear traffic incidents more quickly. Incidents create delays, which create more incidents – and so on. The same premise is the reason the state deployed the Towing and Recovery Incentive Program (TRIP) in 2008. TRIP's goal is to galvanize wrecker companies into clearing crashes with large vehicles, usually commercial tractor trailers, faster. If a wrecker clears an incident in a certain amount of time, they get a payment. These types of incidents averaged more than 200 minutes to clear before 2008. The clearance time is now 30-40 minutes, on average, from the time the tow truck arrives. The stark decrease in time was not gradual, Josey said: "It changed overnight." https://www.ajc.com/news/atlanta-news/gridlock-guy-big-rig-crashes-clear-far-more-quickly-with-gdots-trip-program/YYZM3RSRTJEEFEQXLY23EQKVLA/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

FRA Slows Class I Railroad Implementation Of Improved Track And Train Inspections
Freight Waves, 11/4/2024

[Washington D.C.] In the wake of the disastrous hazardous materials derailment last year in East Palestine, Ohio, the Federal Railroad Administration has repeatedly said it's doing everything it can to improve rail safety. Yet under Administrator Amit Bose the FRA has stymied Class I railroad efforts to combine automated track and equipment inspections with traditional visual inspections in ways that weed out the highest number of defects that can cause derailments. Railroads are permitted unlimited use of automated track inspection systems that rely on lasers, machine vision, and other technology to find track geometry defects. But without a waiver from the FRA, railroads cannot simultaneously scale back the required frequency of visual inspections of main lines where the automated systems are deployed. https://www.freightwaves.com/news/fra-slows-class-i-railroad-implementation-of-improved-track-and-train-inspections

NHTSA To Study How Drivers React To Crash Avoidance Tech
Land Line, 11/6/2024

Crash avoidance technologies are often touted as the answer to any problems involving roadway safety. But how do humans interact with the technology? The National Highway Traffic Safety Administration hopes to soon have the answer to that question. In a notice that is scheduled to be published in the Federal Register on Thursday, Nov. 7, NHTSA has announced a study aimed at determining how human drivers react to all of the gadgets. "The objective of his driving research is to examine driver behavior in using crash avoidance warning systems and assess effects of human-machine interface characteristics on drivers' behavior and driver response in crash-imminent scenarios," NHTSA wrote in the notice. "The research will involve driver behavior observation while driving on a test track, public roads or in a simulated environment." https://landline.media/nhtsa-to-study-how-drivers-react-to-crash-avoidance-tech/

ANALYST COMMENTARY: Driver assistance technology is designed to increase safety and crash avoidance but, in some cases, it can create a false sense of security in drivers who pay less attention than they should, relying instead on the automated systems. The Insurance Institute for Highway Safety (IIHS) reports that forward looking crash avoidance systems are helping to reduce both the number and severity of crashes but also notes that drivers need to be ready and able to respond to warnings or interventions in order for them to work. Many vehicles do not adequately track whether the driver is paying attention to the road or prepared to take over in an emergency. Alerts for distracted driving often arrive too late to correct dangerous behavior. The National Highway Traffic Safety Administration (NHTSA) wants to study this interaction between people and various types of driver assistance software. On 7 November 2024, the NHTSA published a notice of the study in the Federal Register and requested public input. The proposed study titled "Crash Avoidance Warning System Human-Machine Interface (HMI) Research" seeks to conduct research using up to 200 licensed drivers without assisted devices between the ages of 25 to 65. Under controlled conditions, the NHTSA

plans to "examine driver behavior in using crash avoidance warning systems and assess effects of human-machine interface characteristics on drivers' behavior and driver response in crash-imminent scenarios." Complete details of the study and instructions for public input can be found at: https://public-inspection.federalregister.gov/2024-25821.pdf.

CYBERSECURITY

US: GPS And AI Technology Help Buses Power Through Traffic
Mass Transit, 10/30/2024

Empowering buses to zoom through traffic signals and past cars stalled in traffic may be the magic sauce needed to get riders back on public transit. "Bus rapid transit is, like, the thing right now," said Tim Menard, CEO and founder of LYT. "Transit is in a huge renaissance." His transportation technology company works to integrate priority vehicles like emergency or transit vehicles into a city's traffic management system. LYT has worked with cities including Portland, Ore.; San Jose, Calif.; and Boston to give certain vehicles more priority on the roadways than others, using technology to introduce signal priority as cities themselves move forward with projects like dedicated bus lanes. Transit organizations have been quick to embrace bus rapid transit (BRT) routes along primary corridors as solutions to decrease travel times — removing buses from clogged city streets by giving them their own lane. https://www.masstransitmag.com/technology/news/55239177/us-gps-and-ai-technology-help-buses-power-through-traffic

Cisco Patches Critical Vulnerability In Industrial Networking Solution
Security Week, 11/7/2024

Cisco on Wednesday announced patches for dozens of vulnerabilities in its enterprise products, including a critical-severity flaw in Unified Industrial Wireless software. The critical bug, tracked as CVE-2024-20418 (CVSS score of 10/10), allows a remote, unauthenticated attacker to inject commands on the underlying operating system, with root privileges. The issue exists because the web-based management interface of the industrial networking solution does not properly validate input, allowing an attacker to send crafted HTTP requests. "A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system of the affected device," Cisco notes in its advisory. https://www.securityweek.com/cisco-patches-critical-vulnerability-in-industrial-networking-solution/

ANALYST COMMENTARY: Cisco's recent security advisories highlight critical vulnerabilities in several key enterprise and industrial products, notably CVE-2024-20418, a command injection flaw with a CVSS score of 10.0. This vulnerability impacts the Catalyst IW9165D, IW9165E, and IW9167E access points when operating in Ultra-Reliable Wireless Backhaul (URWB) mode, potentially allowing remote, unauthenticated attackers to execute arbitrary OS commands with root privileges. The root cause lies in improper input validation within the web-based management interface, enabling attackers to

leverage crafted HTTP requests to gain control. Organizations running version 17.14 or earlier are advised to update to version 17.15.1 to mitigate this risk. Cisco also addressed CVE-2024-20536, a high-severity SQL injection vulnerability in the Nexus Dashboard Fabric Controller (NDFC). This flaw allows authenticated attackers to execute arbitrary SQL commands via a crafted REST API request, which could compromise database integrity by modifying or deleting critical data. Another critical fix targets CVE-2024-20484, a denial-of-service (DoS) vulnerability in Cisco's Enterprise Chat and Email (ECE) solution. Exploiting this vulnerability could disrupt customer-facing services, requiring a manual restart to restore functionality. Cisco's patches for these high-impact vulnerabilities and an additional set of medium-severity flaws in various management solutions reinforce the importance of rigorous input validation and the need for immediate patching. While Cisco has not detected active exploitation, the nature of these vulnerabilities demands prompt action to secure impacted systems.