Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

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

November 8, 2024

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (CISR) MONTH

The Transportation Systems Sector-Specific Plan

The Transportation Systems Sector-Specific Plan details how the National Infrastructure Protection Plan risk management framework is implemented within the context of the unique characteristics and risk landscape of the sector. Each Sector Risk Management Agency develops a sector-specific plan through a coordinated effort involving its public and private sector partners. The Postal and Shipping Sector was consolidated within the Transportation Systems Sector in 2013 under Presidential Policy Directive 21. The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

Subway Surfer Loses Limbs After Being Hit By Harlem Train: Sources
PIX 11, 11/7/2024

[Harlem, New York] A subway surfer lost her arm and leg after she was hit by a train in a Manhattan subway station Wednesday night, according to police sources and the MTA. The woman, 18, was trying to climb on top of a moving No. 2 train when she fell between two cars and onto the tracks in the West 135th Street-Lenox Avenue subway station in Harlem at around 6:10 pm., according to the MTA and NYPD. The victim was hit by a southbound No. 2 train and was rushed to the hospital in critical condition, police said. The teen lost her arm and leg, sources said. The teen was still in critical condition as of Friday morning, police said. Police have used drones to save 114 people in the past year, including a 9-year-old, according to Mayor Eric Adams. Yet at least six people have died subway surfing this year, an increase from 2023, according to NYPD data. https://pix11.com/news/local-news/manhattan/subway-surfer-loses-arm-and-leg-after-being-hit-by-train-in-harlem-sources/

Nearly 30 Hospitalized After Bus Rolls Onto Side Near Rochester
New York Upstate, 11/7/2024

[Rochester, New York] Nearly 30 people were hospitalized Thursday morning after a bus rolled onto its side on a highway near Rochester, officials said. The bus was heading westbound on Interstate 490

around 7:10 a.m. when it went on its side and spun 180 degrees in reverse, according to Todd Baxter, the Monroe County sheriff. Twenty-eight people were taken to four area hospitals, many with minor injuries, according to Frank Manzo, the chief and CEO of the local ambulance service. One person was brought out of the bus through a roof hatch and transported in critical condition. Baxter's chief deputy, Michael Fowler, said the bus had left New York City around 12 a.m. and was making drop-offs at various cities along the Thruway, including just before the crash in Rochester. The final destination was intended to be Niagara Falls. https://www.newyorkupstate.com/news/2024/11/nearly-30-hospitalized-after-bus-rolls-onto-side-near-rochester.html

METRO Bus Driver Stabbed In Altercation Along Highway 249 And Gessner, Houston Police Say
ABC 13, 11/8/2024

[Houston, Texas] A METRO bus driver was stabbed during some sort of altercation Friday morning on the northwest side, authorities told ABC13. Numerous police cars were spotted at the scene along Highway 249 and Gessner. According to a METRO spokesperson, the bus driver, a woman, suffered injuries to her hand, head, and shoulder while on the bus. She was taken to the hospital with non-life-threatening injuries. It wasn't immediately known if the alleged attacker was a passenger or someone else. The suspect ran away, but was later taken into custody by police. https://abc13.com/post/metro-bus-driver-stabbed-altercation-highway-249-gessner-northwest-side-houston-police-say/15526922/

TERRORISM & EXTREMISM

What Is Accelerationism, The White Supremacist Ideology Promoting Power Station Attacks
CNN, 11/8/2024

A man "dedicated to white supremacist" beliefs is facing federal charges in an alleged plot to use an explosives-laden drone to blow up a Nashville energy facility "in furtherance of his accelerationist ideology," a federal criminal complaint filed this week says. Accelerationism "refers to a white-supremacist belief that the existing state of society is irreparable and that the only solution is the destruction and collapse of the 'system,'" the complaint continues. It is "premised on the idea that steps can be taken to speed up the collapse of the system, to wit: the destruction of the US power grid, among other acts of violence." After his arrest Saturday in Nashville, Skyler Philippi, 24, was charged with attempted use of a weapon of mass destruction and attempted destruction of an energy facility, the US Justice Department said. He's detained without bond and due back in court Wednesday. His attorney told CNN he couldn't comment on the case. https://www.cnn.com/2024/11/08/us/accelerationism-meaning-manifesto-theory-accelerationist/index.html

ANALYST COMMENTARY: On 2 November 2024, Skyler Philippi, age 24, was arrested by law enforcement personnel while attempting to disable an electricity substation in Nashville, Tennessee in furtherance of white supremacist accelerationist ideology. Philippi had been the subject of a months

long Federal Bureau of Investigation (FBI) investigation and intended to fly an explosive-laden unmanned aircraft system (UAS/drone) into an electricity substation in hopes that it would disrupt the U.S. power grid and lead to widespread chaos and societal collapse. At its core, accelerationism is the idea that a rapid and drastic series of actions aimed at disrupting the status quo in some way will lead to radical societal changes. The origins of the ideology are often traced back to Karl Marx, who in the 1840s argued that free trade would hasten social revolution in capitalistic societies by increasing tensions between the poor and the rich. Up until the 2010s, accelerationist ideology generally referred to a left-wing ideology in which proponents strategized ways to move Western societies beyond capitalism and theorized what a viable post-capitalist future might look like. In the late 2010s, accelerationist ideology gained traction among white supremacists and has been widely circulated in far-right publications, manifestos, and chat groups. It gained specific notoriety after the manifesto of Brenton Harrison Tarrant, a white supremacist who in 2019 committed two consecutive mass shootings at two Muslim houses of worship in New Zealand, made international news. Tarrant's manifesto included a section titled, "Destabilization and Accelerationism: Tactics" which has circulated throughout far-right terrorist and extremist organizations and has been cited as inspiration for several far-right terrorist attacks since 2019. Of specific note to the surface and public transportation communities, Philippi, the individual motivated by white supremacist accelerationist ideology in the 2 November 2024 incident, attempted to obtain a train derailer prior to committing to the idea of using an explosive laden drone to attack the electricity sector. Philippi was apparently unsuccessful in his attempts to acquire a derailer, and it is unclear if he intended to use the derailer to target a specific surface or public transportation rail line.

Long Island Man Trying To Travel To Middle East To Join ISIS Arrested At JFK: Federal Prosecutors
ABC 7, 11/6/2024

[New York] A Long Island man was arrested Wednesday at JFK as he tried to board a flight to Qatar, from where he intended to travel to Syria and join ISIS, federal prosecutors said. Syed Aman, 28, expressed his support for ISIS through social media posts in an online forum, sent money to an individual he believed to be an Islamic State operative and made arrangements to travel to Syria, according to the criminal complaint. For the last month, Aman has been talking with an FBI source about his plan to join ISIS in Syria. Aman expressed that "jihad and hijrah," referring to traveling to ISIS-controlled territory and waging war on ISIS's behalf, are "the most important thing, more than anything else at the moment," the complaint said. https://abc7ny.com/post/li-man-attempting-travel-middle-east-join-isis-arrested-john-kennedy-international-airport-federal-prosecutors/15518672/

SECURITY & SAFETY AWARENESS

MN: Crime On Metro Transit Buses And Trains Increased During The Summer, But Has Decreased This Year From 2023
Mass Transit Magazine, 11/8/2024

[Minnesota] Crime aboard Metro Transit buses and trains increased during the summer months into September, but crime has declined overall so far this year and is below 2023 levels. In the third quarter that ended Sept. 30, crime increased 6.7% when compared with the same period last year, according to a presentation at a Metropolitan Council committee meeting Wednesday. The top crime: People smoking on public transit. Smoking is usually among the top complaints of passengers using Metro Transit. Some 831 citations for smoking were issued by Metro Transit police the first three quarters of this year, versus 161 in 2023. The 5,556 crimes reported in the first three quarters of this year is an 8.4% decrease when compared with the 6,066 crimes reported during the same period in 2023.
https://www.masstransitmag.com/safety-security/news/55241402/mn-crime-on-metro-transit-buses-and-trains-increased-during-the-summer-but-has-decreased-this-year-from-2023

Decades-Long Uptick In Attacks On Transit Workers, Including On The CTA, Carries Implications For Employees And Riders
Transit Talent, 11/4/2024

[Chicago, Illinois] The recent violence is a snapshot of an issue that has long been a concern for the unions representing train and bus operators in Chicago. It is part of a nationwide, decades-long uptick in attacks on transit workers, one researcher found, with implications for transit employees, riders and the systems themselves. “Transit workers are not just in the wrong place at the wrong time,” said Lindiwe Rennert, a researcher at the Urban Institute who has studied violence against transit employees. “They’re not just another member of the public who’s in a potentially dangerous public space. They’re representatives of institutions. It is because of their role that they are seeing less safe conditions than other members of the public.” In 2023, there were 90 major assaults on CTA workers: 52 on bus employees and 38 on rail workers, federal data shows. Across both bus and rail, it was the highest number of major attacks on employees since at least 2008, the data shows. Complete data isn’t yet available for 2024, but through June there had been 13 attacks on rail workers and 26 on bus workers.
https://www.transittalent.com/articles/index.cfm?story=Uptick_In_Attacks_On_Transit_Workers_11-4-2024

Insider Warns Of Cargo Theft Rings In Two Major U.S. Cities
Land Line, 11/7/2024

As cargo theft continues to climb across the United States, one industry insider is telling carriers in Chicago and Los Angeles to be on high alert. In a recent report from Overhaul – an Austin, Texas-based company providing “supply chain visibility and risk-monitoring solutions for in-transit shipments” – the

company said it had received intelligence that indicated an "active criminal crew" was targeting loads near O'Hare International Airport in Chicago. Additionally, Overhaul anticipated that Los Angeles would also see an increase in cargo thefts during the fourth quarter of 2024. "It's important to note that cargo thieves are constantly evolving their tactics and strategies, so it's crucial for logistics providers to stay informed and adapt their security measures accordingly," Overhaul said in its report. "By staying vigilant and taking proactive measures to protect cargo, we can help prevent theft and ensure the safe delivery of our clients' goods." https://landline.media/insider-warns-of-cargo-theft-rings-in-two-major-u-s-cities/

ANALYST COMMENTARY: On 11 October 2024, a stopped Union Pacific (UP) freight train was looted in Chicago, Illinois by dozens of people. Numerous box cars were breached and emptied of their contents. The targeted cars, which were not labeled, contained consumer electronics and small appliances. Dozens of people accompanied by multiple vehicles (including at least one moving truck) were involved in the effort. Overhaul, a risk management company for the freight industry reported that attacks like this are likely to increase, especially in Chicago and Los Angeles, as we approach the holiday season. Overhaul identified common tactics and techniques used by cargo thieves, which include preoperational surveillance to identify patterns and vulnerabilities in shipping, using GPS tracking devices such as Apple's Air Tag, to track shipment routes, identifying and targeting containers with high value contents, and using fraud to misdirect loads. The direct attacks on semi-trailers, intermodal containers, and rail box cars that take place in Chicago and Los Angeles are almost certainly preceded by criminal intelligence gathering. Danny Ramon, head of intelligence and response for Overhaul, reported that during the first half of 2024, a 49% "surge" in reported cargo theft incidents occurred compared with the first half of 2023. Overhaul's analysts believe the numbers will continue to rise. Ramon told Land Line, "Right now, we are 100% seeing increases across all verticals of cargo theft, whether that's product targeting or the various modes that they're using." CargoNet, which also specializes in supply chain and shipping risk management, theft prevention, and recovery services, identified "organized crime rings as a primary driver of the increasing theft trends." This suggests many of these incidents are not crimes of opportunity, but organized attacks. Trucks and trains are safest when they are in motion. Cargo vulnerability increases exponentially when the intermodal transport is stationary.

Train Safety System Failed In Moments Before Fatal Crash In Wales, Investigation Shows
The Guardian, 11/5/2024

An automated system that helps train wheels grip the tracks failed on one of the trains that crashed head-on in mid-Wales on 21 October, investigators have revealed. The Rail Accident Investigation Branch (RAIB) said the westbound train involved in the collision in Talerddig, near Llanbrynmair, in Powys, was fitted with a system to discharge sand automatically on to the rails should the wheels slide when braking. The system, however, did not appear to work in the crucial moments when the train was braking before the crash. The RAIB said an inspection of the train after the accident showed that the

sanding hoses on the leading vehicle of the train were “blocked and apparently unable to discharge sand”. https://www.theguardian.com/uk-news/2024/nov/05/cause-of-fatal-train-crash-in-wales-revealed

CYBERSECURITY

TSA Proposes New Cybersecurity Requirements For Some Railroads, Other Transportation Systems
Trains, 11/7/2024

The Transportation Security Administration has proposed a rule that would require cybersecurity risk management and reporting requirements for some freight and passenger railroads, as well as rail transportation. The Notice of Proposed Rulemaking, published today in the Federal Register, also covers some bus and pipeline operations. The TSA estimates that under the rule’s criteria, 73 of the approximately 620 U.S. freight railroads and 34 of approximately 92 passenger rail and transit operators would be subject to the requirements. “TSA has collaborated closely with its industry partners to increase the cybersecurity resilience of the nation’s critical transportation infrastructure,” TSA Administrator David Pekoske said in a press release. “The requirements in the proposed rule seek to build on this collaborative effort and further strengthen the cybersecurity posture of surface transportation stakeholders. We look forward to industry and public input on this proposed regulation.” https://www.trains.com/trn/news-reviews/news-wire/tsa-proposes-new-cybersecurity-requirements-for-some-railroads-other-transportation-systems/

ANALYST COMMENTARY: On 7 November 2024, the Transportation Security Administration (TSA) filed a Notice of Proposed Rule Making (NPRM) in the Federal Register called “Enhancing Surface Cyber Risk Management.” TSA states the purpose of the proposed rule is to “impose cyber risk management (CRM) requirements on certain pipeline and rail owner/operators and a more limited requirement, on certain over-the-road bus (OTRB) owner/operators, to report cybersecurity incidents.” Prior to implementation, TSA is requesting feedback from the public and industry stakeholders on ten specific areas of interest in the proposed rule. Among the more noteworthy concerns, TSA is requesting comments on “whether proposed requirements for supply chain risk management should also include requirements to ensure that any new software purchased for, or to be installed on, Critical Cyber Systems meets CISA's Secure-by-Design and Secure-by-Default principles.” The mandates TSA plans to implement will have a cost factor and it is important for companies to weigh in on whether the requirements will be overly burdensome or if there are lower cost options that would also meet the requirements. Most importantly, TSA is proposing to “require owner/operators to have a Cybersecurity Assessment Plan (CAP) to annually assess and audit the effectiveness of their TSA-approved Cybersecurity Operational Implementation Plan (COIP).” Trains.com explains that this component of the rule would “require an annual cybersecurity evaluation; a cybersecurity implementation plan identifying those responsible for the program, critical systems, and measures to recover from a cybersecurity incident; and an assessment plan that includes a schedule for

cybersecurity assessments, an annual report of results, and identification of unaddressed vulnerabilities." There is also a reporting requirement that mandates "owner/operators, and higher-risk bus-only public transportation and over-the-road bus owner/operators, currently required to report significant physical security concerns to TSA, to also report cybersecurity incidents to CISA." The proposed rule is open for comments through February 5, 2025 and instructions for submitting input can be viewed at: https://www.federalregister.gov/documents/2024/11/07/2024-24704/enhancing-surface-cyber-risk-management

Critical Auth Bugs Expose Smart Factory Gear to Cyberattack
Dark Reading, 11/1/2024

Critical security vulnerabilities affecting factory automation software from Mitsubishi Electric and Rockwell Automation could variously allow remote code execution (RCE), authentication bypass, product tampering, or denial-of-service (DoS). That's according to the US Cybersecurity and Infrastructure Security Agency (CISA), which warned yesterday that an attacker could exploit the Mitsubishi Electric bug (CVE-2023-6943, CVSS score of 9.8) by calling a function with a path to a malicious library while connected to the device — resulting in authentication bypass, RCE, DoS, or data manipulation. The Rockwell Automation bug (CVE-2024-10386, CVSS 9.8), meanwhile, stems from a missing authentication check; a cyberattacker with network access could exploit it by sending crafted messages to a device, potentially resulting in database manipulation.
https://www.darkreading.com/vulnerabilities-threats/critical-auth-bugs-smart-factory-cyberattack

ANALYST COMMENTARY: The recent Cybersecurity and Infrastructure Security Agency (CISA) advisory regarding critical vulnerabilities in Mitsubishi Electric and Rockwell Automation factory automation software underscores serious risks to industrial control systems (ICS) integral to smart factory operations. The Mitsubishi Electric vulnerability (CVE-2023-6943, CVSS 9.8) allows for remote code execution (RCE), authentication bypass, and potential denial-of-service (DoS) through the exploitation of a function that executes a malicious library path. This flaw could facilitate deep system manipulation, posing significant threats to operational integrity and safety. Similarly, the Rockwell Automation vulnerability (CVE-2024-10386, CVSS 9.8) results from a missing authentication check, enabling attackers to send crafted messages for database manipulation, potentially impacting data integrity across critical processes. Both ICS suppliers have issued mitigations, and the urgency for patching is underscored by the high CVSS scores and the expanding attack landscape targeting ICS, particularly by advanced persistent threats (APTs) from Russia and China. Additionally, noncritical vulnerabilities include an out-of-bounds read in Rockwell's FactoryTalk ThinManager (CVE-2024-10387, CVSS 7.5) leading to potential DoS, and authentication bypass issues within Mitsubishi Electric's FA Engineering Software Products (CVE-2023-6942, CVSS 7.5) and MELSEC iQ series (CVE-2023-2060, CVSS 8.7). These vulnerabilities highlight the need for robust access controls, rigorous patch management, and secure network segmentation. As cyber assaults on critical infrastructure intensify, timely

mitigation actions are crucial to protect operational continuity and prevent disruption in high-value industrial sectors.