From: Smith, Gary (TPD)
Sent: Thur 8/17/2023 4:12:38 PM
Subject: SSRIG Weekly Intelligence Summary 31- 2023 (August 17, 2023)
Received: Thur 8/17/2023 4:17:23 PM
SSRIG Weekly Summary 31-2023.pdf
23-0150 WSFC SETA - Washington State Fair (01Sep23) - 15Aug23 (U-FOUO).pdf
Washington State Fair 2023.pdf

Also Attached is the Washington State Fusion Center (WSFC) Special Event Threat Assessment (SETA) for the upcoming 2023 Washington State Fair and attached is the South Sound Regional Intelligence Group (SSRIG) Threat Assessment for the Washington State Fair 1-24 September

South Sound Regional Intelligence Group

SSRIG email: PCINTEL@piercecountywa.gov

Weekly Summary

#31-2023 August 17, 2023

Gary Smith
Intelligence Analyst
Gary.Smith@ci.tacoma.wa.us
(253) 594-7964

REGIONAL

WA Man on His Way to Sturgis Rally Arrested for Terrorist Threats

Puget Sound Auto Theft Task Force (PSATTF) releases auto theft stats for July 2023

OFFICER SAFETY

PC to Arrest for Robbery 1st.

Att Murder, Aslt, Att Rpe: Island (Tacoma PD)

OFFICER AWARENES

ATTEMPT TO LOCATE – MISSING PERSON

CYBER THREATS

CISA: New Whirlpool Backdoor Used in Barracuda ESG Campaign

US Critical Infrastructure Likely To Face Chinese Cyberattacks Amid Taiwan Conflict

PUBLIC SAFETY

A Longer-Lasting and More Powerful Treatment – New Antibody Reverses Effects of Potent Opioid

Border agents seize enough lethal drugs this fiscal year to kill more than 6 billion people

NATIONAL

Nationwide Swatting Campaign Demonstrates Employment of New Tactics

Swatting at Synagogues

(U//FOUO) Transnational: Domestic Violent Extremists and Criminal Actors Will Likely Continue Utilizing "OpenInfraMap" in Plots Targeting Electrical Infrastructure, Increasing the Likelihood and Impact of Successful Attacks

INTERNATIONAL

(U) Mexico: Authorities Discover a Criminal Surveillance Camera Network

Britain Warns of Possible Terrorist Attacks in Sweden

Other National/International Articles of Interest (Links):

Gary L. Smith
Gary L. Smith
Criminal Intelligence Analyst
Regional Intelligence Group
TPD/PCSD
Tacoma, WA
(253) 594-7964
(253) 405-6214 (C)
gary.smith@cityoftacoma.org
gary.smith@piercecountywa.gov

"There must be a Lone Ranger!" 

TACOMA /PIERCE COUNTY REGIONAL INTELLIGENCE UNIT

Special Event Threat Assessment

23-01

Wednesday, August 16, 2023

Det. Sgt. John Delgado (253) 341-1369
john.delgado@piercecountywa.gov

Gary L. Smith, Intel Analyst
gary.smith@cityoftacoma.org (253) 594-7964

(U) Washington State Fair Threat Assessment Overview 2023

Overview:
(U) The Washington State Fair is being held in Puyallup, Washington from 01–24 September 2023. The 5-year average attendance is between 1.1 and 1.2 million guests.

Fair Hours: On Weekends 09:30am - 10:30pm.
On Week Days 9:30am - 9:30pm. Some hours on Fridays and Sundays fluctuate. All Tuesdays are closed and Weds 6 SEP is closed. To see times and dates click-on the following link: https://www.thefair.com/general-info/dates-times/

(U) SEAR Level
(U//FOUO) The Washington State Fair has been designated a SEAR 3 event of national and/or international importance that requires only limited federal support.

Potential Threats:

Five major threats that have been used within the past year that could affect the State Fair:
1. Active Shooter or "Low-tech" assaults involving edged weapons and blunt objects, targeting spectators in the fairgrounds or those just walking towards the fairgrounds
2. IED attack with a bomb or some type of device strategically placed to bring harm & injury to crowds
3. Vehicle ramming targeting large crowded areas in, or just outside the fairgrounds, or at displays.
4. Drone attack dropping a bomb or some type of explosive device in a congested area, or just malicious use of drones during concert events.
5. Gang confrontation

(U) The United States remains in a high criminal threat status. Lone offenders and small groups motivated by a range of ideological beliefs and personal grievances continue to pose a persistent and lethal threat to the Homeland. Both domestic violent extremists (DVEs) and those associated with foreign terrorist organizations continue to attempt to motivate supporters to conduct attacks in the Homeland, including through violent extremist messaging and online calls for violence. In the coming months, factors that could mobilize individuals to commit violence include their perceptions of the 2024 general election cycle, upcoming High Profile Trial (Tacoma Police) in Tacoma starting 18 SEP and legislative or judicial decisions pertaining to sociopolitical issues. Likely targets of potential violence include US critical infrastructure, faith-based institutions, individuals or events associated with the LGBTQIA+ community, schools, racial and ethnic minorities, and government facilities and personnel, including law enforcement.

Recent Threat Activities:

*(U) On June 17, 2023, a mass shooting occurred at the Gorge Amphitheatre, near George, Washington. The shooter opened fire at a campground near the amphitheater, killing two people and wounding two others

* (U) July 01, 2023, An argument between multiple groups of people led to gunfire in a Puyallup church parking lot on that Saturday evening, injuring an innocent bystander. Puyallup Police said those involved were attending the Taste of Northwest in the Puyallup Fairgrounds. Puyallup Police said a dozen vehicles were hit by bullets as well. Shell casings of multiple calibers were located, they believe several guns were used and numerous people were involved in shooting at each other.

* (U) On August 04, 2023 a Bethlehem PA. man accused of threatening to set off explosives at the music festival, Musikfest, had homemade explosives and a homemade gun in his home when he was arrested Friday. The police announced the 53-year-old man was charged in the case. He was arraigned on two felony counts of possessing a weapon of mass destruction and misdemeanor offenses of possessing a prohibited offense weapon and possession of drugs and drug paraphernalia. Court documents state improvised explosive devices with black explosive powder and a fuse, as well as modified grenades, were found in the investigation Those documents also report he had a homemade shotgun capable of firing a 12-gauge round. Bethlehem PD received tips Thursday evening that he planned to set off an explosive at Musikfest; however, they say no specific time or place was provided.

* (U) On August 09, 2023 [in Rapid City, South Dakota] A man reportedly on his way to the Sturgis Rally with guns and possible explosives was arrested and charged with making a terrorist threat. John Charles Matthew Mann, 42, from Washington State was arrested Saturday during a traffic stop in Butte County. A court document from the Butte County State's Attorney's Office says when Mann was pulled over, law enforcement found two AR-15s, body armor, three handguns, bomb-making material, and a device that police say appeared to be a pipe bomb. Law enforcement also found a several hundred-page manifesto titled Manifesto: Descent into the Rational Justification for Genocide. The manifesto included descriptions of murder, mass killings, abduction and sexual molestation of children, and suicidal ideation. Mann is from University Place, Washington.

(U) Profile of an Active Shooter: An active shooter is an individual engaged in killing or attempting to kill people in a confined and populated area. In most cases, active shooters use firearms and there is no pattern or method to their selection of victims. Active shooter situations are unpredictable and evolve quickly. Typically, the immediate deployment of law enforcement is required to stop the shooting and mitigate harm to victims. Because active shooter situations often are over within 10 to 15 minutes, before law enforcement arrives on the scene, individuals must be prepared mentally and physically to deal with an active shooter situation.

(U) Bombing (IED/SVIED/VBIED): A device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals, and designed to destroy, incapacitate, harass, distract, or achieve mass destruction to people and property. Such explosives are typically devised from non-military components and are either set to detonate remotely or directly by some type of trigger; such devices may include *Improvised Explosive Devices (IED), Suicide-Vest Improvised Explosive Device (SVIED), or Vehicle-Borne Improvised Explosive Devices (VBIED)* which use explosives to weaponize cars, trucks, motorcycles, and even bicycles.

(U) Vehicle Ramming:
The use of a vehicle as a weapon in a terrorist attack is not new. Recent terrorist incidents and violent extremist propaganda demonstrate that the use of vehicles as a weapon continues to be of interest by those wishing to cause harm. Attacks of this nature require minimal capability, but can have a devastating impact in crowded places with low levels of visible security.

(U) (U//FOUO) Drones/Remote-Controlled Model Aircrafts: The SSRIG possesses no specific reporting regarding illicit plans to use Drones to target the Washington State Fair; Drones are increasingly worrisome due to their mass availability, popularity, and ease of use. Malicious use of Drones poses a potential risk to spectators, volunteers, security personnel, and first responders at sanctioned and non-sanctioned events around the Puyallup area.

(U) Additionally, unauthorized drones or unmanned aircraft systems (UAS) flying in close proximity to event venues and participants can cause accidental or intentional harm.

(U) Gangs: One of the biggest threats to the State Fair may come in the form of gang-on-gang rivalry confrontations in which innocent bystanders get in the way. There continues to be a high level of drive-by shootings in the Tacoma **area** and there is a potential for revenge attacks occurring against rival gang members during the Event. Gang-related violence has increased over the past four years and we are seeing a "fight on sight" mentality between rival street gangs in Pierce County. When they encounter each other — in public or in private — it is likely to turn violent.

(U//FOUO) Possible indicators of preoperational surveillance or attack planning include:

(U//FOUO) Suspicious probing of facility public access points potentially to identify a physical security weakness.

(U//FOUO) Loose or bulky clothing, often inappropriate for the weather and circumstances, can conceal a vest bomb, weapons or other articles (though many have used backpacks instead of vest bombs, particularly in the summer).

(U//FOUO) Unusual or prolonged interest in or attempts to gain sensitive information about security measures of personnel, entry points, peak days and hours of operation, and access controls such as alarms or locks.

(U//FOUO) Observation of security reaction drills or procedures; multiple false alarms or fictitious emergency calls to same locations or similar venues.

(U//FOUO) Suspects may also be hugging their packages, or keep checking the contents of a backpack or heavy shopping bag.

(U//FOUO) Attempts by a commercial vehicle driver to unnecessarily or unlawfully infiltrate areas where crowds are gathered.

(U//FOUO) Commercial motor vehicles being operated erratically, at unusual times, or in unusual locations, particularly in heavy pedestrian areas.

(U//FOUO) Presentation of altered or questionable driver's license, proof of insurance, credit cards, or other required documents when purchasing or renting vehicles.

International Based Threats:
Every year the State Fair dates occur during the Anniversary of 9/11. Terrorists inspired by foreign ideologies continue to attempt to exploit security vulnerabilities through a variety of tactics, including creating sophisticated devices they believe could bypass security measures; emplacing devices in locations with limited to no security presence; or opting to conduct attacks on locations that have significant security outside of controlled access points. Terrorists continue to use large crowds and seemingly innocuous items such as backpacks and luggage to conceal improvised explosive devices (IEDs) from detection by law enforcement and security personnel. Increased awareness and continued outreach to front line security, law enforcement, first responders, and the public can continue to provide opportunities for interdiction and disruption of potential plots.

*Support to al-Qaeda / ISIS continues, when a 17-year-old in Philadelphia was arrested on August 11, 2023 in connection with a terrorism probe. The FBI said the 17-year-old male was arrested on state charges and was allegedly communicating with the group Katibat al Tawhid wal Jihad (KTJ). KTJ was designated as a global terrorist group in 2022 and affiliated with al-Qaeda, officials said. A law enforcement official told media that the suspect was radicalized online. The FBI said the teen had access to firearms and had recently purchased items and materials commonly used in the construction of improvised explosive devices (IED). Among the items allegedly purchased were tactical equipment, chemicals, wiring, and devices often used as remote detonators. Authorities say some of the items were purchased in the last few weeks. The suspect had conducted "general research" into specific targets, and not only in the Philadelphia area, the FBI added.

The SSRIG urges state, regional, local, tribal, and private security partners to maintain increased vigilance for indicators of pre-operational surveillance and suspicious activity, to include being aware that the State Fair, the surrounding events and activities during this timeframe could influence terrorists, lone offenders, and criminal extremists to act with little or no warning.

Other Criminal Activity of Concern:
--Passing counterfeit money
--Employee theft issues
--Vehicle prowl/theft
--Police/First Responder Impersonators

Officer Safety:
**Ambush attacks against law enforcement officers remain a threat to officer safety, with the number of attacks per year holding steady, the proportion of fatal attacks on officers attributable to ambushes are increasing. Concerns about targeted violence against police are on the rise, while officers must not only be guardians of the public but also be prepared to respond to violence targeting them. Officers standing and conducting traffic & crowd control duty for long hours outside the State Fair grounds at intersections or barricades need to be vigilant with their personal situational awareness for their own safety!

Patrol Tactics:
- Prior to patrol, check for any visible signs of tampering with your patrol vehicle.
- Avoid concealed stationary locations to run radar or while observing traffic patterns.
- Alternate vehicle approaches using both driver and passenger side of vehicles.
- When staffing permits, use two person patrols, effective coordination and communication with area law enforcement agencies are key.
- Know the deficiencies and shortfalls in the communication systems within your patrol areas.
- Always maintain a high state of awareness on and off duty, given the nature of our profession and the potential for violence.

**Law enforcement personnel are reminded to remain ever vigilant and aware of our surroundings both on and off duty.

In conclusion: A higher likelihood exists within the areas of the State Fair for exposure to public safety threats resulting from adverse gang interactions, criminal extremists, anti-police agitations, nuisance drones, and misdemeanor acts by opportunists having criminal intent. Historically, these incidents result in public disturbances, impromptu demonstrations, thefts, and nuisances related to public intoxication, disorderly conduct, and criminal mischief.

**Currently, there is no information indicating a specific terrorist threat to any venue or event related to the Washington State Fair in Puyallup. There is also no specific evidence of a criminal group or element intentionally targeting observers or participants for criminal purposes. The above information is a reminder for those Law Enforcement officers covering this to be aware of for security purposes. If any Law Enforcement Officers or Fair Officials see or receives any suspicious activity/behavior such as possible surveillance, questions by individuals about security postures at critical infrastructure or locations where an event that may experience a large number of people in a confined space, please notify the SSRIG at PCINTEL@co.pierce.wa.us.

WSFC Tracking Number # 23-0150

Washington State Fusion Center
Special Event Threat Assessment

Phone: 1-877-843-9522
E-mail: intake@wsfc.wa.gov

Tracked By: HSEC-8 and WSFC SIN-1

WASHINGTON STATE FAIR (SEPTEMBER 1-24, 2023)

(U) Special Event Assessment Rating: SEAR 3 – An event of national and/or international importance that requires only limited federal support.

Washington STATE FAIR

(U) Event Description:

(U) The Washington State Fair is being held September 1-24, 2023, at the Washington State Fair Events Center in Puyallup, Washington. With more than one million people expected to attend, it is the largest fair in the Pacific Northwest, and includes concerts, art and animal exhibits, and the Puyallup Rodeo. Daily attendance can range from 30,000 to 130,000 people depending on the day of the week, weather conditions, and scheduled high-profile concerts. All gates will have a law enforcement presence, and all guests will be subject to weapons detection screening upon entering.

(U) Executive Summary:

(U//FOUO) The Washington State Fusion Center (WSFC) is not currently aware of any credible or specific threats targeting the Washington State Fair, or the Washington State Fair Events Center. However, given the ongoing surge in gun violence and mass shootings nationwide, there is an increased risk for large public gatherings to experience random violence, targeted violence, and mass casualty incidents.

(U) The United States remains in a heightened threat environment. Lone offenders and small groups motivated by a range of ideological beliefs and personal grievances continue to pose a persistent and lethal threat to the Homeland. Both domestic violent extremists (DVEs) and those associated with foreign terrorist organizations continue to attempt to motivate supporters to conduct attacks in the Homeland, including through violent extremist messaging and online calls for violence.[1]

- (U) On July 22, 2023, an illegal street racing event led to a shooting near the Capitol Hill Block Party in downtown Seattle. Four people were injured and taken to Harborview Medical Center. The crowd resisted responding officers, complicating their efforts to get to the victims.[2,3]
- (U) On July 1, 2023, after attending The Taste Northwest in Puyallup, Washington, an argument between multiple individuals led to gunfire in a nearby church parking lot, injuring one bystander.[4,5]
- (U) On June 17, 2023, a mass shooting occurred at the Gorge Amphitheatre, near George, Washington. The shooter opened fire at a campground near the amphitheatre, killing two people and wounding two others.[6,7,8]

(U) Other likely threats exist from nuisances related to public intoxication and various criminal activities such as theft, disorderly conduct, and assault—as well as vehicle accidents and possible road rage incidents caused by event-related traffic congestion.[9,10,11] Additionally, unauthorized drones or unmanned aircraft systems (UAS) flying in close proximity to event venues and participants can cause accidental or intentional harm.[12]

(U) Key Findings:

- (U//FOUO) The WSFC is not currently aware of any credible or specific threats targeting the Washington State Fair, or the Washington State Fair Events Center.
- (U//FOUO) Given the ongoing surge in gun violence and mass shootings nationwide, there is an increased risk for large public gatherings to experience random violence, targeted violence, and mass casualty incidents.

WASHINGTON STATE FAIR

Start Date: September 1, 2023	City: Puyallup	Location: Washington State Fair Events Center	Estimated Crowd Size: > 1,000,000
End Date: September 24, 2023	County: Pierce	Venue Type: Open-Air	Waterborne: No [2]
Timeframe: See Website	Region: 5	Venue Access: Highly Restricted [1]	Fireworks: Yes [3]

(U) Mitigation and Prevention Measures:

(U//FOUO) The security footprint for a special event extends beyond the perimeters of the event itself, and could have cascading effects on surrounding areas and critical infrastructure. Recognizing indicators of terrorist activity and having appropriate emergency planning and response measures in place could reduce the risk to the event or venue. For more information on the threats, vulnerabilities, and protective measures for special events, reference the additional resources listed below.

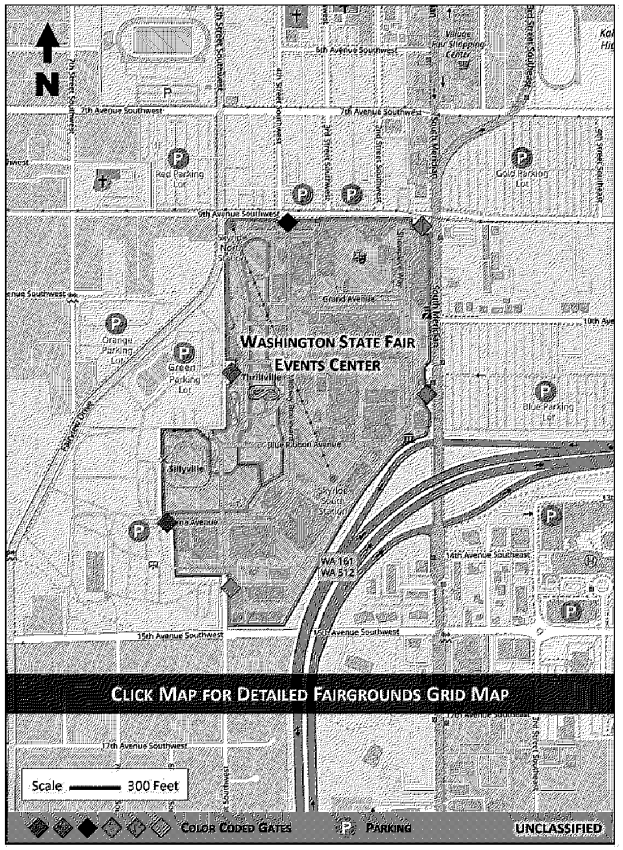
(U) Suspicious Activity – Indicators and Behaviors:

- (U) Reported theft of explosives or consumer grade fireworks. [Suquamish Police J23000297]
- (U) Theft of law enforcement, security, and public safety uniforms. [SPD 2023-178470]
- (U) Operating a UAS in a manner that poses a threat of harm to people or property.
- (U) An individual who may have recently acquired firearms and ammunition in combination with making online threats.
- (U) Persons in crowded areas wearing clothing that is unusually bulky or atypical for the season or event, possibly to conceal explosives or weapons.

(U) Additional Resources: [HSIN Login Required for Access *]

- 23-0045 WSFC – 2023 Annual Threat Assessment – 18Apr23 (U-FOUO) *
- CISA – Suspicious or Unattended Items (U)
- NCTC – US Violent Extremist Mobilization Indicators – 28Dec21 (U)
- HSIN Washington Infrastructure Protection (WA-IP) – Unmanned Aircraft Systems (UAS) (U-FOUO) *
- HSIN Washington Infrastructure Protection (WA-IP) – Vehicle Rammings (U-FOUO) *

1 – (U) Event has significant security measures placed around event. The event will be either credentialed or possess multiple checks (e.g., bag search, metal detectors).
2 – (U) Is a significant portion of the event's perimeter within 200 feet of a body of water that is navigable by a small power boat?
3 – (U) Fireworks show every Friday night at approximately 2200.



TACOMA /PIERCE COUNTY REGIONAL INTELLIGENCE UNIT

WEEKLY SUMMARY

31-2023 Thursday, August 17, 2023

Det. Sgt. John Delgado (253) 341-1369
john.delgado@piercecountywa.gov

Gary L. Smith, Intel Analyst
gary.smith@cityoftacoma.org (253) 594-7964

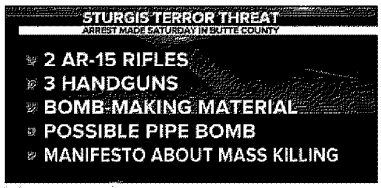
REGIONAL

WA Man on His Way to Sturgis Rally Arrested for Terrorist Threats

[Rapid City, South Dakota] A man reportedly on his way to the Sturgis Rally with guns and possible explosives was arrested and charged with making a terrorist threat. John Charles Matthew Mann, 42, from Washington State (University Place) was arrested Saturday during a traffic stop in Butte County.

A court document from the Butte County State's Attorney's Office says when Mann was pulled over, law enforcement found two AR-15s, body armor, three handguns, bomb-making material, and a device that police say appeared to be a pipe bomb.

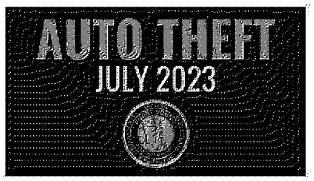
Law enforcement also found a several hundred-page manifesto titled Manifesto: Descent into the Rational Justification for Genocide. The manifesto included descriptions of murder, mass killings, abduction and sexual molestation of children, and suicidal ideation.



Mann is being charged with one count of terroristic threats, a class 5 felony, and one count of use of a hoax substance or device to cause fear, a class 6 felony. His initial appearance was Tuesday where his bond was modified to $75,000 but was later changed to $250,000 after a request from the state.

He's scheduled for arraignment on September 6. Court records say Mann is from University Place, Washington. Source; Daily Dot, 8/9/2023

https://www.blackhillsfox.com/2023/08/10/man-arrested-terrorist-threats-his-way-sturgis/



Puget Sound Auto Theft Task Force (PSATTF) releases auto theft stats for July 2023

The auto theft stats for July 2023 are in. There were 642 vehicles reported stolen in Pierce County and 1,696 reported stolen in King County. That's an average of about 75 per day! Our team is out there every day working to tackle this problem, but there are also things you can do to lessen your risk of becoming a victim:

– Remove or hide all valuables

– Lock your car

– Don't leave keys or fobs inside

– Don't leave your vehicle running unattended (exhaust in cold months makes these vehicles easy to spot)

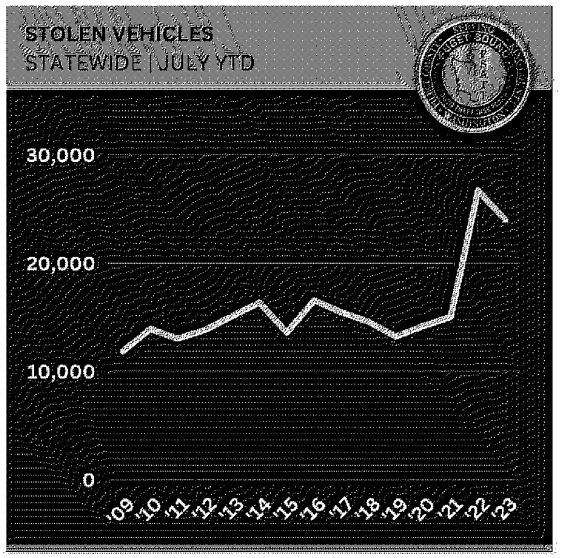
– Use anti-theft devices (alarm, kill switch, steering wheel lock)

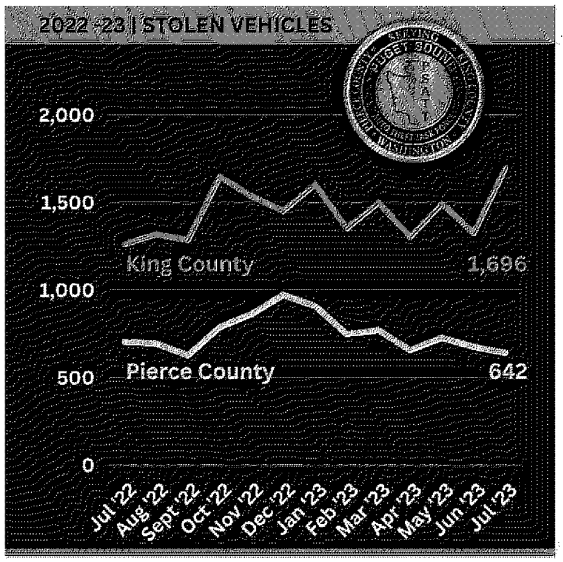
– Park in well-lit areas

While it's important for all vehicle owners to consider using an anti-theft device, we strongly encourage residents of apartment complexes to make this a priority because these complexes are a top target for car thieves. Steering wheel locks are strongly recommended for owners of Hyundai and Kia models that are vulnerable to theft. Even if you have already upgraded your software, we still suggest using a steering wheel lock as a visual deterrent. Otherwise, you may end up with a shattered window and a damaged ignition before the thief realizes your car can't be stolen. Multiple theft attempts are reported each day.

We also suggest leaving a GPS tracker, such as an Air Tag or Tile, in your vehicle so that you (we) can track it if it does get stolen.

So far this year, 24,025 vehicles have been reported stolen statewide.





Link: https://blog.piercecountywa.gov/autothefttaskforce/2023/08/16/psattf-releases-auto-theft-stats-for-july-2023/

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

OFFICER SAFETY

Special Bulletin

TACOMA POLICE DEPARTMENT

Bulletin Number: S23-150 **August 16, 2023**

Det. Scott Meffen #277
Tacoma Police Department
Robbery Unit

Office: (253) 830-6556
Cell: (253) 533-0228
Email: Smeffen@cityoftacoma.org

PC to Arrest for Robbery 1st.
23-209-01970

Suspect
-Jacobski, Jared R.
-05/19/1983
-6'1"
-Unknown address
(Homeless living in an RV)

On July 23rd, 2023, at approximately 0600 hours Jacobski committed a home invasion, armed robbery. Jacobski was **armed with a gray 9mm handgun** during the robbery. Jacobski was with another Pacific Islander male (currently unknown) who was also armed with a handgun. Jacobski is known to frequent the "Oakland" area of Tacoma. He may also be in an RV around 5600 S. Yakima Ave. Jacobski was recently involved in a shooting that's being investigated by TPD.

If Jacobski is located there is PC for his arrest. A booking form is at TPD Ops Desk. Tow any vehicle Jacobski is in back to TPD secure storage for a search warrant. If Jacobski is arrested, please notify Detective Scott Meffen at 253-533-0228 or Detective Garret Walk 253-318-7393 for an interview.

PC AT THIS TIME – SUSPECT IS ARMED AND DANGEROUS –

Special Bulletin

TACOMA POLICE DEPARTMENT

Bulletin Number: S23-124a **August 15th , 2023**

Det. C. Brooks
Tacoma Police Department
Criminal Investigations
Cell (253) 606-1321
Email cbrooks@cityoftacoma.org

Att Murder, Aslt, Att Rpe: Island (Tacoma PD)

WARRANT/OFFICER SAFETY-ISLAND HAS A UNCONFIMRED FELONY NO BAIL WARRANT OUT OF CHELAN COUNTY AND HAS THREATENED TO SHOOT IT OUT WITH LAW ENFORCEMENT BEFORE GOING BACK TO JAIL

Island, Marcellus V.
DOB 02/09/1980
B/M 6 foot, 185 lbs black hair
Address: possibly living in his vehicle LKA/incident address 4366 E Q St Tacoma
WA #CGC4456 2006 Pontiac Grand Prix Blue in color

ConsideredArmed and Dangerous-Last known to be in possession of 2 small firearms (possibly a .380 cal handgun)

Island has an unconfirmed Felony No Bail Warrant out of Chelan County for UPOF X3 and UPCS.
CONFIRM WARRANT PRIOR TO SERVICE

If located notify Detective C. Brooks @ 253-606-1321.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

OFFICER AWARENESS

Pierce County
Sheriff's Department
CRIMINAL INVESTIGATIONS DIVISION

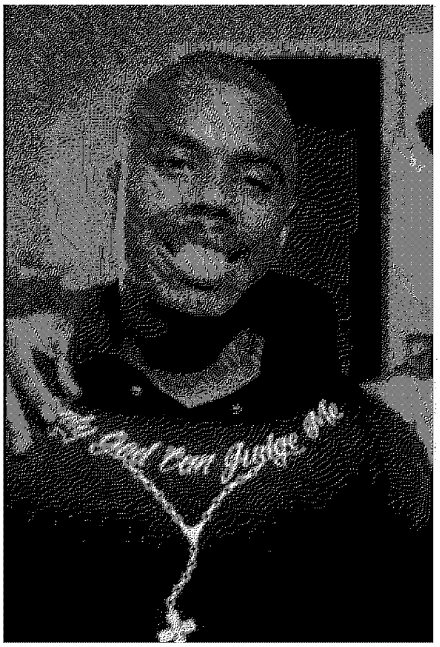
SPECIAL
BULLETIN

PCSD CID 23-052s | PCSD CRIMINAL INVESTIGATIONS DIVISION | August 16, 2023

ATTEMPT TO LOCATE – MISSING PERSON

Pierce County Sheriff's Detectives are attempting to locate Missing Person, Tionne J Curry. He is listed as a missing person under PCSD #23-224-02160.

Curry was reported missing on 08-12-2023. He was last seen leaving his residence at Mashburn Adult Family Home at around 2045 hours and did not return to the residence. He is diagnosed with schizophrenia and has not been taking his medication since he left the home. Curry has a history of drug use and frequents gas stations and convenience stores.
If Curry is located, please clear him as a missing person with SS911 and notify Detective Monti Minion at monti.minion@piercecountywa.gov.



NAME: Tionne J. Curry
DOB: 05-07-1991
PHY: Black Male, 5'10", 180 lbs., black/brown, brown eyes
LKA: 5915 258th St Ct E. Graham WA 98338
Clothing: Last seen wearing a gray jacket and blk shorts.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

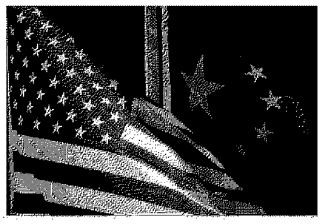
CYBER THREATS

CISA: New Whirlpool Backdoor Used in Barracuda ESG Campaign

Security researchers have discovered a third novel backdoor that was used in attacks on users of Barracuda ESG appliances recently. The US Cybersecurity and Infrastructure Security Agency (CISA) has released a new advisory detailing the malware, dubbed "Whirlpool." It claimed the backdoor established a TLS reverse shell to a command-and-control (C2) server. "This artifact is a 32-bit ELF file that has been identified as a malware variant named 'Whirlpool,'" the document noted. "The malware takes two arguments (C2 IP and port number) from a module to establish a Transport Layer Security (TLS) reverse shell. The module that passes the arguments was not available for analysis." Source; Infosecurity Magazine, 8/11/2023

Analyst Comment The Cybersecurity and Infrastructure Security Agency (CISA) has released a report detailing a new backdoor malware discovered in attacks on Barracuda Email Security Gateway (ESG) appliances. The backdoor, dubbed Whirlpool, "establishes a Transport Layer Security (TLS) reverse shell to the Command-and-Control (C2) server." CISA has released three reports on backdoor malware variants affecting Barracuda ESG appliances. The malwares are associated with the exploitation of CVE-2023-2868, which is a remote command injection vulnerability affecting Barracuda ESG Appliance, versions 5.1.3.001-9.2.0.006. The flaw was first discovered in May 2023, but has been actively exploited since October 2022. Mandiant published a report linking the active exploitation of CVE-2023-2868 to Chinese threat actor UNC4841. Barracuda ESG is software that filters inbound and outbound email and protects customer data. It can be deployed as a physical or virtual appliance, or in a public cloud environment on AWS or Microsoft Azure. The attack is largely thought to be an espionage-motivated attack as the threat actors use the backdoors to maintain persistence in a victim's system. The previously discovered malware variants reported by CISA are Seaspy, Submarine, and Barracuda Exploit Payload and Backdoor. Rapid7 has advised that "Barracuda is urging ESG customers to immediately decommission and replace all impacted ESG physical appliances irrespective of patch level."

US Critical Infrastructure Likely To Face Chinese Cyberattacks Amid Taiwan Conflict



U.S. critical infrastructure entities have been warned by Cybersecurity and Infrastructure Security Agency Director Jen Easterly regarding the possibility of disruptive Chinese cyberattcks in the event of U.S. involvement in a potential invasion of Taiwan, according to The Record, a news site by cybersecurity firm Recorded Future. "In some of the products that we put out earlier this year, a cybersecurity advisory talked about Chinese state-sponsored actors living off the land. So not malware but using the native processes of a computer to hide in those systems. Source; SC Media, 8/15/2023

Analyst Assessment On 12 August 2023, while speaking at the DEF CON hacker conference in Las Vegas, Nevada, Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly warned that "China's hackers have been positioning themselves to conduct destructive cyberattacks on U.S. critical infrastructure." According to Director Easterly, cyberattacks leveraged against critical infrastructure by China would represent a significant pivot in the tactics, techniques, and procedures (TTPs) observed in Chinese hackers, which historically has "largely consisted of a barrage of espionage and their of data but not destructive attacks designed to harm systems." David Pekoske, the director of the Transportation Security Administration (TSA), also spoke at the DEF CON panel and said that critical infrastructure operators need to prepare for possibility of such cyberattacks immediately to ensure they are not caught off-guard in the future. These warnings are consistent with the assessments contained in the February 2023 National Threat Assessment, in which the Office of the Director of National Intelligence (ODNI) reported that "China almost certainly is capable of launching cyber-attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems." In May 2023, three months after the National Threat Assessment was released, Microsoft's Threat Intelligence team reported that they had "uncovered stealthy and targeted malicious activity focused on post-compromise credential access and network system discovery aimed at critical infrastructure organizations in the

United States," and that the malicious activity was being carried out by a state-sponsored cyber actor based in China known as Volt Typhoon. According to the Microsoft Threat Intelligence team, Volt Typhoon was assessed with moderate confidence to be "pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises." Source; Over the–Road-Bus Intelligence Awareness Daily (OTRBIAD) Report

PUBLIC SAFETY

A Longer-Lasting and More Powerful Treatment – New Antibody Reverses Effects of Potent Opioid

August 11, 2023 (SciTech Daily). Scripps Research Institute, San Diego, CA - In the study, published in *ACS Chemical Neuroscience* on August 3, 2023, the researchers developed a human antibody that binds very tightly to carfentanil, fentanyl, and other fentanyl variants. In rodents, they showed that administering a solution of the antibody shortly after an overdose reverses the potentially deadly respiratory depression caused by carfentanil, the most dangerous of the variants. The results suggest that the antibody could be a more powerful, longer-lasting treatment for synthetic opioid overdose, compared to existing options. Fentanyl and carfentanil overdoses currently are treated with the mu-opioid receptor-blocking drugs naloxone and naltrexone, but these treatments are sometimes ineffective against synthetic opioids even [when] large doses [are administered]. Moreover, the benefits of these treatments typically last for less than an hour after dosing—potentially allowing respiratory depression from fentanyl or carfentanil (which persist much longer in the body) to resume. To obtain antibodies, the team vaccinated rodents with a molecule they designed that would elicit antibodies against carfentanil, fentanyl, and variants.

The rodents were engineered to produce human antibodies (rather than rodent antibodies, which would trigger an unwanted immune response if administered to humans). Among the resulting antibodies, the researchers were able to identify several that bind to carfentanil with super-high affinity—and bind very strongly to fentanyl and several other fentanyl derivatives. They then selected the most potent of these antibodies, modified it to be more lightweight (so that it would get quickly into the bloodstream), and further altered it so it would persist in the blood for days. Tests in rodents showed that the optimized [single-chain variable fragment] scFv, dubbed C10-S66K, did indeed have a powerful effect at reducing carfentanil's actions on the brain—reversing carfentanil-driven respiratory depression when injected 15 minutes after a heavy carfentanil exposure. The effect after about 40 minutes was stronger than naloxone's and was still increasing after two hours, whereas naloxone's peaked at 30 minutes and swiftly declined.

Source;https://scitechdaily.com/a-longer-lasting-and-more-powerful-treatment-new-antibody-reverses-effects-of-potent-opioid/?expand_article=1&_sm_au_=isVkkVZrn5kNWvT7NGqvvK6qTvMRG

Border agents seize enough lethal drugs this fiscal year to kill more than 6 billion people

U.S. Customs and Border Protection [CBP] officials alone have seized enough lethal drugs this fiscal year through June to kill more than 6.4 billion people. The amounts of lethal doses they've seized of fentanyl, methamphetamine, and cocaine are enough to kill the U.S. population 19 times. Fiscal year through June, CBP agents have seized 22,000 pounds of fentanyl at ports of entry nationwide, according to most recent data. They also seized 175,000 pounds of methamphetamine and over 70,000 pounds of cocaine. These amounts are greater than what was seized in all of fiscal 2022. Two milligrams of fentanyl are considered a lethal dose. One pound, equivalent to 453,592.4 milligrams, is enough to kill 226,796 people. Twenty-two thousand pounds is enough to kill nearly 5 billion people. According to AddictionResources.net, a lethal dose of cocaine is over 30 mg; a lethal dose of methamphetamine is an estimated 200 milligrams. Based on these estimates and the seizure amounts, CBP agents seized

enough lethal doses of methamphetamine to kill nearly 397 million people and enough lethal doses of cocaine to kill over one billion people. Combined, fiscal year through June, enough lethal drugs have been seized by CBP alone to kill over 6.4 billion people – greater than 19 times the U.S. population of over 335 million.

These seizures exclude those made by state and other federal agencies. In Texas, for example, over 422 million lethal doses of fentanyl have been seized through its border security mission Operation Lone Star. In Arizona, one multiagency effort resulted the seizure of enough illicit drugs, including fentanyl, to kill over 40 million people. In one single carload bust in Los Angeles, authorities seized enough fentanyl to kill over 600,000 people. In Florida, one multiagency bust seized enough fentanyl to kill the state's entire population, and that was after a previous bust that seized enough to kill half the state's population. https://www.abqjournal.com/news/national/border-agents-seize-enough-lethal-drugs-this-fiscal-year-to-kill-more-than-6-billion/article_6692bba4-ce9b-5bed-bca7-4366369093eb.html August 14, 2023 (Albuquerque Journal).

NATIONAL

LAW ENFORCEMENT SENSITIVE

NEW YORK CITY POLICE DEPARTMENT

TACTICAL ASSESSMENT

Intelligence Operations & Analysis Section

Nationwide Swatting Campaign Demonstrates Employment of New Tactics

"SWATTING"

Swatting is the criminal act of falsely reporting a crime or emergency in order to evoke a law enforcement response—often in the form of a SWAT team—to a victim's residence, place of work, or targeted location in an attempt to harass or intimidate them. Swatting permits online malicious actors, referred to as "trolls," to target victims beyond the virtual sphere by prompting law enforcement intervention at their homes and businesses.

The NYPD Intelligence & Counterterrorism Bureau (ICB) has observed a recent series of nationwide swatting incidents orchestrated by an international network of racially and ethnically motivated actors, who are employing a variety of unique tactics in an attempt to disrupt the daily operations of targeted institutions across the U.S., including in the New York City area. Since 24 July 2023, there have been at least five swatting incidents in New York City, including three directed at synagogues in Manhattan over the past two weeks. NYPD online observations indicate that these swatters operate on encrypted channels within online gaming communities where they recommend swatting targets, distribute potential swatting methods, and share the results of swatting attempts. These malicious actors, who regularly propagate white supremacist, anti-Semitic, and neo-Nazi rhetoric and content online, have targeted religious institutions in many of these swatting attempts in order to intimidate perceived rivals and/or members of marginalized groups. The NYPD has observed swatters in these incidents employ a variety of technologies aimed at perpetrating these threats anonymously, including the use of virtual private networks (VPNs), Voice over Internet Protocol (VoIP) numbers, and two-factor authentication bypass tools.

- The NYPD has observed these swatters prioritize the targeting of locations that offer livestreaming services, enabling them to view the swatting and subsequent evacuations in real time. To date, the most frequently exploited live streams are those of religious institutions, specifically churches and synagogues, which broadcast religious services to remote audiences.

- In addition to traditional swatting tactics, such as fraudulent 911 calls to falsely report emergencies and direct threats to targeted institutions, these online users have orchestrated swattings through the use of anonymous suicide and crisis counseling services. After an anonymous user is paired with a counselor in an online chatroom, the user will threaten acts of violence and provide the counselor with the address of a targeted institution to trick law enforcement personnel into responding to that particular location.

- These online users document and share their swatting efforts, keeping score and competing with each another. It is common practice for these swatters to record a target institution's livestream as proof of success and to share the livestream among likeminded users within the gaming communities. Swatters have also livestreamed themselves while making fraudulent 911 calls, incorporating real time suggestions from likeminded users.

- The NYPD assesses these swatters are conscious of operational security, and take extensive measures to remain anonymous. Online observations indicate:

- Groups of swatters share Virtual Private Network (VPN) accounts to hide their true IP addresses and make it appear as if they are connecting to the internet from a region of their choice, which sometimes corresponds to the location of the target they intend to swat.

- Swatters create "throwaway" email addresses for single or limited use applications, and bypass the two factor authentication requirements of email providers by using free temporary phone numbers acquired online.

- Using "throwaway" email addresses, swatters create and share accounts on virtual applications that provide users access to free, anonymous phones numbers. These phone numbers operate with a Voice over Internet Protocol (VoIP), allowing users to make calls using WiFi, rather than relying on a telephone service provider.

- While unconfirmed if employed in this recent series of swattings, past swatters have relied on digital synthesizers and artificial intelligence (AI) tools to mask their true voices.

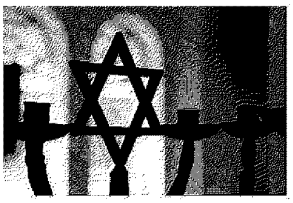
SITUATIONAL AWARENESS

Based on ongoing swatting incidents nationwide, including in the New York City area, the NYPD recommends the following best practices for uniformed members of service:

- Supervisors should **ensure all personnel are apprised of this ongoing nationwide swatting campaign,** including the common tactics utilized by these online malicious actors.
- Officers should continue to respond to emergency calls with the impression that they are truthfully reported, maintaining **elevated situational awareness.**
- While responding, officers should **attempt to verify the validity of the reported emergency** by contacting the incident reporter and/or the targeted institution for additional information.
- Officers should remain aware that they may be filmed and/or livestreamed by swatters as they respond to a reported emergency.

Source; New York Police Department, Intelligence Operations and Analysis Section

Swatting at Synagogues



The Anti-Defamation League (ADL) called this week for law enforcement and community leaders to act, as 28 synagogues and ADL offices across the country have been the victim of fake bomb threats and swatting calls. Some synagogues targeted were livestreaming their services as police arrived, interrupting services. The caller of the hoax then posted clips of the incidents online, reported the NYT. A group of online 'trolls' have been the source of the calls that include anti-semitic language and the group has also been linked to targets that includes African-American churches and at least one news organization. On Saturday, a Manhattan synagogue was vandalized by an individual who was later arrested, reported the New York Daily News. A second act of vandalism to a Yeshiva in the same neighborhood occurred nine months ago.

*Analyst Assessment** Though these swatting incidents have an anti-Semitic bias, they are also examples of extremists using the internet to publicize their messaging and harass their perceived enemies. Law enforcement is extremely sensitive to reports of violence at places of worship, schools, or public gatherings. Any call reporting violence will elicit a major response. The arriving units may evacuate a building, causing congregates to exit in fear and disrupting services till the location is properly searched. The callers are using technology to select targets across the US, capturing the incidents on livestream to amplify their message, then posting the results on social media. All calls for emergency assistance must be treated as legitimate until determined to be a hoax. Source: Watchline@fdny.nyc.gov

(U//FOUO) Transnational: Domestic Violent Extremists and Criminal Actors Will Likely Continue Utilizing "OpenInfraMap" in Plots Targeting Electrical Infrastructure, Increasing the Likelihood and Impact of Successful Attacks

(U//FOUO) According to a Wisconsin Statewide Intelligence Center (WSIC) Critical Infrastructure Analytic Report Update dated 10 AUG 23, in 2023, two racially or ethnically motivated violent extremist – white supremacists (RMVE-WS) were arrested for attempting to destroy electrical infrastructure. Authorities discovered that the suspects used OpenInfraMap to research electrical infrastructure.

- **(U//FOUO)** On 03 FEB 23, two RMVE-WS in Maryland were charged with conspiracy to destroy an energy facility. The suspects allegedly planned to shoot at electrical substations to cause a "cascading failure" that would destroy the City of Baltimore, according to federal intelligence reporting. According to the criminal complaint, they exploited OpenInfraMap to share substation locations in Maryland when selecting which targets to attack for maximum impact to the power grid.

(U//FOUO) Since 2021, online actors in RMVE-WS associated communication channels continue to encourage exploitation of OpenInfraMap when planning attacks against electrical infrastructure:

- **(U//FOUO)** On 07 DEC 22, a suspected RMVE-WS public instant messaging platform channel user encouraged supporters to terrorize and stress the system by sabotaging local power grids and resources and provided a hyperlink to OpenInfraMap for "learn[ing] more about where power grids are located", according to federal intelligence reporting.

- **(U//FOUO)** On 09 AUG 22, a user of a suspected RMVE-WS public instant messaging chat group posted location information regarding critical infrastructure in the US, Canada, and Mexico and encouraged exploiting OpenInfraMap for information regarding critical infrastructure in the US and other countries, according to federal intelligence reporting.

- **(U//FOUO)** On 15 OCT 21, a user of an RMVE-WS-aligned Telegram channel suggested supporters familiarize themselves with infrastructure in their area using OpenInfraMap and provided a link to the site, according to fusion center reporting.

(U//FOUO) Since 2022, anonymous and unaffiliated actors communicating in online image boards discussed OpenInfraMap as a tool that could be used to plan attacks against electrical infrastructure targets.

- **(U//FOUO)** On 13 DEC 2022, an anonymous image board user created a thread titled "The fate of the USA depends on people not finding out where these boxes are" that contained a hyperlink to OpenInfraMap. Other users participating in the thread discussed vulnerabilities, methods of attacks, and target selection for attacking electrical infrastructure, according to federal intelligence reporting.

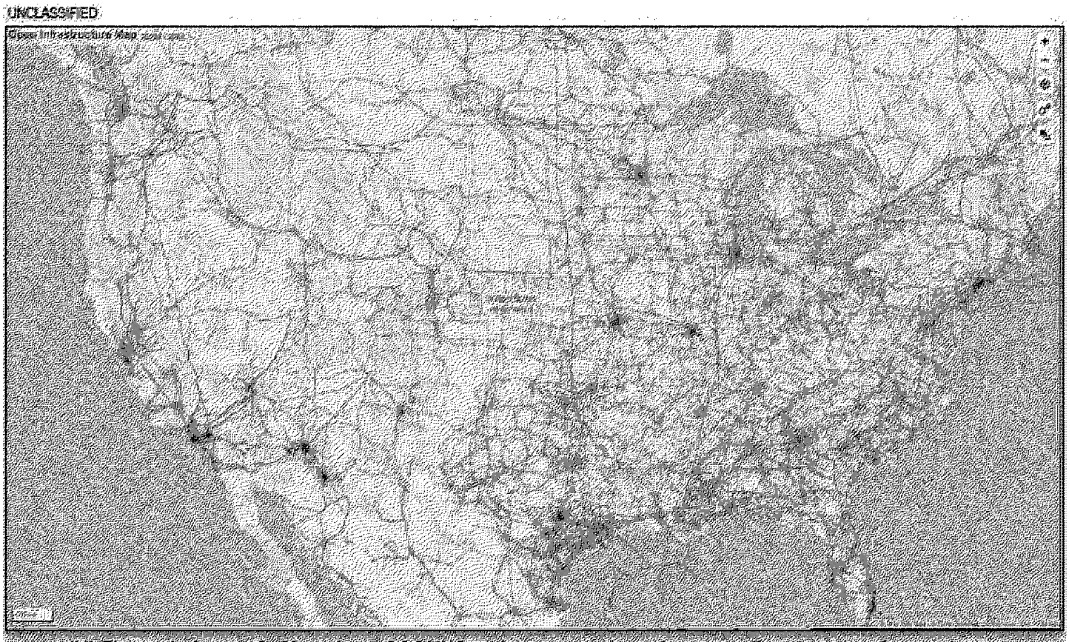
- **(U//FOUO)** On 13 DEC 2022, an anonymous image board user responded to a thread discussing recent attacks on US electrical infrastructure in North Carolina, Oregon, and Washington. The subject posted a hyperlink to OpenInfraMap for "Full electrical infrastructure map," according to federal intelligence reporting.

(U) OpenInfraMap

(U) OpenInfraMap is a custom view of OpenStreetMap, a free, open-source and collaborative geographic online database. OpenInfraMap was created by a UK-based software developer to map and highlight infrastructure documented on OpenStreetMap yet "invisible or not obvious" while using the default OpenStreetMap rendering. Infrastructure information layers visible on OpenInfraMap include power, solar generation, telecoms, oil and gas, and water (See Figure 1 below).

Specific layers can be selected and deselected per user interests. Information on OpenInfraMap is largely dependent upon geo-mapper input.

UNCLASSIFIED



(U) Figure 1: OpenInfraMap view of CONUS with power, solar, telecoms, oil and gas, and water layers toggled.
(Source: https://openinframap.org/)

(U//FOUO) Electrical infrastructure information available from OpenInfraMap includes but is not limited to electrical towers, power lines, minor distribution centers, substations, generating stations, and power plants. OpenInfraMap also contains a list of 12,932 power plants, generating stations, and other electrical infrastructure facilities in the United States with detailed information regarding operating companies, electrical output (MW), power source (i.e., hydro, solar, gas, coal, nuclear, etc.), method (i.e., combustion, fission, photovoltaic, etc.), and hyperlinks to wikidata on certain locations when available (See Figure 2 below).

UNCLASSIFIED

All 12932 power plants in the United States

Name	Operator	Output	Source	Method	Wikidata
Grand Coulee Dam		6,809 MW	hydro	water storage	Q1030391
Bedford Solar	O2 emc	6,000 MW	solar	photovoltaic	Q118721542
W. A. Parish Electric Generating Station	NRG Energy	4,008 MW	coal,gas	combustion	Q12910297
Palo Verde Nuclear Generating Station	Arizona Public Service Company	3,937 MW	nuclear	fission	Q1503007
West County Energy Center	Florida Power & Light	3,750 MW	gas	combustion	Q28403763
Browns Ferry Nuclear Power Plant	Tennessee Valley Authority	3,568 MW	nuclear	fission	Q16580555
PSEG Salem and Hope Creek Nuclear Generating Stations	PSEG	3,470 MW	nuclear	fission	Q15162715
Crystal River Power Plant	Duke Energy	3,325 MW	gas	combustion	Q5191330
Monroe Power Plant	DTE Electric Company	3,300 MW	coal	combustion	Q2944698
Plant Bowen	Georgia Power	3,232 MW	coal	combustion	Q2247203
Gibson Generating Station	Duke Energy	3,145 MW	coal	combustion	Q2944668
John Amos Power Plant	Appalachian Power	2,933 MW	coal	combustion	Q11978950
Bath County Pumped Storage Station	Virginia Electric & Power Co	2,862 MW	hydro	water-pumped-storage	Q1119214
Turkey Point Nuclear Generating Station	Florida Power & Light	2,861 MW	gas,nuclear	fission	Q1739486
Plant McDonough-Atkinson	Georgia Power	2,648 MW	gas	combustion	Q11968799
James H. Miller Electric Generating Plant	Alabama Power	2,822 MW	coal	combustion	Q11977652
Bruce Mansfield Power Station	FirstEnergy	2,741 MW	coal	combustion	Q991403
South Texas Project Electric Generating Station	South Texas Project Nuclear Operating Company	2,709 MW	nuclear	fission	Q371397

(U) Figure 2: OpenInfraMap statistics list for power plants within the United States. (Source: https://openinframap.org/stats/area/United%20States/plants)

(U) Potential informational advantages of OpenInfraMap might include:

• **(U//FOUO)** Impact scoping for attacks: Information found on OpenInfraMap may help threat actors to determine the range of impacted populations more accurately for a proposed attack. Attackers could select certain substations, power plants, and power lines-based wattage and service areas to tailor the 'downstream' effects of disrupted electricity service.

• **(U//FOUO)** Comprehensive and Consolidated Information: Other publicly available information sources on electrical infrastructure vary greatly from state to state and information that they provide. OpenInfraMap contains a consolidated data source with comprehensive information on potential targets at the local, state, and national levels.

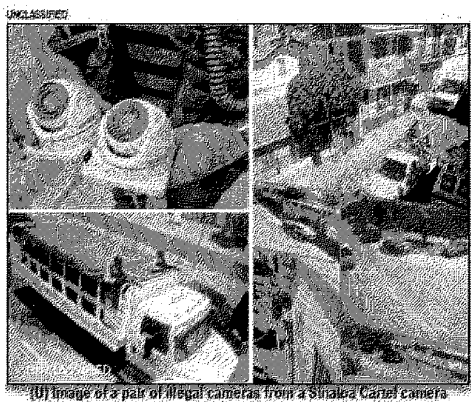
• **(U//FOUO)** Replacing Traditional Pre-Operational Attack Planning Steps: Use of OpenInfraMap could circumvent certain observable preoperational attack planning indicators and behaviors (i.e., observation/surveillance and acquisition of expertise), challenging law enforcement and the public's ability to detect and deter potential attacks.

(U//FOUO) WSIC Comment: WSIC assesses domestic violent extremists and criminal actors will likely continue utilizing OpenInfraMap (https://openinframap.org/) in plots targeting electrical infrastructure, increasing the potential likelihood and impact of successful attacks. Indicators associated with this assessment would include reporting of subjects leveraging information from OpenInfraMap to replace traditional pre-operational activities (observation, surveillance, acquisition of expertise); reporting of online actors discussing the impact of potential attacks with targets selected using OpenInfraMap; and reporting of disrupted plots against electrical infrastructure where actors used OpenInfraMap.

(U/FOUO) WSIC assesses that awareness and ability to report observable pre-operational attack planning indicators, specifically acquisition of expertise and observation/surveillance, will almost certainly be crucial for preventing future attacks to electrical infrastructure in Wisconsin. While use of OpenInfraMap alone is not inherently indicative of criminal activity or pre-operational attack planning, we encourage recipients of this product to take the full context of use and activity into account when reporting. (WSIC, Critical Infrastructure Analytic Report Update, Domestic Violent Extremists and Criminal Actors Will Likely Continue Utilizing "OpenInfraMap" in Plots Targeting Electrical Infrastructure, Increasing the Likelihood and Impact of Successful Attacks10 AUG 23) Source; Army Threat Integration Center (ARTIC).

INTERNATIONAL

(U) Mexico: Authorities Discover a Criminal Surveillance Camera Network



(U) Image of a pair of illegal cameras from a Sinaloa Cartel camera network and screenshots of military personnel and criminal rivals taken throughout the city of Tecate. (Source: ZETA Tijuana)

(U) According to a San Diego-Law Enforcement Coordination Center (SD-LECC) Articles of Interest (AOI) in the Mexican Press Bulletin dated 10 AUG 23, on 01 AUG 23 authorities in Tecate, Mexico discovered images from privately owned surveillance cameras throughout Tecate inside a USBUS WhatsApp group chat on the cell phone of a murdered Sinaloa Cartel associate. Information provided to authorities and law enforcement investigations revealed the Sinaloa Cartel installed approximately 100 cameras throughout the city, highways, and rural areas of Tecate and use the cameras to surveil law enforcement and military personnel and their Cartel Jalisco Nueva Generación (CJNG) rivals. Authorities are having difficulty accessing and confiscating the cameras because most of the cameras are on private properties.

(U//FOUO) SD-LECC Comment: Mexican drug trafficking organizations will likely continue to leverage technology, including surveillance cameras, small unmanned aircraft systems (sUAS), and communication applications, to optimize their drug trafficking and criminal activities by surveilling authorities and rivals and sharing information between criminal cells. According to a July 2023 article citing a Mexican security specialist, Mexican criminal groups have increased their use of technology, including surveillance cameras, applications, and sUAS, to fortify their security posture, facilitate their drug trafficking operations, and spy on authorities and rivals. Sinaloa Cartel criminal cells operate command, control, communications, and computer centers in Sinaloa to surveil authorities and improve their security posture while conducting drug-related criminal activities, according to the same article. Criminal groups in Tijuana, Mexico have also used sUAS in furtherance of their criminal activities. According to a US Border Patrol (USBP) officer interviewed by a news outlet in March 2023, human smuggling and drug trafficking groups have increased their use of sUAS along Sector San Diego's area of responsibility to surveil USBP agents and facilitate their criminal activities. (SD-LECC, AOI in the Mexican Press, Product Number: 2023-16, 10 AUG 23) Source; Army Threat Integration Center (ARTIC).

Britain Warns of Possible Terrorist Attacks in Sweden

[Sweden] Britain on Sunday warned citizens going to Sweden of possible terrorist attacks following Koran burnings by anti-Islam activists that have outraged Muslims. In updated travel advice, Britain's foreign ministry said Swedish authorities had successfully disrupted some planned attacks and made arrests. "You should be vigilant at this time," it said, adding that "terrorists are very likely to try and carry out attacks in Sweden" with places visited by foreigners potential targets. In a statement acknowledging Britain's changed travel advice, Sweden's National Security Advisor Henrik Landerholm reiterated the increased threats to Sweden since the burnings. Landerholm said the storming of Sweden's embassy in Iraq on July 19, an attempted attack on its embassy in Lebanon on Aug. 9, and also the Aug. 1 shooting of an employee at a Swedish consulate in Turkey contributed to the risk assessment. Source; Reuters, 8/14/2023

Analyst Comment In recent weeks, anti-Islam activists in Sweden have conducted a series of demonstrations that involve publicly burning the Quran, which is the central religious text of Islam. These demonstrations have heightened tensions worldwide and resulted in a Swedish embassy in Iraq being stormed by Iraqi protestors, a Swedish embassy in Lebanon being subjected to an attempted attack, and an employee at the Swedish consulate in Turkey being shot. Henrik Landerholm, Sweden's National Security Adviser, has said that there are signs of a "heightened threat" to Sweden by terrorist actors because of the demonstrations, and that "representatives of terrorist groups have called for attacks against Sweden. States and other actors have helped amplify such messages." Landerholm also claimed that terrorist

organizations who previously considered Sweden as a "legitimate target" for attacks now consider it to be a priority target. On 1 August, the Swedish government emplaced new security protocols and identity checks along their borders to prevent threat actors from entering the country. Over the past week, many western nations, including the governments of the U.K., the U.S., and Australia, have warned travelers to exercised increase caution in Sweden due to the increased threats of terrorism. The warning issued by U.K. government claims that "terrorists are very likely to try and carry out attacks in Sweden," and that places visited by tourists are potential targets. Source; Surface Transportation & Public Transportation ISAC Transit & Rail Intelligence Awareness Daily Report (TRIAD)

Other National/International Articles of Interest (Links):

3 teens arrested after armed robberies, police pursuit in Pierce County
https://komonews.com/news/local/pierce-county-teens-arrested-armed-robberies-tacoma-police-chase-spike-strips-stolen-car-portland-avenue-canyon-road-east-i5

Report: Tacoma sees drastic drop in killings, down nearly 40% since 2022
https://www.fox13seattle.com/news/tacoma-sees-drastic-drop-in-killings-so-far-this-year

Washington had highest year-over-year drug overdose death increase in US, data show
https://www.king5.com/article/news/health/washington-highest-drug-overdose-death-increase/281-cadc59d5-8462-426a-a1a7-9439d6636948

Fentanyl test strips could become more widely distributed in Washington after recent law change
https://www.king5.com/article/news/health/fentanyl-test-strip-access-washington/281-6ce6b018-ce17-4833-9764-3488b342586e

Large Drug Bust in Puget Sound Region Leads to Arrest of Suspected Trafficker
https://original.newsbreak.com/@seattle-updates-1598685/3123474893300-large-drug-bust-in-puget-sound-region-leads-to-arrest-of-suspected-trafficker

(U) Pennsylvania – Teenage Supporter of Islamic Extremism Arrested
https://www.nbcnews.com/politics/justice-department/17-year-old-supporter-islamic-extremism-arrested-philadelphia-rcna99818

(U) Sacramento – California Synagogues Evacuated During Services as Wave of Bomb Threats Enters Fourth Week
https://jweekly.com/2023/08/14/2-california-synagogues-evacuated-during-shabbat-services-as-wave-of-bomb-threats-enters-4th-week/

(U) Senior ISIS Official Killed During Joint Operation In Raqqa, Syria
https://gazettengr.com/senior-islamic-state-official-killed-in-eastern-syria-raid/

4 cautions for school attack planning
https://www.police1.com/school-safety/articles/4-cautions-for-school-attack-planning-e4zqFuhTLxbjk7ux/?utm_source=Police1&utm_campaign=c68e4a0652-EMAIL_CAMPAIGN_2023_08_17_04_17&utm_medium=email&utm_term=0_5584e6920b-c25aa06759-%5BLIST_EMAIL_ID%5D

*TPD/PCSD Homeland Security Reports Received this week 7.

From: Smith, Gary (TPD)
Sent: Fri 4/28/2023 2:47:40 PM
Subject: SSRIG Weekly Intelligence Summary 17 - 2023 (April 28, 2023)
Received: Fri 4/28/2023 2:49:53 PM
SSRIG Weekly Summary 17-2023.pdf

South Sound Regional Intelligence Group

SSRIG email: PCINTEL@piercecountywa.gov

Weekly Summary

#17-2023 April 28, 2023

Gary Smith
Intelligence Analyst
Gary.Smith@ci.tacoma.wa.us
(253) 594-7964

REGIONAL

(U//FOUO) United States: Online Sharing of Tactics from Firearms Attacks Increases Threat to US Electrical Infrastructure

(U//LES) Demand for Synthetic Opioid Nitazene in Spokane, Washington, as of late 2022

(U//FOUO) Online Child Exploitation Group 764 Encourages Victim Self-Mutilation and Suicide

OFFICER SAFETY

(U) Bandidos Motorcycle Club Members Expected to Travel to Washington State to Attend Memorial Service on 29 April 2023

OFFICER AWARENESS

PC to Arrest- Drive-By Shooting; TPD Case # 2310101748

OFFICER SAFETY CONCERN – HOMICIDE SUSPECT

ATTEMPT TO IDENTIFY-ARMED ROBBERY SUSPECTS

Theft/Fraud Suspect Traveling in Washington

Information: Eluding and Street Racing Suspect

CYBER THREATS

(U) Cyber: New Credential-Stealing Malware Advertised on Telegram

(U//FOUO) Cyber: Criminals Exploit Online Marketplaces to Engage in Carjackings and Resale of Stolen Vehicles

PUBLIC SAFETY

FBI: Active Shooter Incidents Fell in2022 but Remained Relatively High

NATIONAL

(U//FOUO) United States: Juveniles Will Likely Leverage Explosives Availability to Target Secondary Schools

Pitt Researchers Collect Data on Where Train Accidents Occur and What They Threaten

INTERNATIONAL

Germany Arrests 28-Year-Old Syrian Over 'Radical Islamist' Bomb Plot

Sudan in Chaos

Other National/International Articles of Interest (Links):

Gary L. Smith
Gary L. Smith
Criminal Intelligence Analyst
Regional Intelligence Group
TPD/PCSD
Tacoma, WA
(253) 594-7964
(253) 405-6214 (C)
gary.smith@cityoftacoma.org
gary.smith@piercecountywa.gov

"There must be a Lone Ranger!" 

TACOMA /PIERCE COUNTY REGIONAL INTELLIGENCE UNIT

WEEKLY SUMMARY

17-2023 Friday, April 28, 2023

Det. Sgt. John Delgado (253) 341-1369
john.delgado@piercecountywa.gov

Gary L. Smith, Intel Analyst
gary.smith@cityoftacoma.org (253) 594-7964

REGIONAL

(U//FOUO) United States: Online Sharing of Tactics from Firearms Attacks Increases Threat to US Electrical Infrastructure

Violent extremists are increasingly sharing tactics for attacking power stations, DHS Warns

(U//FOUO) According to a US Department of Homeland Security Office of Intelligence and Analysis (DHS I&A) Counterterrorism Mission Center Intelligence In Focus (IIF) dated 24 APR 23, in the past year, domestic violent extremists (DVEs) and other potential criminal actors have increased sharing of tactics from several firearms attacks against electrical power stations, likely escalating the threat to electrical infrastructure in the United States. Following a series of publicized, unrelated firearms attacks against electrical infrastructure over the past year, DVEs have increasingly circulated online messaging and operational guidance promoting attacks against this sector. The perpetrators of the attacks targeted electrical substations and transformers using tactics that can challenge law enforcement's ability to identify suspects and that have the potential to cause at least localized power disruptions.

• **(U)** Unidentified threat actors used firearms in several recent attacks against electrical infrastructure in the United States with varied success in destroying components critical to maintaining localized service. In December 2022, an unidentified perpetrator shot two substations in Moore County, North Carolina, causing power outages spanning several days and straining a wide range of businesses and healthcare, emergency, and other community services, according to media reporting.

• **(U//FOUO)** Over the past year, DVEs have shared best practices for firearms attacks against electrical infrastructure, including detailed diagrams, simplified tips for enhancing operational security, and procedures for disabling key components of substations and transformers, according to DHS and media reporting. The tactics used in recent firearms

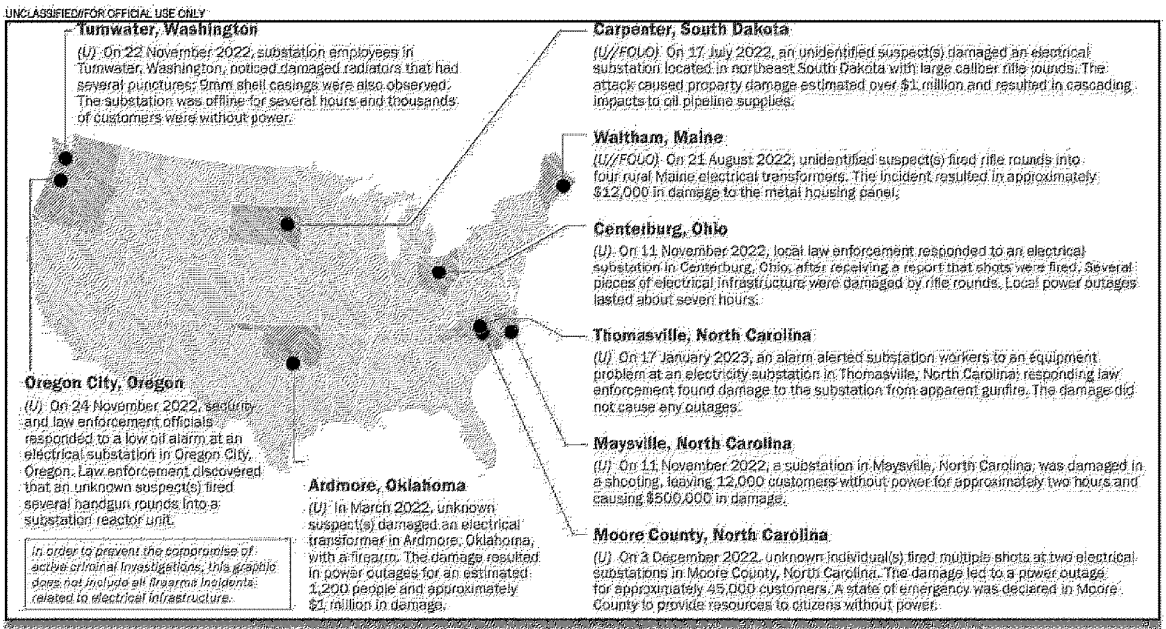
attacks are generally consistent with this guidance and have prevented law enforcement from identifying any of the perpetrators.

• **(U//FOUO)** DVEs and other criminal actors have referenced media coverage of the attacks, noting that they demonstrate proof-of-concept and are the best examples of successful attacks over the past decade, according to DHS and media reporting. Two racially and ethnically motivated violent extremists in Maryland referenced the North Carolina attack and were using publicly available information to identify substations for an attack before the plot was disrupted by law enforcement in February, according to a federal criminal complaint.

(U//FOUO) Firearms attacks could become more appealing and spread to other infrastructure sectors because they offer a low-risk/high-reward opportunity, other sectors feature similar vulnerabilities, and damage to electricity subsector targets could have cascading effects on other sectors. For example, similar tactics could be used to attack transportation and telecommunications targets if threat actors perceive these targets as sharing similar vulnerabilities, such as remote locales and a lack of onsite security personnel or other perimeter security measures. Threat actors also may target electrical infrastructure to indirectly disrupt operations they perceive as harmful to the environment or vital to law enforcement's ability to respond to criminal activity.

• **(U//FOUO)** Easily accessible rural infrastructure assets—such as pipeline systems, energy substations, and cell towers—are typically lightly guarded with cameras and simple physical barriers like fences and gates, making them vulnerable to low-risk firearms attacks that result in significant disruptions. Attacks on platforms in rural areas are harder to investigate, given the lack of witnesses and a longer police response time, judging from media and private sector reporting. Violent extremist media highlighting other vulnerable infrastructure could motivate offenders to target other less traditional critical infrastructure sectors.

• **(U//FOUO)** Blackouts caused by attacks on electrical infrastructure have the potential to cause strain or disrupt other critical infrastructure sectors, including communications; water and wastewater; public health; transportation; healthcare; and nuclear reactors, materials, and waste. In July 2022, components of an electrical substation in South Dakota were targeted by high-caliber rifle rounds, causing power outages and cascading disruptions to the Keystone Pipeline, according to government officials.



(U) Image of Selected Firearms Attacks on Electrical Critical Infrastructure Since March 2022

(U//FOUO) Targeting Electrical Infrastructure Appeals to Various Domestic Violent Extremist Ideologies

(U//FOUO) Racially or ethnically motivated violent extremist messaging promoting narratives about accelerating societal collapse and encouraging a race war in support of accelerationist ideology has offered the most detailed instructions for firearms attacks against electrical infrastructure, though motives for attacks over the past year likely include various ideological and other motivations. Other DVE ideologies may share views that attacking electrical critical infrastructure is an effort toward achieving societal collapse. For example, involuntary celibate violent extremists have celebrated recent attacks on electrical infrastructure and encouraged additional attacks to "cripple the lifestyles" of the US populace, according to DHS reporting. (DHS I&A Counterterrorism Mission Center, Product Number: DHS-IA-IF-2023-08320, 24 APR 23)

Analyst Comment Following multiple high-profile attacks on US power substations last year, extremists have stepped up sharing of "online messaging and operational guidance promoting attacks against this sector," says the DHS bulletin, which was distributed to US critical infrastructure operators on Monday. The information and tactics shared by extremists online include "detailed diagrams, simplified tips for enhancing operational security, and procedures for disabling key components of substations and transformers," DHS warned. The last year saw a flurry of physical attacks and vandalism on US electric infrastructure. Tens of thousands of people lost power in Moore County, North Carolina, in December after Duke Energy substations were damaged by gunfire. On Christmas, thousands of people lost power in Pierce County Washington after someone vandalized multiple substations there. Source; DHS

SITUATIONAL INFORMATION REPORT
FEDERAL BUREAU OF INVESTIGATION
(Potential Activity Alert)
SEATTLE DIVISION
Approved for Release: 20 April 2023
SIR Number: SIR-00353349742

(U//LES) Demand for Synthetic Opioid Nitazene in Spokane, Washington, as of late 2022

SOURCE: (U) An FBI Agent.

(U//LES) FBI Seattle is releasing this Situational Information Report to raise awareness amongst law enforcement and public safety officials regarding the possible appearance of the synthetic opioid nitazene in Spokane, Washington, as of late 2022. (Analyst comment: "Nitazene" describes a group of powerful illicit synthetic opioids linked to overdose deaths in several states. Until recently, the drug had been seen primarily in the midwestern, southern, and eastern United States.)

(U//LES) As of late 2022, FBI Seattle received reporting indicating demand for nitazene in the Spokane area. According to the reporting, drug users requested nitazene due to its potency, which was allegedly "twenty times" stronger than powdered fentanyl. In September 2022, suppliers planned to bring nitazene into the Spokane area.

(U//LES) As of April 2023, FBI Seattle did not possess any other information regarding the use or sale of nitazene in Spokane.

(U) This report has been prepared by the SEATTLE Division of the FBI. Comments and queries may be addressed to the SEATTLE Division at 206-622-0460. Source; Via Washington State Fusion Center

SITUATIONAL INFORMATION REPORT FEDERAL BUREAU OF INVESTIGATION
(Activity Alert)
SEATTLE DIVISION

Approved for Release: 24 September 2022 SIR Number: SIR-00350036819

(U//FOUO) Online Child Exploitation Group 764 Encourages Victim Self-Mutilation and Suicide

SOURCE A: (U) A write-in to this agency. SOURCE B: (U) An employee of the FBI.
SOURCE C: (U) An officer of another law enforcement agency.

(U//FOUO) Online child exploitation group 764, also known as 764CVLT, targets vulnerable minors and coerces them to self-harm, produce child sex abuse material (CSAM), commit acts of animal cruelty, and live-stream their deaths by suicide via social media platforms. Victims who do not comply face retribution in the forms of extortion, doxing,[1] fedding,[2] and swatting.[3] Online groups KasKar, AAST, Legion, 7997, and Maniac Murder Cult (MYK) are offshoots of or affiliated with 764.

(U//FOUO) 764 members distribute the coerced content in online groups across social media platforms including Discord, Telegram, and Signal. 764 subjects identify and groom victims found on online videogames that offer chat functionality, including AmongUs and Roblox, as well as social media applications such as Instagram, Snapchat, Omegle, and Discord. Online mental health forums also provide opportunities for 764 members to identify highly vulnerable minors. Cutting serves as a physical identifier of potential 764 involvement. 764 members pressure victims into cutting "fan signs" or symbols into their bodies. These fan signs can include the subject's username or initials, "764," "cvlt," or white supremacist symbols such as swastikas.

(U//FOUO) 764 subjects target LGBTQ+ youth, racial minority youth, and minors who struggle with mental health issues to include depression, eating disorders, and suicidal ideation. Investigations into this group are complicated by the fact that many victims and subjects of 764 appear to be minors, with some subjects as young as 13 and victims as young as 12. 764's primary goal appears to be to coerce victims into producing more gore and/or explicit material, or to live-stream their deaths by suicide, rather than financial extortion. However, financial extortion has occurred in small amounts on some occasions.

[1] *ANALYST NOTE:* Doxing is defined as searching for and publishing private or identifying information about a particular individual on the internet, typically with malicious intent.

[2] *ANALYST NOTE:* Fedding is defined as the action or practice of writing or calling into a federal agency with the intent of federal law enforcement making contact with a target victim. This is similar to swatting, but with federal agents showing up to the victim's residence rather than a SWAT team.

[3] *ANALYST NOTE:* Swatting is defined as the action or practice of making a prank call to emergency services in an attempt to bring about the dispatch of a large number of armed police officers to a particular address. 764 members are known to swat victims as well as each other.

(U) This report has been prepared by the SEATTLE Division of the FBI. Comments and queries may be addressed to the SEATTLE Division at 206-622-0460. Source; Via Washington State Fusion Center

OFFICER SAFETY

Upcoming OMG Activity

SITUATIONAL INFORMATION REPORT
FEDERAL BUREAU OF INVESTIGATION
(Potential Activity Alert)
SEATTLE DIVISION
Approved for Release: 26 April 2023
SIR Number: SIR-00353445402

(U) Bandidos Motorcycle Club Members Expected to Travel to Washington State to Attend Memorial Service on 29 April 2023

SOURCE A: (U) An officer of another law enforcement agency.
SOURCE B: (U) An officer of another law enforcement agency.

(U//LES) The purpose of this Situational Information Report (SIR) is to raise awareness among law enforcement personnel and public safety officials regarding an expected increased presence of Bandidos Motorcycle Club members (Bandidos) traveling to Sedro Woolley, Washington in late April 2023 in order to attend a memorial service. The Bandidos MC is an identified "one-percenter," outlaw motorcycle gang (OMG).

(U//FOUO) A memorial service for Bryan Denson (Denson), the Bandidos Chapter President for Skagit County, is scheduled for 1pm on 29 April 2023 at Sonrise Christian Center, located at 10217 Collins Road, Sedro Woolley, Washington 98284. Denson passed away following a motorcycle accident in Mount Vernon, Washington on 18 March 2023. An estimated 250 people are expected to attend the service.

(U//FOUO) Reporting indicates Bandidos members plan to gather at a gas station on Bow Hill Road in Skagit County, Washington prior to the service and ride to the Sonrise Christian Center as a group. Members plan to meet at an unknown location following the service.

ANALYST NOTE: The referenced gas station is believed to be The Skagit Bow Hill Gas & Food Mart, located at 18520 Bow Hill Road, Bow, Washington 98232 (NFI).

(U//FOUO) ANALYST NOTE: Due to multiple upcoming funerals for Bandidos members in Texas, the number of out of state Bandidos traveling to Washington State for this memorial service may be limited.

(U//FOUO) FBI Seattle possesses no information regarding specific threats or planned acts of violence during these events. However, similar events involving Bandidos chapters have been associated with the potential for violence.

(U//FOUO) This report is for situational awareness for law enforcement personnel. Details of the event remain fluid. Recipients are requested to contact FBI Seattle if any positive information is developed regarding suspicious activity or potential violence by OMGs in Washington State.
(U) This report has been prepared by the SEATTLE Division of the FBI. Comments and queries may be addressed to the SEATTLE Division at 206-622-0460. Source; Via Washington State Fusion Center

OFFICER AWARENESS

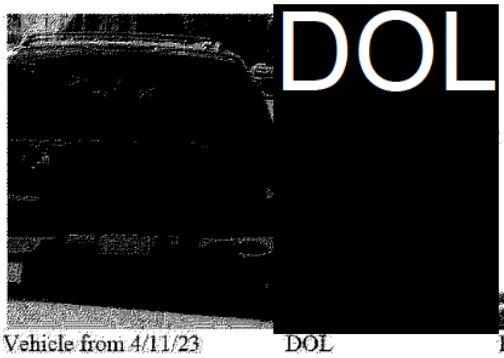
Special Bulletin

TACOMA POLICE DEPARTMENT

Bulletin Number: S23-060 **April 28, 2023**

Det. R. Beck
Desk: 253-591-5679 Cell: 253-278-7020 RBeck@CityofTacoma.org

PC to Arrest- Drive-By Shooting
TPD Case # 2310101748



Vehicle from 4/11/23 DOL


BWC on 4/25/23

Cota Castro, Jose Angel
09/17/91
I/M, 511, 205 long Black hair, unshaven

Associated Vehicle:
Green 2004 Chevy Tahoe WA-CBR5004

Address: 2317 S 96th Street BLDG C #315 (Terra heights) Tacoma,

On 04/11/23, Cota-Castro was involved in a road rage incident in the area of S. 38th and Tacoma Avenue. As a result Cota-Castro pointed and shot a single round at another driver. The incident was recorded on dash-cam from the victim vehicle.

Cota-Castro uses multiple variations of his last name to include: Cota, Castro and Ancheta.

The listed vehicle is not registered to Cota-Castro but was parked at the address as recent as 04/25/23.

The firearm used in the incident and vehicle have not been recovered. Please use appropriate caution if contacting Cota-Castro as he has history of Assault 3, Eluding and listed "Highly Violent" through DOC.

If located please Notify Det. Beck by phone for an interview. The vehicle should be impounded for a search warrant and transported to TPD. Probable Cause exists to arrest and book Cota-Castro under the listed case number for Drive-by Shooting.

Det. Beck 253-278-7020 RBeck@CityofTacoma.org

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

Pierce County
Sheriff's Department
CRIMINAL INVESTIGATIONS DIVISION

SPECIAL BULLETIN

PCSD CIB 23-026s | PCSD CRIMINAL INVESTIGATIONS DIVISION | April 27, 2023

OFFICER SAFETY CONCERN – HOMICIDE SUSPECT

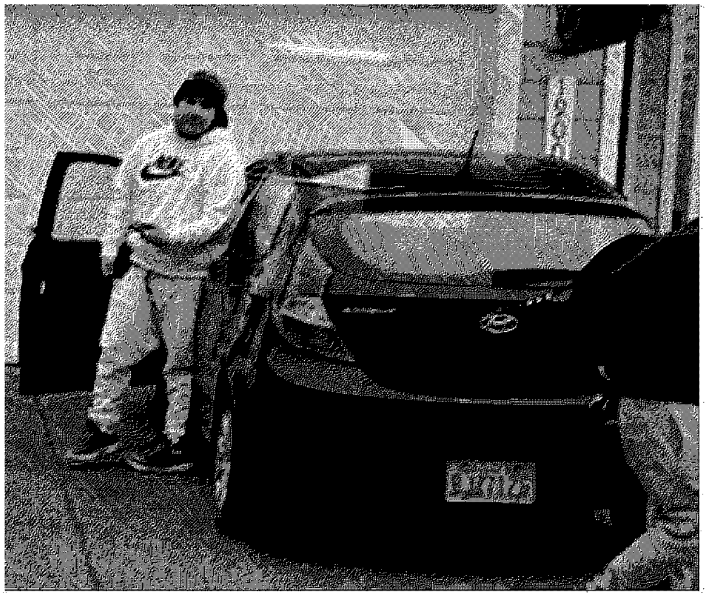
The Pierce County Sheriff's Department is advising law enforcement to use caution with regard to the pictured vehicle, and any associated occupants. Manuele Samaga, is currently being investigated as a third suspect in a Homicide (PCSD Case #23-028-01706).

There is NO PROBABLE CAUSE yet for Manuele Samaga.
Samaga has access to firearms. The other two suspects have already been arrested. It is likely Samaga knows or believes he is being investigated by law enforcement, so use extreme caution.

Do not stop, arrest or detain based on this bulletin. If this vehicle or any of the persons pictured below are contacted, use caution, as the firearm in this case has not been recovered.

Do not question Samaga or mention this case if he is stopped. Contact Detective Jacob Lawrence 253-377-5356 jacob.lawrence@piercecountywa.gov, if you have any contact with Manuele Samaga.

NAME: Manuele I Samaga
DOB: 06/30/2004
PHY: 5'06" / 235 / BRO
LKA: 19002 96th Ave Ct E, Puyallup WA
VEH: Black 2013 Hyundai Accent WA License BJZ7126 (photo of Vehicle Below)



*** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY ***

Pierce County Sheriff's Department
CRIMINAL INVESTIGATIONS DIVISION

SPECIAL BULLETIN

PCSD CIB 23-027s | PCSD CRIMINAL INVESTIGATIONS DIVISION | April 27, 2023,

ATTEMPT TO IDENTIFY-ARMED ROBBERY SUSPECTS

Pierce County Sheriff's detectives are attempting to identify the suspects responsible for an ARMED ROBBERY under PCSD Case #23-114-01725.

On April 25th, at 1637 hours, a 12-year-old boy was robbed at gun point of his silver necklace. The juvenile was walking home from school in the 178th block of 19th Ave E. when a gray pick-up truck possibly a Toyota Tacoma passed him then made a U-turn and came back and stopped. A Hispanic male in his 20s exited the passenger's side of the truck, pointed a black handgun at the victim and demanded the victim's silver chain necklace. After receiving the necklace, the suspect struck the victim in the face with the gun before getting back into the truck and fleeing. The victim said there were two older males in the truck.

SUSPECTS: Hispanic male mid-twenties 5'9'' med with a buzz-cut. Suspects 2 and 3 were only described as older males.

If you have any information on the identity of this suspect, the vehicle or similar incidents, please contact Detective D. Moss Sr. at 253 798-7721 or darren.moss@piercecountywa.gov.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

SHERIFF
WASHINGTON COUNTY

ATTEMPT TO ID / BOLO
Case 50-23-5371
Deputy Tom Brown

Theft/Fraud Suspect Traveling in Washington

On 04/11/2023, the pictured suspect used stolen credit cards to buy numerous expensive items at the Apple Store in Tigard OR (7273 SW Bridgeport Rd). The cards had been in a wallet stolen at St Vincent Hospital in Portland.

Please be on the lookout for this suspect and the pictured vehicle, which he was traveling in at the Apple Store. If your agency has any related cases or helpful information, please contact WCSO Deputy Tom Brown.

FURTHER INFO: On the day of the crime, an Apple AirTag in the stolen wallet transmitted northward on I-5 in Washington State. It stopped at several locations (including Emerald Queen Casino at 2920 East R St in Tacoma) on the same day, en route to the Seattle area.

The AirTag continues to transmit near Pacific Medical Center (1200 12th Ave S) in Seattle from 0700- 1500 hrs on Monday-Friday. And overnight, the device's signal is consistently near 11215 26th Ave S in Burien, where the AirTag appears to be left in a parked vehicle. **We're currently contacting agencies in those areas, but if you have any helpful information, don't wait for us to reach out! Please use the email link above.

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

KENT POLICE DEPARTMENT

BULLETIN# 23-18 UPDATE

Published by: Commander J. Bava
E-mail: jbava@kentwa.gov
Phone: 253-856-5834 or 206-573-1724
Date: 04/27/2023
Case: #23-5110

Information: Eluding and Street Racing Suspect

SOCIAL MEDIA 08/2022

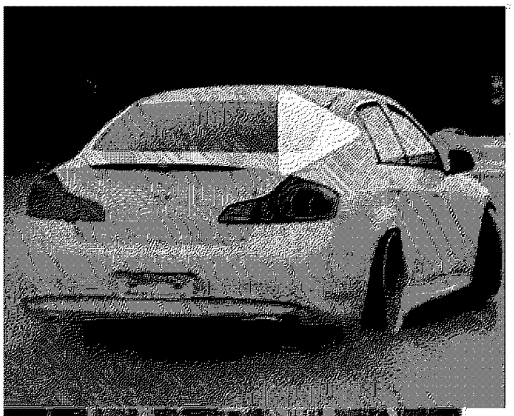
Matthew N. SLOBODA
08/31/2001

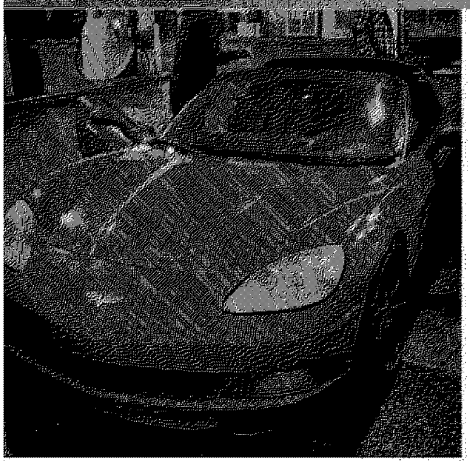
3824 90th Ave. E., Edgewood

2012 Infiniti G37 (white)
WA: LEM403J

2006 Chevrolet Corvette
(red convertible)
CA: 6TEC929

HISTORY OF ELUDING
DWLS 3RD DEGREE
ACTIVE MISDEMEANOR WARRANT



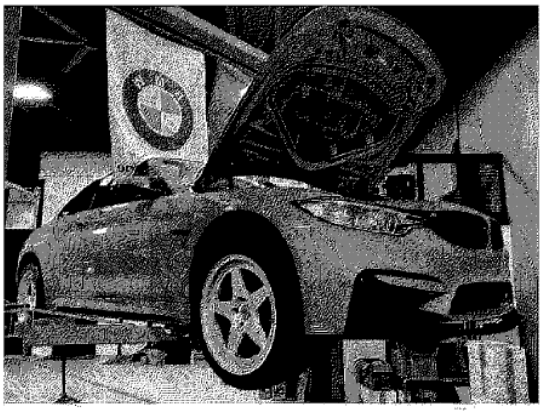


Matthew Sloboda is a frequent participant at illegal street race events in both Kent and Renton. Preliminary investigation has identified him as the driver of the pictured Infiniti G37 as well as the blue BMW M4 coupe seen in a viral video drifting around a marked police vehicle on 04/16/2023.

He also has history of attending street races in the pictured red Chevrolet Corvette (convertible).

***** FOR OFFICIAL USE ONLY *** LAW ENFORCEMENT USE ONLY *****

The blue BMW has been identified as belonging to Joshua Chuyeshkov



WA STATE DOL 09/22/2022

DOL

Joshua M. CHUYESHKOV
10/22/2000

29541 200th Ct. SE, Kent

2015 BMW M4 (blue)
WA: BRR7711

Please contact Commander Bava at 253-856-5834 or 206-573-1724 if Sloboda is contacted or the Infiniti or BMW are located. Kent Police will impound those vehicles for evidence.

There is no PC to arrest either subject at this time. The case remains under investigation.

Sloboda has an active misdemeanor warrant from Sumner Municipal Court (#2A0465206, DWLS 3rd degree, $2,500 bail). Please confirm prior to arrest.

CYBER THREATS

(U) Cyber: New Credential-Stealing Malware Advertised on Telegram

(U) According to a US Naval Criminal Investigative Service (NCIS) Multiple Threat Alert Center (MTAC) Cyber Threat Division Threat Awareness Message (TAM) dated 21 APR 23, security researchers have identified two new variants of credential-stealing malware that are being advertised for sale via the Telegram platform. Credential-stealing malware can be extremely dangerous for victims, as it could allow malicious actors to bypass security measures for logging in, providing them with access to numerous online accounts and an abundance of sensitive data. Malicious actors can use stolen credentials for a variety of follow-on operations ranging from financial theft to large-scale cyberespionage operations. Additionally, malicious actors commonly sell or post compromised credentials to underground forums, potentially making the credentials available to other threat actors worldwide.

(U) One of the newly identified variants of malware, dubbed "Zaraza Bot" by its developers, is being advertised on a popular Russian Telegram channel and likely rented on a subscription basis. Zaraza Bot can take screenshots from victims' devices and targets 38 different browsers including Google Chrome and Microsoft Edge, to steal login credentials for victims' email, banking, and other high-value accounts. Although the browsers typically encrypt stored passwords, according to reporting, Zaraza Bot is capable of decrypting them. Zaraza Bot then leverages Telegram as its command and control (C2) to transfer the stolen data back to the actors. Although the initial infection vector associated with Zaraza Bot

is unknown, malicious cyber actors can use a variety of methods to distribute credential-stealing malware, including phishing emails, fake advertisements, and malicious apps.

(U) A second type of credential-stealing malware that has been recently advertised on Telegram has been dubbed "Legion" by its developers. The developers, who use the moniker "Forza Tools," have a large group of followers on their Telegram channel, as well as a YouTube channel which they use to post malware tutorials. Legion attempts to steal credentials for a variety of online accounts, primarily focusing on compromising email accounts, which can be used to send mass phishing emails. Legion is also capable of hijacking short message service text messages on compromised devices, likely to steal the content of text messages and to send malicious text messages to additional victims.

(U) Because Telegram allows users to remain anonymous and provides them with encrypted communications, cybercriminals and state-sponsored advanced persistent threat (APT) groups are increasingly using it to advertise malware for sale, distribute malware, and transfer stolen data. In the past year, security researchers have discovered multiple other types of malware and services that have been advertised via different Telegram channels, including Titan Stealer, MacStealer, and services that allow malicious actors to purchase malware bundles and "how-to" guides, such as the "Eternity Project" malware-as-a-service (MaaS).

(CUI) NCIS MTAC Cyber Threat Division Comment: NCIS assesses that while the newly observed credential-stealing malware currently poses a low threat to US Department of Navy networks and personnel, the threat may increase as the actors continue to promote the malware via Telegram channels and increase their customer base. NCIS assesses this with moderate confidence, based on reporting highlighting the increasing use of Telegram by malicious actors worldwide to buy and sell various types of malware. Many types of malware promoted on Telegram appear to be primarily focused on stealing credentials, as the credentials can be used in a wide range of malicious activities. Personnel should follow the below recommendations to help prevent an accidental malware download and protect accounts from a potential compromise.

- (U) Ensure devices are updated and running reputable antivirus software.

- (U) Refrain from opening emails, text messages, or social media messages from unknown or suspicious senders; regardless of whether the sender is legitimate, carefully review any content/links/attachments sent.

- (U) Go directly to reputable websites for information or account access rather than clicking on a link received by a third-party source.

- (U) Use multi-factor authentication when possible.

- (U) Refrain from saving credentials in browsers.

- (U) Use different password and username combinations for different accounts.

- (U) Use complex passwords and change them often.

Sources; (NCIS MTAC Cyber Threat Division, TAM, Product Number: NCIS-TAM-CYBR-N035-FY23, 21 APR 23) via ARMY THREAT INTEGRATION CENTER (ARTIC)

(U//FOUO) Cyber: Criminals Exploit Online Marketplaces to Engage in Carjackings and Resale of Stolen Vehicles

(U//FOUO) The FBI New Haven, in coordination with the FBI's Office of Private Sector (OPS), prepared this Liaison Information Report (LIR) to inform cross-sector partners about criminal actors engaged in carjackings using online marketplaces, mobile phone applications, and the enticement of cash purchases. The use of online marketplaces is appealing to criminal actors because online personas/profiles are easily created using minimal personally identifiable information, giving criminal actors anonymity from their victims. Additionally, by conducting cash transactions, criminal actors are incentivized by limiting the

victim's recourse.

(U//FOUO) In one case, criminal actors created a social media profile using a moniker and negotiated the purchase price of a motor vehicle through an online marketplace. Upon completion of the test drive, the criminal actors brandished a firearm at the seller at the time of payment, demanded the title, and forced the seller out of the vehicle. Following the theft of the vehicle, the carjackers deleted the social media profile. The carjackers, now in possession of the stolen motor vehicle, created a second profile using a moniker on another online marketplace and advertised the vehicle for sale. The criminal actors negotiated the sale of the vehicle with a buyer, who also used a moniker on the online marketplace. Per the online marketplace records, after the sale was completed, the buyer re-contacted the criminal actors, questioned the legitimacy of the transaction, and demanded additional financial compensation, but the criminal actors did not respond. The buyer advised law enforcement they subsequently re-sold the vehicle and believed it had been shipped out of the country.

(U//FOUO) In another instance, the same criminal actors used the same modus operandi to carjack another victim and resell the stolen vehicle. Upon registering the vehicle, the unsuspecting buyer learned the vehicle had been reported stolen and attempted to contact the criminal actors. They discovered the criminal actors had changed their profile name to another moniker and the telephone number for re-contact was no longer in service.

(U//FOUO) While an indicator alone does not accurately determine a carjacking and resale scheme, the totality of behavior, message delivery, and other relevant circumstances should be evaluated when considering notification of security/law enforcement personnel.

(U//FOUO) The following suspicious activities/indicators include but are not limited to any individual, group, or activity (observe these indicators in context and not individually):

- **(U//FOUO)** Increasing contact or presence of potential vehicle buyers or sellers on online marketplaces with newly created social media profiles with a limited history.

- **(U//FOUO)** Unsolicited contact from social media profiles with a nominal number of contacts and photos.

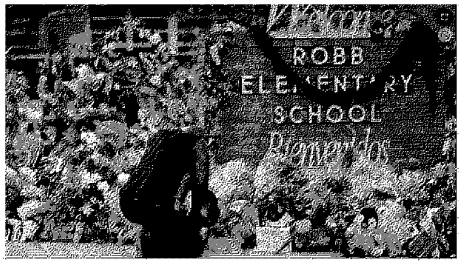
- **(U//FOUO)** Potential buyers or sellers of vehicles refusing to conduct a transaction at a police station or other established safe location; and

- **(U//FOUO)** Seller's advertising vehicles with "too good to be true" pricing or prices noticeably below the vehicle's estimated value.

(U//FOUO) The FBI's Office of the Private Sector disseminated this LIR; please direct any requests and questions to your FBI Private Sector Coordinator at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices. (FBI New Haven, in coordination with FBI's OPS, LIR, Product Number: LIR230413006, 13 APR 23) Source; via the Army Threat Integration Center (ARTIC)

PUBLIC SAFETY

FBI: Active Shooter Incidents Fell in2022 but Remained Relatively High



The FBI is reporting a slight decline in the number of "active shooter" incidents last year but says the tally still surpassed the levels seen in most of the last five years. The FBI defines an active shooter as "one or more individuals actively engaged in killing or attempting to kill people in populated area" such as a school or nightclub.

The FBI is reporting a slight decline in the number of "active shooter" incidents last year but says the tally still surpassed the levels seen in

most of the last five years.

The FBI defines an active shooter as "one or more individuals actively engaged in killing or attempting to kill people in a populated area" such as a school or nightclub.

Not all shootings are counted as active shooter incidents by the FBI. Excluded are cases of self-defense, gang violence, drug violence, and domestic disputes. In a report released on Wednesday, the FBI said it counted a total of 50 active shooter incidents in 2022, down from 61 the previous year.

But that number is still 67% higher than five years ago when there were 30 active shooter incidents in the country. "While we see a decrease from 2021 to 2022, we see over time, over the past 20 years since we've been reporting on active shooter incidents, and certainly in the last five years, there has been an overall increase in this number," a senior FBI official said during après call with reporters.

The biggest increase in recent years came in 2021. When the number of active shooter incidents jumped from 40 to 61, according to the report. Although fewer people died in active shooter incidents in 2022 than in 2021, the total casualty count — deaths and injuries combined —was higher last year than the year before. The shootings caused a combined 313 casualties, including 100 killed and 213 wounded, up from 243 in 2021, including 103 people killed and 140 wounded, the report said. Last year's casualty count was the highest in five years, the report said. According to the report, 13 of the 50 incidents last year resulted in mass killings, defined as four or more people shot dead in single incident.

Not everyone agrees on what constitutes a mass shooting, however. The Gun Violence Archive uses a broader definition that encompasses incidents with at least four victims, either injured or killed. By this definition, the non-profit tallied 646 mass shootings last year, more than ten times the number reported by the FBI

.
In its report, the FBI singled out four incidents that claimed the most lives or inflicted the most injuries last year.

On May 24, a gunman entered Rob Elementary School in Uvalde, Texas, opening fire on students and staff. Nineteen children and two adults were killed. It was the deadliest school shooting since 2012, when a gunman killed 20 children and six adults at Sandy Hook Elementary Schooling Newtown, Connecticut. Ten days before the Uvalde massacre, another gunman entered supermarket in a predominantly African American neighborhood of Buffalo, New York, killing ten people and injuring three.

The two incidents with the highest number of injuries but fewer deaths occurred in Highland Park, Illinois, and Colorado Springs, Colorado.

On July 4, a gunman perched atop a commercial building fired into an Independence Day parade crowd, killing seven and wounding 48 others.

On November 19, five people were killed and 28 others wounded when a gunman opened fire in an LGBTQ club. The FBI says it tracks active shooter incidents to give law enforcement agencies and the public a baseline understanding of the problem.

This year's report offers a wealth of details about the shooters, the time and location of the shootings, and the types of weapons used in the assaults.

Among the report's key findings:
· Of the 50 shooters, 47 were male. They ranged in age between 15 and 70 years old. Four shooters wore body armor, while two acted as snipers.
· In nearly half of the incidents, the shooter had a known connection to the location, the victim or both.
· In the incidents, the shooters used a total of 61 weapons, including 29 handguns, 26 rifles, three shotguns, and three unknown firearms.
· The 50 active shooter incidents occurred in 25 states and the District of Columbia, with Texas reporting six incidents, more than any other state.

· The shootings took place in seven types of locations, including open spaces, commercial buildings, residences, educational facilities, government buildings, houses of worship, and a healthcare facility.

For 2021, FBI highlighted an emerging trend involving "roving active shooters," or gunmen who shoot in multiple locations. That trend was observed in 2022 as well, the senior FBI official said without giving a number. Source; Homeland Security News Wire

Analyst Comment On 26 April, the Federal Bureau of Investigation (FBI) and the Advanced Law Enforcement Rapid Response Training Center (ALERRT) at Texas State University published a joint report titled "Active Shooter Incidents in the U.S. in 2022." For the purpose of the report, the FBI defines an active shooter incident as one or more individuals actively killing or attempting to kill people in a populated area with a firearm. Shootings resulting from another criminal act, like gang violence or drug-related, are not counted as active shooter incidents. In 2022, the FBI designated 50 shootings as active shooter incidents, which is 18% lower than the number of incidents the U.S. saw in 2021 (61), but still 66.7% higher than the number of incidents reported in 2018 (30). Thirteen of the 50 incidents meet the federal criteria for a mass killing: three or more killings in a single incident. The 2022 active shooter incidents resulted in 313 casualties, substantially higher than the 243 casualties caused by active shooters in 2021. However, the number of deaths from active shooter incidents in 2022 (100) declined slightly from 2021 (103) despite the higher number of casualties. Two of the 50 incidents in 2022 occurred on transit infrastructure – the 17 March 2022 shooting on a Broward County bus in Florida, and the 12 April 2022 shooting at the 36th Street Station in Brooklyn, New York. The full report can be viewed at: https://www.fbi.gov/file-repository/active-shooter-incidents-in-theus-2022-042623.pdf/view

Source; Over the–Road-Bus Intelligence Awareness Daily (OTRBIAD) Report.

NATIONAL

(U//FOUO) United States: Juveniles Will Likely Leverage Explosives Availability to Target Secondary Schools

(U//FOUO) According to an FBI Bulletin dated 05 APR 23, the FBI assesses juvenile threat actors in the United States likely will leverage the availability of pre-made improvised explosive devices (IEDs), bomb-making materials, and IED construction instructions to target US secondary schools, resulting in student and staff casualties, and an erosion of public confidence in school officials and law enforcement (LE) personnel. This assessment is made with high confidence, based on open-source news reports; officers of other LE agencies; FBI agents with direct access; an FBI agent with direct access, who obtained the information from an interview of a subject; and an FBI agent with direct access, who obtained the information through legal process returns.

(U//FOUO) The FBI bases this assessment on the key assumptions explosive precursor chemicals (EPCs) will remain available through both physical retail stores and online vendors, and juveniles will maintain internet access to receive guidance for creating IEDs from online resources. The FBI further assumes most secondary schools in the United States have limited capability to detect the introduction of IEDs into the school's facility or setting. Finally, the FBI assumes IEDs are available to juveniles through in-person networks, legal fireworks stands, or complicit adults and legal guardians willing to acquire IEDs and bomb-making materials for juveniles who request them for purported entertainment purposes. If the FBI obtained information suggesting juveniles consider, but reject, the use of explosives in future school attacks, confidence in this assessment would decrease. If juveniles become aware of enhanced security measures nationwide to specifically screen for the attempted introduction of IEDs into school buildings, the likelihood of this assessment would decrease. In the long term, the FBI assesses juvenile threat actors likely will plan and successfully conduct complex attacks using IEDs in coordination with firearms when targeting US secondary schools to ensure their fame and notoriety, further complicating LE response to active shooter incidents.

(U//FOUO) Juveniles Likely Will Leverage IED Availability to Target Secondary Schools, Resulting in Casualties and an Erosion of Public Confidence in School Officials and LE Personnel

(U//FOUO) The FBI assesses juvenile threat actors in the United States likely will leverage the availability of pre-made IEDs, bomb-making materials, and IED construction instructions to target US secondary schools, resulting in student and staff casualties, and an erosion of public confidence of school officials and LE personnel. This assessment is based on juveniles in Pennsylvania conspiring to attack their school using IED information obtained from the internet, a juvenile and their parent manufacturing an IED that inadvertently exploded in the juvenile's classroom, juveniles in Nebraska purchasing IEDs from a complicit adult, and juveniles across the United States plotting unconnected bombings against their schools, which LE disrupted.

• **(U)** Between May 2021 and October 2021, according to three open-source news reports, US LE officials arrested six juveniles for plotting to conduct attacks using IEDs against two high schools and another unidentified target. In two incidents, LE searches identified functional IEDs. In the third incident, an LE search found evidence of incendiary devices.

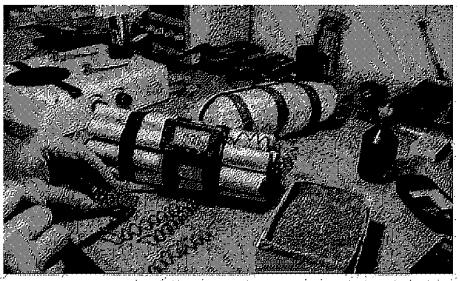
• **(U//FOUO-LES)** In September 2021, according to an open-source news report, LE officials in Pennsylvania arrested four juveniles for conspiring to attack their high school. The date of attack was planned for the 25th anniversary of the 1999 Columbine High School massacre in Colorado, which killed 13 students and teachers. They were charged with multiple violations, including unlawful possession of weapons of mass destruction (WMDs) and possession of explosive material. One of the juveniles possessed components for IEDs, IED-making instructions, and an incendiary device at their home. According to an officer of another LE agency, one of the juveniles used the internet to obtain instructions on how to construct IEDs.

• **(U//FOUO-LES)** According to an officer of another LE agency, on 08 MAR 21, a 16-year-old student accidentally detonated explosive materials he had brought to school for unknown purposes. According to an FBI agent with direct access, on 08 MAR 21, authorities conducted a search of the juvenile's home and found EPCs and bomb-making materials. A subsequent interview with the student and his father revealed they manufactured hex methylene triperoxide diamine (HMTD) from the chemicals found at the residence.

• **(U//FOUO)** According to an FBI agent with direct access, who obtained the information from an interview of a subject, in December 2021, multiple juveniles purchased illegal homemade fireworks from an adult residing in Omaha, Nebraska. According to an FBI agent with direct access, the adult's text message conversations from July 2021 identified the adult was aware his illegal homemade fireworks were sometimes purchased by juveniles who used them to destroy portable toilets on multiple occasions. Identified juveniles used the same homemade fireworks to destroy a stone mailbox with sufficient damage that local LE notified the Joint Terrorism Task Force, according to an FBI agent with direct access, who obtained the information through legal process returns.

(U) Perspective

(U//FOUO) LE continues to face multiple challenges with identifying juvenile IED threat activity in schools, including limited bystander reporting, juveniles' access to the internet, and school security practices. The FBI and National Counterterrorism Center (NCTC) examined the role of bystanders in detecting terrorist activity. The FBI and NCTC identified family members and peers as the largest bystander groups but noted those groups most often communicate their concerns directly to the person of concern rather than LE. These individuals experience significant psychological barriers to making a report on their peer or family member to LE, leading to a majority of those bystanders not intervening to prevent acts of violence when they become aware of concerning behavior. For example, juveniles who purchased illegal homemade fireworks in Omaha attended multiple secondary schools in the Omaha



metropolitan area. The students shared videos of off-campus property destruction caused from using the illegal homemade fireworks and advertised on social media, inviting other juveniles to witness future detonations of the devices in-person. Despite this awareness, neither the juvenile bystanders who attended the detonations in-person nor other juvenile bystanders who saw the advertisements but did not attend reported the incidents to LE or school officials. Although the illegal homemade fireworks used in Omaha did not represent a terrorist act and occurred off the school campus, the failure of multiple peer bystanders to report information about illegal use of explosive devices to LE or school officials highlights the remaining vulnerability for bystanders to report any violent activity.

(U) Juveniles have used their access to online websites and social media to freely communicate threats under the false pretext of anonymity. December 2021 featured a large number of violent threats, particularly related to shootings and bombings, made on social media against schools, which increased the LE presence at schools, public safety statements by school districts, and the disruption of school activities. Despite these increased precautions, school shootings in the United States increased to a record high of 55 in 2022, compared to the previous record of 35 in 2021.

(U//FOUO-LES) The assessment in this intelligence bulletin diverged from the analysis in the 28 DEC 22 FBI Strategic Perspective: Executive Analytic Report (SPEAR), titled "(U//FOUO) Juvenile School Bombing Plotters Detail Their Plans in Writing," which assessed juvenile school bomb plotters provide insight into their plans through their private personal writings, allowing close contacts to identify and report violent plans. This bulletin differs from the SPEAR by indicating bystanders in some instances include complicit adults and legal guardians who provide juveniles access to bomb-making materials.

(U//FOUO) This intelligence bulletin aligns with the 13 SEP 21 Joint Counterterrorism Assessment Team First Responder's Toolbox article, titled "(U) Intervention Options for Minors Vulnerable to Violent Extremism Activity." In that product, NCTC, US Department of Homeland Security (DHS), and FBI assessed some minors were vulnerable to violent extremist messaging that appealed to a variety of developmental and psychological needs. NCTC further assessed either COVID-19 isolation or an increased use of social media by minors affects minors' susceptibility to terrorist messaging. One example featured a minor who was arrested for preoperational online activities pertaining to information on bomb making and photos of IEDs. Although this intelligence bulletin does not focus on the extremist propaganda, it does align with the article's assessment on juveniles' online capabilities to obtain information and make connections with nefarious actors.

(U//FOUO) FBI Comment: In the long term, the FBI assesses juvenile threat actors likely will plan and conduct complex attacks using IEDs in coordination with firearms when targeting US secondary schools to ensure their fame and notoriety, further complicating LE response to active shooter incidents. The complexity, planning, and execution of school attacks continue to evolve toward greater violence and higher mortality rates as juvenile offenders switch from handguns to fully automatic weapons and IEDs and learn from past school shootings' successes and failures. Federal, state, and local LE officials, mental health workers, and education personnel have the opportunity to work with school districts and state departments of education to develop procedures for schools to monitor student activity on their technology networks, provide training on research related to construction of IEDs, develop procedures for reporting suspicious activity, and create screening procedures for potential IEDs. Local threat assessment and threat management teams can further work with school districts through referrals to their internal threat assessment teams and maintain bi-directional communication with schools when concerns arise. Through engagement with suicide prevention hotlines and hotlines providing mental health support to teenagers, LE has the opportunity to develop additional procedures that preserve caller privacy while also identifying callers with the potential to use IEDs. Lastly, state fusion centers have the opportunity to expand the Nationwide Suspicious Activity Report Initiative to connect with anti-bullying hotlines present in some states to detect indicators of possible IED production.

(U//FOUO) Indicators juveniles are planning complex attack with IEDs include:

- **(U//FOUO)** Attending school with explosive residue on their personal items.
- **(U//FOUO)** Conducting explosive-related research on school computers without appropriate purpose or approvals.
- **(U//FOUO)** Discussing school attacks that are more deadly and cause more notoriety than previous attacks.

• **(U//FOUO)** Posing unusual or suspicious questions during science courses related to EPCs, including handling procedures, procedures for acquiring such materials, and whether the school has such materials on hand.

• **(U//FOUO)** Theft of EPCs from school laboratories attributed to an enrolled student.

• **(U//FOUO)** Sharing videos of explosions and claiming credit for the explosions; and

• **(U//FOUO-LES)** Encouraging others to conduct explosive and firearm attacks against schools.

Sources; (FBI, Juveniles Likely Will Leverage Explosives Availability to Target Secondary Schools, Bulletin, 05 APR 23) via the Army Threat Integration Center (ARTIC)

Pitt Researchers Collect Data on Where Train Accidents Occur and What They Threaten

[Pennsylvania] Railroad safety continues to be a concern after the East Palestine derailment in February and the train wreck in Harmar Township last May. A group of University of Pittsburgh researchers gathered data to identify where train derailments occur in southwestern Pennsylvania and the risk these accidents pose. The concern surrounding train derailments is still top of mind. "After East Palestine, everyone was kind of like, 'what are we going to do next?'" said Daniel Bain, associate professor with the Geology and Environmental Science Department at the University of Pittsburgh. Bain felt compelled to start researching train accidents after the February derailment in East Palestine. Bain is one of the founding members of the Pittsburgh Water Collaboratory. Source; CBS, 4/26/2023

Analyst Comment Researchers at the University of Pittsburgh have been studying train derailment trends in Southwestern Pennsylvania by reviewing and plotting all rail accidents the Federal Railroad Administration (FRA) has for the region between 2011 and 2022. Their findings reportedly indicate that "211 of the 270 accidents were within 300 yards of a major river." According to a Pittsburgh Water Collaboratory report, 22% of train derailments in the region from 2011 to 2021 "involved HAZMAT cargo." When approached about the risks of water contamination, Allegheny County Emergency Services Chief Matt Brown said that the dangers posed are "not just with trains.

The most dangerous by volume and frequency is by vehicle. But all methods of transportation are included, such as river barge, pipeline, airplane, and trains." Brown also said that the assessed level of risk "can change based on method of transportation, product or chemical type, volume or amount of product, frequency of occurrence or potential and many times location or geography," and that from "the threat and risk perspective, flash flooding continues to remain [Allegheny County's] greatest potential risk."

Source; Over the–Road-Bus Intelligence Awareness Daily (OTRBIAD) Report.

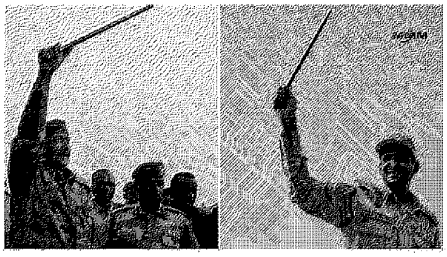
SSRIG Comment For us in the Pacific Northwest we have a lot of train traffic (mainly BNSF) that goes over multiple waterways and the largest is the Puget Sound. The same threats and risks mentioned above apply here for Emergency Management to consider in planning.

INTERNATIONAL

Germany Arrests 28-Year-Old Syrian Over 'Radical Islamist' Bomb Plot

[Hamburg, Germany] German authorities arrested a 28-year-old Syrian national on Tuesday morning, one of two brothers suspected of planning to blow up civilian targets using a homemade explosives belt for "radical Islamist and jihadist" reasons, a statement said. Public prosecutors in the northern port city of Hamburg carried out searches as part of a joint probe with police, arresting the man whom they believed bought raw materials for bomb-making off the internet over several weeks. Source; Reuters, 4/25/2023

Analyst Comment On 25 April, German police arrested a 28-year-old Syrian man in Hamburg, Germany on suspicion of planning to carry out an explosives attack motivated by Islamic extremism. According to the statement released by prosecutors, the 28-year-old man and his 24-year-old brother allegedly "planned an attack with a home-made explosive belt, out of a radical Islamist and jihadist motivation in order to carry out an attack against civilian targets." The man has not been named by authorities, and he was allegedly "helped and encouraged" by his 24-year-old brother who lives in Kempten, Bavaria. The 24-year-old brother was also detained by German authorities during the investigation. Investigators believe the men had been purchasing raw bomb-making materials off the internet for several weeks. Authorities have not remarked on any specific targets the man may have had, but during the investigation over 250 police searched properties in Hamburg and Kempten where they seized "large amounts of evidence including chemical substances." Source; Surface Transportation & Public Transportation ISAC Transit & Rail Intelligence Awareness Daily Report (TRIAD)



Sudan in Chaos

For the last two weeks, two generals and their armies have been locked in a power struggle in Sudan, mostly in the capitol of Khartoum. Intense fighting has forced foreign governments and the UN to evacuate their citizens from embassies and international organizations, reports BBC. The conflict has shutdown normal life and created a humanitarian crisis. Seventy percent of the hospitals are not functioning, a laboratory containing infectious diseases was seized creating a possible biological hazard, and food and fuel are becoming scarce. The struggle pits one general, Abdel Fattah al-Burhan, who controls the Sudanese Army against Mohamed Hamdan Dalgo, who commands the Rapid Support Forces (RSF). The RSF is connected to war crimes and has links to the Russian Wagner Group. The disintegration into a civil war could have significant impacts on neighboring fragile nations and present opportunities for extremist groups to exploit.

Analyst Assessment The UN World Food Programme (WFP) warned that the violence in Sudan, where a third of the country already struggles with food shortages, has the potential to push millions into a famine. A recent report focused on the link between food insecurity and conflict, found that extremist groups use opportunities providing food and resources to drive recruitment. The WFP also warned that up to 13 million Afghanis are experiencing famine attributed to state violence, political mismanagement, and waning international support. Information found in the Discord leak revealed that ISIS-K operating in Afghanistan was consolidating and plotting attacks on western targets like embassies, churches and business centers. On Tuesday, German security forces in Hamburg arrested two Syrian brothers planning an explosive attack motivated by Islamic extremism. Currently this past week or more two Americans have been killed during this crisis. Source; Watchline@fdny.nyc.gov

Other National/International Articles of Interest (Links):

United States: Two Men Sentenced For Planning To Attack U.S. Electric Substations
https://www.dispatch.com/story/news/courts/2023/04/21/white-supremacists-sentenced-in-ohio-for-plot-to-attack-power-grid/70140160007/

The ABCs of AI: 20 key terms every police officer should know
https://www.police1.com/artificial-intelligence/articles/the-abcs-of-ai-20-key-terms-every-police-officer-should-know-BJIDkqEk32RrPvvf/

160,000 rounds of ammo stolen from Ohio Police Division
https://www.wtrf.com/top-stories/160000-rounds-of-ammo-stolen-from-ohio-police-division/

Worldwide: Critical Infrastructure Hit By Supply Chain Attack Behind 3CX Breach
https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise

'Coma in a Bottle': Custom, border patrol officers seize 6 gallons of liquid ecstasy in Philadelphia
https://6abc.com/coma-in-a-bottle-liquid-ecstasy-philadelphia-gamma-butyrolactone-chemical-seized-date-rape-drug/13189641/

3 high schoolers charged with 1st-degree murder in rock-throwing incidents
https://6abc.com/3-high-schoolers-charged-with-1st-degree-murder-in-rock-throwing-in/13189683/

Guardsman in leak case wanted to kill a 'ton of people': US
https://apnews.com/article/leaked-documents-air-national-guardsman-jack-teixeira-d7c8dbaeb3b7a5ae69faeab04ede2ab0

What cops can learn from YouTube
https://www.police1.com/police-training/articles/what-cops-can-learn-from-youtube-XyqTTYE5WGXXsTRL/?utm_source=Police1&utm_campaign=b4e105a82f-EMAIL_CAMPAIGN_2023_04_27_07_12&utm_medium=email&utm_term=0_5584e6920b-6f9733b5d3-%5BLIST_EMAIL_ID%5D

*TPD/PCSD Homeland Security Reports Received this week 7.