OFFICE of PRIVATE SECTOR

Liaison Information Report (LIR)
Cross Sector/Industry

LIR 180914001

14 September 2018

College Campuses Vulnerable to Threats Stemming from Homegrown Violent Extremists

The FBI's Office of Private Sector (OPS), in coordination with the FBI Counterterrorism Division (CTD), the Department of Homeland Security (DHS), and the National Counterterrorism Center (NCTC), is providing this LIR to private sector partners to highlight the potential threat stemming from homegrown violent extremists (HVEs)[a] on college campuses. Identifying radicalized individuals and reporting suspicious activity to the FBI and other law enforcement partners is critical to safeguarding the Homeland.

Since 2006, there have been at least four attacks conducted by HVEs on college campuses; all four attackers were students or alumni of the schools they attacked. In some instances, these attacks were conducted on college campuses in response to perceived injustices or personal grievances. In other instances, college campuses were likely chosen as attack targets due to the attacker's familiarity with the campus. Some individuals have also attempted to radicalize[b] others on college campuses. Violent extremist ideologies could appeal to a range of emotional needs—such as desiring a sense of belonging, identity, or attention-seeking through rebellion—often experienced by young adults, a cohort historically targeted by violent extremist messaging via public and private social networking platforms

Studies of terrorist actors have identified particular behaviors that have been observed prior to or during mobilization to violence. Any one of these behaviors, which are identified in the *Homegrown Violent Extremist Mobilization Indicators* booklet that is available at https://www.dni.gov/index.php/nctc-newsroom/nctc-resources/item/1904-homegrown-violent-extremist-mobilization-indicators, may be insignificant on its own, but when observed in combination with other suspicious behaviors—particularly advocacy of violence—may constitute a basis for reporting the individual to law enforcement. Some observed activities that may be suspicious include constitutionally protected activities. These activities should not be reported absent articulable facts and circumstances that support the reporter's suspicion that the observed behavior is not innocent but, rather, reasonably indicative of criminal activity associated with

[a] (U//FOUO) The FBI, DHS, and NCTC define an HVE as a person of any citizenship who has lived and/or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically motivated terrorist activities (including providing support to terrorism) in furtherance of political or social objectives promoted by a foreign terrorist organization but is acting independently of direction by a foreign terrorist organization. HVEs are distinct from traditional domestic terrorists who engage in unlawful acts of violence to intimidate civilian populations or attempt to influence domestic policy without direction from or influence from a foreign actor.

[b] (U//FOUO) The FBI, DHS, and NCTC define radicalization as the process through which an individual changes from a nonviolent belief system to a belief system that includes the willingness to actively advocate, facilitate, or use unlawful violence as a method to affect societal or political change.

terrorism. These indicators include material support to terrorist groups, indicators of violent extremist radicalization, and indications of travel overseas to engage in violence. Students, professors, and staff are best positioned to observe violent extremist behaviors in students. If suspicious activities warranting the attention of law enforcement are observed, please contact the nearest state and major urban area fusion center or local FBI field office and follow the state's suspicious activity reporting protocol.

The FBI's Campus Safety Program works with campus security and law enforcement personnel to provide information, guidance, and training to mitigate terrorism threats. DHS's Academic Engagement Office provides higher education institutions with engagement and outreach on security issues and facilitates regular training exercises to enhance emergency preparedness. NCTC's Directorate of Strategic Operational Planning is developing a training curriculum for faculty and students on radicalization indicators.

Additional Resources:

- *Don't Be a Puppet: Pull Back the Curtain on Violent Extremism* is a free online interactive awareness program that exposes the destructive reality of violent extremism so young adults are more aware and better informed. The site addresses the "who, what, why, and how" of violent extremism using quizzes and videos to encourage learning. This standalone program can also be used as a resource by civic groups, parents, teachers, and others to raise awareness of the growing impact of violent extremism. The site, developed and sponsored by the FBI, can be found at https://cve.fbi.gov.

- *Innovate against Hate* provides funding for university student teams to design, pilot, and implement social or digital initiatives with the goal of countering hate and extremism while promoting values of fairness, equity, and inclusion. The competition, previously sponsored by DHS, is funded by the Anti-Defamation League and managed by EdVenture Partners. More information can be found at https://www.adl.org/innovate-against-hate.

This LIR was created and disseminated from OPS's Sector Analytic Unit. 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

OFFICE of PRIVATE SECTOR

Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.