



Homeland
Security

Office of Intelligence and Analysis



OFFICE OF INTELLIGENCE AND ANALYSIS
INTELLIGENCE NOTIFICATION

19 December 2014

~~(U//FOUO)~~ **Security Awareness for the 2014 Holiday Season**

~~(U//FOUO)~~ Prepared by the DHS Office of Intelligence and Analysis (I&A). Coordinated with the NPPD Office of Cyber and Infrastructure Analysis and the NPPD Office for Bombing Prevention.

~~(U)~~ **Overview:**

~~(U//FOUO)~~ DHS I&A has no specific intelligence indicating any terrorist groups or violent extremists are currently advancing plots to occur during the 2014 holiday season.

~~(U//FOUO)~~ While al-Qa'ida, its affiliates, or allies usually prioritize attack timing based on operational readiness rather than specific date selection, homegrown violent extremists* (HVEs) and lone offenders† in the past have sought to target large gatherings that sometimes occur during the holiday season.

~~(U//FOUO)~~ Additionally, we assess that many of the recent calls by Islamic State of Iraq and the Levant (ISIL) and its supporters on violent extremist web forums and social media for violence in the Homeland, specifically against law enforcement and government personnel, are being made in retaliation for ongoing US airstrikes in Iraq and Syria. However, there is currently no specific or credible information to indicate a threat to the Homeland during the 2014 holiday season from ISIL, HVEs, or other violent extremist groups overseas specifically associated with these conflicts.

~~(U//FOUO)~~ Recent world events highlight our concern for the potential for HVEs and lone offenders to evade detection until operational. Given the nature of the HVE threat, we remain concerned HVEs—and particularly those acting alone—could conduct an attack with little to no warning. We are continuing to monitor events overseas for potential Homeland implications.

~~(U//FOUO)~~ Although we are unaware of any specific domestic terrorist threats during the holiday period, DHS assesses domestic terrorists will remain focused on their traditional targeting interests and pose a persistent threat of violence, including assaults, shootings, and incidents involving improvised explosive or incendiary

* ~~(U//FOUO)~~ DHS defines 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 or to intimidate civilian populations or attempt to influence domestic policy without direction from or influence from a foreign actor.

† ~~(U//FOUO)~~ DHS defines a lone offender as an individual motivated by one or more violent extremist ideologies who, operating alone, supports or engages in acts of violence in furtherance of that ideology or ideologies that may involve influence from a larger terrorist organization or a foreign actor.

devices intended to result in multiple casualties or significant property losses.[‡] Violence by lone offenders and small cells will likely remain the primary domestic terrorist threat due to the greater potential for operational security afforded to those who act independently of larger groups.

(U) Hacker Group Posts Threat Targeting Movie Theaters in the Homeland

(U) On 16 December, a group identifying itself as “Guardians of Peace” posted a message on an identified online message board threatening violence at movie theaters planning to show “The Interview”—a movie involving a fictional plot to assassinate Democratic People’s Republic of Korea (DPRK) leader Kim Jong Un—which was originally scheduled for release on Christmas Day. The post specifically mentioned the events of 11 September 2001 and stated that people should keep their distance from locations showing the movie, including the premiere in New York. It further encouraged people who live in areas where the movie is being shown to leave the area.¹ The film has since been pulled indefinitely from theaters by its parent company.²

(U) Prior to this threat, “Guardians of Peace” claimed responsibility for having infiltrated and released data from Sony Pictures Entertainment (SPE)^{USPER} systems—the movie studio releasing “The Interview”—and defacing several of SPE’s Twitter^{USPER} profiles. “Guardians of Peace” likely acquired terabytes of data from its breach of SPE systems, and so far has released only a portion of this data in a series of nine numbered leaks. In a December 13 online message board post, the group threatened further data releases, stating, “We are preparing for you a Christmas gift. The gift will be larger quantities of data. And it will be more interesting.”^{3,4}

(U//FOUO) DHS I&A is not aware of any specific, credible information indicating a physical threat from “Guardians of Peace” to movie theaters in the Homeland and notes that hacking groups have historically made exaggerated threat statements. Despite a lack of credible threat reporting, mass gatherings have historically been attractive targets and threat actors could view screenings as potentially attractive targets due to the growing media attention. “Guardians of Peace” will likely continue to release portions of the exfiltrated data to keep pressure on Sony, possibly to get the company to destroy all copies of the film or publicly apologize for its production of “The Interview.”

(U//FOUO) Potential Suspicious Activity Indicators

(U//FOUO) DHS I&A remains concerned that terrorists not yet identified could seek to advance or execute attacks with little or no warning. Throughout the holiday season, we encourage federal, state, local, tribal, and territorial law enforcement and public safety officials to remain alert and immediately report suspicious activity and potential behavioral indicators of pre-operational terrorism planning activities, to include suspicious acquisition of materials and construction of explosive devices. Some of these behavioral indicators may be constitutionally protected activities and should be supported by additional facts to justify increased suspicions. No single behavioral indicator should be the sole basis for law enforcement action. The totality of behavioral indicators and other relevant circumstances should be evaluated when considering any law enforcement response or action.

[‡] (U//FOUO) DHS defines domestic terrorism as any act of violence that is dangerous to human life or potentially destructive of critical infrastructure or key resources committed by a group or individual based and operating entirely within the United States or its territories without direction or inspiration from a foreign terrorist group. The act is a violation of the criminal laws of the United States or of any state or other subdivision of the United States and appears to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by mass destruction, assassination, or kidnapping. A domestic terrorist differs from a homegrown violent extremist in that the former is not inspired by and does not take direction from a foreign terrorist group or other foreign actor.

(U//FOUO) We encourage facility owners and operators, security personnel, and first responders to remain vigilant and report suspicious activities and behaviors that may indicate a potential attack.

- » (U//FOUO) Persons in crowded areas wearing clothing that is unusually bulky or atypical for the season, possibly to conceal suicide explosives or weapons.
- » (U//FOUO) Persons asking about theater security screening and evacuation procedures without a reasonable explanation.
- » (U//FOUO) Packages—possibly containing explosives—left unattended in open areas or hidden in trash receptacles, lockers, or similar containers.
- » (U//FOUO) Vehicles with sagging suspension or illegally parked near a theater or where crowds gather prior to or following performances and events.
- » (U//FOUO) Vehicles with modifications made, such as hidden compartments or seating removed, to conceal or make room for explosives.

(U//FOUO) Protective Measures

(U//FOUO) The following protective measures are designed to prevent and/or mitigate vulnerabilities to attack. State and local law enforcement and other security personnel are encouraged to consider the following general, concealed/hand-emplaced, and vehicle-borne IED protective measures.

(U//FOUO) General IED Protective Measures

- » (U//FOUO) Establish comprehensive security and emergency response plans that include interaction and integration with local law enforcement and public safety agencies.
- » (U//FOUO) Test communications equipment with emergency responders.
- » (U//FOUO) Develop mass evacuation procedures, to include considerations for special needs populations (e.g., persons with physical disabilities, non-English speakers).
- » (U//FOUO) Ensure personnel receive training/briefings on indicators of surveillance and reconnaissance (e.g., photography of entrances or access points, questions related to security measures, presence of individuals during off-duty/non-work hours).
- » (U//FOUO) Ensure personnel receive training/briefings on IED/VBIED awareness/recognition and suspicious activity reporting procedures.
- » (U//FOUO) Always be aware of the possibility of secondary devices, particularly along designated evacuation routes or sites.
- » (U//FOUO) If a suspicious item or vehicle is located, evacuate the immediate area (refer to DHS-FBI Bomb Threat Standoff Card for recommended evacuation distances).

~~(U//FOUO)~~ Concealed or Hand-Emplaced IED Protective Measures

- » ~~(U//FOUO)~~ Control access to your facility.
- » ~~(U//FOUO)~~ Where possible, establish access control and personnel/baggage inspection checkpoints.
- » ~~(U//FOUO)~~ Remove objects from facilities which could conceal IEDs (e.g., trash containers, crates).
- » ~~(U//FOUO)~~ Consider all unattended baggage or items in a high traffic, unusual, or otherwise strategic location as hazardous.

~~(U//FOUO)~~ VBIED Protective Measures

- » ~~(U//FOUO)~~ Provide VBIED indicators (e.g., sagging suspension, illegally parked vehicles) to officers and staff.
- » ~~(U//FOUO)~~ Install vehicle barriers and establish vehicle marshaling locations to ensure adequate standoff distances.
- » ~~(U//FOUO)~~ Identify locations for conducting vehicle searches and provide vehicle inspection procedures to appropriate staff.
- » ~~(U//FOUO)~~ Conduct searches of suspicious vehicles or vehicles requiring entrance into a secure zone using explosives detection canine teams, when available.
- » ~~(U//FOUO)~~ Use remote parking and shuttle services to keep vehicles away from facilities or mass gatherings.
- » ~~(U//FOUO)~~ Tow illegally parked vehicles.

~~(U//FOUO)~~ Additional counter-IED/VBIED protective measures, resources, and tools from the DHS Office for Bombing Prevention can be found on TRIPwire ~~(b)(7)(e)~~ dhs.gov.

~~(U)~~ Report 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 <http://nsi.ncirc.gov/resources.aspx>.

~~(U)~~ Tracked by: HSEC-1.1, HSEC-1.5, HSEC-1.6, HSEC-1.10, HSEC-8.1, HSEC-8.3, HSEC-8.8

¹ (U); New York Cinema Cancels "The Interview" Premiere After Hackers' Threat;

<http://money.cnn.com/2014/12/16/technology/security/sony-hackers/index.html>; accessed 17 December 2014.

² (U); Sony Drops 'The Interview' Following Terrorist Threats; <http://www.nytimes.com/2014/12/18/business/sony-the-interview-threats.html>; accessed 18 December 2014.

³ (U); iSight Partners; Hacktivism Intel-1311691; "#GOP May Continue Releasing Data Despite 'The Interview' Cancellation"; 17 December 2014

⁴ (U); RiskBased Security; "A Breakdown and Analysis of the December, 2014 Sony Hack";

<https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/>; accessed 18 December 2014.