UNCLASSIFIED//FOR OFFICIAL USE ONLY

Office of Intelligence and Analysis
Homeland Security

Homeland Security Assessment

(U//FOUO) Preventing Attacks by Animal Rights Extremists and Eco-Terrorists: Fundamentals of Corporate Security

13 April 2006

(U) Attention: Federal Departments and Agencies, State Homeland Security Advisors, Security Managers, State and Local Law Enforcement, Local and Tribal governments, Information Sharing and Analysis Centers, and International Partners

(U) Distribution Notice: Requests for further dissemination must be approved by the DHS/Office of Intelligence & Analysis (I&A) - Production Management at IA.PM@hq.dhs.gov.

(U) Scope

(U//FOUO) Attacks against corporations by animal rights extremists and eco-terrorists are costly to the targeted company and, over time, can undermine confidence in the economy. Within this context, the goal of eco-terrorists and animal rights extremists is to disrupt and ultimately shut down corporations that are perceived to violate the ideology of the terrorist organizations. Although we have no specific, credible information at this time suggesting animal rights extremists and eco-terrorists are planning to target known corporations, we encourage private sector owners and operators to remain vigilant, report suspicious activity, and continue to enhance protective measures.

*(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.*

(U) This product contains U.S. 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 USPER information has been minimized. Should you require the minimized USPER information, please contact the DHS/I&A Production Management Division at IA.PM@hq.dhs.gov.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U) Key Findings

(U//FOUO) Extremists use a variety of tactics to intimidate, impede, and disrupt corporations and corporate activities that are perceived as threats to the environment and animal rights.

- **(U//FOUO) Extremists are known to threaten and target staff and family members of offending corporations as part of a persistent campaign of domestic terrorism.**
- **(U//FOUO) Extremists infiltrate corporations, hack into their computer systems, and compromise sensitive corporate information.**
- **(U//FOUO) Protecting proprietary and personal information of corporate staff members, to include rosters, phone numbers, account information, and e-mail accounts, is essential to reducing the risk of domestic extremist attacks.**

(U) Simple but Effective Tactics

(U//FOUO) A primary objective of animal rights and environmental extremists is to attack corporations that are perceived to operate contrary to the extremists' ideology. They use non-invasive tactics such as organizing protests and flyer distribution. They also seek to raise the cost of doing business by low-technology acts of vandalism such as graffiti, sending continuous faxes in order to drain the ink supply in company fax machines, inundating computers with e-mails causing them to crash, and tying up company phone lines to prevent legitimate calls.

(U//FOUO) Other tactics they use against companies are more invasive and directed at staff and their families. These include verbal harassment; direct threats; releasing personal information over the Internet such as an employee's home address, phone number, or credit card number; videotaping an employee's family activities; visiting employees' homes; and vandalizing personal property.

(U//FOUO) Extremists may obtain critical information about a targeted company by accessing sensitive information stored on company computers. They may obtain such access through their employment with the company, burglary, computer hacking, or other means. Once access is obtained, extremists can retrieve sensitive company information, identify company affiliates, and steal business accounts and credit card numbers. Extremists use this information to disclose corporate secrets, disrupt partnerships, jeopardize the company's finances, and expose activities that may reflect negatively on the company or their personnel.

(U) SHAC: A Case Study in Extremist Methodology

(U//FOUO) Stop Huntingdon Animal Cruelty USDEK (SHAC) is an extremist organization that aggressively attacks the corporate sector in defense of animal rights. SHAC's ideology parallels that of the Animal Liberation Front (ALF). The two groups also share guiding principles that animals deserve moral rights and considerations. SHAC's primary target—Huntingdon Life Sciences (HLS)—is one of the world's largest research organizations that conducts product testing on animals. Although headquartered in the United Kingdom, HLS has facilities in the United States. SHAC's goal is to shut down HLS, using intrusive tactics against HLS facilities, its management, employees, shareholders, clients, and others who are loosely affiliated with the company. SHAC's Web site encourages supporters to invade offices, post personal information on the Internet, smash windows, use fire bombs, and, if necessary, physically abuse people.

(U//FOUO) According to the FBI, animal rights extremists were responsible for several corporate attacks in 2005.

- (U//FOUO) Extremists in April crashed a U.S. company's computer server by inundating it with e-mail and creating an estimated damage of $1.25 million.
- (U//FOUO) SHAC's Web site claimed that animal rights extremists in October used an auto-dialer to overwhelm the telephone service of a Delaware investment firm, which prevented customers from calling the firm and resulted in lost sales. The extremist actions stopped when the targeted company agreed to sell all of its HLS stock.
- (U//FOUO) Also in October, SHAC's Web site claimed responsibility for an e-mail harassment campaign against a Wisconsin firm, demanding that the firm sell its shares of HLS stock. The firm agreed to SHAC's demand and lost an estimated $1.4 million from the sale.
- (U//FOUO) SHAC-affiliated extremists in December conducted an attack against a California investment firm by jamming its phone lines with repeated calls to prevent it from doing business with potential customers and incurring a loss in sales.

(U) Securing Corporate Information

(U//FOUO) Combating animal rights and environmental extremist attacks against the corporate sector parallels the strategy used in fighting corporate espionage. Similar to individuals conducting corporate espionage, animal rights extremists and eco-terrorists prefer to infiltrate a business and learn about its personnel and the details of company operations. Access to company information is powerful, and extremists use this

knowledge to destroy or disrupt operations. A corporation becomes a soft target and susceptible to possible infiltration by extremists when corporate security is neglected.

(U) Suggested Protective Measures

(U//FOUO) The same methodology and countermeasures used to detect and disrupt corporate espionage could also be used to detect and disrupt possible extremist infiltration. A strong internal corporate security program may prevent extremists from conducting a terrorist attack that would disrupt operations, drain company finances, and harm employees, their associates, and family members.

(U//FOUO) Protective measures are recommended to shield company assets, safeguard sensitive information, and prevent a domestic extremist attack. Listed below are some practical strategies that can be used to counter a variety of domestic extremist attacks against a business.

(U//FOUO) Guidelines for Corporate Security:

- (U//FOUO) Verify the legitimate business needs of all approaching vehicles and personnel as well as check multiple forms of valid identification for each facility visitor.
- (U//FOUO) Clear all service personnel in advance and maintain a roster of cleared personnel, with any/all substitutions made in advance.
- (U//FOUO) Keep and maintain comprehensive records of all official identification cards, badges, and decals distributed, document any anomalies, and cancel access to items lost or stolen.
- (U//FOUO) Advise employees to challenge visitors or question unfamiliar individuals to ensure they have a need to be in a specific area. Some corporate facilities may require company badge and photo identification.
    - (U//FOUO) Service personnel (for example, janitors, contracted cleaners, and vendors), during work and after hours, should always be escorted. They are often overlooked in security procedures because they blend in and are easily accepted in the work space.
- (U//FOUO) Substantiate and verify all prospective employees' work experience and references. Aggressively resolve any questionable information on resumes and/or application forms.

— (U//FOUO) Make computer security a high priority.

  — (U//FOUO) If possible, encrypt all outgoing electronic communication and attachments.

  — (U//FOUO) Implement a process to periodically change users' computer passwords.

  — (U//FOUO) Install computer network firewalls and continuously test corporate computer systems to ensure hackers do not penetrate these systems.

— (U//FOUO) Install locks on all doors, filing cabinets, and overhead storage areas. Similarly, passwords should always be used to access computer systems.

— (U//FOUO) Coordinate, test, and maintain emergency response plans that include local, state, and federal governments.

— (U//FOUO) Clearly articulate and enforce company security policies and practices. Provide periodic security awareness training to personnel at all levels. No employee is immune to possible elicitation or infiltration of a persistent adversary.

(U//FOUO) Guidelines for Company Employees:

— (U//FOUO) Protect corporate rosters to prevent extremists from acquiring personal information such as organization structure, employee names, positions, phone numbers, e-mail addresses, and home addresses.

— (U//FOUO) Never discuss proprietary information with anyone without a need to know. Suspicious inquiries about a company or its personnel should be reported immediately. At first glance, potential adversaries may ask questions that appear innocent, but gradually become more detailed.

— (U//FOUO) Protect itineraries, vacation dates, locations, and reservations when traveling; targeting can occur at any time and in areas outside the work place and residence.

— (U//FOUO) Always shred documents rather than throwing them in the trash. Seemingly innocuous information can be used to answer questions or fill information gaps that could later be used to target a company or employee.

— (U//FOUO) Be cognizant that wireless transmissions of phone and computer communications are susceptible to intercept and exploitation if they are not encrypted.

(U) Reporting Notice:

(U) DHS encourages recipients of this document to report information concerning suspicious or criminal activity to the local FBI Joint Terrorism Task Force (JTTF) and the Homeland Security Operations Center (HSOC). The FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm, and the HSOC can be reached by telephone at 202-282-8101 or by e-mail at HSOC.Common@dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the HSOC. The NICC can be reached by telephone at 202-282-9201 or by e-mail at NICC@dhs.gov. 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, when this information is available, and a designated point of contact.

(U) For comments or questions related to the content or dissemination of this document, please contact the DHS/I&A Production Management Division at IA.PM@hq.dhs.gov.

(U) Tracked by:

(U) TERR 060000-01-05
(U) HSEC 030000-01-05
(U) HSEC 040000-01-05
(U) CRIM 040000-01-05
(U) ENVR 070000-01-05