Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

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

November 14, 2024

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (CISR) MONTH

The Current Threat Environment

Critical infrastructure faces a wide range of threats and risks, from naturally occurring events to human induced disruptions of both accidental and malicious origins. Numerous natural hazards adversely affect physical critical infrastructure such as transportation networks, telecommunications systems, and energy infrastructure. The threat of terrorism and targeted violence remains elevated and is increasingly local and often aimed at public gatherings and populated spaces. The diversity, complexity, and expanse of our nation's physical infrastructure pose their own unique challenges. Additionally, critical infrastructure assets and systems are highly interconnected and interdependent, both domestically and internationally, increasing the likelihood of cascading failures across multiple sectors. Increased digitization of the systems and processes that underpin the functioning of critical infrastructure amplifies the risk for assets and systems' exposure to heightened physical and cyber threats from malicious actors. The impact of cyberattacks is costly in nature, as governments and critical infrastructure owners and operators spend millions of dollars rectifying the damage caused to their assets, systems, and reputations. A shifting geopolitical landscape intensified national security concerns and demonstrated that targeting critical infrastructure can be a primary attack vector. This can occur both in a conflict setting, as well as through indirect, long-term foreign interference campaigns. These concerns highlight that domestic investment in infrastructure security and resilience can both strengthen national security and serve as a strategic deterrent. All of these factors demand a greater focus on resilience. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/criticalinfrastructure-security-and-resilience-month

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

Person Killed On Market Street In San Francisco Near Embarcadero BART Station
CBS News, 11/13/2024

[San Francisco, California] A person was killed on Market Street outside the Embarcadero BART station in San Francisco Wednesday morning and the search for the suspect caused significant delays on the BART and Muni Metro system. San Francisco police said officers responded to Market and Main Streets at 5:49 a.m. regarding a person who was bleeding. Officers found a male victim suffering from an unspecified injury on Market Street just outside an entrance to the BART/Muni Metro Embarcadero station and

began first aid until medics arrived at the scene, police said. Despite the efforts of emergency responders, the victim was pronounced dead at the scene.
https://www.cbsnews.com/sanfrancisco/news/san-francisco-market-street-embarcadero-homicide-bart-station/

NYPD Seeks Suspects In Series Of Subway Robberies And Assaults Across NYC
FOX 5, 11/13/2024

[New York] Police are searching for the suspects who robbed and assaulted people inside multiple subway stations in separate incidents across the city. On Thursday, Oct. 10, at approximately 5 a.m. inside the Bleecker Street subway station, a 60-year-old man was punched in the head and face. Police said the 60-year-old man was seated on a bench on the southbound "6" train platform when he was approached by two unknown males. The suspects then punched and kicked the man and stole $65 from his pocket before leaving the station, police said. Police said he was taken by EMS to NYC Health+Hospitals/Bellevue. https://www.fox5ny.com/news/nypd-seeks-suspects-series-subway-robberies-assaults-across-nyc

18-Year-Old Arrested In Connection To Shooting Near RTA Bus Hub
WHIO, 11/13/2024

[Dayton, Ohio] A man has been charged in connection to a shooting near an RTA bus hub in downtown Dayton on Monday. Ge'Neale Galloway, 18, is booked into the Montgomery County Jail on initial charges of felonious assault, tampering with evidence, and obstruction of official business, according to online jail records. News Center 7 previously reported that Monday afternoon Dayton police and medics were called to the area of South Jefferson Street for reports of a shooting. A man was walking on the sidewalk when he passed Galloway and appeared to say something to him, according to an affidavit and statement of facts. Galloway then took a gun from his jacket and shot the man three times, the affidavit and statement of facts state. Galloway then ran from the scene before being arrested minutes later on the Main Street bridge. https://www.whio.com/news/local/18-year-old-arrested-connection-shooting-near-rta-bus-hub/SZS3FSM3OZDWJESMOMY3VHFQUM/

13 Hurt When Tractor-Trailer Collides With Bus Carrying Military Personnel On New Jersey Turnpike
ABC 6, 11/14/2024

[Runnemede, New Jersey] More than a dozen people were hurt when a bus carrying military personnel collided with a tractor-trailer on the New Jersey Turnpike in Runnemede, Camden County. The crash happened in the northbound lanes of the highway just south of Interchange 3 around 1 p.m. Wednesday. The bus appears to have been hit from behind by the tractor-trailer. Video from Chopper 6 showed a number of police, firefighters and medics on the scene. State police say 13 people were injured, including a truck driver and 12 people on the bus with military personnel. There was no word on the

conditions of those hurt. The military personnel being transported on the bus are from Maryland. https://6abc.com/post/bus-tractor-trailer-involved-crash-new-jersey-turnpike-runnemede-camden-county/15543237/

TERRORISM & EXTREMISM

17-Year-Old Arrested Over Alleged Terror Plot
DW, 11/12/2024

[Flensburg, Germany] Prosecutors in the northern German city of Flensburg said on Tuesday that a youth arrested last week was planning an Islamist terror attack. He had "sufficiently concrete plans for an attack" to warrant an arrest, they added, saying there was also evidence of his radicalization. The young man had been detained a week earlier in the town of Elmshorn and remains in custody while police continue the investigation. Authorities have not confirmed much about the suspect, including how they caught wind of his plan or the details of his arrest. They have said that he planned to utilize a large vehicle, such as a truck, for an attack. https://www.dw.com/en/germany-17-year-old-arrested-over-alleged-terror-plot/a-70763378

SECURITY & SAFETY AWARENESS

Explosive Device Found, Detonated Outside Torrance Courthouse
FOX 11, 11/13/2024

[Torrance, California] An urgent investigation is underway in Torrance after an apparent explosive device was located outside the courthouse Tuesday morning with a note nearby. SkyFOX was above the scene when a robot poked what looked like an orange bag or balloon, that exploded. Also visible from SkyFOX was a letter next to the device that said in all caps, "these get bigger," and what appeared to be a collection of possible BBs or pellets nearby. "Further evaluation of the evidence by LASD will determine investigative strategy going forward." The Los Angeles County Sheriff's Department Arson Explosives Detail is actively investigating the incident. https://www.foxla.com/news/torrance-bomb-threat-courthouse-explosive-device

ANALYST COMMENTARY: At approximately 7:15 a.m. on 13 November 2024, Torrance Police Department and Los Angeles County Sheriff's Department (LASD) personnel responded to a suspicious package outside the Torrance Superior Court in Torrance, California. According to law enforcement and media sources, the suspicious package was a "orange inflatable item [appeared to be an inflated and tied orange contractor bag] attached to what may have been a cooler [on] a bench near the courthouse entrance." The "cooler" appeared to be a five-gallon Igloo-style beverage dispensing cooler. A handwritten note that read, "these get bigger … killers loose - killing inocent (sic)" was found near the device. Law enforcement deployed an LASD bomb squad robot to investigate the device, and

the inflated bag exploded when the robot came into contact with it. The explosion was relatively small – the bench remained largely undamaged and the cooler that was touching the bag during the explosion only shifted slightly from the blast. It is unclear if there was any shrapnel in the bag, though local media outlets reported that BBs or pellets were found nearby. Nobody was injured during the incident. Following the incident, Los Angeles Superior Court officials announced that the courthouse would remained closed throughout 13 November and reopen on 14 November. The LASD and Federal Bureau of Investigation (FBI) are investigating the incident. Officials have not released any additional information regarding the incident, and it is unclear what kind of explosive material was inside the bag, who emplaced the device, and what their motive may have been.

TRANSCOM Commander Visits DLA To Discuss Current Partnerships And Future Collaboration Opportunities
U.S. TRANSCOM, 11/13/2024

[Fort Belvoir, Virginia] Challenges such as the contested logistics environment, supply chain resiliency, and data interoperability were top topics as senior leaders from U.S. Transportation Command (TRANSCOM) and the Defense Logistics Agency (DLA) met at the McNamara Headquarters Complex here Nov. 7. DLA is TRANSCOM's largest volume customer, representing 42% of the organization's total support to the Defense Department. DLA Energy Deputy Commander David Kless also explained the role TRANSCOM plays in ensuring global bulk fuel distribution and delivery. "DLA's role as the Integrated Material Manager compliments TRANSCOM as the single manager for global bulk fuel management and delivery," Kless said. "Today, 62% of DLA fuel is moved by TRANSCOM."
https://www.ustranscom.mil/cmd/panewsreader.cfm?ID=7B07480E-0141-FF53-935FA8EA477BCF74&yr=2024

NTTC Calls Out EV Adoption Challenges
Bulk Transporter, 11/13/2024

National Tank Truck Carriers "vehemently disagrees" with the Federal Highway Administration's assertion that fleet operators are "increasingly embracing EVs as viable alternatives to conventional diesel-powered vehicles," according to comments NTTC filed last week in response to FHWA's request for information (RFI) on medium- and heavy-duty electric charging technologies and infrastructure needs. "America's tank truck industry is implementing clean technologies to increase the efficiency and cleanliness of its fleets, but NTTC members counter the false narrative that truck electrification is embraced by our industry. It is not a viable technology for our use at this time," wrote Will Lusk, NTTC director of education and government relations, in a letter submitted just before the agency's Nov. 12 deadline. https://www.bulktransporter.com/green-trends/article/55242646/nttc-calls-out-ev-adoption-challenges-for-the-tank-truck-industry

ANALYST COMMENTARY: Transitioning to cleaner emissions in the trucking industry is a goal that is largely still in the research, development and testing phase. Some trucking companies are concerned

that the desire to transition to greener fuels and cleaner emissions could outpace their logistical ability to achieve that goal. On 12 September 2024, the Federal Highway Administration (FHA) published a request for information regarding "Medium- and Heavy-Duty Electric Charging Technologies and Infrastructure Needs." The FHA acknowledged that the industry is making strides towards complying with government mandates and sought additional information about the process and industry needs. The National Tank Truck Carriers (NTTC) responded that converting trucks from diesel to electric vehicles (EV) is not universally embraced by the trucking industry, stating "Simply, the high risks and costs of electric Class 8 tractor equipment pose a serious threat to the businesses required to comply with regulations as proposed by federal and state activity." The NTTC objected to the speed at which the FHA is demanding change and cited a study commissioned by the Clean Freight Coalition, which found electrifying the entire U.S. commercial trucking fleet could cost nearly $1 trillion. This is cost prohibitive for the trucking industry and fails to consider other viable options like clean diesel or hydrogen. NTTC also pointed out that tank truck carriers hauling fuel and water are "often among the first responders to natural-disaster sites, and electric-vehicle adoption could hinder their efforts to provide life-saving relief services." Prematurely forcing the industry to adopt ambitious EV standards would not only cripple the industry but also impact public safety.

A Trucker Uses AI To Boost Efficiency For LTL Operations
Supply Chain Brain, 11/8/2024

[Pennsylvania] Pennsylvania-based PITT OHIO has been providing less-than-truckload (LTL), warehousing, and full truckload freight-shipping services for more than 40 years. In a bid to make its trucking and delivery services more efficient, PITT OHIO replaced its legacy operating systems with an artificial intelligence-powered enterprise model that has saved the company more than $11 million since the platform was first launched. In the brainstorming phase, the company sought to develop a system that was data-driven and reliable, and included dispatching, pickup and delivery information, all capable of managing PITT OHIO's entire fleet of drivers across its U.S. operations centers. https://www.supplychainbrain.com/articles/40617-a-trucker-uses-ai-to-boost-efficiency-for-ltl-operations

CYBERSECURITY

2023 Top Routinely Exploited Vulnerabilities - Key Vulnerabilities Affecting Transportation Systems
Cybersecurity & Infrastructure Security Agency, 11/12/2024

Five Eyes coauthored this joint Cybersecurity Advisory in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations. This advisory provides details, collected and compiled by the authoring agencies, on the Common Vulnerabilities and Exposures (CVEs) routinely and frequently exploited by malicious cyber actors in 2023 and their associated Common Weakness Enumerations (CWEs). Malicious cyber actors

exploited more zero-day vulnerabilities to compromise enterprise networks in 2023 compared to 2022, allowing them to conduct operations against high priority targets. The authoring agencies strongly encourage vendors, designers, developers, and end-user organizations to implement the following recommendations, and those found within the Mitigations section of this advisory, to reduce the risk of compromise by malicious cyber actors. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-317a

ANALYST COMMENTARY: On 12 November 2024, the Cybersecurity and Infrastructure Security Agency (CISA) released a 30-page Joint Cybersecurity Advisory titled 2023 Top Routinely Exploited Vulnerabilities in collaboration with the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and their Australian, Canadian, New Zealand, and UK counterparts. The product details a number of Common Vulnerabilities and Exposures (CVEs) that were "routinely and frequently exploited by malicious cyber actors in 2023 and their associated Common Weakness Enumerations (CWEs)." In the report, the authoring agencies' key findings were that "malicious cyber actors exploited more zero-day vulnerabilities to compromise enterprise networks" in 2023 than they did in 2022, and that most frequently exploited vulnerabilities in 2023 were initially exploited as zero-days. They also found that malicious cyber actors had "the most success exploiting vulnerabilities within two years after public disclosure of the vulnerability," and that international cybersecurity efforts had been successful in mitigating the amount exploitation malicious cyber actors were able to do with zero-day vulnerabilities. The product also includes a robust mitigations section, though the authoring agencies also recommended that the global community implement security-centered product development lifecycles to try and find vulnerabilities during testing, increase incentives for responsible vulnerability disclosure like a bounty system for finding bugs, and use sophisticated endpoint detection and response (EDR) tools to improve the detection rate of zero-day exploits. The advisory also encourages organizations to ask their software providers to discuss their secure by design programs to become better informed on what the providers are doing to safeguard programs and remove vulnerabilities.

FBI, CISA Say Chinese Hackers Breached Multiple US Telecom Providers In Targeted Attack
FOX News, 11/13/2024

The Cybersecurity and Infrastructure Security Agency (CISA) and the FBI said that People's Republic of China (PRC) hackers breached commercial telecommunication service providers in the U.S. The breached entities have been warned, and the agencies are proactively alerting other potential targets of elevated cyber activity. "The U.S. government's continued investigation into the People's Republic of China (PRC) targeting of commercial telecommunications infrastructure has revealed a broad and significant cyber espionage campaign," the agencies said Wednesday in a joint release. The agencies said that PRC-affiliated actors have compromised networks at multiple telecommunications companies to enable the theft of customer call record data, as well as private communications of a "limited number of individuals who are primarily involved in government or political activity." https://www.foxnews.com/tech/fbi-cisa-say-chinese-hackers-breached-multiple-telecom-providers-targeted-attack

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

VEILDrive Attack Exploits Microsoft Services To Evade Detection And Distribute Malware
The Hacker News, 11/6/2024

An ongoing threat campaign dubbed VEILDrive has been observed taking advantage of legitimate services from Microsoft, including Teams, SharePoint, Quick Assist, and OneDrive, as part of its modus operandi. "Leveraging Microsoft SaaS services — including Teams, SharePoint, Quick Assist, and OneDrive — the attacker exploited the trusted infrastructures of previously compromised organizations to distribute spear-phishing attacks and store malware," Israeli cybersecurity company Hunters said in a new report. "This cloud-centric strategy allowed the threat actor to avoid detection by conventional monitoring systems." Hunters said it discovered the campaign in September 2024 after it responded to a cyber incident targeting a critical infrastructure organization in the United States.
https://thehackernews.com/2024/11/veildrive-attack-exploits-microsoft.html

ANALYST COMMENTARY: The VEILDrive campaign shows us a sophisticated use of Microsoft's SaaS environment to deploy malware in ways that evade conventional detection methods. By exploiting trusted Microsoft services such as Teams, SharePoint, Quick Assist, and OneDrive, the attackers bypass standard security filters, leveraging the trust placed in these legitimate platforms. Initially, they gained access by impersonating an IT team member and using an account from a prior victimized organization (Org A), sending Teams messages to employees of Org C to gain remote access via Quick Assist. This approach exploited Teams' "External Access" feature, which enables external organizations to communicate directly by default. Once remote access was secured, the attackers distributed malware using links to SharePoint-hosted ZIP files containing remote management tools like LiteManager and Java-based payloads, employing OneDrive as a command-and-control (C2) channel. The Java-based malware deployed through this campaign utilizes hard-coded Entra ID credentials to authenticate with OneDrive, executing PowerShell commands via the Microsoft Graph API. As a contingency, it establishes a secondary C2 connection using HTTPS to an Azure VM, allowing attackers to retain command execution control if the primary channel is disrupted. The straightforward design of this malware, which eschews obfuscation, contrasts with typical evasive techniques, reflecting a strategy that prioritizes leveraging trusted channels over concealment. Mitigation requires both monitoring of legitimate SaaS service usage patterns and tighter control over external access policies in environments like Teams. Further, integrating robust behavioral analytics and anomaly detection tools can help identify irregularities associated with unauthorized access attempts or unusual file-sharing activity in cloud applications.