Office of Infrastructure Protection

National Protection and Programs Directorate
Department of Homeland Security

2011 Chemical Sector Security Summit

Baltimore, MD

Theft-Diversion and the Chemical Facility Anti-Terrorism Standards (CFATS)

July 6, 2011

Homeland Security

Overview

- The Chemical Facility Anti-Terrorism Standards (CFATS) requires covered facilities to meet Risk Based Performance Standards (RBPS).
- One of the RBPS (#6) deals with the prevention of **Diversion**:

  Deter theft or diversion of potentially dangerous chemicals

- Chemical diversion goes beyond terrorism, and should be of concern to all business operators in the chemical sector. Chemical diversion can include economic crime, narcotics operations, technology diversion, and tax evasion.
- Diversion is a form of misappropriation; however, it is not quite so straightforward. We will examine it in greater detail in this briefing.

What Is Diversion?

- Diversion is a form of misappropriation.
- The key to understanding diversion is recognizing that the crime is the ***acquisition*** of a material that one should not possess. In this regard, diversion is different from theft, and it must be looked at as such.
- Remember that not all chemical diversions are clear criminal acts under the law. Sometimes the diversion of chemicals is part of a larger criminal conspiracy.

Diversion: Beyond the Federal Interest

- Diversion imposes costs on companies in many ways:
  - — It can lead to institutional corruption, becoming a “gateway” crime that extends to employees.
  - — Public opinion can dramatically turn against a company that has failed to prevent a diversion.
  - — Competitiveness and markets can suffer if companies are undercut by their own products.
  - — Companies may become liable for environmental damage if materials are mishandled.
  - — Companies may incur civil exposure if materials harm people or property.
  - — Companies may even incur criminal exposure due to egregious negligence.
  - — In many cases, companies have to cover the cost of diverted materials.

Understanding Diversion

- Diversion is the act of acquiring a product (or service) by means of deception.
- Types of deception vary and do not always include the failure to compensate the targeted company.
- The deceptive process that is used (roughly) defines the type of diversion.
- In all cases, the common factor is that the targeted company causes the diverted goods to be put into motion.

Getting Paid ≠ No Crime

- In some--but not all--diversion schemes, the company that supplies the diverted material may pay for it and not realize a diversion has occurred.
- In many other types of diversion schemes, the victim company will not be paid (or not fully paid) and realize that something is not right. However, this kind of situation will often be attributed to other things, such as bankruptcy due to customer error or misfiled records.
- Getting paid for a material ***does not mean*** the recipient should have the material.

Common Types of Diversion

- Hijacking
- Dummy Company
- Breakout Scheme
- Co-opted Customer
- False Flag
- Pretext Purchase
- Cyber Attack on Business Management System

Major Targets of Diversion

- Diversions where the target company is not paid:
  - — Hijacking
  - — Dummy Company
  - — Breakout Scheme
  - — Cyber Attack on Business Management System
- Typical Targets:
  - — ***Chemicals***
  - — ***Drugs***
  - — Electronic Goods
  - — Construction Materials
  - — Designer Clothes, Shoes, etc.

Major Targets of Diversion (Cont.)

- Diversions where the target company is (or may be) paid:
  - — False Flag
  - — Breakout (Early Stages)
  - — Co-Opted Customer
  - — Pretext Purchase
- Typical Targets:
  - — ***Chemicals***
  - — ***Drugs***
  - — Liquor
  - — Cigarettes

Hijacking

- Hijacking is a type of diversion that relies on deception, force, corruption, or a combination thereof.
  - — Perpetrator entices a company to put the target commodity in motion by submitting an order.
  - — The route, carrier, time of shipment and/or time of delivery is known by the perpetrator, thereby allowing a hijack to be planned.
  - — Actual hijack may be by force, stealth, corruption or coercion.
  - — The perpetrator knows exactly where and when a given commodity is going to be, outside its normal security envelope.
  - — Hijacking has major disadvantages to terrorists, most notably because it might immediately alert security forces that a dangerous material is in the wrong hands.

Dummy Company

- Another very simple diversion:
  - — Perpetrator rents a space, usually for a short amount of time.
  - — Perpetrator may or may not actually establish a company, or may partially establish one (such as getting a Tax ID number and bank account).
  - — Perpetrator will then establish a line of credit with a company, usually through salespersons who are anxious to sign up a new, big customer and may not check proper credentials.
  - — Perpetrator orders materials on credit.
  - — Materials are delivered, and then the materials and the company suddenly disappear.
  - —The disadvantage to this approach for terrorists is that security forces may become aware of the acquisition of materials before they are used.

Breakout

- This is a variation on the Dummy Company diversion:
  - — A real company is acquired, usually on credit.
  - — The company, perhaps an established customer, orders a lot of material on credit.
  - — The perpetrator orders as much materials as his credit allows. He then declares bankruptcy and disappears.
  - — Breakout may not be a desirable approach for terrorists, because it could involve long timelines and possible interest from the courts.
  - — Breakout can be effective in acquiring a complex capability – something involving the acquisition of a number of different types of materials and equipment.

Co-Opted Customer

- A diversion where an existing customer is co-opted by a terrorist group or criminal enterprise. The co-option could be by coercion, infiltration, purchase, bribery, deception, or even ideology.

  —The existing customer begins ordering the materials that terrorists or criminals want.

  — The customer will usually pay for the material ordered.

  — This type of diversion can run for a long time without being detected, especially in a co-opted company that has the cash flow to cover the losses of diverted materials.

  — This is a difficult form of diversion to defend against. From a counterterrorism point of view, it is one of the most dangerous, and is generally detectable ***only*** by the private sector.

False Flag, Type 1

- Type 1: Complete False Flag
  - — Perpetrator calls and represents himself as an established customer with a new delivery address.
  - — Perpetrator places order and company ships materials to the new address.
  - — Facility and materials then disappear.
  - — Same as Dummy Company diversion and uses the name (paperwork, order numbering, etc) as one of the company's actual customers.
  - — In most cases, target company will not be paid and becomes aware of the diversion to report it.

False Flag, Type 2

- Type 2: Partial False Flag
  - — This is a non-violent type of Hijacking diversion.
  - — Perpetrator places order as a legitimate customer with the correct delivery address. When the company delivers the material, the perpetrator steals it.
  - — The Type 2 False Flag is usually so confusing for two victim companies that security forces will ***not*** be notified. Thus, this might be an attractive diversion option for terrorists.
  - —This is a type of diversion that may be used to get materials from a company that has good security and whose customers are not as diligent.

Pretext Purchase

- A very simple and straightforward diversion:
  - — Perpetrator calls company and makes false statements. For example: “I am Dr. Smith, chair of the chemistry Department at the University of Chicago. Please send me 10 kg of RDX for research purposes.”
  - — Company executes transaction.
  - — This is a very safe way for terrorists to acquire materials. It is also very unlikely that a failed attempt will be reported to security forces or that a successful acquisition will come to the attention of security forces.
  - — This was the method employed by the NYPD in operation “Green Cloud.”
  - — This is among the most likely type of diversion a company will face.

Cyber Attack on Business Management System

- This diversion is probably the safest way for a terrorist group to get their hands on things that they shouldn't have. If successful, it is very unlikely to be detected; if it fails, it is very unlikely to be reported.
  - — Perpetrator hacks into the victim's company business management system and orders a shipment to go to a particular address, either one time or on a recurring basis.
  - — Perpetrator may direct the system to spread-load the cost in fraction of cents across a broad range of other customers in an attempt to dilute or erase footprints.
  - — This diversion is very hard to detect in a larger company because it requires fairly sophisticated audit protocol.

DHS Expectations: General

- Facilities have been advised if their Security “Risk Issues” includes a Theft/Diversion concern.
- The Tier-specific RBPSs are not very different:
  - Measures are effective in deterring and reducing the likelihood of theft/diversion.
  - Vigorous measures are ***extremely*** effective in deterring theft/diversion.

DHS Expectations: Specific

- There is a specific set of measures that DHS will be expecting to see, depending on the facility's Tier level. These include:
  - — Know your customer provisions
  - — Monitoring Chemicals of Interest (COI)
  - — Inventory controls
  - — Tamper detection
  - — Cybersecurity
  - — Security incident reporting
  - — Restricted access to COI
  - — Background checks on personnel who have access to materials or the systems that control them
  - — Physical security around COI
  - — Control of vehicles around COI
  - — Inspection of vehicles around COI

Simple Measures

- Restricted access to COI
- Background checks on personnel who have access to materials or the systems that control them
- Physical security around COI
- Control of vehicles around COI
- Inspection of vehicles around COI

Complex Measures

- **Know Your Customer Provisions:** Effective against a broad range of diversion types.
- **Monitoring of COI:** Depending on Tier level, we expect your program to allow law enforcement to prevent the worst outcome.
- **Inventory Controls:** Goes hand-in-hand with monitoring COI.
- **Tamper Detection:** To allow the detection of the loss of part of a load or supply.
- **Cybersecurity:** In most cases, protected and complemented by non-cyber verification.
- **Security Incident Reporting:** Both internal to your company and external to security forces.

Deterring and Preventing Diversion: Knowing

- Know who your customers are in detail
  - — What is their business?
  - — What is their market share?
  - — What are their capacities?
  - — How do they operate?
- Know your industry
  - — How much is too much?
  - — What is the real market?
- Know your product (or raw material)
  - — What else can this stuff be used for?
  - — What else would one need to misuse this material?

Deterring and Preventing Diversion: Watching

- Watch your sales
  - — “Too good to be true” usually is!
- Watch your shipments
  - — Do shipments match expectations?
  - — Do they go where they are supposed to go?
  - — Do they arrive intact?
- Watch your payments and terms
  - — Paying in cash? (Not typical in B2B transactions)
  - — Personal credit card?
  - — Pick up at your place with their pick-up truck?

Deterring and Preventing Diversion: Internal

- Train your personnel
  - — Customer Service Representatives, sales personnel, credit department, accounts receivable, and auditors.
  - —They are part of the program or they are part of the problem!
- Prevent traditional theft
  - — Especially internal — corruption spreads!
- Educate your customer
  - — Make sure the recipient of a dangerous material understands his or her obligations.

Know Your Customer

- What is his business? What is his customer base?
- Where does he do his banking?
- What is his payment pattern? What is his ordering pattern?
- What are his delivery addresses?
- What is his market share?
- What is in his warehouse, right now?
- How did he find you?
- Does he know what he is talking about?
- If you haven’t been to visit, you probably don’t really know him.

References

- Please be sure to read the ***CFATS Risk Based Performance Standards Guidelines***, which is available on www.dhs.gov/chemicalsecurity.
- Another excellent source document on counter-diversion programs is the Drug Enforcement Administration's (DEA) ***Chemical Handler's Manual***, which will soon be available on the DEA and/or its website. Talk to your inspector or local field office for more details.

Homeland Security

For more information visit:
www.dhs/gov/criticalinfrastructure

Lawrence M. Stanton
Senior Technical Advisor
lawrence.stanton@DHS.gov