Office of Intelligence and Analysis

NOTE

(U//FOUO) Use of Small Arms: Examining Lone Shooters and Small-Unit Tactics

3 September 2010

(U//FOUO) Prepared by the DHS/I&A Homeland Counterterrorism Division, Terrorist Targets and Tactics Branch and the FBI Directorate of Intelligence/Counterterrorism Analysis Section. Coordinated with the National Counterterrorism Center/Directorate of Intelligence. The Interagency Threat Assessment and Coordination Group reviewed this product from the perspective of our nonfederal partners.

(U) Scope

(U//FOUO) This Note was prepared to support federal, state, and local government agencies and authorities, and other entities in developing and prioritizing protective and support measures relating to an existing or emerging threat to homeland security.

(U) Key Findings

(U//FOUO) DHS and the FBI assess that, given the current evolving and diversifying Homeland threat environment, recent incidents involving small arms operations here in the United States and abroad demonstrate the need for continued vigilance and awareness. Small arms operations could be employed through a range of tactics from a lone shooter—as illustrated by the 1 September incident in Silver Spring, Maryland at the headquarters of a U.S. cable network—to a small-unit assault operation.

(U//FOUO) DHS and the FBI assess that the scale and complexity of any such type attack are dependent on a variety of factors, to include the sophistication and training of the attackers, the parameters of their targets, and the local security environment.

IA-0461-10

(U//FOUO) Homeland Threat Posed by Lone Shooters

(U//FOUO) Recent lone shooter attacks in the United States illustrate the effectiveness of the small arms tactic and the need for maintaining vigilance and awareness of the possibility that individuals may use this attack method in furtherance of a political or social agenda. The high degree of operational security lone attackers generally observe complicates the ability of law enforcement and homeland security authorities to detect their plans in advance of the attacks.

— (U) On 1 September 2010, a U.S. person armed with a replica weapon and starter pistol—subsequently determined to only fire blanks—took hostages at the Silver Spring, Maryland headquarters building of a U.S. cable network and threatened to open fire. The standoff ended when the U.S. person was killed by law enforcement.

— (U//FOUO) On 5 November 2009, a U.S. Army Officer allegedly opened fire at the Fort Hood military installation's Readiness Center in Killeen, Texas, killing 12 and wounding at least 31. He was armed with two pistols, according to Army officials.*

— (U) On 10 June 2009, an 88 year-old male with white supremacist sympathies opened fire with a rifle at the U.S. Holocaust Museum in Washington, D.C., killing a security guard. The attacker, who was wounded by return fire and arrested on the scene, died on 6 January 2010 prior to the conclusion of his trial.

(U//FOUO) Incidents involving lone gunmen in the United States demonstrate the potential danger, lethality, and effectiveness of an unrehearsed small arms attack by a single individual with little or no training, and underscore the potentially higher consequences of an assault attack involving multiple operatives.

(U//FOUO) Small-Unit Tactics Overseas

(U//FOUO) Terrorist and violent insurgent groups overseas—operating in nations battling violent civil unrest—have long favored small-unit assault tactics, in which small teams of operatives storm a target using small arms to defeat security. The frequency of these attacks almost certainly stems from perceptions of their effectiveness, the prevalence of small arms instruction at terrorist and militant training camps, and the widespread availability of assault weapons in conflict regions. In July and August 2010, three of these attacks occurred in locations as disparate as Somalia, Russia's North Caucasus, and Afghanistan.

— (U) On 24 August 2010, at least two members of the Somalia-based terrorist organization al-Shabaab—a gunman and a suicide bomber—stormed the Muna Hotel in Mogadishu disguised as police officers, killing at least 33 people, including four members of the Somali Parliament.

* (U) MSNBC, "Army Adds Charge Against Rampage Suspect," 2 December 2009, http://www.msnbc.msn.com/id/34243082/ns/us_news-tragedy_at_fort_hood/, accessed 3 September 2010.

— (U//FOUO) On 21 July 2010, six attackers—probably insurgents from the North Caucasus—used small arms to kill two security guards and gain entry to a Russian hydroelectric plant. Once inside the facility, they detonated improvised explosive devices (IEDs), destroying two of the plant's three hydropower generators.

— (U) In an early July 2010 attack on an international development organization's compound in Kabul, Afghanistan, insurgents breached the front gate with a vehicle-borne improvised explosive device (VBIED). Five operatives armed with assault rifles and small IEDs entered and attacked the facility, killing five and injuring more than 20 people.

(U) The 2008 Mumbai Attack

(U//FOUO) In November 2008, 10 operatives divided into small teams, who received specialized training from the Pakistan-based terrorist organization Lashkar-e-Tayyiba, infiltrated India by boat. The terrorists used small arms, hand grenades, and IEDs to attack multiple lightly secured facilities, including hotels and a rail station in Mumbai. The teams that stormed the Taj Mahal and Oberoi Trident hotels took hostages, leading to a multi-day standoff with police. Ultimately, 166 people and all but one of the attackers were killed. The Mumbai operation stands as the most well-known example of a small-unit assault operation.

(U//FOUO) Homeland Threat Posed by Small-Unit Tactics

(U//FOUO) Given recent events and success of small arms tactics and the evolving, diversified threat faced by the United States from al-Qa'ida and those inspired by its ideology to commit acts of violence, DHS and FBI assess that transnational terrorist groups and homegrown violent extremists[†]—whether trained overseas or in the United States—could employ small-unit assault tactics in the U.S.

(U//FOUO) Although DHS and FBI have no information indicating transnational terrorists have attempted to execute a small-unit assault operation in the Homeland, we note that homegrown violent extremists, such as the six individuals found guilty in 2008 of plotting and training to use small arms to launch an assault on Fort Dix, New Jersey, have considered small arms-based assault tactics.

(U//FOUO) DHS and the FBI assess that the scale and complexity of any such type attack are dependent on a variety of factors, to include the sophistication and training of the attackers, the parameters of their targets, and the local security environment.

[†] (U//FOUO) For the purposes of this document, DHS and the FBI define a homegrown violent extremist as a United States-based individual who is inspired to commit acts of violence in furtherance of objectives promoted by a foreign terrorist organization, but who acts without direction from the foreign terrorist organization.

(U//FOUO) Failure of Homeland IED Attacks May Increase Attractiveness of Small-Unit Assault Tactics

(U//FOUO) Recent failed bombing attacks targeting the Homeland—a 25 December 2009 attempt by an alleged al-Qa'ida in the Arabian Peninsula operative to detonate an IED on a flight from the Netherlands to Detroit, and an unsuccessful VBIED attack in Times Square by a self-confessed Tehrik-e Taliban Pakistan operative—illustrate the complexity that terrorist organizations face in training and deploying operatives to the Homeland to carry out attacks using explosives.

(U//FOUO) While terrorist organizations almost certainly will continue to attempt future Homeland attacks using IEDs, it is also possible that operational planners will recognize that small arms attacks do not require mastery of IED construction or risk the failure of a complex bomb design.

(U//FOUO) Importance of Suspicious Activity Reporting

(U//FOUO) We face an increased challenge in detecting terrorist plots underway by individuals or small groups acting quickly and independently or with only tenuous ties to foreign handlers. State, local, tribal and private sector partners play a critical role in identifying suspicious activities and raising the awareness of federal counterterrorism officials.

— (U//FOUO) The men plotting to assault Fort Dix in 2006 were discovered only after an attentive store clerk alerted authorities to a videotape of training activities the group attempted to have copied. It is unlikely this type of information would come to the attention of federal officials unless reported by private sector and state, local, and tribal partners through suspicious activity reporting channels.

(U//FOUO) Recommended Protective Measures

(U//FOUO) Private sector security and law enforcement agencies can use protective measures to help disrupt or mitigate a terrorist attack in multiple phases—during surveillance, target selection, target infiltration, and engagement with security forces.

(U) Surveillance

— (U//FOUO) Train staff to be aware of unusual events or activities, such as individuals loitering for no apparent reason, sketching, pace counting.

— (U//FOUO) Install and monitor CCTV cameras covering multiple angles and access points.

— (U//FOUO) When possible, establish random security patrols to disrupt potential surveillance efforts.

(U) Target Selection

— (U//FOUO) Establish security at facility access points and potential approach routes.

— (U//FOUO) Know a facility's vendors and, if possible, randomly alter delivery entrances to avoid developing discernable patterns.

— (U//FOUO) Avoid widely distributing site blueprints or schematics and ensure those documents are kept secured.

(U) Target Infiltration

— (U//FOUO) Establish an outer perimeter at target sites to deny access or intercept potential assailants, and ensure security personnel and security measures are in place at all access points.

— (U//FOUO) Establish a credentialing process for facilities.

— (U//FOUO) Conduct background checks on all employees.

(U) Engagement with Security Forces

— (U//FOUO) Encourage local law enforcement to meet with key facility staff to assist in the development and familiarization of emergency evacuation and lock down procedures.

— (U//FOUO) Conduct security sweeps for explosive devices and increase security measures in zones that could be compromised.

— (U//FOUO) Local, state, and federal law enforcement entities should routinely conduct joint training and communication coordination exercises to allow for effective deployment of multiple units in a crisis.

(U) Reporting Notice:

(U) DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the nearest State and Local Fusion Center and to the local FBI Joint Terrorism Task Force. State and Local Fusion Center contact information can be found online at http://www.dhs.gov/files/resources/editorial_0306.shtm. The FBI regional telephone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm and the DHS National Operations Center (NOC) can be reached by telephone at 202-282-9685 or by e-mail at NOC.Fusion@dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the NOC. The NICC can be reached by telephone at 202-282-9201 or by e-mail at NICC@dhs.gov. When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) DHS/I&A would like to invite you to participate in a brief customer feedback survey regarding this product. Your feedback is extremely important to our efforts to improve the quality and impact of our products on your mission. Please click below to access the form and then follow a few simple steps to complete and submit your response. Thank you.

(U) **Tracked by:** HSEC-01-00000-ST-2009, HSEC-01-02000-ST-2009, HSEC-03-00000-ST-2009

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Homeland Security

Office of Intelligence and Analysis

I&A Customer Survey

Product Title: (U//FOUO) Use of Small Arms: Examining Lone Shooters and Small-Unit Tactics

1. Please select the partner type that best describes your organization. Select One

2. How did you use this product in support of your mission?

- ☐ Integrated into one of my own organization's finished information or intelligence products
- ☐ Shared contents with federal or DHS component partners
  - If so, which partners?
- ☐ Shared contents with state and local partners
  - If so, which partners?
- ☐ Shared contents with private sector partners
  - If so, which partners?
- ☐ Other (please specify)

3. Please rank this product's relevance to your mission. ***(Please portion mark comments.)***

- ◯ Critical
- ◯ Very important
- ◯ Somewhat important
- ◯ Not important
- ◯ N/A

4. How could this product or service be improved to increase its value to your mission? ***(Please portion mark comments.)***

5. Was this product provided to you in response to a specific request to DHS I&A? ◯ Yes ◯ No

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

	Very Satisfied	Somewhat Satisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Timeliness of product or support	◯	◯	◯	◯	◯
Responsiveness to your intelligence needs	◯	◯	◯	◯	◯
If you answered yes to question 5, please rate your satisfaction with DHS I&A's communication during the processing of your request	◯	◯	◯	◯	◯

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

Your Name and Position

Your Organization

Your Contact Number or Email

Submit Feedback

Notice to DHS I&A Customers

CLASSIFICATION: **UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Paperwork Reduction Act Compliance Statement

Legal Significance of Office of Management and Budget Control Number: Your response to this feedback request is completely voluntary. The Paperwork Reduction Act requires that the Department of Homeland Security notify respondents that no person is required to respond to the collection of information unless it displays a currently valid OMB control number.

Privacy Act Statement: DHS's Use of Your Information

Principal Purposes: When you provide feedback on an Intelligence and Analysis (I&A) intelligence product, DHS collects your name, position, contact information, and the organization you are representing. We use this information to contact you if we have additional questions about the feedback and to identify trends, if any, in the feedback that you and your organization provide.

Routine Uses and Sharing: In general, DHS will not use this information for any purpose other than the Principal Purposes, and will not share this information within or outside the agency. Aggregate feedback data may be shared within and outside DHS but without including the contact information. In certain circumstances, DHS may share this information on a case-by-case basis as required by law or necessary for a specific purpose, as described in the DHS Mailing and Other Lists System of Records Notice, DHS/ALL-002 (73 FR 71659).

DHS Authority to Collect This Information: DHS requests that you voluntarily submit this information under its following authorities: 5 U.S.C. 301; the Federal Records Act, 44 U.S.C. 3101.

Effects of Not Providing Information: You may opt not to provide the requested information or to provide only some of the information DHS requests. However, if you choose to provide any feedback information, you must provide a classification level as requested on this form. If you opt not to provide some or all of the requested information, DHS will not be able to contact you to fully address your feedback and any additional information needs.

Accessing and Correcting Information: If you need to access or correct the information collected on this form, you should send an email to *ia.feedback@dhs.gov*. You may also direct your request in writing to the appropriate FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under "contacts." Additional instructions are available at that website and in the DHS/ALL-002 System of Records Notice, referenced above.

Return to Form