



Resources Directory for Security Practices in the Transportation of Agricultural and Food Commodities



Resources Directory for Security Practices in the Transportation of Agricultural and Food Commodities

Table of Contents

Introduction	1
Vulnerability & Threat Assessment Tool	3
Security Planning Guide	11
Highway Watch® Program	20
FBI Field Offices	25
FDA Office of Criminal Investigations	29
USDA Office of Inspector General	29

Introduction

This Resources Directory for Security Practices in the Transportation of Agricultural and Food Commodities has been produced by the Agricultural and Food Transporters Conference (AFTC) of the American Trucking Associations.

The directory contains tools for evaluating vulnerability and threat potentials for commercial transporters of agricultural and food commodities, and for developing security plans for these transporters. Additionally, this directory contains contact information for both industry and government entities that report and communicate critical information dealing with terrorists or other threats to the transportation industry.

Transportation companies can voluntarily use the information and tools in this directory to secure their facilities, educate their drivers and other key personnel, and communicate critical information to the appropriate authorities for analysis, coordination, and communication.

The Vulnerability and Threat Assessment Tool (VTA) is a voluntary risk assessment tool designed to meet the basic security evaluation requirements for the agricultural and food transportation sectors of America's trucking industry. Companies can use the VTA to determine security vulnerabilities in their operations and identify measures to protect their facilities, equipment, and personnel from intentional harmful activity.

The Security Planning Guide component of the directory is a tool which can be voluntarily used to apply the information derived from the VTA in the development of a security plan for transportation companies.

For those companies transporting agricultural and food commodities, it is recommended that they also utilize the USDA/AFTC Guide for Security Practices in Transporting Agricultural and Food Commodities.

These tools and contact information can be valuable resources in a company's ongoing efforts to secure its facilities, protect its personnel, and help make America's food supply safe and secure for all our nation's citizens.

Vulnerability & Threat Assessment Tool

Introduction

The Vulnerability and Threat Assessment Tool (VTA) is a voluntary and integral component of the AFTC Resources Directory in Transporting Agricultural and Food Commodities. This risk assessment tool, developed with specific input from the commercial agricultural and food transportation industries, is designed to meet the basic security requirements for the agricultural commodity and food transportation sectors of America's trucking industry. Trucking companies engaged in the transportation of agricultural commodities and food are urged to voluntarily utilize the VTA to determine security vulnerabilities in their operations and to identify security measures to better protect their facilities and equipment from intentional harmful activity.

The U.S. Transportation Security Administration (TSA) and U.S. Department of Transportation (DOT) have issued new rules that vulnerability assessments and transportation security plans constitute sensitive security information (SSI), requiring motor carriers to take specific measures to protect them from disclosure:¹

The requirements of the rule include:

- Marking all "sensitive security information" (SSI) with a specific warning text (see new page).
- Taking "reasonable steps to safeguard SSI...from unauthorized disclosure."
- Limiting disclosure of SSI to authorized "covered persons" with a "need-to-know."
- Reporting any unauthorized disclosures.
- "Destroying SSI completely to preclude recognition" when the information is no longer needed.

Required SSI Marking

- Each page (including the title page) of the security plan (or any other SSI) must be conspicuously marked at the top with the statement: **"SENSITIVE SECURITY INFORMATION."**
- The following statement also must appear on the bottom of each page:
"WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520."

¹See 69 *Federal Register* 28066 (May 18, 2004). This interim final rule represents the Administration's initial strategy to safeguard this information and will likely be revised in the near future.

Vulnerability and Threat Assessment (VTA) Tool

TERM®(Threat, Exposure and Response Matrix - Ag Security)²

This tool TERM®-AG SECURITY is designed to be a simplified way for agricultural and food transporters to rapidly assess general and specific threats (principally from acts of terrorism) and vulnerabilities related to the transportation of agricultural and food products.

While this tool is an excellent starting point, TERM®-AG SECURITY is not intended to fully replace a specific Vulnerability and Threat Assessment (VTA) performed by a competent security entity.

TERM®-AG SECURITY Section A is organized into 4 parts:

- Part 1. Introduction
- Part 2. Vulnerabilities
- Part 3. Threats
- Part 4. Integrating Vulnerabilities and Threats to Identify Exposure

Section A – TERM®-AG SECURITY

Part 1. Introduction

TERM®-AG SECURITY is designed to be utilized by the commercial agricultural and food transportation industries to better protect the food supply of the United States of America. Food is a critical infrastructure component as identified by the White House, USDA, and the Department of Homeland Security (DHS).

TERM®-AG SECURITY deals only with vulnerabilities, threats, and their relationship with each other that yield “exposures.” Identification of these security exposures are needed to address Security Plans, Training Programs, and Security Exercises. The following process will identify those “Exposures.”

As you can see from the diagram of the TotalSecurity.US Management System (TSMS™), the starting point of a security program is a good VTA. It would be wasteful to put security measures in place if your vulnerability was extremely low or if, in fact, the threat level was not high enough to take action. The color-coded Homeland Security Advisory System (HSAS) (*see Appendix B, page 18*) helps us manage this dynamic. Your limited security resources need to be applied to the greatest exposures first and then appropriately applied to the other significant exposures. TERM®-AG SECURITY Section A will start you on that process.

² TERM®-AG SECURITY is used with permission of www.TotalSecurity.US. Not for resale and may not be commercially copied, modified, or replicated in any way.

The Security Planning Guide will provide the tools to create a security plan.



Part 2. Vulnerabilities

Start with what you know best, your own operations. Vulnerabilities in the TERM®-AG SECURITY application refer to your weaknesses, not the opponent's capabilities or intentions.

Using TERM®-AG SECURITY

1. Create a document for a draft TERM®-AG SECURITY Section A containing a table as shown here.

#	Vulnerabilities	How Apparent is the Vulnerability? Ease to Discover (1-5)	Seriousness to Operation and Product (1-5)	Vulnerability Score (1-10)
1	Example: Unauthorized Access to Cargo Enroute	4	5	9
2				
...				
15				

2. Review the Vulnerabilities in the following table. Select which Vulnerabilities seem logical and applicable to your operation. List them in the Vulnerabilities column at #1 above. Notice there are references to "Other" vulnerabilities. Consider any "Other" Vulnerabilities and add them to the list in the Vulnerabilities column in #1 above. You should end up with at least 10 Vulnerabilities and depending on the size of your company or the depth you want to go, you may end up with as many as 25-100 Vulnerabilities. The VULNERABILITIES categories in all upper case are highly recommended for inclusion as a minimum in your list.

VULNERABILITIES

1. PERSONNEL SECURITY	11. Unauthorized Access to Information – (Physical)
2. Employees with Criminal Records	12. UNAUTHORIZED ACCESS TO CARGO
3. Employees who may be Criminal or Terrorist Sympathizers	13. Unauthorized Access to Keys
4. Co-opted Employee	14. ENROUTE SECURITY
5. EMPLOYEE AS TERRORIST	15. HIJACKED VEHICLE
6. UNAUTHORIZED ACCESS	16. THEFT OF A VEHICLE
7. UNAUTHORIZED ACCESS TO CARGO STORAGE AREAS	17. UNAUTHORIZED ACCESS TO CARGO
8. UNAUTHORIZED ACCESS TO PARKED VEHICLES	18. Diversion
9. THEFT OF A VEHICLE	19. OTHER
10. Unauthorized Access to Information – (Electronic)	20. OTHER

3. Now “Score” each vulnerability. The Score has two components. Approach this with the perspective of “A”, how apparent is the vulnerability or how hard would it be for an insider or an outsider to discover this vulnerability, and “B”, how serious is this vulnerability to the survival, efficiency of my operations, and the integrity of agricultural commodities transported.
 - a. Assign a value based on your judgment on a scale of 1-5 with 5 indicating that the vulnerability is readily apparent or extremely easy to discern and 1 indicating that the vulnerability is not apparent at all or extremely difficult to discover. Put that 1-5 Score in the “How Apparent” column.
 - b. Assign a value based on your judgment on a scale of 1-5 with 5 indicating that the vulnerability, if exploited, would be extremely serious to the survival, efficiency of your operations, and the integrity of agricultural commodities in your care and with 1 indicating that the vulnerability, if exploited, would be relatively insignificant to the survival, efficiency of your operations, and the integrity of agricultural commodities items in your care. Put that Score in the Seriousness column.
4. Now add the Apparent and Serious Scores into a final Score in the Vulnerability column.
5. Rank the vulnerabilities in descending order based on the Vulnerability Score column.

The above simple 5-step process should produce a good list of perceived vulnerabilities. Be aware that this list is very likely not all-inclusive. It is a list based upon your judgments and will correspond in quality and scope to the quality and scope of your assessments.

Part 3. Threats

Threats in the TERM®-AG SECURITY application refer to the capabilities of those who wish to inflict harm or disrupt operations. Generally, threats are external but not always. There could be a threat that is eventually manifested from an internal source.

Using TERM®-AG SECURITY

6. Add to your VTA document in draft TERM®-AG SECURITY Section A, a table as shown below.

Threats	How Present is the Threat? 1-5 *(Homeland Security Advisory System) 1-5 (1= Green, 5=Red)	Seriousness to Operation and Product (1-5)	Threat Score (1-10)
Example: Contamination of a Product	4	5	9
Imbed a "Mole" Employee	3	5	8

***Note:** See Appendix B on page 18 for HSAS conditions and descriptions.

7. Review the THREATS in the following table. Select which threats seem logical and applicable to your operation. List them in the Threats column on the previous page. Notice there are references to "Other" threats. Consider any "Other" threats and add them to the list in the Threats column. The THREATS in all caps are highly recommended for inclusion as a minimum in your list.

THREATS

(These include both Weapons and Tactics)

1. Aerial Chem/Bio Weapon (delivered by air)	11. Hostage Taking
2. Assault	12. INCENDIARY WEAPON (including vehicle)
3. Biological Weapon (standoff or introduced directly)	13. Information System Attack
4. Chemical Weapon (standoff or introduced directly)	14. Mail Bomb (including Chem/Bio)
5. Communicable Disease Introduction (standoff or introduced directly)	15. MOLE – an employee or person with malicious intent employed or imbedded in the organization
6. CONTAMINATION OF PRODUCT (At any point in the chain of custody from origin to enroute)	16. Poison (standoff or introduced directly)
7. Extortion	17. THEFT OF VEHICLE
8. FIREARMS ATTACK OR USE	18. Trojan Horse (where the vehicle may serve as the host – knowingly or not – to deliver a threat to a target)
9. HIJACKING	19. TRUCK BOMB
10. HOAX	20. Other

8. Now “Score” each THREAT. The Score has two components. Approach this with the perspective of “A”, how “Present” is the THREAT, and “B” how serious is this THREAT, if it was successfully pressed home, to the survival, efficiency of your operations, and the integrity of agricultural commodities in your care.
 - a. Assign a value based on your judgment on a scale of 1-5 with 5 indicating that the THREAT is very “Present” and 1 indicating that the THREAT is not apparently “Present” at all. Put that 1-5 Score in the “How Apparent” column.
 - b. Assign a value based on your judgment on a scale of 1-5 with 5 indicating that the THREAT, if it was successfully exploited, would be extremely serious to the survival, efficiency of your operations, and the integrity of agricultural commodities in your care and with 1 indicating that the THREAT, if it was exploited, would be relatively insignificant to the survival, efficiency of your operations, and the integrity of agricultural commodities in your care. Put that Score in the Seriousness column.
9. Now add the Apparent and Serious Scores into a final Score in the THREAT Score column.
10. Rank the vulnerabilities in descending order based on the THREAT Score column.

The above simple process should produce a good list of your perceived THREATS. Be aware that this list is very likely not all-inclusive. It is a list based upon your judgments and will correspond in quality and scope to the quality and scope of your assessments.

Part 4. Integrating Vulnerabilities and Threats to Identify Exposure

Now, put Vulnerabilities and Threats together to identify “Exposures.” This is, in fact, creating a terrorist scenario where you see what weapons and tactics terrorists may try to use to exploit your vulnerabilities.

This is the most important part of the process. It is also the most time consuming part of the process, but it is worth it. Take the time to do this right, and you will be rewarded with a good product.

1. Combine the tables you have created thus far, as shown in the Rollup Table, on page 10.
 - a. Take one Vulnerability at a time and list it in the Vulnerability column.
 - b. Put its associated Score in the Vulnerability Score column.
 - c. Look at the list of Threats and select each Threat and its Threat Score that could exploit that Vulnerability and list them in the Threat column and Threat Score column, giving each Threat and Threat Score its own cell. If you list more than one Threat that could exploit the specific Vulnerability, you will have blank corresponding cells in the Vulnerability column and Vulnerability Score columns so you will need to copy the “working” Vulnerability column and Vulnerability Score columns into the blank cells. At this point, you should have all of the cells in any utilized row containing text or a numerical value.
 - d. Repeat this process in steps a through c above for each Vulnerability, applying the relevant threats to that vulnerability until all the vulnerabilities have been addressed. This is the MOST IMPORTANT PART OF THIS PROCESS!
2. Now you will add a new column to the right called Exposure Score. Here is your reward!
 - a. Add the Vulnerability Score and Threat Score for Each Row and put the value in the Exposure column.
 - b. Sort this new TERM®-AG SECURITY Section A table in descending order based on the Exposure Score column.
3. You now have an assessment of your relative specific exposures from the greatest to the least exposure, based upon your input of specific Vulnerabilities and Threats.

EXAMPLE: Rollup table of **Vulnerability** and the **Threats** that might exploit that Vulnerability thus creating an **Exposure**

Vulnerability	Apparent	Serious	Vulnerability Score	Threat	Present	Serious	Threat Score	Exposure Score
Access to Product Enroute	4	5	9	Contamination (Product)	4	5	9	18
Access to Product Enroute	4	5	9	"Mole" Contaminates	3	5	8	17
Hijacking of Vehicle Enroute	3	5	8	Truck Bomb	2	5	7	15
Hijacking of Vehicle Enroute	3	5	8	Incendiary Attack	2	4	6	14
		0				0	0	
		0				0	0	
		0				0	0	
		0				0	0	
		0				0	0	
		0				0	0	
		0				0	0	
		0				0	0	
		0				0	0	
		0				0	0	

Congratulations!

This completes your Section A, Vulnerability and Threat Assessment (VTA).

Security Planning Guide

Introduction

The Security Planning Guide is a tool which can be used to apply the information derived from the VTA, into a security plan for your commercial agricultural and food transportation company.

There are various types of formats that have been developed for the creation of security plans in the post 9/11 environment. One of the most effective formats available was created for the Federal Motor Carrier Safety Administration for the transportation of hazardous materials (HAZMAT) in transit. The format utilized in this Security Planning Guide is built on that model and has been modified, as necessary, to apply to the transportation of agricultural and food commodities.

There are many ways to write effective security plans. The methodology presented in this guide has been field tested and is recognized by the United States Department of Agriculture and the Agricultural and Food Transporters Conference of the American Trucking Associations as a valid methodology, which can be of assistance in the formulation of a security plan for your company.



This Security Planning Guide is organized into 4 parts.

- Part 1. Personnel Security
- Part 2. Unauthorized Access Security
- Part 3. Enroute Security
- Part 4. Plan Administration

These elements of a security plan can be very effective. Because trucking companies transport many agricultural commodities, including hazardous materials, some consistency in approach will be beneficial and efficient. Therefore, this AFTC Security Planning Guide will be generally organized like that for HM-232, (HM 232, Hazardous Materials Security Regulatory Requirements*) to address the elements of Personnel Security, Unauthorized Access, Enroute Security, and Plan Administration. Naturally, specific implementation in the agricultural and food commodity transportation environment will differ from that in the HM 232 environment.

*DOT/RSPA - 49-CFR Sections 172.800 and 172.802.

Assumptions

1. Operation and Site Specific Security Plans should be written to address the Operation and Site Specific Vulnerabilities, Threats, and Exposures identified in Section A of the VTA.
2. If there is no identified Vulnerability, Threat, or Exposure, no action is required.
3. Much has been learned and utilized from related Security Planning work such as that done by the Food Safety and Inspection Service (FSIS) and the Federal Motor Carrier Safety Administration in HM 232.
4. It is beneficial to address Primary Security Objectives in the plan and then discuss Specific Security Measures that support a Primary Security Objective, and in what HSAS Color Coded Threat Level they may be deployed, as shown in the example table below.

#1 Primary Security Objective (PSO): Secure unattended vehicles				
	Security Measures to implement the PSO			
HSAS Color Code	Policy or Procedure	Technology or Hardware	Training and Drills	Costs
Green				
Blue				
Yellow	Require employees to lock their vehicles.	Provide XYZ locks.	Teach employees what the lock policy is and how to use the XYZ locks.	\$1,400
Orange				
Red				

Part 1. Personnel Security

In Part 1, look at the Threats identified in Section A of the VTA.

For any applicable Threat, create one or more Primary Security Objectives.

Then, populate the table, as appropriate, with Security Measures by creating measures or selecting from the list of measures offered in Appendix A for your consideration.

See the example below for the THREAT: MOLE.

THREAT: MOLE

#1 Primary Security Objective (PSO): Prevent Employment of a "Mole"				
Security Measures to implement the PSO				
HSAS Color Code	Policy or Procedure	Technology or Hardware	Training and Drills	Costs
Green	Conduct pre-employment background checks for new hires.			\$50/each
Blue				
Yellow	Conduct background checks of existing employees.		Highway Watch® training for all employees.	\$50/each for background checks. Highway Watch® training is free of charge.
Orange				
Red				

Add another PSO Table for any other Personnel Security Threat you identified in your Section A.

Part 2. Unauthorized Access Security

In Part 2, look at the Threats identified in Section A of the VTA.

For any applicable Threat related to Unauthorized Access, create one or more Primary Security Objectives.

Then, populate the table, as appropriate, with Security Measures by creating measures or selecting from the list of measures offered in Appendix A for your consideration.

See the example below for the THREAT: THEFT OF VEHICLE.

THREAT: THEFT OF VEHICLE				
#1 Primary Security Objective (PSO): Prevent Theft of Vehicle				
Security Measures to implement the PSO				
HSAS Color Code	Policy or Procedure	Technology or Hardware	Training and Drills	Costs
Green	Institute a key control policy where keys are kept in dispatch office lockbox and dispatcher issues keys.	Provide safe for dispatch office to house keys.	Train employees on the key control policy.	Safe - \$600, Training - \$300
Blue				
Yellow	Require employees to lock vehicles with secondary XYZ locks. Dispatcher issues XYZ locks and maintains keys.	Provide 30 XYZ locks (1 per vehicle)	Teach employees what the lock policy is and how to use the XYZ locks.	Locks - \$1,500
Orange				
Red				

Add another PSO Table for any other Unauthorized Access Security Threat you identified in your Section A.

Part 3. Enroute Security

In Part 3, look at the Threats identified in Section A of the VTA.

For any applicable Threat related to Enroute Security, create one or more Primary Security Objectives.

Then, populate the table, as appropriate, with Security Measures by creating measures or selecting from the list of measures offered in Appendix A for your consideration.

See the example below for the THREAT: HIJACKING.

THREAT: HIJACKING

#1 Primary Security Objective (PSO): Prevent Hijack of Vehicle				
Security Measures to implement the PSO				
HSAS Color Code	Policy or Procedure	Technology or Hardware	Training and Drills	Costs
Green	Institute a locked vehicle policy where operators are required to lock the vehicle while enroute and also to take the keys each time they leave the vehicle.		Train employees on the locked vehicle policy.	Training - \$200
Blue	1. Institute a duress code and reporting policy. 2. Require Highway Watch® training for all enroute and dispatch employees.		1. Train employees on duress codes. 2. Provide Highway Watch® training to all enroute and dispatch employees.	Highway Watch® training is free of charge.
Yellow	All drivers are required to call in every 8 hours.			
Orange	All drivers are required to call in every 4 hours.			
Red	All drivers are required to call in every 2 hours.			

Add another PSO Table for any other Enroute Security Threat you identified in your Section A.

Part 4. Plan Administration

Once you have populated Part 1 Personnel Security, Part 2 Unauthorized Access Security, and Part 3 Enroute Security with as many PSO's that are required, you will have completed your draft Security Plan. The plan may run ten to twenty pages or more, but it will be an easily maintained document and will provide for good management oversight of the plan. It also has the added benefit of arranging security measures in a manner that addresses the Homeland Security Advisory System (HSAS).

It is recommended that the VTA Tool and Security Planning Guide be updated annually or whenever there is a significant change in environment, operations, or a specific security concern or incident.

It is recommended that training and drills be conducted to internalize the elements of the Security Plan and to highlight possible needed upgrades to the Plan.



As the above graphic of the TotalSecurity.US Management System (TSMS™) shows, you have now completed two of the four components (Vulnerability and Threat Assessment and Security Plans) of your security program. The other two components (training and drills, exercise and incidents) can be implemented once the first two components have been completed.

APPENDIX A. Security Measures for Consideration

Draft Security Measures – WARNING - NOT ALL INCLUSIVE		
Policy and Procedure	Hardware and Software - Equipment	Training
<p>Access Control Measures Assembly Plan, Convoy, Counter-surveillance, Deception Operations, Decontamination, Evacuation, Evacuation Plan, Explosives Handling, Landscaping, Laws and Ordinances, Layered Approach to Defense, Lock down Plan, Media Plan, PA System, Personnel Plans, Policies and Procedures, Remote access to facility controls and cameras, Response Team, Armed Response Team, Hazmat Response Team, Medical Plan, Safe Haven Plan, Screening, Searches of Persons, Searches of Places, Searches of Things, Security Officers Unarmed and/or Armed, Signage, Surveillance, Sweeps, Training, Trenches, Tunnels, Vehicle Patrol, Vehicle Screening (Solid Shield), Vehicles, Police/Security/Other Deterrence,</p>	<p>Access Control Measures (Manned, Proximity, Biometric, etc.), Aerial Patrol, Alarms, Audio Surveillance, B-1 Computer Security Devices, Backup Generators, Barbed Wire, Barrier (Jersey), Barrier to Observation, Barrier to Vehicle, Biometrics, Blast Wall or Structure, Bomb Blanket, Bomb Mitigation Container Systems (replace Trash Cans), Cameras, Chemicals, CNS weapons, Concertina Wire, Decontamination, Electricity (incl. Taser), EMP, Equipment, Facility Equipment, Fencing, Fire, Fire Fighting Equipment, Firearm, Firewalls, Global Positioning System, Gross Decontamination, Guard Towers, Halon/Inert Gas, Hard Cover from Direct Fire, Hide Position, High Pressure Water, Infra-red lighting, Integrated early warning, Internet remote surveillance, K-9 arrest dog, K-9 bomb dog, Landscaping, Laser, Lighting, Locks, Metal Detector hand held, Metal Detector walk thru, Moats, Motion Sensors, Night Vision, Obstacles, Overhead protection, PA System, Planters, Protective Vest, Radiological Detection, Remote access to facility controls and cameras, Remote sensing, Screening, Seals, Searches of Persons, Searchlights, Seismic intrusion detection, Signage, Surveillance, Sweeps, Trenches, Tunnels, UPS, Vehicle Screening (Solid Shield), Vehicles, Police/Security/Other Deterrence, Water, Water Cannon, Water Hose, Water Supply, Window Treatments, X-Ray</p>	<p>Access Control Measures (Manned, Proximity, Biometric, etc.), Aerial Patrol, Alarms, Altitude Chamber, Armored Vehicle, Assembly Plan, Audio surveillance, B-1 Computer Security Devices, Backup Generators, Barbed Wire, Barrier (Jersey), Barrier to Observation, Barrier to Vehicle, Biometrics, Blackout, Blast Wall or Structure, Bomb Blanket, Bomb Mitigation Container Systems (replace Trash Cans), Cameras, Casing and Rehearsal Detection, Chemical and Biological Training, Chemicals, CNS weapons, Concertina Wire, Convoy, Counter-surveillance, Deception Operations, Decontamination, Design, Electricity (incl. Taser), EMP, Equipment, Evacuation, Evacuation Plan, Explosives Handling Training (incl. EOD), Facility Equipment, Fencing, Fire, Fire Fighting equipment, Firearm, Firearms, Training, Firewalls, Foot Patrols, Global Positioning System, Gross Decontamination, Group Training, Guard Towers, Halon/Inert Gas, Hard Cover from Direct Fire, Hide Position, High Pressure Water, Individual Training, Infra-red lighting, Integrated early warning, Internet remote surveillance, K-9 arrest dog, K-9 bomb dog, Landscaping, Laser, Laws and Ordinances, Layered Approach to Defense, Legal Training, Lighting, Lock down Plan, Locks, Media Plan, Metal Detector hand held, Metal Detector walk thru, Mines, Moats, Motion sensors, Night Vision, Obstacles, Overhead protection, PA System, Personnel Plans, Planters, Policies and Procedures, Protective Vest, Radar – air, Radar – ground, Radiological Training, Remote access to facility controls and cameras, Remote sensing, Response Team, Armed Response Team, Hazmat Response Team, Medical Plan, Safe Haven Plan, Screening, Seals, Searches of Persons, Searches of Places, Searches of Things, Searchlights, Security Officers Unarmed and/or Armed, Seismic intrusion detection, Signage, Surveillance, Sweeps, Training, Trenches, Tunnels, UPS, Vehicle patrol, Vehicle Screening (Solid Shield), Vehicles, Police/Security/Other Deterrence, Water, Water Cannon, Water Hose, Water Supply, Win Against Terrorism Training, Window Treatments, X-Ray</p>

APPENDIX B - Homeland Security Advisory System



1. LOW CONDITION (GREEN). This condition is declared when there is a low risk of terrorist attacks. Federal departments and agencies should consider the following general measures, in addition to the agency-specific Protective Measures they develop and implement:

- Refining and exercising, as appropriate, preplanned Protective Measures;
- Ensuring personnel receive proper training on the Homeland Security Advisory System and specific preplanned department or agency Protective Measures; and
- Institutionalizing a process to assure that all facilities and regulated sectors are regularly assessed for vulnerabilities to terrorist attacks, and all reasonable measures are taken to mitigate these vulnerabilities.

2. GUARDED CONDITION (BLUE). This condition is declared when there is a general risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Condition, Federal departments and agencies should consider the following general measures, in addition to the agency-specific Protective Measures that they will develop and implement:

- Checking communications with designated emergency response or command locations;
- Reviewing and updating emergency response procedures; and
- Providing the public with any information that would strengthen its ability to act appropriately.

3. ELEVATED CONDITION (YELLOW). An Elevated Condition is declared when there is a significant risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures, in addition to the Protective Measures that they will develop and implement:

- Increasing surveillance of critical locations;
- Coordinating emergency plans as appropriate with nearby jurisdictions;
- Assessing whether the precise characteristics of the threat require the further refinement of preplanned Protective Measures; and
- Implementing, as appropriate, contingency and emergency response plans.

4. HIGH CONDITION (ORANGE). A High Condition is declared when there is a high risk of terrorist attacks. In addition to the Protective Measures taken in the previous Threat Conditions, Federal departments and agencies should consider the following general measures, in addition to the agency-specific Protective Measures that they will develop and implement:

- Coordinating necessary security efforts with Federal, State, and local law enforcement agencies or any National Guard or other appropriate armed forces organizations;
- Taking additional precautions at public events and possibly considering alternative venues or even cancellation;
- Preparing to execute contingency procedures, such as moving to an alternate site or dispersing their workforce; and
- Restricting threatened facility access to essential personnel only.

5. SEVERE CONDITION (RED). A Severe Condition reflects a severe risk of terrorist attacks. Under most circumstances, the Protective Measures for a Severe Condition are not intended to be sustained for substantial periods of time. In addition to the Protective Measures in the previous Threat Conditions, Federal departments and agencies also should consider the following general measures, in addition to the agency-specific Protective Measures that they will develop and implement:

- Increasing or redirecting personnel to address critical emergency needs;
- Assigning emergency response personnel and pre-positioning and mobilizing specially trained teams or resources;
- Monitoring, redirecting, or constraining transportation systems; and
- Closing public and government facilities.

Highway Watch® Program

What is Highway Watch®?

Highway Watch® is the highway sector's national safety and security program that uses the skills, experiences, and "road smarts" of America's transportation workers to help protect critical infrastructure and the transportation of goods, services, and people.



Highway Watch® is administered by the American Trucking Associations (ATA) under a cooperative agreement with the U.S. Transportation Security Administration (TSA). The Highway Watch® coalition engages scores of the highway sector's leading organizations to train hundreds of thousands of transportation workers throughout the industry. Each state program is coordinated by a locally designated organization such as the state trucking association.

How does Highway Watch® work?

Highway Watch® volunteers are trained by security professionals, law enforcement, and other expert personnel. Highway Watch® participants are given observational tools and the opportunity to exercise their skills to spot problems such as homeland security concerns, stranded vehicles, impaired drivers or unsafe road conditions, and report them rapidly and accurately to the authorities.

Highway Watch® participants - transportation infrastructure workers, commercial and public truck and bus drivers, and other highway sector professionals - are specially trained to recognize potential safety and security threats and avoid becoming a target of terrorists or to spot a terrorist threat to others. The Highway Watch® effort seeks to prevent terrorists from using large vehicles or hazardous cargoes as weapons and to help protect America's critical infrastructures and people. Highway Watch® participants are also reminded to use wireless location and communication technologies properly when reporting safety hazards, unsafe road conditions, auto accidents, and other roadway concerns.

Highway Watch® reports are combined with other information sources and shared both with Federal agencies and the Sector by the Highway ISAC.

How do Highway Watch® participants make their reports?

After completing the Highway Watch® training, transportation professionals use cell phones and other telecommunications equipment to contact emergency personnel through a special Highway Watch® hotline - providing emergency responders with precise location and incident information. A trained operator at the Highway Watch® Call Center verifies the highway professional's identity (each participant has a unique Highway Watch® ID number) and location and then routes the call to the appropriate law enforcement authorities in that area. The Call Center correlates the location

information and routes the call to the proper response agency in that area or to the proper state or regional emergency dispatch center. Additionally, Highway Watch® training instructs all participants to use 911 for life threatening emergencies.

What type of training do Highway Watch® drivers receive?

Highway Watch® participants attend a comprehensive training session before they become certified Highway Watch® members. This training incorporates both safety and security issues. Participants are instructed on what to look for when witnessing traffic accidents and other safety-related situations and how to make a proper emergency report. Highway Watch® curriculum also provides anti-terrorism information, such as: a brief account of modern terrorist attacks from around the world, an outline explaining how terrorist acts are usually carried out, and tips on preventing terrorism. From this solid baseline curriculum, different segments of the highway sector have or are developing unique modules attuned to their specific security related situation.

What is the Highway ISAC and how does it work?

The Highway Information Sharing and Analysis Center (Highway ISAC) is a critical component to the Highway Watch® effort and serves as the analytical and communications focal point for the Highway Watch® program. In close cooperation with the Department of Homeland Security (DHS) and intelligence and law enforcement agencies, the Highway ISAC, a nationwide team of well-trained and experienced transportation security professionals, collectively detect, assess, report, process, analyze, and respond to incidents which might pose a threat to national security.

When a security-related call is made to the Highway Watch® hotline, the operator notifies local law enforcement authorities. A report of the incident is then generated and forwarded to the Highway ISAC where it is shared with government intelligence officials and other law enforcement agencies.

Are Highway Watch® professionals paid extra? Are there any financial incentives to join the program?

Highway Watch® participants are self-motivated and do not seek compensation for participation. They participate because they want to do their part to keep America safe.

How are Highway Watch® professionals identified?

Highway Watch® participants receive certificates of completion and individual ID cards at the conclusion of the training course.

Why do local government and safety officials become involved with Highway Watch®?

Local officials and law enforcement authorities become involved in the Highway Watch® program because they recognize the value in having extra “sets of eyes and ears” on the road. They also appreciate that the services Highway Watch® provides augments their existing resources.

Is there any outreach communication to Highway Watch® participants?

As needed, the Highway Watch® hotline sends out alerts to trained participants. These alerts may include national security updates, Amber Alerts, and “be on the look out” (or BOLO) requests.

Highway Watch® Information Sharing and Analysis Center (ISAC)

Currently operated by the ATA, in cooperation with the TSA and supported by the Highway Watch@ Coalition and Anti-Terrorism Working Group and the National Infrastructure Protection Center of the DHS, the Highway ISAC benefits the entire transportation industry.

Its mission is to serve as an alert system, leveraging the Internet and other communication channels, to provide the transportation industry with incident, threat, and vulnerability information.

By compiling industry and government intelligence in one location, the Highway ISAC assists both the private and public sectors in creating security measures, planning for emergencies, and protecting our nation's citizens and infrastructure.

How To Use ISAC

The ISAC is for the daily operations management or organizations involved in the transportation industry. You must be either a trained Highway Watch® driver or have completed an application to gain access to the ISAC.

Why Report Information?

Much of what is considered "intelligence" comes from hundreds of "normal" bits of information that are on the streets or in the public domain, open for all to see. These bits of information, when combined with the "secret" information universe of intelligence professionals and that of law enforcement, make up the base from which investigations can be successfully conducted to thwart terrorists' nefarious operations.

Transportation companies and their employees are rich sources of information based upon their corporate security systems and personal observances.

Information flow is not just one way, from government to industry. The critical link-communicating this information to those who can tie the code together-is the patriotic duty of everyone. Industry needs to play its important role and push information to government in a form that is useful and in time to be acted upon.

The Homeland Security Act of 2002 and other national laws regarding terrorist related information protect information you submit from the public disclosure enabled in the Freedom of Information Act -- protecting your company and personal privacy.

You can always submit information anonymously. However, providing a way for you to be contacted by law enforcement agencies allows these agencies to verify the validity of the information and to obtain additional facts that may be very important to their investigations.

Terrorist Attacks Don't Just Happen

There are always operational acts which precede a terrorist attack. Here are the operational components:

Targeting- Terrorists carefully choose a target, weighing the probability of weapon access, numbers of casualties, and political significance.

Casing - Terrorists study the target and approaches to the target and assess the situation until they have an intimate knowledge of all dangers and opportunities.

Surveillance - The terrorists want no surprises. Before an attack, the watch on the target will likely be continuous. Rehearsal -Terrorists don't have resources to waste. They usually practice before they act.

Attack Profile - Only after all the above is accomplished will a terrorist plan get underway, leading to the actual attack.

Attack - Terrorists would mount an attack every day if they could, but they cannot. They need to take the time and effort to assure a high probability of success. It is a serious mistake to think they are irrational. They are very intelligent.

Despite this thorough planning, there is a weakness. Everything has to go right for the terrorist. If he is "made," he will either delay or halt his plans. The bottom line – we need to detect them in only one place or one part of their process to cause, at the very least, a disruption of their operation.

Communicate!

Transportation professionals can observe things such as: trucks parked under bridges, routes that make no sense, abandoned rigs, drivers who don't really know their businesses, shipping practices that make no sense, or any of a thousand items that an experienced professional is well suited to discern.

Report – Remembering I-T-A-L-K

Call 911 if you have an emergency or see what appears to be an attack in progress.

Remember the reporting format: I-T-A-L-K

Identify - yourself and provide the receiving agency with your confidential Highway Watch® registered identification number (HWWID).

Time - provide the receiving agency with the exact time of your incident observation.

Activity - provide the receiving agency with a concise and accurate description of your observation, the activity you are seeing.

Location - provide the receiving agency with your physical location. (You may choose to provide a GPS location, mile marker location, street address, or prominent terrain/structure feature.)

Keep - attempt to keep observing without endangering your personal safety or that of your associates.

Helping Government Intelligence Agencies To 'Connect The Dots'

It is important that information be transmitted into the information network of the Federal government so it can be collated and compared with information from many sources of intelligence. Don't simply rely on local agencies to pass this information along for you.

The DHS encourages individuals to report information concerning suspicious activity with either terrorism or criminal potential to the local FBI Joint Terrorism Task Force office or to other appropriate authorities.

The Transportation Security Administration's 24-hour Command Center can be reached at 571-227-1881 or 571-227-1882.

Individuals can reach the DHS (NIPC) Watch and Warning Unit at 202-323-3205, also toll free at 888-585-9078, or by e-mail.

Industry Security Links

- Cargo Tips – <http://www.cargotips.org/>
- The Intel Center – www.intelcenter.com
- ISAC Council – <http://www.isaccouncil.org/about/>
- J.J. Keller & Associates, Inc. – http://www.jjkeller.com/resourcecenters/security/home.htm?action_code=79335
- Safety and Loss Prevention Management Council – <http://www.truckline.com/cc/councils/slpmc/>
- Total Security Services International, Inc. – www.totalsecurity.us
- U.S. Chamber of Commerce – <http://www.uschamber.com/government/issues/defense/homelandsecurity/>
- USDA's Homeland Security Office – Tel. 202-720-7654

FBI Field Offices

The FBI Field Offices are located in major cities throughout the United States and in San Juan, Puerto Rico. All of the FBI Field Offices may be contacted 24 hours a day, every day.

ALABAMA

2121 8th Ave. N.,
Room 1400
Birmingham, AL 35203
205/326-6166

One St. Louis Centre
1 St. Louis St., 3rd Floor
Mobile, AL 36602
334/438-3674

ALASKA

101 East Sixth Avenue
Anchorage, AK 99501
907/258-5322

ARIZONA

201 East Indianola Ave.
Suite 400
Phoenix, AZ 85012
602/279-5511

ARKANSAS

Two Financial Centre
10825 Financial Centre
Parkway, Suite 200
Little Rock, AR 72 11
501/221-9100

CALIFORNIA

Federal Office Building
11000 Wilshire Blvd.
Suite 1700
Los Angeles, CA 90024
310/477-6565

4500 Orange Grove Ave.
Sacramento, CA 95841
916/481-9110

Federal Office Building
9797 Aero Drive
San Diego, CA 92123
858/565-1255

450 Golden Gate Ave.
13th Floor
San Francisco, CA 94102
415/553-7400

COLORADO

Federal Office Building
1961 Stout St., 18th Floor, Room 1823
Denver, CO 80294
303/629-7171

CONNECTICUT

Federal Office Building
150 Court St., Room 535
New Haven, CT 06510
203/777-6311

DISTRICT OF COLUMBIA

601 4th St., N.W.
Washington, DC 20535
202/278-2000

FLORIDA

7820 Arlington Expressway Suite 200
Jacksonville, FL 32211
904/721-1211

16320 Northwest Second Ave.
North Miami Beach, FL 33169
305/944-9101

Federal Office Building
500 Zack St., Room 610
Tampa, FL 33602
813/273-4566

GEORGIA

2635 Century Parkway, Northeast, Suite 400
Atlanta, GA 30345
404/679-9000

FBI Field Offices

HAWAII

Kalaniana'ole Federal Office Building
300 Ala Moana Blvd.
Room 4-230
Honolulu, HI 96850
808/521-1411

ILLINOIS

E.M. Dirksen Federal Office Building
219 South Dearborn St.
Room 905
Chicago, IL 60604
312/431-1333

400 West Monroe St.
Suite 400
Springfield, IL 62704
217/522-9675

INDIANA

Federal Office Building
575 North Pennsylvania St., Room 679
Indianapolis, IN 46204
317/639-3301

KENTUCKY

600 Martin Luther King Jr. Place, Room 500
Louisville, KY 40202
502/583-3941

LOUISIANA

2901 Leon C. Simon Dr.
New Orleans, LA 70126
504/816-3000

MARYLAND

7142 Ambassador Road
Baltimore, MD 21244
410/265-8080

MASSACHUSETTS

One Center Plaza, Suite 600
Boston, MA 02108
617/742-5533

MICHIGAN

P.V. McNamara Federal Office Building
477 Michigan Ave., 26th Floor
Detroit, MI 48226
313/965-2323

MINNESOTA

111 Washington Ave., South, Suite 1100
Minneapolis, MN 55401
612/376-3200

MISSISSIPPI

Federal Office Building
100 West Capitol St.
Room 1553
Jackson, MS 39269
601/948-5000

MISSOURI

1300 Summit
Kansas City, MO 64105
816/512-8200

2222 Market St.
St. Louis, MO 63103
314/231-4324

NEBRASKA

10755 Burt St.
Omaha, NE 68114
402/493-8688

NEVADA

John Lawrence Bailey Building
700 East Charleston Blvd.
Las Vegas, NV 89104
702-385-1281

NEW JERSEY

1 Gateway Center, 22nd Floor
Newark, NJ 07102
973/792-3000

NEW MEXICO

415 Silver Ave., SW, Suite 300
Albuquerque, NM 87102
505-224-2000

FBI Field Offices

NEW YORK

200 McCarty Ave.
Albany, NY 12209
518/465-7551

One FBI Plaza
Buffalo, NY 14202
212/384-1000

26 Federal Plaza, 23rd Floor
New York, NY 10278
212/384-1000

NORTH CAROLINA

Wachovia Building
400 South Tyron St., Suite 900
Charlotte, NC 28285
704/377-9200

OHIO

550 Main St., Room 9000
Cincinnati, OH 45202
513/421-4310

Federal Office Building
1240 East 9th St., Room 3005
Cleveland, OH 44199
216/522-1400

OKLAHOMA

3301 West Memorial Drive
Oklahoma City, OK 73134
405/290-7770

OREGON

Crown Plaza Building
1500 Southwest 1st Ave., Suite 400
Portland, OR 97201
503/224-4181

PENNSYLVANIA

William J. Green Jr., Federal Office Building
600 Arch St., 8th Floor
Philadelphia, PA 19106
215/418-4000

U.S. Post Office Building
700 Grant St., Suite 300
Pittsburgh, PA 15219
412/471-2000

PUERTO RICO

U.S. Federal Building
150 Carlos Chardon Ave., Room 526
Hato Rey, San Juan, PR 00918
787/754-6000

SOUTH CAROLINA

151 Westpark Blvd.
Columbia, SC 29210
803/551-4200

TENNESSEE

John J. Duncan Federal Office Building
710 Locust St., Suite 600
Knoxville, TN 37902
865/544-0751

Eagle Crest Building
225 North Humphreys Blvd., Suite 3000
Memphis, TN 38120
901/747-4300

TEXAS

1801 North Lamar, Suite 300
Dallas, TX 75202
214/720-2200

660 S. Mesa Hills Drive
El Paso, TX 79912
915/832-5000

2500 East TC Jester
Houston, TX 77008
713/693-5000

U.S. Post Office Courthouse Building
615 East Houston St.,
Suite 200
San Antonio, TX 78205
210/225-6741

FBI Field Offices

UTAH

257 Towers Building
257 East, 200 South,
Suite 1200
Salt Lake City, UT 84111
801/579-1400

VIRGINIA

150 Corporate Blvd.
Norfolk, VA 23502
757/455-0100

1970 E. Parham Road
Richmond, VA 23228
804/261-1044

WASHINGTON

1110 Third Ave.
Seattle, WA 98101
206/622-0460

WISCONSIN

330 East Kilbourn Ave.,
Suite 600
Milwaukee, WI 53202
414/276-4684

FDA'S Office of Criminal Investigations (OCI) Field Offices

Food processors, transporters, and retailers should not hesitate to contact FDA's Office of Criminal Investigations (OCI), when they are victims of product tampering, threats, or incidents. OCI's 24-hour emergency response number is 301-443-1240 (Office of Emergency Operations).

USDA'S Office of Inspector General (OIG) Investigations Field Offices

USDA's 24-hour Emergency Response Number: 1-800-424-9121 (Emergency Operations Center)

The Office of Inspector General (OIG) is the criminal investigative arm of the U.S. Department of Agriculture and has a wide range of investigative functions ranging from complex fraud cases, such as export loan guarantee fraud and crop insurance, to basic investigative functions, such as assaults on USDA associates.

The USDA OIG has jurisdiction over theft of food stamps, large-scale food stamp trafficking, usually for \$10,000 or more or involving drug sales, and a variety of other high dollar frauds involving food stamps or electronic benefit transfer cards.

OIG Headquarters:

Jamie Whitten Building
1400 Independence Avenue SW., Room 9-E
Washington, DC 20250
Phone: 202/720-5677, Fax: 202/690-6305

Notes

