EYES ON THE GROUND

Right of way professionals are well positioned to protect information

BY BETH MINEAR, ESQ.

Around the globe, homeland security concerns are at the forefront of most considerations in nearly every business. Gone are the days when we can observe a terrorist threat or incident through the comfortable distance of a television or newspaper.

The reality is, threats can happen anywhere and they are ever-present. In response, the United States Department of Homeland Security (DHS) trademarked a campaign urging citizens, "If you see something, say something." Information is disseminated through public service announcements, a smart-device app, at airports and on the DHS website, as well as other messaging venues.

Given the sheer physical coverage by the right of way sector, there is no other single industry better positioned to serve as eyes on the ground. Working on projects that span from rural countryside to crowded cities across the U.S., it is likely that our professionals will be in a position to observe something out of the ordinary, if it occurs. Successful agents are characteristically skilled in observation and analysis. By recognizing threats to the public and our critical infrastructure, and learning how to become part of the active reporting framework already in place, we can aid law enforcement in early threat identification and response.

Where Threats Originate

Some threats come from hackers and the seemingly endless number of viruses bombarding the computer networks of banks, utilities and government entities, where sensitive or private information may be compromised or stolen. The Wikileaks saga exposed the government's understanding that there are also hard targets in the United States vulnerable to attack, especially pipelines. In response, the Transportation Security Administration is actively monitoring for potential attacks on the pipeline sector.

According to the Department of Homeland Security, suspicious activity can include both common and unusual items—from packages to vehicles—that appear to be out of place. However, this also includes individuals who take an unusual interest in a building, asset or landmark, lingering beyond mere tourism or curiosity, or those who ask an inordinate amount of detailed questions about a facility, area or process.

The reality is that it has become far more likely that homegrown individuals will perpetrate acts of terror on our soil. Many attempts have already occurred against the energy sector, including improvised explosive devices on pipelines in Oklahoma and well pads in Pennsylvania. Whether landowners, environmentalists, anti-fracking activists or otherwise, homegrown terror has become a reality, and identifying the perpetrators is now one of our biggest challenges.

Cities across the U.S. have implemented the Department of Homeland Security's public service campaign that urges citizens to report any suspicious activity.

Critical Infrastructure Information

On a typical project, right of way professionals are privy to proprietary maps, engineering plans and detailed drawings that are critical to identifying parcels and evaluating project routes. From a homeland security perspective, this data might be considered critical infrastructure information. Whether it's plans for high-speed rail, replacement of electric transmission towers or power generation, natural gas, liquefied natural gas or petroleum pipelines or for state and federal highways, our industry has access to crucial information on the country's hard targets.

For both regulated and unregulated entities, submitting engineering or construction drawings to state or federal authorities are often required for both environmental and non-environmental permitting. In order to protect critical infrastructure information under the entity's Freedom of Information Act (FOIA) equivalent, our clients should have a clear understanding of how to submit this information and what mechanisms must be in place, such as a cover letter with specific reservations.

Many companies require a specific stamp to identify maps and documents to governmental custodians so that they can legally protect information and keep it from the public. Specific understanding of the Critical Infrastructure Information Act of 2002 (Homeland Security Act of 2002, Public Law 107-296) is helpful, and prudent right of way companies should understand and be able to converse with clients about its protections. The Homeland Security Act designates some of the nation's assets as critical infrastructure and establishes a program for the protection of such information from public dissemination, whether through FOIA or otherwise.

Regulatory Oversight

There are specific protections for submission of large-scale project footprints, engineering and/or construction drawings of projects for which the Federal Regulatory Commission (FERC) is the regulator. After September 2001, FERC acted decisively by flexing its federal muscle. One month following the attacks, FERC issued PL-02-1-000,

a regulation by which information deemed critical energy infrastructure information (CEII) would be removed, and in the future, such information would not be posted in public. Under FERC regulations, CEII is defined as "specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure." Subsequent issuances have further defined and modified the CEII regulations, including the expectation that landowners can see scrubbed maps for infrastructure routes potentially crossing their properties, but with proper handling and submission, the strength of FERC's original response has largely withstood onslaught by those seeking to weaken it.

In 2013, attackers severed underground lines before shooting at a substation's transformers in California, causing more than $15 million in damage.

Specifically for the electric transmission sector, in January 2008, FERC issued Order No. 706 approving eight Critical Infrastructure Reliability Standards (CIP-002-1 through CIP-009-1), amended by Version 2 of the standards, which became enforceable in April 2010. The CIP standards require certain users, owners and operators of the bulk-power system to comply with specific standards to safeguard critical cyber assets and protect real-time power generation, transmission and distribution infrastructure from cyber intrusions and exploits. This means that electric companies and their contractors must have specific cyber safeguards in place to protect critical infrastructure information from cyber capture.

Proceed with Caution

Whether an administrative professional who is responsible for filing detailed plans to accompany permits, or the project manager who oversees training and process management standards on behalf of a client, each right of way practitioner should understand how critical their role can be to our nation's security. At project kick-off meetings, everyone should be briefed about the need to shield critical infrastructure information and how to protect it. The agent's employer will likely be asked to sign confidentiality and/or non-disclosure agreements regarding the same. Though candor is one of the hallmarks of a good right of way company and team, the additional understanding of how critically sensitive some information can be will certainly differentiate one company from another.

So in the event that a right of way agent sees something out of the ordinary, no matter how innocuous, whom should they tell? The Department of Homeland Security has representatives in local law enforcement and designated state offices nationwide. Before you start work for a new client or in a new jurisdiction, coordinate with your employer and client company so that you have the number designated for your locale to initiate a suspicious activity report. In making the report, be prepared to detail who or what you saw, when you saw it, where it occurred, why you were suspicious, as well as your contact information.

With our vast numbers and wealth of geographic outreach and expertise, right of way professionals can become important contributors to our nation's interests. Whether as eyes and ears on the ground or as guardians of the information about our critical infrastructure, we have a duty to know, understand and demonstrate the discipline and communication skills necessary to protect our client's assets and the public as a whole. If you see something, say something. ✪

Contract Land Staff is one of ten charter member companies of the Right of Way Consultants Council, which supports the best practices recommended in this article. For more information on membership or resources, please visit www.rowcouncil.org.

Beth is Vice President and Project Management Strategist for Contract Land Staff, and has expertise in capital infrastructure improvement projects, public financing and eminent domain matters.