Session No. 630

An Effective Facility Security Plan

Michael R. Roop
Director Safety and Security
Environmental Resources Management SW
Houston, Texas

OK, you have taken the correct initial steps. You have determined that your facility does indeed contain critical assets that need to be protected. Further, you have performed a threat assessment looking at both internal and external threats to your facility. You also have completed a security vulnerability assessment to determine how susceptible your strengths and weaknesses make you for an attack. You recognize that you may be a low risk for an attack – but a risk all the same. You are in the process of "fixing" the weak areas that the vulnerability assessment exposed to you. Now, you must also prepare a thorough security plan that meets the Department of Homeland Security (DHS) requirements and, more importantly, gives you a sense that your facility is as prepared as it can be.

The focus of this article is simply that. What does DHS expect and how can you meet those expectations given a limited budget, manpower allotment, and time. And remember, your goal should go beyond regulatory compliance to include exploiting every opportunity to be better prepared.

DHS Performance Based Requirements

DHS has set a litany of performance standards that facilities must meet. Note that there is a difference in prescriptive laws (think, "thou shalt not exceed the posted speed limit") versus performance requirements which are objective based (think, "get to your destination by whatever route you want to take"). So, the idea here is to find the best, most efficient route for your facility recognizing that different facilities may well find different "best" routes to their objective.

Security Plan Objectives:

1. Deter – fill the criminals' path with difficult and frustrating obstacles
2. Detect – early discovery of the criminals' intent
3. Delay – distract, frustrate, and slow the criminals' path to their objective
4. Respond – facility personnel, security personnel, law enforcement, fire department, etc.

All of the objectives must be combined into a cohesive plan working one with the other. A weakness in any of the objectives can mean a successful, catastrophic criminal attack on your facility affecting your property, people, the community, and ultimately, the nation and the world. Remember that the terrorists' objective is to create a lasting fear of death and destruction in order to advance the terrorists' political/social/religious agenda.

The DHS list of protective measures listed below in *Italics* is extensive. Most of the DHS measures are intuitive, but the author will add clarifying comments and suggestions to further the readers understanding.

(1) *Restrict Area Perimeter. Secure and monitor the perimeter of the facility.*

Obviously, fences, gates, and other barriers (natural and man-made) come to mind when we think of access control. Vehicles also make good barriers as do security personnel manning a post. Make sure that posted signage is obvious and its message clear – unauthorized personnel are prohibited.

The monitoring of the perimeter can be challenging. Closed Circuit Television (CCTV) and security posts along the perimeter are recommended. Security guard foot patrols are also desirable, but expensive. One good alternative is inside the fence patrols conducted by facility personnel. A 10 or 15 minute walk is good exercise and should be considered a vital safety support role for employees. More on the employees' role later…

(2) *Secure Site Assets. Secure and monitor restricted areas or potentially critical targets within the facility;*

DHS is referring to tangible and intangible targets (people, information, product, processes, etc.) that need protecting. Again, barriers restricting access and the observation of those areas are called for.

(3) *Screen and Control Access. Control access to the facility and to restricted areas within the facility by screening and/or inspecting individuals and vehicles as they enter, including,*

> *(i) Measures to deter the unauthorized introduction of dangerous substances and devices that may facilitate an attack or actions having serious negative consequences for the population surrounding the facility; and*
>
> *(ii) Measures implementing a regularly updated identification system that checks the identification of facility personnel and other persons seeking access to the facility and that discourages abuse through established disciplinary measures;*

Wouldn't it be cool to have full body X-ray machines that all employees and visitors had to walk through to enter your facility?! Short of that movie version of security, what can your facility do to discourage and hopefully prevent unwelcome people and stuff entering your facility? One option for unwanted people is the new Transportation Workers Identification Card (TWIC) issued by the DHS after a background check. The system uses an electronic reader and is very difficult to forge or counterfeit. Of course, there is a cost, but one that is relatively reasonable. The card has a picture ID as well as fingerprint ID. The TWIC program is simple – no card, no entry without escort. To deter contraband, random searches of vehicles, lunch boxes, and even electronic wand body searches are considered prudent expediencies in today's world. Metal detectors are also a consideration.

Now, that DHS phrase, "*that discourages abuse through established disciplinary measure"* is really sort of silly. Security, like other life safety concerns, must be a ZERO TOLERANCE program! Violating security measures could very well result in wide-spread death and destruction and, thus, demands that policy be strictly adhered to!

(4) Deter, Detect, and Delay. Deter, detect, and delay an attack, creating sufficient time between detection of an attack and the point at which the attack becomes successful, including measures to:

> *(i) Deter vehicles from penetrating the facility perimeter, gaining unauthorized access to restricted areas or otherwise presenting a hazard to potentially critical targets;*

Problem…how do you facilitate necessary commercial traffic into your facility while preventing criminals from breeching your gates with a truck load of explosives? One recommended solution is staggered barricades requiring extremely slow speeds to negotiate.

> *(ii) Deter attacks through visible, professional, well maintained security measures and systems, including security personnel, detection systems, barriers and barricades, and hardened or reduced value targets;*

A captured document from a European terrorist group summarized the criminal determination quite well. In essence, the document said that if an obstacle is placed in their path, they will go around it. But if the obstacle is too difficult to overcome, they will find another target. The critical lesson here is to harden your facility's target perception. There are so many other easy targets available to criminals that if you make your facility appear to be difficult to defeat, the chances are very good that you will tremendously reduce the risk of attack.

> *(iii) Detect attacks at early stages, through counter surveillance, frustration of opportunity to observe potential targets, surveillance and sensing systems, and barriers and barricades; and*

Monitoring is crucial. And the very best and most pervasive monitoring capability most facilities have, but do not sufficiently utilize, is its people – ALL of its people. A key player in the development of Intel, Andrew Grove, wrote a business book entitled, "*Only the Paranoid Survive"*. Of course, for the most part, he was referring to competitors. Many managers may respond, "Yes, but competitors are REAL threats." Those same managers must recognize that there are also real criminal threats to their facility. As promised earlier in this article, incorporating every employee into your facility security program strengthens that program exponentially. Make security part of your safety program, because it really is! A little paranoia is a very good thing when it comes to protecting your workplace.

> *(iv) Delay an attack for a sufficient period of time so to allow appropriate response through on-site security response, barriers and barricades, hardened targets, and well-coordinated response planning;*

Appropriate response is ultimately law enforcement that can arrest or kill the criminals (admittedly the author's preferred response) and the fire department who can limit the criminals' efficacy.

(5) Shipping, Receipt, and Storage. Secure and monitor the shipping, receipt, and storage of hazardous materials for the facility;

Your DOT security plan should closely dovetail with your facility security plan.

(6) Theft and Diversion. Deter theft or diversion of potentially dangerous chemicals;

Remember that most facilities are not particularly valid targets for the terrorist criminal because of the plant's location, size, lack of a large surrounding population, etc. However, the products inside the facility may make an excellent intermediary for causing tremendous damage.

(7) Sabotage. Deter insider sabotage;

Again, your own people know each other and probably can recognize when something seems amiss. No, this is not a demand to have your folks spy on one another! However, if a fellow employee is acting strangely, it certainly makes sense to keep an eye out if for no other reason than that employee's safety. Does it bear repeating, "A little paranoia is a very good thing when it comes to protecting your workplace"?

(8) Cyber. Deter cyber sabotage, including by preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Process Control Systems (PCS), Industrial Control Systems (ICS), critical business system, and other sensitive computerized systems;

Enough said.

(9) Response. Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders;

Additionally, establish a relationship with the FBI as well as the DHS. Their advice and assistance will be needed if you are confronted with an actual incident or potential problem.

(10) Monitoring. Maintain effective monitoring, communications and warning systems, including,

> *(i) Measures designed to ensure that security systems and equipment are in good working order and inspected, tested, calibrated, and otherwise maintained;*

Like the equipment within your facility that make product, your security equipment must also be on the PM (preventive maintenance) list.

> *(ii) Measures designed to regularly test security systems, note deficiencies, correct for detected deficiencies, and record results so that they are available for inspection by the Department; and*

(iii) Measures to allow the facility to promptly identify and respond to security system and equipment failures or malfunctions;

"Promptly" should be translated to IMMEDIATELY to facilitate your new ZERO TOLERANCE policy.

(11) Training. Ensure proper security training, exercises, and drills of facility personnel;

Bring in outside facilitators for this because you need an outsider's experience and senses to train and test your people. Employees should be trained to and rewarded for questioning everything. Nuances should not be ignored, but investigated. Train employees to be aware of their surroundings and to be skeptical of anything that does not feel, sound, or look right.

(12) Personnel Surety. Perform appropriate background checks on and ensure appropriate credentials for facility personnel, and as appropriate, for unescorted visitors with access to restricted areas or critical assets, including,

(i) Measures designed to verify and validate identity;

(ii) Measures designed to check criminal history;

(iii) Measures designed to verify and validate legal authorization to work; and

(iv) Measures designed to identify people with terrorist ties;

Once again, the TWIC program mentioned above will meet the requirements of this section.

(13) Elevated Threats. Escalate the level of protective measures for periods of elevated threat;

This does not have to be a national or international measuring stick. By working with local and regional law enforcement, a facility can make its own decision to upgrade security.

(14) Specific Threats, Vulnerabilities, or Risks. Address specific threats, vulnerabilities or risks identified by the Assistant Secretary for the particular facility at issue;

(15) Reporting of Significant Security Incidents. Report significant security incidents to the Department and to local law enforcement officials;

So, what does "significant" mean? If an incident or threat can possibly affect the safety of persons beyond your perimeter fence line, it must be considered significant.

(16) Significant Security Incidents and Suspicious Activities.
Identify, investigate, report, and maintain records of significant security incidents and suspicious activities in or near the site;

(17) Officials and Organization. Establish official(s) and an organization responsible for security and for compliance with these standards;

Your organization should consist of an internal roles and responsibilities flow chart that is vetted through management, table top drills, and outside public and private consultancies' input to maximize thoroughness.

(18) Records. Maintain appropriate records; and

As indicated above, your records are subject to review by DHS. As importantly, records help you indentify and rectify problems with your program.

(19) Address any additional performance standards the Assistant Secretary may specify.

Finally, your program should be evergreen. It should be reviewed, tested, and updated as technology, threats, and the world changes. One thing that the Iraq war has taught us is that as we adjust to the terrorists' methods and begin to thwart their criminal activity, they will devise new ways to attack us.

Summary

Devising a good security plan requires you to be thorough. The DHS has given you a clear outline of what it expects by delineating objectives that your program must achieve. The author is convinced that you must recruit all of your employees to take a major role in your security program or it will not accomplish the one objective all us want – preparedness.