Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

Public Transportation ISAC
Transit & Rail Intelligence Awareness Daily Report (TRIAD)

November 13, 2024

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (CISR) MONTH

Delivering Results For America USDOT Progress Report: 2021–2023

Delivering Results for America describes the progress that the Department has made addressing the strategic goals and challenges facing our transportation system. Boosted by historic levels of funding provided by the Bipartisan Infrastructure Law, the Department has made great strides towards transforming our transportation system – making transportation safer, more reliable, more sustainable, and more affordable for travelers across our nation. Even as we celebrate the many milestones highlighted in this report, we continue to work tirelessly to stand up new programs and policies and get funding out to communities as swiftly and efficiently as possible. Working together with our partners across the nation, we strive to deliver the world's leading transportation system.
https://www.transportation.gov/sites/dot.gov/files/2024-02/USDOTAccomplishmentsProgressReport2021%E2%80%932023.pdf

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

AFD Responds To 'Hazardous Materials Incident' Near Tesla Gigafactory, Precautionary Evacuations Issued
KXAN, 11/13/2024

[Austin, Texas] On Wednesday, the Austin Fire Department said it was responding to a hazardous materials incident at an address close to the Tesla Gigafactory. AFD said crews were responding to the 13000 block of Tesla Pvt E7 Road for reports of a possible crack in a pipeline, and Atmos Energy was working to shut off the valves and make the necessary repairs. The immediate area of the incident was evacuated as a precaution, according to AFD. The precautionary evacuation was for a cooling station in the area, not the Tesla Gigafactory. According to Atmos Energy, a construction crew working at 1 Tesla Road in Austin damaged a natural gas pipeline. The department said traffic should be expected in the area while crews respond. https://www.kxan.com/news/local/austin/traffic-alert-afd-responds-to-hazardous-materials-incident-near-tesla-gigafactory/

Amtrak Service Suspended Between Penn Station And New Haven Until Midday After Bronx Transformer Explosion And Track Fires
1010 WINS, 11/13/2024

[New York] Amtrak service between New York Penn Station and New Haven remains suspended Wednesday after multiple fires broke out near train tracks in the Bronx a day prior. The transit company said service is expected to resume by 2 p.m. Wednesday as crews assess and repair damage to the tracks. The FDNY responded to two separate fires near the tracks in the Morris Park section of the Bronx, just a quarter mile apart on Tuesday. The first fire, at 2:16 p.m., was a transformer fire at the Parts Authority Auto Parts warehouse on Bronxdale Avenue, a 60,000-square-foot building used for the storage of auto parts, hydraulic equipment, pallets, and vehicles.
https://www.audacy.com/1010wins/news/local/amtrak-service-suspended-between-penn-station-and-new-haven

NYPD: Male Sought In Connection To Alleged Attack On Brooklyn Subway Worker
SI Live, 11/12/2024

[Brooklyn, New York] The NYPD is seeking the public's assistance in identifying a man who allegedly punched an MTA subway worker after the worker asked him to extinguish marijuana he was smoking on a Brooklyn train platform last week. It was reported to police that on Friday, Nov. 1, at approximately 8:45 a.m., a 58-year-old male train operator observed an unidentified male smoking marijuana on the southbound 3 Train platform of the New Lots Avenue subway station. The MTA employee reportedly asked the unidentified male to extinguish the marijuana, at which point the individual allegedly punched the victim multiple times in the head and face, knocking him down to the floor of the platform, according to a statement from the NYPD's Deputy Commissioner of Public Information.
https://www.silive.com/crime-safety/2024/11/nypd-male-sought-in-connection-to-alleged-attack-on-brooklyn-subway-worker.html

TERRORISM & EXTREMISM

Northwestern Security and AI Lab Releases New Terrorism Early Warning System Forecasts
Northwestern University 11/12/2024

Artificial intelligence (AI) models trained on unclassified, open-source data can predict terrorist attacks, combat drone-based assaults, aid in deepfake and malware detection, and counter advanced phishing and cyber-attacks in real time. The Northwestern Security and AI Lab (NSAIL) team is a leader among a growing multidisciplinary community developing and deploying AI technologies to address these global threats and protect against malicious actors around the world. On October 17, during NSAIL's annual "Conference on AI and National Security," director V.S. Subrahmanian unveiled new reports generated by the Northwestern Terror Early Warning System (NTEWS), a machine-learning platform that models terrorist behavior to forecast the likelihood and types of attacks that specific terrorist groups will carry

out within the next six months.
https://www.mccormick.northwestern.edu/news/articles/2024/11/northwestern-security-and-ai-lab-releases-new-terrorism-early-warning-system-forecasts/

ANALYST COMMENTARY: Northwestern University is pioneering an effort to leverage the capabilities of artificial intelligence (AI) and machine learning to generate predictive analytics for use in public safety and counter terrorism. The Northwestern Security and AI Lab (NSAIL) Director, V.S. Subrahmanian, stated "Counterterrorism organizations need the power to be able to predict the approximate time frames and types of attacks that terror groups might carry out in the coming months. Armed with such knowledge, they can better direct intelligence collection resources, allocate counter-terrorism resources, and decide on optimal security strategies." Northwestern is careful to point out that their predictive analytics cannot identify specific dates, times, or locations of impending attacks, but they can reasonably predict the tactics, techniques and procedures (TTP) likely to be used by a particular group and identify that a particular group is in the pre-attack planning stages which can provide a potential time window. This information, combined with publicly available information on the geography the group is operating in, their conflicts, and interactions with any structured government or security forces, attacks on the public or government facilities, etc., can provide strong indicators of planned behavior. NSAIL plans to release monthly NTEWS Terror Forecast reports on Abu Sayyaf, Boko Haram, Lashkar-e-Taiba, Indian Mujahideen, Al-Shabaab, and Jama'at Nusrat al-Islam wal-Muslimin. Individuals can sign up with an official organizational email address to receive the forecasts.

UK Police Officer Arrested On Suspicion Of Terrorism Offence For Supporting Hamas
Metro, 11/12/2024

[Gloucestershire, United Kingdom] A serving British police officer has been arrested on suspicion of supporting the Palestinian militant group Hamas, which governs the war-torn Gaza Strip. The Gloucestershire Police officer was detained today at a property in Gloucester on suspicion of a terrorism offence. The man, who is in his 30s, is suspected of providing support for a proscribed organisation contrary to Section 12 of the Terrorism Act 2000. Gloucestershire Police revealed that his 'suspected support relates to activity online'. He has been taken to a police custody unit outside of the Gloucestershire area. A vehicle and an address in Gloucester are being now being searched as part of the investigation. Gloucestershire police assistant chief constable Arman Mathieson said: 'The arrest of a serving officer on suspicion of such a serious offence will no doubt cause our communities concern, as it does everyone who works for Gloucestershire Police. https://metro.co.uk/2024/11/12/uk-police-officer-arrested-suspicion-terrorism-supporting-hamas-21979772/

SECURITY & SAFETY AWARENESS

NYU Retracts Study That Found Vast Majority Of MTA Workers Were Harassed Or Assaulted In Pandemic
Gothamist, 11/12/2024

[New York] NYU has retracted a survey of MTA subway and bus workers that found 89% of respondents claimed to have been assaulted or harassed on the job. In a letter to the MTA on Friday, the lead researcher Robyn Gershon said her team had "detected anomalies" in the data it used for the study, which was published in August. The survey was supposed to have been emailed only to transit workers, but NYU discovered it had been posted on a public Facebook group. "In light of this, we have concluded that the database was likely contaminated and that the veracity of the data … is not verifiable," Gershon wrote. When the study came out, the MTA disputed the findings, claiming a survey of 1,297 transit workers was not representative of the more than 50,000 transit workers employed by the agency.
https://gothamist.com/news/nyu-retracts-study-that-found-vast-majority-of-mta-workers-were-harassed-or-assaulted-in-pandemic

ANALYST COMMENTARY: On 21 August 2024, researchers at New York University's (NYU) School of Global Public Health published a report in the Journal of Urban Health that claimed "the vast majority of [Metropolitan Transportation Authority (MTA)] subway and bus workers say they were harassed or assaulted on the job during the pandemic." The study alleged that it "was based on surveys filled out by 1,297 public-facing transit workers who were members of Transport Workers Union Local 100 between 2020 and 2023" and that 89 percent of respondents were the victims of harassment or assault. The MTA contested the findings when the study was first published, claiming that the 1,297 respondents' answers were not representative of the experiences of their 50,000 employees. New York City Transit President Demetrius Crichlow also responded to the findings by saying, "These incidents do not occur anywhere near as frequently as the report suggests." On 8 November 2024, the project's lead researcher, Robyn Gershon, wrote a letter to the MTA stating that the authors had "detected anomalies" in the data it used for the study, and that the survey used to collect data had been shared outside of the transit employees. Gershon wrote that because they were unable to confirm that only transit operators had filled out the survey, the researchers "have concluded that the database was likely contaminated and that the veracity of the data … is not verifiable." NYU has since retracted the study and is "taking corrective measures," though it is unclear what these measures are.

Truckers Are Not Using Paid Parking, Calling It 'Ridiculous,' Survey Reveals
Land Line, 11/12/2024

Paid truck parking is becoming more prevalent, but a new survey reveals that most truck drivers are unwilling to fork over cash to park their trucks. The OOIDA Foundation recently surveyed truckers about truck parking, including insights on paid parking and how drivers look for parking. Comprised mostly of

owner-operators, a majority of respondents indicated they will not pay to park. Specifically, 58% of truckers surveyed said they do not use paid parking. The main reason for avoiding paying for truck parking is it is too expensive, costs are too high and rates are too low. Drivers also refuse to pay for parking on principle, calling it "ridiculous." Other reasons include no need (home often, regional/local runs), spots are taken and a preference for rest areas. https://landline.media/truckers-are-not-using-paid-parking-calling-it-ridiculous-survey-reveals/

ANALYST COMMENTARY: On 9 November 2024, a driver was traveling on Interstate 80 (I-80) near Gary, Indiana when his passenger vehicle drifted out of its lane and slammed into the back of a tractor trailer that was parked on the shoulder of the road. The collision killed the driver of the passenger car. This incident, and others like it, draw attention to the nationwide problem of truck parking. The American Trucking Associations reports that "A chronic, nationwide shortage of truck parking is forcing America's professional truck drivers into an untenable position—either violate federal hours-of-service regulations that mandate rest breaks at specific times, or park in unsafe and unauthorized locations. Ninety-eight percent of truck drivers regularly experience this fraught scenario—a problem that grows more pervasive as cities across the country prohibit trucks from parking within city limits." U.S. Department of Transportation Secretary Pete Buttigieg stated that "I know that truck parking is an issue that most Americans probably don't think about every day—but it's [a] vitally important one… And that's because it's a life and death issue." Industry groups and stakeholders have been working to solve the problem and States have been adding truck parking in strategic areas for driver and public safety. One approach has been to build fee-based parking lots that currently cost an average of $18 a night. Carriers that employ drivers typically do not reimburse this parking fee and the paid parking lot providers do not offer any amenities other than an off-highway place to park. The result of this is that truckers are not using the paid lots when it is free to park on the side of the road or in a public rest stop, if they can find one. Long haul drivers that are on the road for many days at a time opt for free parking because the fees add up. Another issue is that a plot of land large enough to accommodate commercial truck parking is very expensive unless it is located far enough from any services that the price of land is lower, but then it is too far off the main travel route to be worth it. Land Line reports that drivers are now losing driving time because they are searching for parking, and six in 10 drivers report shutting down their drive early so they can search for a place to park and get their rest. Travel centers and truck stops that offer some amenities remain the most sought-after destinations for commercial drivers.

Pay Your Fare: MBTA Dispatches Engagement Team To Encourage Riders To Pay Up
WBUR, 11/12/2024

[Medford, Massachusetts] Stationed by the ticketing kiosks at the MBTA's Ball Square station in Medford on a recent afternoon, two members of the T's new "fare engagement" team were ready intercept riders. … Call it a soft start. For now, the T says the goal is to help riders navigate the transit system. But it's also a introduction to the idea someone will soon be checking that riders have paid their

fare, said the T's chief of policy and strategic planning, Lynsey Heffernan. "At some point in time, those individuals will also start to check payment," she said. The new team is part of the T's strategy to maximize fare collection on the Green Line and ultimately on buses, too. Heffernan said the T needs riders to "make sure they know how to pay and also understand why it's important for the MBTA." The T counts on fares to support its operating budget. Several years ago, 31% of the system's operating funds came from rider fares. This year, fares will only contribute 15%, partly due to the drop in ridership since the pandemic. https://www.wbur.org/news/2024/11/12/mbta-fare-evasion-revenue-boston-massachusetts

Freight Fraud Is A Massive Problem: It's Time To Steal An Idea From The Credit Card Industry
Freight Waves, 11/12/2024

Freight fraud has become one of the most pressing issues in the logistics sector. What once was a domain of petty crime has now escalated into a sophisticated network often connected with offshore criminal organizations, particularly in regions like Eastern Europe, India, Pakistan and Africa. Insights from industry leaders such as Truckstop, DAT, Triumph and the Transportation Intermediaries Association (TIA) indicate a sharp rise in freight fraud, with a fourfold increase since before the COVID-19 era. The financial toll could soon hit nearly $1 billion, fueled by the profitability of these schemes and the challenges in prosecuting offenders who operate outside U.S. legal reach, where the FBI's jurisdiction is limited. https://www.freightwaves.com/news/freight-fraud-is-a-massive-problem-its-time-to-steal-an-idea-from-the-credit-card-industry

Illinois Commerce Commission Approves Multiple Rail Safety Upgrades
Transportation Today, 11/12/2024

[Illinois] The Illinois Commerce Commission (ICC) announced they have approved several new rail safety upgrades throughout Southern Illinois. According to the ICC, new automatic warning gates and highway grade approach improvements will be installed at highway rail grade crossings in Franklin and Marion counties, along Pump Station Road, River Road, Main Street, and W 4th Street over Union Pacific Railroad tracks. "Enhancing the safety of Illinois' rail crossings is vital for everyone who lives, works, and travels along train tracks," ICC Commissioner Michael T. Carrigan said. "Infrastructure improvements like the ones in Kinmundy and Royalton will help upgrade essential warning systems, reducing the risk of collisions and fostering safer travel for everyone." https://transportationtodaynews.com/news/34301-illinois-commerce-commission-approves-multiple-rail-safety-upgrades/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

CYBERSECURITY

Beware Of Phishing Emails Delivering Backdoored Linux VMs!
Help Net Security, 11/5/2024

Unknown attackers are trying to trick Windows users into spinning up a custom Linux virtual machine (VM) with a pre-configured backdoor, Securonix researchers have discovered. The attack began with a phishing email, they believe, but they weren't able to pinpoint the intended victims. The email included a link pointing to an unusually big ZIP file (285 MB), and its name – OneAmerica Survey.zip – points to the likely lure: a survey by OneAmerica Financial, a US company offering financial services. "When the user extracts the archive, they're presented with a single file (shortcut) 'OneAmerica Survey' and a 'data' directory containing the entire QEMU installation directory," the researchers explained.
https://www.helpnetsecurity.com/2024/11/05/phishing-oneamerica-survey-linux-vm-backdoor/

ANALYST COMMENTARY: The recent campaign uncovered by Securonix highlights a sophisticated use of social engineering and virtualization to breach Windows systems by tricking users into running a malicious Linux VM via QEMU. The attackers exploit phishing emails with a large ZIP file, named deceptively to resemble a financial survey, which contains a QEMU installation and a shortcut file to execute the VM setup. Once activated, the VM spins up a customized Tiny Core Linux environment with an SSH-enabled backdoor, allowing attackers to conduct a range of malicious activities on the host machine. The attackers employ a layered approach, starting with the execution of a BAT file that triggers a decoy error image, masking the launch of QEMU and subsequent installation of backdoor components. Through the Chisel tool, the backdoor maintains persistence by tunneling traffic over websockets to a C2 server, bypassing traditional network defenses. Chisel's configuration enables covert communication, reinforcing the campaign's stealth. Notably, the reliance on legitimate tools like QEMU and Chisel aids in evading detection, as these software instances appear benign under many monitoring solutions. Moreover, the unusually large ZIP file circumvents some antivirus scanning parameters, while the isolated Linux environment hampers endpoint detection within the VM itself. To mitigate these risks, Securonix recommends close monitoring of large files in malware-staging directories, unusual execution paths for legitimate tools, and robust endpoint logging for processes like PowerShell. Enhanced vigilance for atypical virtualization activity on Windows hosts could also preemptively disrupt such threats.