



OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN FOCUS

11 MARCH 2024

DHS-IA-IF-2024-00927

PUBLIC SAFETY AND SECURITY

(U//FOUO) Threat to High-Profile Officials and Secondary Targets Likely Increased as Online Messaging Promotes Targeting Private Residences

(U//FOUO) The threat to high-profile public and private sector officials and their families and staff has likely increased, judging from a recent uptick in online messaging promoting attacks at their homes, doxing and swatting incidents, and several notable attacks. Private residences are frequently less secure than attack venues where high-profile officials have traditionally been targeted, like government buildings and corporate offices, and lack the more robust security measures of those locations, leaving the targets and their families and employees at their homes vulnerable to attack. Recent attacks at private residences have occurred during a period of overall increased political polarization, target hardening of more traditional attack locations, and the prevalence of conspiracy theories targeting industry and government officials.

- **(U//FOUO)** In online messaging over the last 18 months, threat actors of various ideologies have promoted attacks against high-profile government and private sector officials at their homes and shared several tactics to increase operational security and the effectiveness of attacks. For example, in July 2023, Telegram channels that promote accelerationist racially or ethnically motivated violent extremist (RMVE) content recirculated a meme with the message “Start Hunting Your Tech CEOs for Sport” with excerpts from a book advocating for targeting penthouse windows with assault rifles, according to an organization that monitors extremism online.^a These online calls are often accompanied by promotion of or actual incidents of doxing specific targets’ personally identifiable information (PII), a tactic which reduces obstacles for attacks. For example, a US state’s Secretary of State and their family members were doxed in December 2023 following their decision to remove a former US president from the state’s 2024 ballot. The doxing resulted in online threats and a swatting incident at their home address.

^a (U) Please see Definitions at the end of this product.

- (U//FOUO) Traditional targets have increased target hardening security measures—including layered measures such as surveillance, access control, metal detectors, K9s, and suspicious activity training for security personnel—and require more complex planning than soft targets. This probably drives potential attackers to prioritize private residences, as they perceive homes to be accessible with limited obstacles or interdiction, and better suited to their preferred simple tactics and weapons.
- (U//FOUO) While targeting private residences is not a new tactic, 7 of 10 known attacks or disrupted plots against high-profile officials since 2018 occurred in the last two years, based on a review of a limited body of reporting. Attacks against private residences since 2018 have resulted in at least three deaths and at least two serious injuries not only to the intended target, but to family members and employees of the targets, based the same reporting. For example, in October 2022, the spouse of then-Speaker of the US House of Representatives was attacked by an armed perpetrator while inside of their home. The attacker made statements indicating he was looking for the Speaker, but they were not home at the time of the incident.

(U//FOUO) **Multiple Challenges for Law Enforcement Detection and Disruption**

(U//FOUO) According to our review of attacks since 2018, actors motivated by both ideological and personal grievances target private residences, creating a diverse set of potential motivating factors that challenge law enforcements' ability to detect and disrupt plotting. Additionally, the prevalence of sensitive PII on both the Surface Web and the Dark Web and the use of mapping software allows threat actors to conduct preoperational surveillance and planning in a virtual environment, improving operational security and further complicating law enforcement detection. This use of online information and platforms to plan attacks against private residences, particularly the access to personal addresses, reduces the need for attackers to conduct preoperational and preparatory behaviors like location casing, stalking, and harassment, minimizing opportunities for law enforcement to mitigate these attacks.

(U//FOUO) **The targeting of private residences highlights the need for collaborative mitigation strategies among local, state, and federal partners.** Mitigating these attacks will require broader implementation of personal security and law enforcement best practices and continuous information sharing among the different levels of government. Timely and robust sharing of leads and information regarding violent extremist messaging and behavioral indicators associated with such plotting will be key to

informing the operational responses of state, local, tribal, and territorial (SLTT) governments and federal law enforcement partners.

- (U//FOUO) **Implementing personal security practices could effectively mitigate some threats to government officials and high-profile individuals.** By regularly using programs designed to remove PII from online platforms and practicing operational security, such as removing staff credentials, license plates, medical information, and identification cards from public-facing communications like social media posts, the unintended spread of PII can be minimized. Establishing target hardening measures around private residences, like physical security and camera systems, may deter threat actors from mobilizing against a target's residence.
- (U//FOUO) **Local and state level law enforcement agencies are the first line of defense against attacks at officials' home residences and provide the best opportunity for mitigation.** Establishing expeditious procedures for concerning calls, like suspicious person reports in the vicinity of high-profile officials' home residences, as well as ensuring officer awareness of possible attractive soft target locations in their area of responsibility could help local law enforcement decrease response times in the case of an attack.
- (U//FOUO) **Continuous intelligence sharing across all levels of government would help increase SLTT law enforcements' ability to proactively respond to these types of threats.** As traditional targets like federal and state offices experience an increase in target hardening efforts, intelligence sharing of violent extremist messaging advocating for tactical shifts from those locations to softer locations for attacks would help trigger collaborative mitigation strategies by federal and SLTT law enforcement agencies.



OFFICE *of* INTELLIGENCE *and* ANALYSIS

INTELLIGENCE IN FOCUS

11 MARCH 2024

(U//FOUO) Attacks and Plots Against High-Profile Public and Private Sector Officials at Private Residences Between 2018–2024

(U//FOUO) Since 2018, we have observed at least 10 notable instances of attacks or plots where the perpetrator targeted high-profile public and private sector officials at their private residences. Based on limited available reporting, attacks against private residences may have increased over the last two years, with 7 of the 10 attacks occurring since the beginning of 2022. Almost all the attackers used firearms resulting in a total of two injuries and three fatalities. In 4 of the 10 attacks, the victim was a family member or an employee of the intended target. In each case, the perpetrator allegedly perceived the intended target of the attack or plot as the driving force behind their ideological or personal grievance. Of note, this dataset was compiled by a review of available open source reporting on the use of this tactic and may not constitute a complete list of attacks or plots at private residences. This list is intended as a representative sample of the notable use of this tactic in recent years.

OVERALL GRAPHIC CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY

PERPETRATOR/ ALLEGED PERPETRATOR	DATE OF ATTACK OR PLOT	LOCATION	OVERVIEW OF THE ATTACK OR PLOT	INJURIES AND FATALITIES	ALLEGED MOTIVATIONS AND DOCUMENTED IDEOLOGIES
Self-identified anarchist group, incident still under investigation	1/12/2024	Portland, Oregon	A self-identified anarchist group allegedly set fire to a parked car outside a city commissioner’s home as a “call to action” and “warning” to other politicians. The car belonged to a family member of the commissioner.	No injuries or fatalities	The self-identified anarchist group claimed responsibility for the arson as an “act of community self-defense” and expressed regret for not setting the other two vehicles outside the home on fire. The post also stated it was a warning to other politicians and a call to action for other anarchists.
Alleged Perpetrator Pedro Argote ^{USPER}	10/19/2023	Hagerstown, Maryland	The perpetrator allegedly shot the judge in his driveway while his wife and son were at home.	1 fatality	The perpetrator was previously involved in a divorce proceeding where he lost custody of his children that the judge presided over hours before the attack.
Alleged Perpetrator Solomon Peña ^{USPER}	12/4/2022– 1/3/2023	Multiple locations in Albuquerque, New Mexico	The perpetrator allegedly hired two men to carry out shootings at the homes of two state legislators and two county commissioners. The individual was indicted on 14 criminal charges and is currently awaiting trial.	No injuries or fatalities	The perpetrator allegedly lost a bid for state house and believed election fraud conspiracy theories were to blame for his loss.
Perpetrator David Depape ^{USPER}	10/28/2022	San Francisco, California	The perpetrator entered the bedroom of former Speaker of the House; however, only their spouse was home at the time. The perpetrator was able to strike the victim with a hammer before police could subdue him. Police restrained the perpetrator and later found a roll of tape, white rope, a second hammer, a pair of rubber and cloth gloves, and zip ties from the crime scene. Officers observed a broken glass door to the back porch. He was convicted of federal assault and attempted kidnapping charges and is currently awaiting sentencing. He also awaits trial on separate state charges for the incident.	1 injury	The perpetrator was motivated by broad anti-government sentiment and was a known consumer of conspiracy theories, including QAnon and 2020 fraudulent election narratives.
Alleged Perpetrator Nicholas John Roske ^{USPER}	6/8/2022	Chevy Chase, Maryland	The perpetrator allegedly traveled from California to Maryland, intending to kill a Supreme Court Justice. He arrived at the residence of a current Justice in the early morning hours and was observed loitering outside of the residence. The individual had a firearm and multiple rounds of ammunition. The alleged perpetrator was indicted on federal charges and is currently awaiting trial.	No injuries or fatalities	The perpetrator was allegedly motivated by Supreme Court of The United States opinions on abortion access, an upcoming firearm control case, and the school shooting in Uvalde, Texas.

(U//FOUO) Attacks and Plots Against High-Profile Public and Private Sector Officials at Private Residences Between 2018–2024 (Cont.)

OVERALL GRAPHIC CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY

PERPETRATOR/ ALLEGED PERPETRATOR	DATE OF ATTACK OR PLOT	LOCATION	OVERVIEW OF THE ATTACK OR PLOT	INJURIES AND FATALITIES	ALLEGED MOTIVATIONS AND DOCUMENTED IDEOLOGIES
Perpetrator Douglas Uhde	6/3/2022	New Lisbon, Wisconsin	The perpetrator entered the home of a local judge, where he restrained and murdered him using a firearm before committing suicide. It was later determined that the perpetrator had a list in his vehicle with other government officials on it with several government officials on it, including two sitting state Governors and the US Senate Majority Leader.	1 fatality	The perpetrator was previously sentenced to jail by the judge in a case over 15 years ago. The suspect was allegedly acting in retaliation for that sentencing.
Alleged Perpetrator Joseph Beecher ^{USPER}	2/2/2022	Meeker, Colorado	The perpetrator allegedly rammed his vehicle into the gates of Michael Bloomberg's ^{USPER} ranch and then made statements to employees that he was looking for Bloomberg or his daughters. After discovering the family was not present, the perpetrator allegedly abducted an employee at gunpoint, forcing her to drive to Wyoming before law enforcement tracked and apprehended the suspect. The suspect is currently being held pending court proceeding on kidnapping charges.	No injuries or fatalities	Court proceedings for this case are still on-going and the alleged perpetrator's motivations are still under investigation. However, the perpetrator did state to his abduction victim that he wanted to "make an international incident" involving his initial targets.
Various affiliates of Wolverine Watchmen Militia ^{USPER}	10/8/2020	Lansing, Michigan	Seven members affiliated with a militia group were found guilty of planning to kidnap the Governor of Michigan at their private vacation home. Members of the group trained, surveilled the property, and explored ways to slow down police response. As of 28 December 2022, the seven members or affiliates of the Michigan militia group have been sentenced to various federal and state charges for their actions.	No injuries or fatalities	The perpetrators opposed COVID-19 pandemic mitigation measures and blamed the intended target for the implementation of the measures. The individuals also adhered to many anti-government conspiracy theories and militia violent extremist (MVE) ideology.
Perpetrator Roy Den Hollander	7/19/2020	North Brunswick, New Jersey	The perpetrator targeted a federal judge's family at their home by knocking on the front door disguised as a delivery driver. The perpetrator then opened fire, killing the judge's son when he opened the door. The judge's husband was also shot multiple times and left in a critical but stable condition. The federal judge was in the basement at the time of the attack and was not injured. The perpetrator was found deceased the next day from a self-inflicted gunshot wound.	1 injury, 1 fatality	The perpetrator held anti-feminist sentiment and had a personal grievance against the judge following a case that she presided over.
Perpetrator Cesar Sayoc Jr. ^{USPER}	10/22/2018	Bedford, New York	The perpetrator, who plead guilty to 65 felonies, sent 16 improvised explosive devices via the US postal service to 13 individuals, including 11 current or former government officials. One package was sent to a residence of a prominent Democratic donor. Local law enforcement received a call about a suspicious package found in a mailbox. The package did not detonate on its own. The target was not home at the time.	No injuries or fatalities	The perpetrator was allegedly motivated by what he perceived to be the enemies of a former United States President and hatred towards his targets. He also adhered to several anti-government conspiracy theories.

Source, Reference, and Dissemination Information

Definitions

(U//FOUO) **Accelerationism:** A concept suggesting that the existing social order should be pushed to such a degree that Western countries become failed states, giving rise to changes that would reshape the world in radical ways. RMVEs following a white supremacist extremism version of accelerationism advocate for acts of social disruption, up to and including violence, and taking violent action to prompt responses that would gain support from those advocating for the superiority of the white race.

(U//FOUO) **Anarchist Violent Extremists (AVEs):** Individuals who seek, wholly or in part, through unlawful acts of force or violence, to further their opposition to all forms of capitalism, corporate globalization, and governing institutions, which they perceive as harmful to society.

(U//FOUO) **Anti-Government or Anti-Authority Violent Extremist (AGAAVE):** Groups or individuals who facilitate or engage in unlawful acts of violence directed at Federal, State, or local law enforcement, other government officials, critical infrastructure, or government facilities in order to affect the conduct of a government or influence the policy of a government by intimidation or coercion, in response to their belief that their liberties are being taken away by the perceived unconstitutional or otherwise illegitimate actions of government officials or law enforcement. Some form of this belief is common to several violent extremist ideologies, including sovereign citizen extremism and militia extremism; anti-government extremists differ from these other categories in that they do not subscribe to these violent extremist ideologies in total, but often adopt elements of these ideologies, including the use of violence in furtherance of their ideology.

(U) **Dark Web:** The least accessible subset of the internet that is comprised of overlay networks hidden from regular search engines and requires specialized software, tools, or network configurations to access. Malicious actors use the Dark Web to communicate about, sell, and/or distribute illegal content or items such as drugs, illegal weapons, malware, and stolen data. However, just like the Surface Web, there are several legitimate activities on the Dark Web as well, including accessing information, sharing information, protecting one's identity, and communicating with others.

(U//FOUO) **Domestic Violent Extremist (DVE):** An individual based and operating primarily within the United States or its territories without direction or inspiration from a foreign terrorist group or other foreign power who seeks to further political or social goals wholly or in part through unlawful acts of force or violence. The mere advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics alone does not constitute violent extremism and may be constitutionally protected. DVEs can fit within one or multiple categories of ideological motivation and can span a broad range of groups or movements. I&A utilizes this term synonymously with "domestic terrorist."

(U) **Doxing:** To publicly identify or publish private information about someone, especially as a form of punishment or revenge. Doxing also is often used by individuals to encourage violence, harass, and intimidate their targets.

(U//FOUO) **Militia Violent Extremist (MVE):** Groups or individuals who facilitate or engage in acts of unlawful violence directed at federal, state, or local government officials or infrastructure in response to their belief that the government deliberately is stripping Americans of their freedoms and is attempting to establish a totalitarian regime. These individuals consequently oppose many federal and state authorities' laws and regulations, particularly those related to firearms ownership, and often

belong to armed paramilitary groups. They often conduct paramilitary training designed to violently resist perceived government oppression or to violently overthrow the US Government.

(U//FOUO) **QAnon:** A complex and constantly evolving conspiracy theory that is promoted by a decentralized online community that has morphed into a real-world movement. The foundational principle holds that a corrupt cabal of “global elites” and “deep state” actors run an international child sex trafficking ring and engage in plots to conduct a coup against a former President of the United States while he was in office. These alleged crimes by members of the cabal will be punished by their mass military detention in Guantanamo Bay and their likely execution. QAnon is a highly participatory and malleable conspiracy theory that encourages adherents to enhance the prominent narratives with new connections or information. QAnon narratives are constantly changing and expanding to include false information about current events and political controversies, which is then woven into the QAnon master narrative.

(U//FOUO) **Racially or Ethnically Motivated Violent Extremists (RMVEs):** Groups or individuals who facilitate or engage in the potentially unlawful use, or threat of force or violence with the intent to intimidate or coerce, in furtherance of political and/or social agendas, which are deemed to derive from bias, often related to race or ethnicity, held by the actor against others, including a given population or group.

(U) **Swatting:** Describes criminal activity by an individual or group who knowingly provides false information to police suggesting that a threat exists at a particular location so that police respond with tactical units, or what is commonly known as a special weapons and tactics (SWAT) team. These sorts of reports can cause unintended harm to the victim, including injury and death, as police seek to stop the reported threat as quickly as possible.

(U) **Surface Web:** The portion of the internet accessible in regular day-to-day activities. It is available to the public using standard search engines and can be accessed using standard web browsers that do not require any special configuration, such as Mozilla Firefox, Microsoft’s Internet Explorer or Edge, and Google Chrome.

Reporting Suspicious Activity

(U) **To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement.** Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit www.dhs.gov/nsi.

Warning Notices & Handling Caveats

(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

(U) **USPER:** This product contains US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label USPER and should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Other US person information has been minimized. Should you require the minimized US person information on weekends or after normal weekday

hours during exigent and time sensitive circumstances, contact the Current and Emerging Threat Watch Office at 202-447-3688, CETC.OSCO@hq.dhs.gov. For all other inquiries, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov.

CLASSIFICATION:



Homeland
Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title:

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: and function:

2. What is the highest level of intelligence information that you receive?

3. Please complete the following sentence: "I focus most of my time on:"

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	☐	☐	☐	☐	☐	☐
Product's relevance to your mission	☐	☐	☐	☐	☐	☐
Product's timeliness	☐	☐	☐	☐	☐	☐
Product's responsiveness to your intelligence needs	☐	☐	☐	☐	☐	☐

5. How do you plan to use this product in support of your mission? (Check all that apply.)

- | | |
|--|---|
| ☐ Drive planning and preparedness efforts, training, and/or emergency response operations | ☐ Initiate a law enforcement investigation |
| ☐ Observe, identify, and/or disrupt threats | ☐ Initiate your own regional-specific analysis |
| ☐ Share with partners | ☐ Initiate your own topic-specific analysis |
| ☐ Allocate resources (e.g. equipment and personnel) | ☐ Develop long-term homeland security strategies |
| ☐ Reprioritize organizational focus | ☐ Do not plan to use |
| ☐ Author or adjust policies and guidelines | ☐ Other: <input type="text"/> |

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product not address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
This product will enable me to make better decisions regarding this topic.	☐	☐	☐	☐	☐	☐
This product provided me with intelligence information I did not find elsewhere.	☐	☐	☐	☐	☐	☐

9. How did you obtain this product?

10. Would you be willing to participate in a follow-up conversation about your feedback?

To help us understand more about your organization so we can better tailor future products, please provide:

Name:
Organization:
Contact Number:

Position:
State:
Email:

Submit
Feedback

[Privacy Act Statement](#)

CLASSIFICATION:

Product Serial Number:

REV: 10 November 2016