Information Sharing & Analysis Center

PUBLIC TRANSPORTATION, OVER THE ROAD BUS, & SURFACE TRANSPORTATION

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

November 4, 2024

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (CISR) MONTH

Help Drive Down Critical Infrastructure Risk And Build Resilience

There are 16 critical infrastructure sectors whose assets, systems, and networks—both physical and virtual— are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or a combination of any of these. Critical infrastructure is a shared resource as well as a shared responsibility. It is important that all individuals and organizations understand the risks; plan, prepare, and train for potential events; and remain vigilant for and report suspicious activity.
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

SUSPICIOUS ACTIVITY & INCIDENT REPORTS

Shooting At West End MARTA Station: 1 Shot, Delays Possible
FOX 5, 11/01/2024

[Atlanta, Georgia] Police are investigating a shooting at the West End MARTA Station that occurred on Friday evening. According to the MARTA Police Department, one person was found with a gunshot wound. The person was alert, conscious, and breathing. It is unclear if the victim was taken to an area hospital for treatment. MARTA officials say all trains running through West End and Garnett stations are boarding on the south side of the platform. This is due to trains only running on one track through those stations in response to the shooting. The name and age of the victim have not been released. It was unclear whether police were actively searching for a shooter or shooters.
https://www.fox5atlanta.com/news/shooting-west-end-marta-station-1-shot-delays-possible

Woman Injured After Stabbing On BART Train In SF; Suspect Arrested, Police Say
ABC 7, 11/3/2024

[Antioch, California] BART police have arrested a suspect wanted in connection with a stabbing that occurred Saturday morning aboard an Antioch-bound train as it approached 24th Street/Mission Station, the transit agency said Sunday afternoon. The suspect, a 34-year-old man, was spotted by a station agent

at Fruitvale Station Sunday around 2 p.m., BART officials said in a press release. The station agent contacted BART police who arrested the suspect without incident, according to BART. The agency had announced Sunday morning that BART police investigators had identified a suspect in connection with the stabbing. Transit officials said that one of BART's more than 4,000 surveillance cameras allegedly caught an initial image of the suspect, which helped investigators to identify him. https://abc7news.com/post/54-year-old-woman-stabbed-bart-train-san-francisco-police-searching-suspect/15502259/

Four Wounded After Axe Used In Fight On Paris Suburban Train
The Guardian, 11/4/2024

[Paris, France] Four teenagers were wounded, two of them seriously, after an axe was used during a fight on a suburban train outside Paris, French police sources have said. One of the victims, all aged 16 or 17, had a hand cut off and another had their skull split open. The main suspect in the incident was later arrested. The two other victims were less seriously injured in the altercation, which a police source said broke out at about 8am (0700 GMT) as the teenagers were on their way to secondary school. It was not immediately clear what triggered the fight, in which weapons including the axe, a knife, a samurai sword and baseball bats were used. https://www.theguardian.com/world/2024/nov/04/paris-suburban-train-axe-wounded

Large Fire Destroys Passenger Train, Cause Unclear
DW, 11/3/2024

[Berlin, Germany] An investigation was underway on Sunday after a passenger train was engulfed in a large fire while stopped at a station on the outskirts of Berlin overnight. Five passengers still on board had to exit the train but were unharmed. The fire department was initially unable to say where and why the fire on Saturday evening had started on the diesel-powered train. Firefighters were called to the Ahrensfelde station on the border between Berlin and Brandenburg after the alarm was raised at about 9:50 p.m. local time. The three-carriage train had been due to start its next trip to the town of Werneuchen when the train driver heard a bang. Smoke appeared and flames were seen, prompting the driver and a female attendant to evacuate the train's five passengers. The fire department extinguished the flames — which by then had engulfed all three cars — and no one was injured, a spokesman said. The train sustained major damage. https://www.dw.com/en/berlin-large-fire-destroys-passenger-train-cause-unclear/a-70676380

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

TERRORISM & EXTREMISM

Local Sheriff Asks FBI To Investigate Death Of Black Man Found Hanging In Alabama
Associated Press, 11/2/2024

[Montgomery, Alabama] The FBI is investigating the death of a Black man in Alabama, who was found hanging in an abandoned house, following a request from a local sheriff amid fears among community members who accuse local law enforcement of longstanding, unchecked misconduct. Sheriff's deputies found Dennoriss Richardson, 39, in September in a rural part of Colbert County, miles away from his home in Sheffield, a city of approximately 10,000 people near the Tennessee River. The Colbert County Sheriff's Office ruled Richardson's death a suicide. But Richardson's wife, Leigh Richardson, has said that is not true, explaining her husband did not leave a note and had no connection to the house where he was found. https://apnews.com/article/alabama-black-man-hanging-death-suicide-fbi-2e2222fe1ce9d5e37b67837734fb4339

Hate Crime And Terrorism Charges Filed After Jewish Man Shot In 'Targeted' Attack
NBC News, 11/1/2024

[Chicago, Illinois] Hate crime and terrorism charges were announced Thursday after a Jewish man was shot while walking to synagogue in Chicago over the weekend in what police now say was a "targeted" attack. Police had earlier this week announced multiple charges against 22-year-old Sidi Mohamed Abdallahi, who originally faced six counts of attempted first-degree murder and seven for aggravated discharge of a firearm at officers and firefighters, among other charges. On Thursday, Abdallahi was charged with an additional felony count of terrorism and one felony count of a hate crime, Chicago's top cop, Supt. Larry Snelling, said. The shooting took place at around 9:30 a.m. Saturday in the 2600 block of W. Farwell, police said, when Abdallahi allegedly opened fire on a 39-year-old man who was walking to synagogue. https://www.nbcnews.com/news/us-news/hate-crime-terrorism-charges-filed-jewish-man-shot-targeted-attack-rcna178348?utm_source=iterable&utm_medium=email&utm_campaign=11585704

SECURITY & SAFETY AWARENESS

Joint ODNI, FBI, And CISA Statement On Russian Election Influence Efforts
Cybersecurity and Infrastructure Security Agency, 11/1/2024

[Washington D.C.] Today, the Office of the Director of National Intelligence (ODNI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI), released the following statement: "The IC assesses that Russian influence actors manufactured a recent video that falsely depicted individuals claiming to be from Haiti and voting illegally in multiple counties in Georgia. This judgment is based on information available to the IC and prior activities of other Russian influence actors, including videos and other disinformation activities. The Georgia Secretary of State has already

refuted the video's claims as false. Russian influence actors also manufactured a video falsely accusing an individual associated with the Democratic presidential ticket of taking a bribe from a U.S. entertainer. https://www.cisa.gov/news-events/news/joint-odni-fbi-and-cisa-statement-russian-election-influence-efforts

ANALYST COMMENTARY: On 1 November 2024, the Office of the Director of National Intelligence (ODNI), the Federal Bureau of Investigation (FBI), and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint statement warning that Russian influence actors were continuing to attempt to "raise unfounded questions about the integrity of the U.S. election and stoke divisions among Americans." In the 1 November press release, the authoring agencies specifically mentioned a recent video that had been manufactured by Russian actors to sow discord in the U.S. and was shared online hundreds of thousands of times. The video depicts two men in a car who claim to be recent Haitian immigrants and say they cast votes in Georgia for the U.S. presidential election within six months of their arrival to the U.S., and encourage other Haitians to come to the U.S. According to the authoring agencies, the video is fake, and experts Clemson University have said that the fake video bears the hallmarks of the Russian disinformation operation known as Storm-1516. According to Darren Linvill of Clemson University, "[The video] narrative is consistent with what we've seen from Storm-1516, especially in recent weeks since they've turned their focus squarely on the U.S. election." While Election Day is almost here, there are no indications that these disinformation campaigns will lighten up in the comings weeks – last week, CISA Director Jen Easterly warned that, "it is between that period when polls close and when the vote is certified that our foreign adversaries will likely be most active in terms of trying to sow partisan discord and undermine American confidence" in the election.

ATA Launches New Truck Safety Management System
Owner Driver, 11/3/2024

[Australia] The Australian Trucking Association has written to its members to announce the release of the new TruckSafe safety management system, or SMS. The launch of the new SMS also includes an owner-driver SMS, which is specifically designed for individuals who operate their own vehicle without other employees involved in transport tasks. TruckSafe was created in 1996 as a response to governmental concerns regarding a perceived lack of safety improvements in the road transport industry. Now, it provides a risk-based approach to chain of responsibility, safety and compliance for its 180 members. TruckSafe Chair Paul Fellows says the new systems have the potential to be a game-changer for those who implement them. https://www.ownerdriver.com.au/ata-launches-new-truck-safety-management-system/

Washington's Supply Chain At Risk With EV Mandates
Freight Waves, 10/31/2024

[Washington State] New zero-emission vehicle (ZEV) mandates on the trucking industry are creating serious challenges for trucking fleets, which face limited and costly options in order to operate legally in Washington state. That should concern all of us, since almost 90% of consumer goods arrive by truck. At issue is the state's adoption of California's Advanced Clean Trucks (ACT) program. ACT is meant to move the industry toward zero emissions for medium- and heavy-duty trucks. Beginning next year, 7% of all heavy-duty trucks sold in Washington must be ZEVs. As manufacturers work toward compliance, Washington truck dealers are being forced to sell new ZEVs before they can sell legacy trucks.
https://www.freightwaves.com/news/washingtons-supply-chain-at-risk-with-ev-mandates

ANALYST COMMENTARY: Unfunded mandates create logistical challenges when legislation or regulations precede funding or the infrastructure required for compliance. In Washington State, zero-emission vehicle (ZEV) mandates combined with the need to stay competitive in the marketplace are creating challenges for trucking firms as a ZEV commercial truck costs more than two and a half times that of a clean diesel commercial truck, according to Freight Waves. In addition to the increased cost, ZEV trucks weigh more due to their batteries, which reduces their allowable cargo weight by two and a half tons, compared to a clean diesel truck. ZEV trucks have a significantly reduced range and Washington does not currently have the charging infrastructure to keep ZEV trucks operational. The permitting and construction time will take years. Freight Waves states that truck dealers in Washington estimate that "ZEV medium- and heavy-duty trucks will not work for 90% of existing routes." EV researchers at the University of Washington reported to Cascade PBS that Washington needs "10 to 100 times more public charging stations" to make ZEVs a viable option. Washington legislators have mandated that beginning in 2025, 7% of all heavy-duty trucks sold in Washington must be ZEVs, according to Freight Waves. Critics argue that this mandate will drive business out of the state and reduce Washington's competitive standing in the marketplace because purchasing a ZEV is not currently cost effective.

CYBERSECURITY

Ransomware Remains Top Cybersecurity Concern For Trucking Industry
CCJ, 10/29/2024

There's so much technology in the trucking industry these days to help carriers improve efficiencies by doing things like eliminating phone calls. But the telephone has become Steve Hankel's best friend. Hankel, the vice president of IT at Johanson Transportation, said he gets phishing emails at least three times a day saying something like "sign this urgent contract." "What I do now is I just delete everything and wait for someone to call if it really is something that they need done right away," he said. He said his

worst nightmare is a cyberattack on the Fresno, California-based 3PL, and every time there's an alert, or one of the company's systems goes down, his first thought is "we're being hacked." "It's ransomware. They're already in. It's kind of like that movie Scream. The call is coming from inside the house," he said during a panel at the National Motor Freight Traffic Association's (NMFTA) annual cybersecurity conference held in Cleveland, Ohio, this week.
https://www.ccjdigital.com/technology/cybersecurity/article/15706980/ransomware-remains-top-cybersecurity-concern-for-trucking-industry

ANALYST COMMENTARY: On 28 October 2024, Stephen Viña, the assistant national cyber director for policy development at the Office of the National Cyber Director (ONCD), highlighted a number of cyber-related threats facing the surface transportation industry while speaking at the National Motor Freight Traffic Association (NFMTA) Cybersecurity Conference 2024. Viña listed a number of threats, ranging from foreign backed advanced persistent threat (APT) campaigns to transnational organized criminals, ransomware, fraud, and thefts resulting from phishing and social engineering. These cyber concerns, particularly those involving ransomware, were echoed by other panelists at the conference, including Peeyush Patel, global chief information security officer at XPO, Steve Hankel, vice president of information technology at Johanson Transportation, and Carrie Yang, senior vice president at cybersecurity insurance broking firm Marsh Cyber Practice. Due to the interconnected nature of the surface transportation industry, organizations inevitably end up using third party software applications in their operations processes which can open their organizations to additional vulnerabilities. According to Patel, many times there has been a data breach in the surface transportation sector, the companies that have had their data exposed remain secure, and the breaches occurred within a third party whose software is being used to handle proprietary data. To mitigate these threats, panelists recommended that the surface transportation industry place increased emphasis on security by design, which is designing systems around security instead of 'adding' security features to existing systems and programs, particularly large scale applications used by multiple organizations.

Black Basta Operators Phish Employees Via Microsoft Teams
HelpNet Security, 10/28/2024

Black Basta ransomware affiliates are still trying to trick enterprise employees into installing remote access tool by posing as help desk workers, now also via Microsoft Teams. Earlier this year, Rapid7 warned about Black Basta using the following social engineering trick: they flood the target employee's email inbox with spam – typically from automated systems or services that send confirmations or notifications – and then phone them to offer assistance, while posing as their organization's IT help desk. Recently, though, they've also started using Microsoft Teams to reach out to potential victims. "After mass email spam events, the targeted users were added to Microsoft Teams chats with external users."
https://www.helpnetsecurity.com/2024/10/28/black-basta-operators-phish-employees-via-microsoft-teams/

Information Sharing & Analysis Center

PUBLIC TRANSPORTATION,
OVER THE ROAD BUS,
& SURFACE TRANSPORTATION

ANALYST COMMENTARY: Researchers have observed the threat actors flooding targeted users' email inboxes with spam, and then subsequently adding them to Microsoft Teams chats with external users operating from Entra ID tenants. These external users masquerade as support, administrative, or help desk staff, often using display names centered around the phrase "Help Desk." The ultimate objective is to coerce the targeted employees into installing remote monitoring and management tools, such as QuickAssist or AnyDesk, under the guise of providing technical support and remediation. In reality, these tools are used to gain initial access to the targeted environment and deploy credential-grabbing malware and network mapping tools. Additionally, the researchers have noted the presence of QR codes on domains featured in the attacks, though their exact function remains unknown. It is conceivable that these QR codes may direct users to further malicious infrastructure. To mitigate these threats, the researchers advise organizations to implement measures such as disabling or limiting communication from external tenants/domains within Microsoft Teams, tweaking email anti-spam policies, enabling comprehensive logging for Teams, creating rules to flag specific phishing chat requests and post-exploitation activities, and educating employees about the latest threats. By adopting these proactive security measures and remaining vigilant, organizations can enhance their resilience against the evolving tactics employed by Black Basta ransomware affiliates and similar threat actors.