

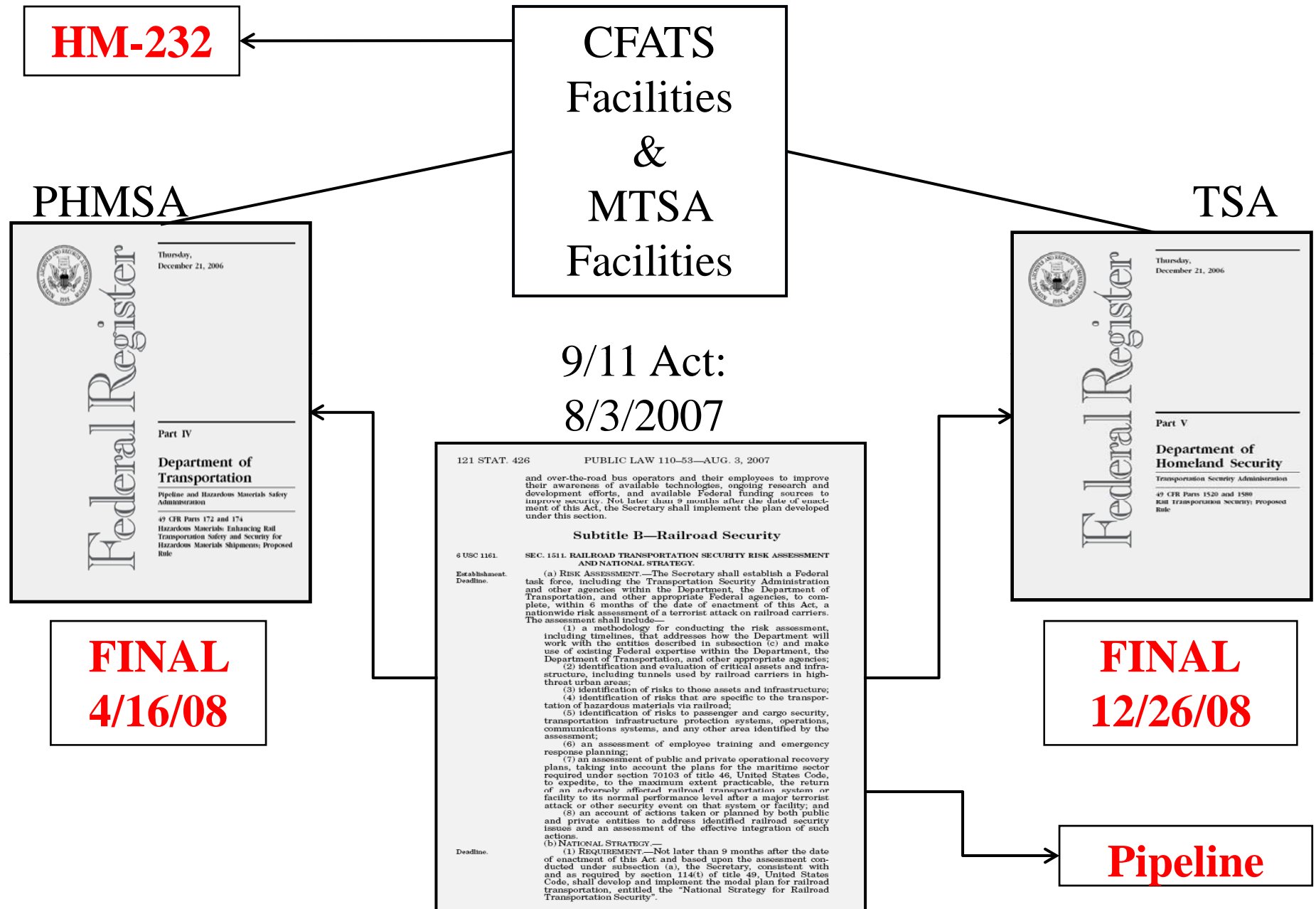
Homeland Security Laws and Regulations: Current and Anticipated Issues for the Port Attorney and Risk Manager

Presented to the:



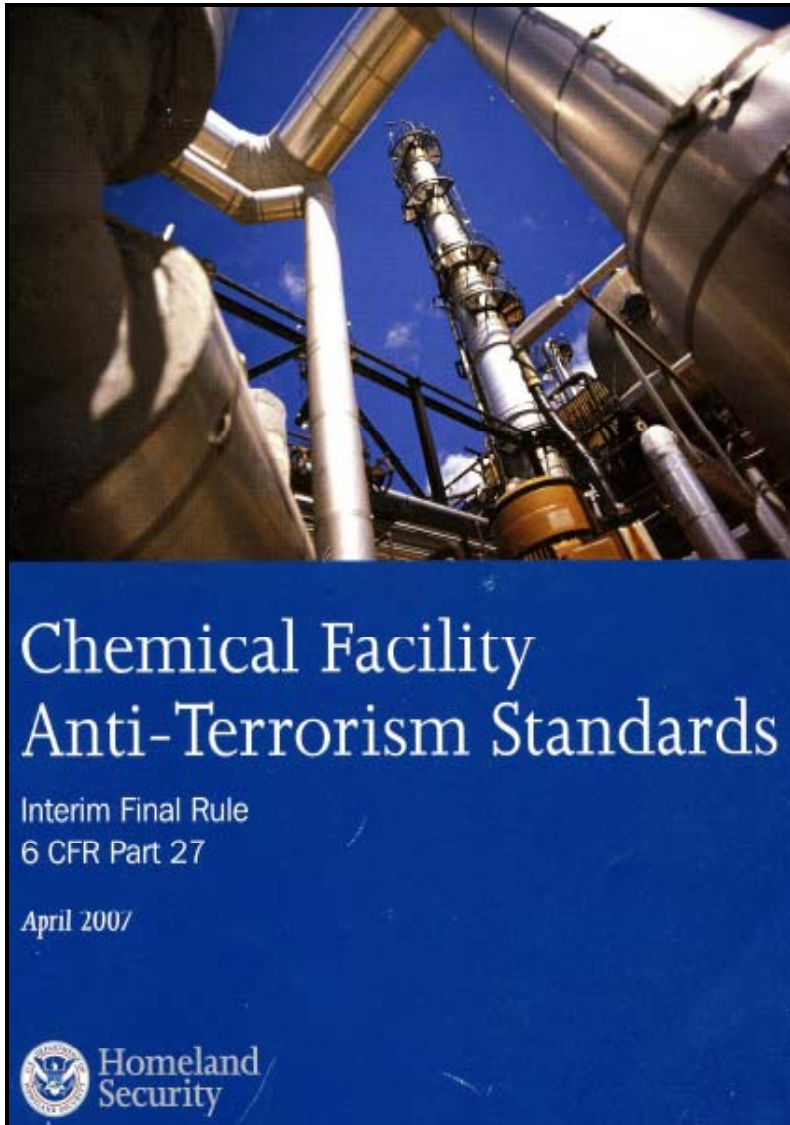
April 17, 2009

Securing the Intermodal Energy Supply Chain: 2009 & Beyond



Chemical Facility Anti-Terrorism Standards: CFATS

The Chemical Facility Anti-Terrorism Standards (CFATS)



- Applies to chemical facilities that “present a high level of security risk.”
- CFATS is a staggered process consisting of four phases: The Top-Screen, the SVA, the SSP, and ongoing compliance.
- CFATS compliance is based on *Risk-Based Performance Standards* rather than prescriptive guidelines.
- CFATS will expire in October 2009; something must occur during the 111th Congress.

The Impact of Homeland Security Regulations: Contract Guards

Risk-Based Performance Standards Guidance

Chemical Facility Anti-Terrorism Standards

October 2008

Version 2.4



FINAL DRAFT

- (1) Restrict Area Perimeter
- (2) Secure Site Assets
- (3) Screen and Control Access
- (4) Deter, Detect, and Delay
- (5) Shipping, Receipt, and Storage
- (6) Theft and Diversion
- (7) Sabotage
- (8) Cyber
- (9) Response
- (10) Monitoring
- (11) Training
- (12) Personnel Surety
- (13) Elevated Threats
- (14) Specific Threats/Risks
- (15) Reporting of Security Incidents
- (16) Security Incidents/Activities
- (17) Officials and Organization
- (18) Records

Application of RBPS

Congress Required the Adoption of Performance Standards...

Therefore DHS cannot Mandate the Precise Manner to Achieve a Specific Security Outcome:

Example: Restrict Area Perimeter

Company A Tier 1 Facility: 12 foot chain-link fence, razor ribbon, microwave intrusion detection system, low-light, pan, tilt, zoom cameras with motion activation, 10 foot clear zone, vehicle cabling.

Company B Tier 1 Facility: 6 foot chain link fence with three strands of barbwire as outer perimeter fence with jersey barriers, 8 foot concrete wall as secondary perimeter, fiber-optic intrusion detection system, combination of fixed cameras and low-light, pan, tilt, zoom cameras.

Company C Tier 1 Facility: Dig a deep moat and

Application of RBPS



Application of RBPS: Tier 1 vs. Tier 4

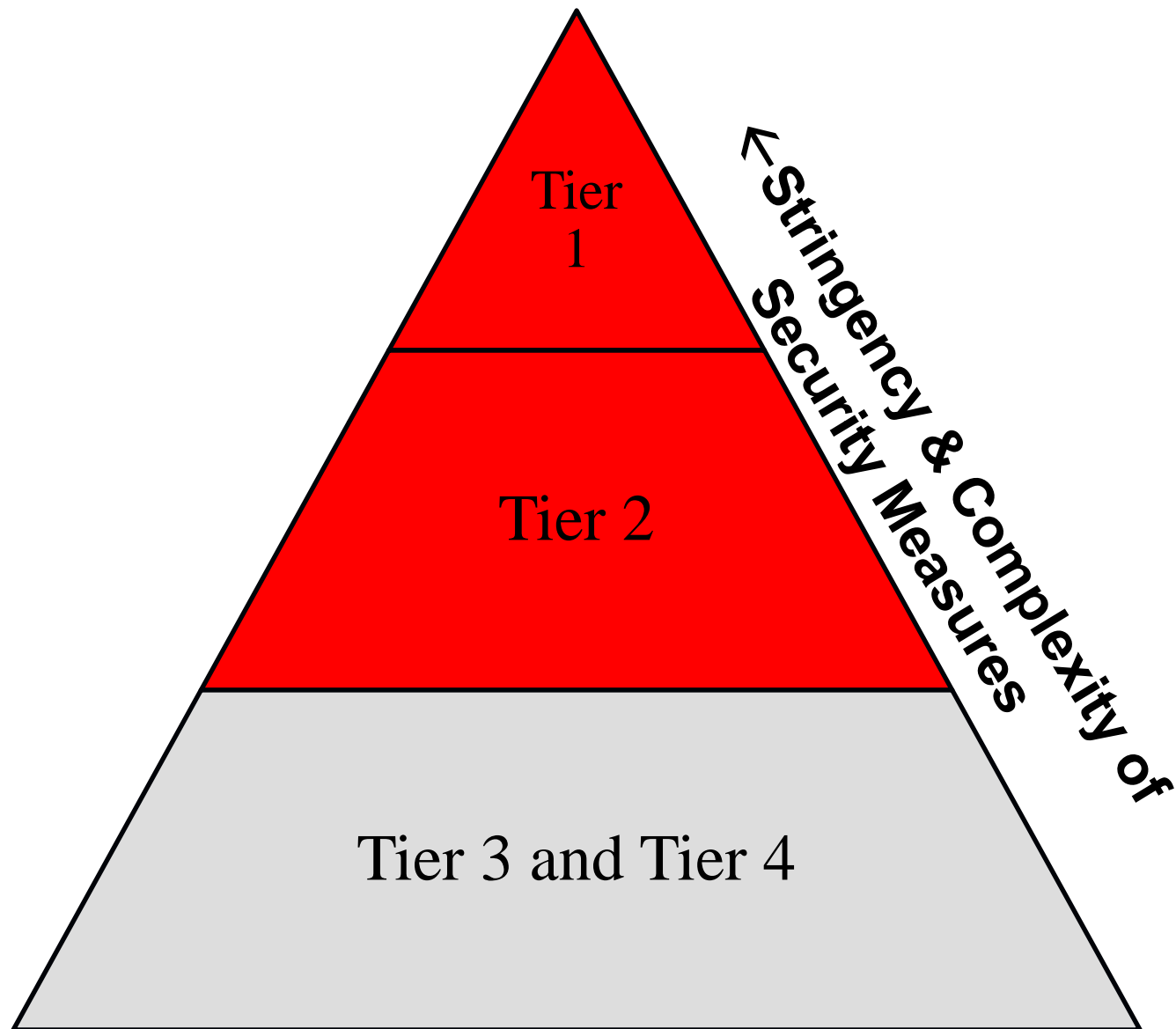
Because the Performance Standards are Risk-Based, a Tier 1 Facility Requires More Stringent Security Than a Tier 4 Facility:

Example: Restrict Area Perimeter

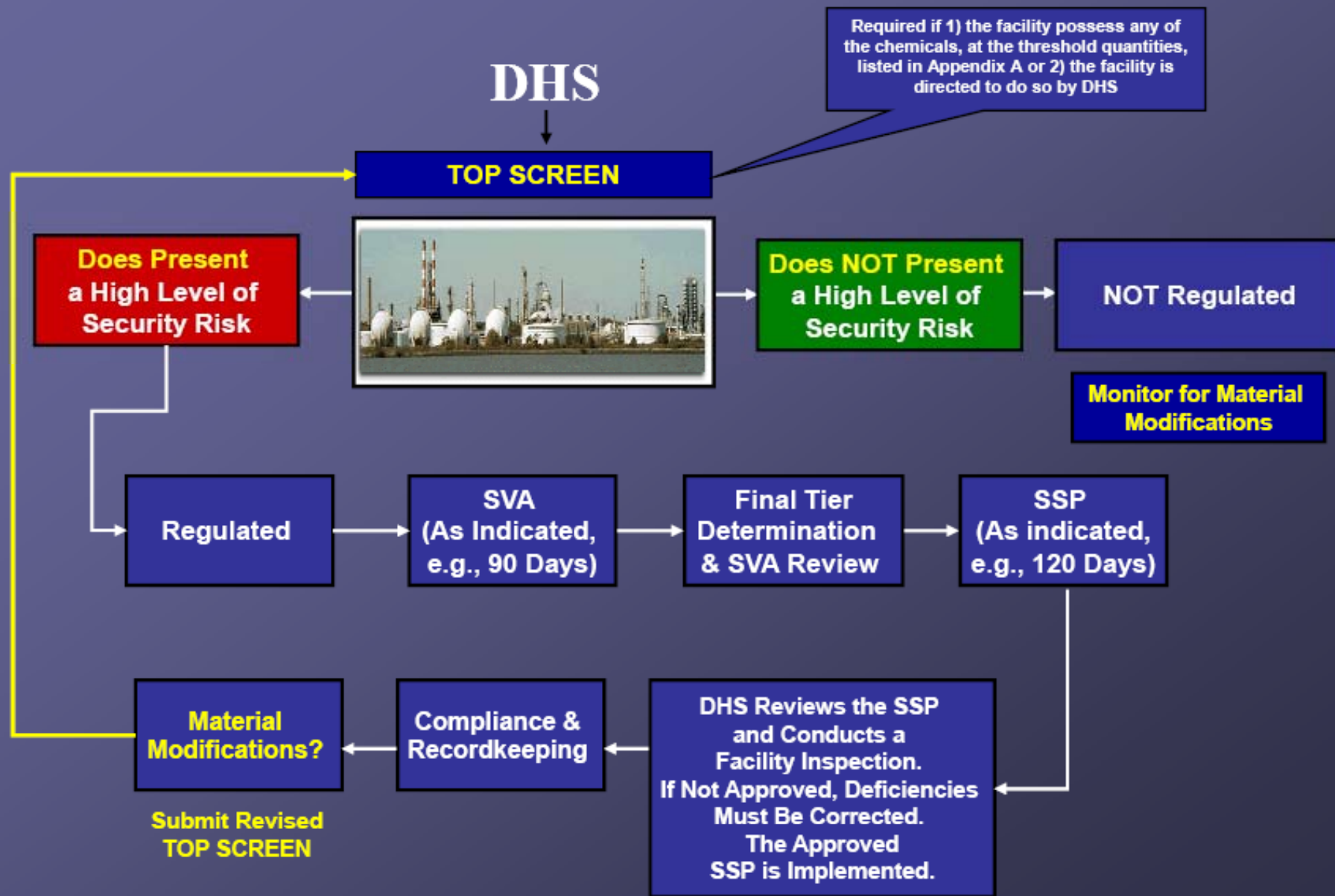
Company A Tier 1 Facility: 12 foot chain-link fence, razor ribbon, microwave intrusion detection system, low-light, pan, tilt, zoom cameras with motion activation, 10 foot clear zone, vehicle cabling.

Company B Tier 4 Facility: 12 foot chain-link fence and razor ribbon.

CFATS: 4 Risk Tiers



CFATS Summary – “30,000 Feet” View



CFATS and Information Protection

SEC. 550. (a) No later than six months after the date of enactment of this Act, the Secretary of Homeland Security shall issue interim final regulations establishing risk-based performance standards for security of chemical facilities and requiring vulnerability assessments and the development and implementation of site security plans for chemical facilities: *Provided*, That such regulations shall apply to chemical facilities that, in the discretion of the Secretary, present high levels of security risk: *Provided further*, That such regulations shall permit each such facility, in developing and implementing site security plans, to select layered security measures that, in combination, appropriately address the vulnerability assessment and the risk-based performance standards for security for the facility: *Provided further*, That the Secretary may not disapprove a site security plan submitted under this section based on the presence or absence of a particular security measure, but the Secretary may disapprove a site security plan if the plan fails to satisfy the risk-based performance standards established by this section: *Provided further*, That the Secretary may approve alternative security programs established by private sector entities, Federal, State, or local authorities, or other applicable laws if the Secretary determines that the requirements of such programs meet the requirements of this section and the interim regulations: *Provided further*, That the Secretary shall review and approve each vulnerability assessment and site security plan required under this section: *Provided further*, That the Secretary shall not apply regulations issued pursuant to this section to facilities regulated pursuant to the Maritime Transportation Security Act of 2002, Public Law 107-295, as amended; Public Water Systems, as defined by section 1401 of the Safe Drinking Water Act, Public Law 93-523, as amended; Treatment Works as defined in section 212 of the Federal Water Pollution Control Act, Public Law 92-500, as amended; any facility owned or operated by the Department of Defense or the Department of Energy, or any facility subject to regulation by the Nuclear Regulatory Commission.

(b) Interim regulations issued under this section shall apply until the effective date of interim or final regulations promulgated under other laws that establish requirements and standards referred to in subsection (a) and expressly supersede this section: *Provided*, That the authority provided by this section shall terminate three years after the date of enactment of this Act.

(c) Notwithstanding any other provision of law and subsection (b), information developed under this section, including vulnerability assessments, site security plans, and other security related information, records, and documents shall be given protections from public disclosure consistent with similar information developed by chemical facilities subject to regulation under section 70103 of title

Federal Register / Vol. 72, No. 67 / Monday, April 9, 2007 / Rules and Regulations 17737

(4) The conclusion of oral arguments, if any are permitted by the Presiding Officer.

(b) The Presiding Officer shall issue an Initial Decision based on the certified record, and the decision shall be subject to appeal pursuant to § 27.440.

(c) An Initial Decision shall become a final agency action on the expiration of the time for an Appeal pursuant to § 27.445.

§ 27.445 Appeals.

(a) *Right to Appeal.* A facility or any person who has received an Initial Decision under § 27.440(a) has the right to appeal to the Under Secretary acting as a neutral appeals officer.

(b) *Procedure for Appeals.* (1) The Assistant Secretary, a facility or other person, or a representative on behalf of a facility or person, may institute an Appeal by filing a Notice of Appeal with the office of the Department headquarter designated by the Secretary.

(2) The Assistant Secretary, a facility, or other person must file a Notice of Appeal within seven calendar days of the service of the Presiding Officer's Initial Decision.

(3) The Appellant shall file with the designated office and simultaneously serve such Notice of Appeal and all subsequent filings on the General Counsel.

(4) An Initial Decision is stayed from the timely filing of a Notice of Appeal until the Under Secretary issues a Final Decision, unless the Secretary lifts the stay due to exigent circumstances pursuant to § 27.410(d).

(5) The Appellant shall file and serve a Brief within 28 calendar days of the notification of the service of the Presiding Officer's Initial Decision.

(6) The Appellee shall file and serve an Opposition Brief within 28 calendar days of the service of the Appellant's Brief.

(c) *Ex Parte Communications.* (1) At no time after the filing of a Notice of Appeal pursuant to paragraph (b)(1) of this section and prior to the issuance of a Final Decision on an Appeal pursuant to paragraph (f) of this section with respect to a facility or other person shall the Under Secretary, his designee, or any person who will advise that official in the decision on the matter, receive from or on behalf of any party, by means of an ex parte communication, information which is relevant to the decision of the matter and to which other parties have not had an opportunity to respond, a summary of such information shall be served on all other parties, who shall have an opportunity to reply to the ex parte communication within a time set by the Under Secretary or his designee.

(2) The consideration of classified information or CVI pursuant to an in camera procedure does not constitute a prohibited ex parte communication for purposes of this subpart.

(3) A facility or other person may elect to have the Under Secretary participate in any mediation or other resolution process by expressly waiving, in writing, any argument that such participation has compromised the Appeal process.

(4) The Under Secretary shall issue a Final Decision and serve it upon the parties. A Final Decision made by the Under Secretary constitutes final agency action.

(5) The Secretary may establish procedures for the conduct of Appeals pursuant to this section.

Subpart D—Other

§ 27.400 Chemical terrorism vulnerability information.

(a) *Applicability.* This section governs the collection, safeguarding, and disclosure of information and records that constitute Chemical terrorism Vulnerability Information (CVI), as defined in § 27.400(a). The Secretary shall administer this section consistent with Section 550(a) of the Homeland Security Appropriations Act of 2007, including appropriate sharing with Federal, State and local officials.

(b) *Chemical terrorism Vulnerability Information.* In accordance with Section 550(a) of the Department of Homeland Security Appropriations Act of 2007, the following information, whether transmitted verbally, electronically, or in written form, shall constitute CVI:

(1) *Security Vulnerability Assessments* under § 27.215.

(2) *Site Security Plans* under § 27.215.

(3) *Documents* relating to the Department's review and approval of

proceeding, or with any representative of such person.

(2) If, after the filing of a Notice of Appeal pursuant to paragraph (b)(1) of this section and prior to the issuance of a Final Decision on an Appeal pursuant to paragraph (f) of this section with respect to a facility or other person, the Under Secretary, his designee, or any person who will advise that official in the decision on the matter, receives from or on behalf of any party, by means of an ex parte communication, information which is relevant to the decision of the matter and to which other parties have not had an opportunity to respond, a summary of such information shall be served on all other parties, who shall have an opportunity to reply to the ex parte communication within a time set by the Under Secretary or his designee.

(2) *Controlled Persons.* Persons subject to the requirements of this section are:

(i) Each person who has a need to know CVI, as specified in § 27.400(a).

(ii) Each person who otherwise receives or gains access to what they know or should reasonably know constitutes CVI.

(3) *Duty to protect information.* A covered person must—

(i) Take reasonable steps to safeguard CVI in that person's possession or control, including electronic data, from unauthorized disclosure. When a person is not in physical possession of CVI, the person must store it in a secure container, such as a safe, that limits access only to covered persons with a need to know;

(ii) Disclose, or otherwise provide access to, CVI only to persons who have a need to know;

(iii) Refer requests for CVI by persons without a need to know to the Assistant Secretary;

(iv) Mark CVI as specified in § 27.400(f);

(v) Dispose of CVI as specified in § 27.400(k);

(vi) If a covered person receives a record or verbal transmission containing CVI that is not marked as specified in § 27.400(f), the covered person must—

(i) Mark the record as specified in § 27.400(f) of this section; and

(ii) Inform the sender of the record that the record must be marked as specified in § 27.400(f); or

(vii) If received verbally, make reasonable efforts to memorialize such information and mark the memorialized record as specified in § 27.400(f) of this section, and inform the speaker of any determination that such information warrants CVI protection;

(viii) When a covered person becomes aware that CVI has been released to

Safeguarding Information Designated As Chemical-Terrorism Vulnerability Information (CVI)

Revised Procedural Manual

September 2008



Section 550 –
Statute (Congress)

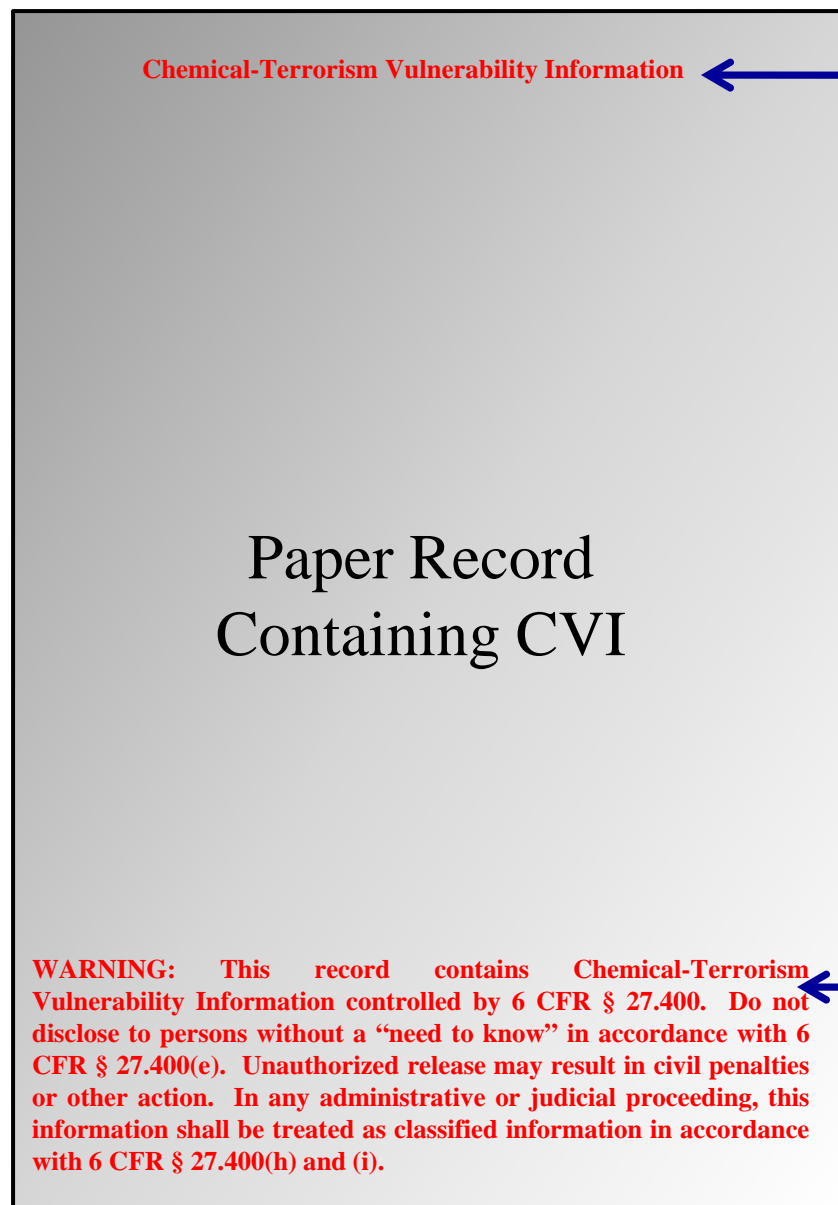
§ 27.400 –
Implementing CVI
Regulations (DHS)

CVI Guidance –
(DHS)



“Day to Day”
Compliance

MARKING CVI



Protective Marking

Distribution Limitation
Statement

MTSA v. CFATS

110TH CONGRESS
2D SESSION

H. R. 5577

To amend the Homeland Security Act of 2002 to extend, modify, and recodify the authority of the Secretary of Homeland Security to enhance security and protect against acts of terrorism against chemical facilities, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MARCH 11, 2008

Mr. THOMPSON of Mississippi (for himself, Ms. JACKSON-LEE of Texas, Mr. MARKEY, Ms. LORETTA SANCHEZ of California, Mr. DICKS, Ms. HARMAN, Mr. DEFazio, Mrs. LOWEY, Ms. NORTON, Ms. ZOE LOFGREN of California, Mrs. CHRISTENSEN, Mr. ETHERIDGE, Mr. LANGEVIN, Mr. CUELLAR, Mr. CARNEY, Ms. CLARKE, Mr. AL GREEN of Texas, Mr. PERLMUTTER, and Mr. PASCRELL) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committee on Energy and Commerce, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

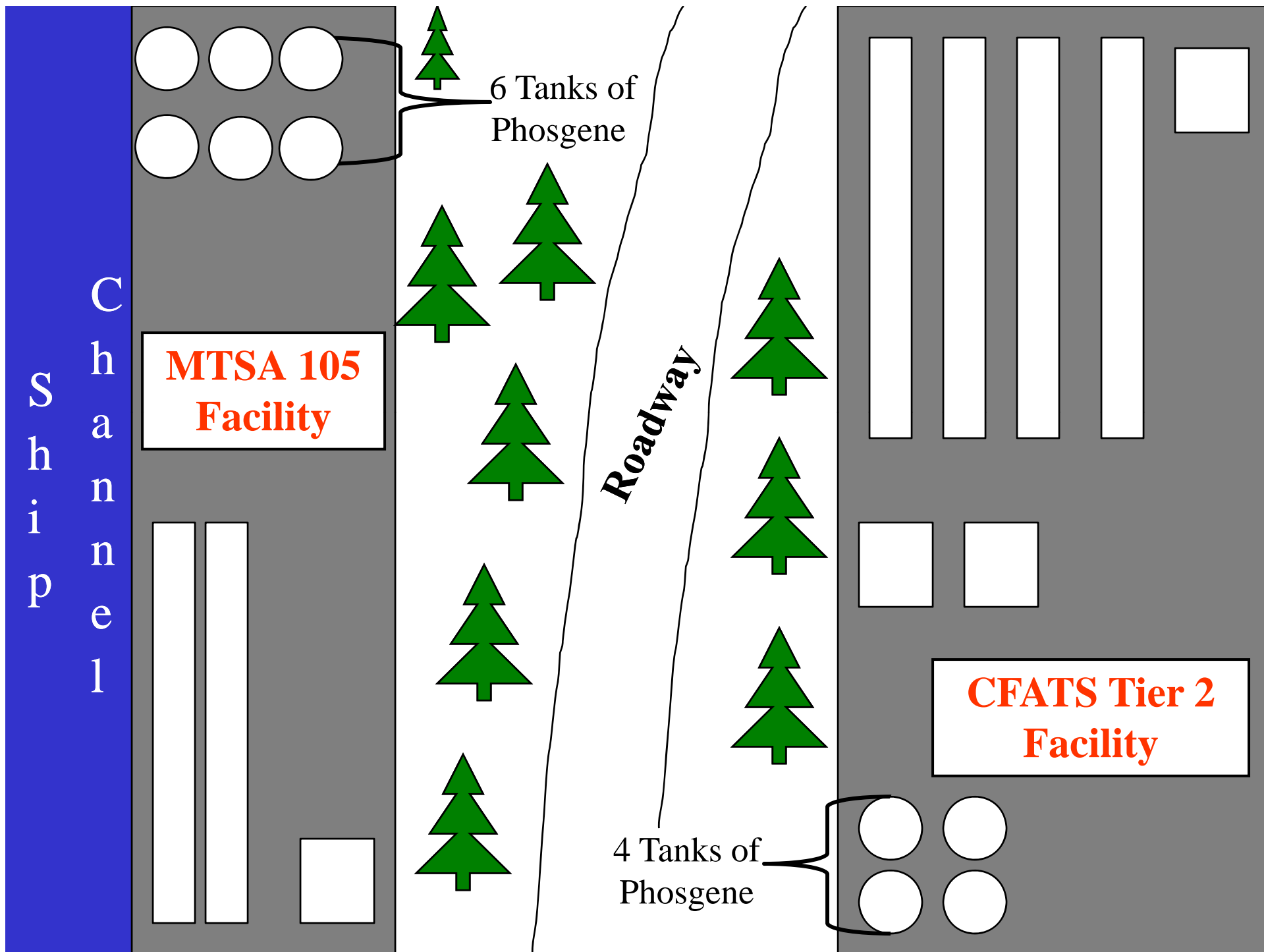
A BILL

To amend the Homeland Security Act of 2002 to extend, modify, and recodify the authority of the Secretary of Homeland Security to enhance security and protect against acts of terrorism against chemical facilities, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

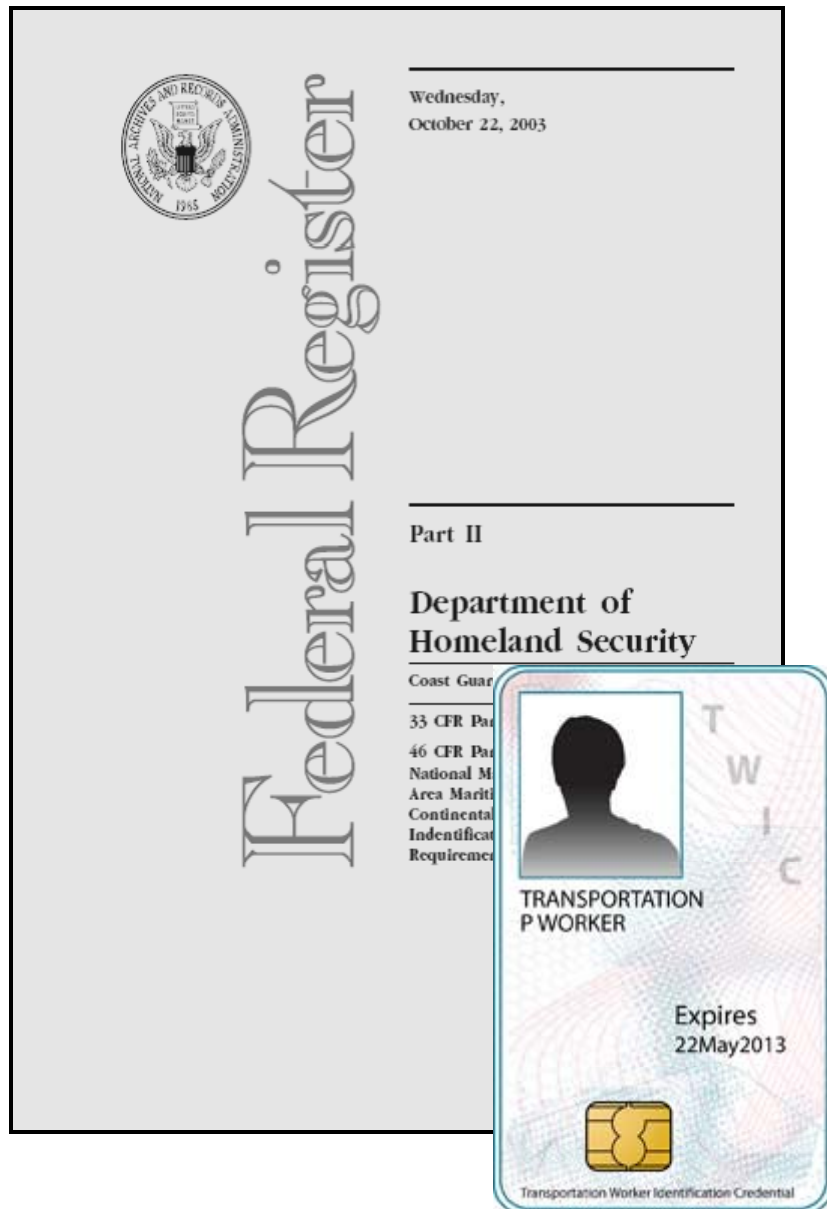
Requires facilities to submit the SVA and SSPs developed pursuant to MTSA (i.e., those facilities that are now statutorily exempt from CFATS) to DHS.

- “The Secretary shall determine the extent to which actions taken by such a chemical facility pursuant to another provision of law fulfill the requirements of this section and may require such a chemical facility to complete any additional action required by this section.”
- This could significantly increase the number of covered facilities.




Transportation Worker Identification Credential (TWIC)

The Maritime Transportation Security Act (MTSA) & TWIC



- Applies to vessels, OCS facilities, and other maritime facilities on navigable waterways.
- Requires the development of a COTP-approved Facility Security Plan (FSP). FSPs must be renewed every 5 years with the first round of renewals occurring in 2009.
- Unescorted access to certain areas of MTSA-regulated sites requires the possession of a TWIC (and hence more compliance actions).

Who Gets a TWIC?



Federal Register

Thursday,
January 25, 2007

Part II

**Department of
Homeland Security**

Coast Guard

33 CFR Parts 1, 20 et al. and 46 CFR
Parts 1, 4 et al.

Transportation Security Administration

49 CFR Parts 10, 12, and 15
Transportation Worker Identification
Credential (TWIC) Implementation in the
Maritime Sector; Final Rule
Consolidation of Merchant Mariner
Qualification Credentials; Proposed Rule

- **All credentialed merchant mariners**
- **Anyone with unescorted access to secure areas of U.S. vessels, facilities, and OCS facilities subject to 33 CFR 104, 105, and 106**
- **Vessel pilots**
- **All individuals working aboard towing vessels that push, pull, or haul alongside tank vessels.**

Who Gets a TWIC?

U.S. Department of
Homeland Security

United States
Coast Guard



Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-3PCP
Phone: (202) 372-1092
Fax: (202) 372-1906

COMDTPUB 16700.40
NVIC 03-07

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 03-07

JUL 2 2007

Subj: **GUIDANCE FOR THE IMPLEMENTATION OF THE TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC) PROGRAM IN THE MARITIME SECTOR**

Ref: a. Title 33 of the Code of Federal Regulations (33 CFR) Parts 101-106
b. Title 49 of the Code of Federal Regulations (49 CFR) Part 1515, 1540, 1570, and 1572
c. NVIC 03-03 Change 1 – Implementation of MTSA Regulations for Facilities
d. NVIC 04-03 Change 2 – Verification of Vessel Security Plans for domestic vessels in accordance with MTSA Regulations and ISPS Code
e. NVIC 05-03 – Implementation of MTSA Regulations for Outer Continental Shelf Facilities

1. **PURPOSE.** This Navigation and Inspection Circular (NVIC) provides guidance on implementation of the Final Rule – Transportation Worker Identification Credential Implementation in the Maritime Sector; Hazardous Material Endorsement for a Commercial Driver's License (72 FR 3492) (referred to as the TWIC rule) – which made major changes to 33 CFR Chapter I Subchapter H, 46 CFR Chapter I Subchapter B, and 49 CFR Chapter XII Subchapter D. The Transportation Worker Identification Credential (TWIC) will satisfy the requirement for a biometric credential as mandated by 46 U.S.C. § 70105, which was enacted by the Maritime Transportation Security Act of 2002 (MTSA) and then amended by the Security and Accountability For Every (SAFE) Port Act of 2006. The information in this NVIC details the enrollment and issuance process, provides guidance for successful execution of compliance requirements, provides clarification of the regulations found in references (a) and (b), and includes a more detailed discussion of the actions required by those regulations, with examples, to increase understanding and promote nationwide consistency. These guidelines are intended to help industry comply with the new regulations and the Coast Guard Captains of the Port (COTP) implement the TWIC Program.

- **Vessel crew**
- **Longshoremen**
- **Drayage truckers**
- **Facility employees**
- **Truckers**
- **Surveyors**
- **Agents**
- **Chandlers**
- **Port chaplains**
- **Casual laborers**
- **Other maritime professionals**

TWIC Enrollment: *Disqualifying Crimes*

	STA: Permanently Disqualifying Crimes (1572.103 et seq.)	STA: Interim (7 year) Disqualifying Crimes (1572.103 et seq.) *NOTE: No violent misdemeanors	
No waiver permitted	Espionage	Bribery	Waiver permitted
	Sedition	Extortion	
	Treason	Dishonesty, fraud, or misrepresentation, including money laundering and identity fraud, in some instances	
	Crime of terrorism (defined in 18 U.S.C. 2332(g) or comparable State law)	Immigration violations	
Waiver permitted	Crime involving a TSI (transportation security incident)	Smuggling	
	Improper transportation of a hazardous material (49 U.S.C. 5124)	Certain drug offenses	
	Unlawful activities concerning explosives	Unlawful activities involving a firearm or other weapon	
	Murder	Arson	
	Making any threat - or maliciously conveying false information known to be false - concerning the deliverance, placement, or detonation of explosive or other lethal device in/against place of public use, state or government facility, public transportation system, or infrastructure facility	Kidnapping or hostage taking	
	Certain RICO Act violations where one of the predicate acts consists of one of the permanently disqualifying crimes	Lesser violations of RICO	
		Assault with intent to kill	
		Robbery	
		Fraudulent entry into a seaport	
		Rape or aggravated sexual assault	

NOTE: Conspiracy or attempt to commit any of these crimes will also disqualify



TWIC Dashboard (Page 1 of 3)

April 2, 2009



Explanation of Dashboard

The TWIC Dashboard provides point-in-time program information on:

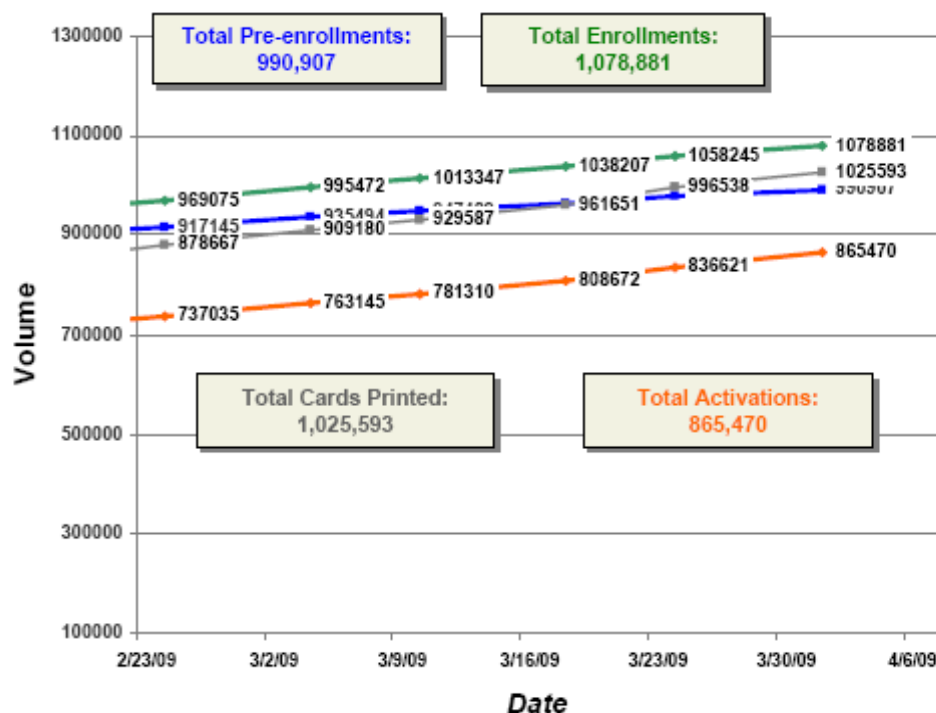
- Enrollment and adjudication-related statistics
- Graph depicting pre-enrollment, enrollment, cards printed & activated trends
- Contact information for TWIC resources
- Total enrollments and activations by location (including total enrollments broken out by occupation type)

Program Statistics

Enrollment/Activation	Measurement (as of 04/01/09)
Pre-Enrollments	990,907
Enrollments	1,078,881
Cards Printed	1,025,593
Cards Activated	865,470
Average Enrollment Time	8.83

Security Threat Assessment	Measurement (as of 03/29/09)
Initial Disqualification Letters	36,390
Appeals Requested	19,875
Appeals Granted	17,868
Waivers Requested	3,082
Waivers Granted	1,433
ALJ Review Requested/Granted	11
Final Disqualification Letters	144
Number of Expired IDTAs	10,204

Enrollment Trending



TWIC Information and Resources

Help Desk: 1-866-DHS-TWIC (1-866-347-8942)
8:00 AM ET - 12:00 AM ET
<http://twicinformation.tsa.dhs.gov/twicinfo/contact.jsp>

Website: www.tsa.gov/twic

TWIC Implementation: Can I Enroll Anyway? No.



Transportation
Security
Administration

INFORMATIONAL BULLETIN

Transportation Worker Identification Credential (TWIC) Program August 28, 2008

In response to a number of inquiries concerning TWIC requirements and the comparability between TWIC and Hazardous Materials Endorsement (HME), we are providing the following questions and answers.

Can employers require their employees to enroll for a TWIC even if their job does not require them to have unescorted access to facilities and vessels regulated by the Maritime Transportation Security Act (MTSA)?

No. All applicants must certify that they need a TWIC to perform their job. Applicants must currently be, or are applying to be, a port worker who requires unescorted access to secure areas of maritime facilities and vessels regulated by MTSA; or they are a commercial HME driver licensed in Canada or Mexico. Applicants also certify that the information they provide during the enrollment process is true, complete, and correct. If required, civil or criminal action may be taken if an individual provides false information or makes false certifications (per 49 CFR 1570.5 and 18 U.S.C. 1001).

Where in the TWIC regulation is this topic covered?

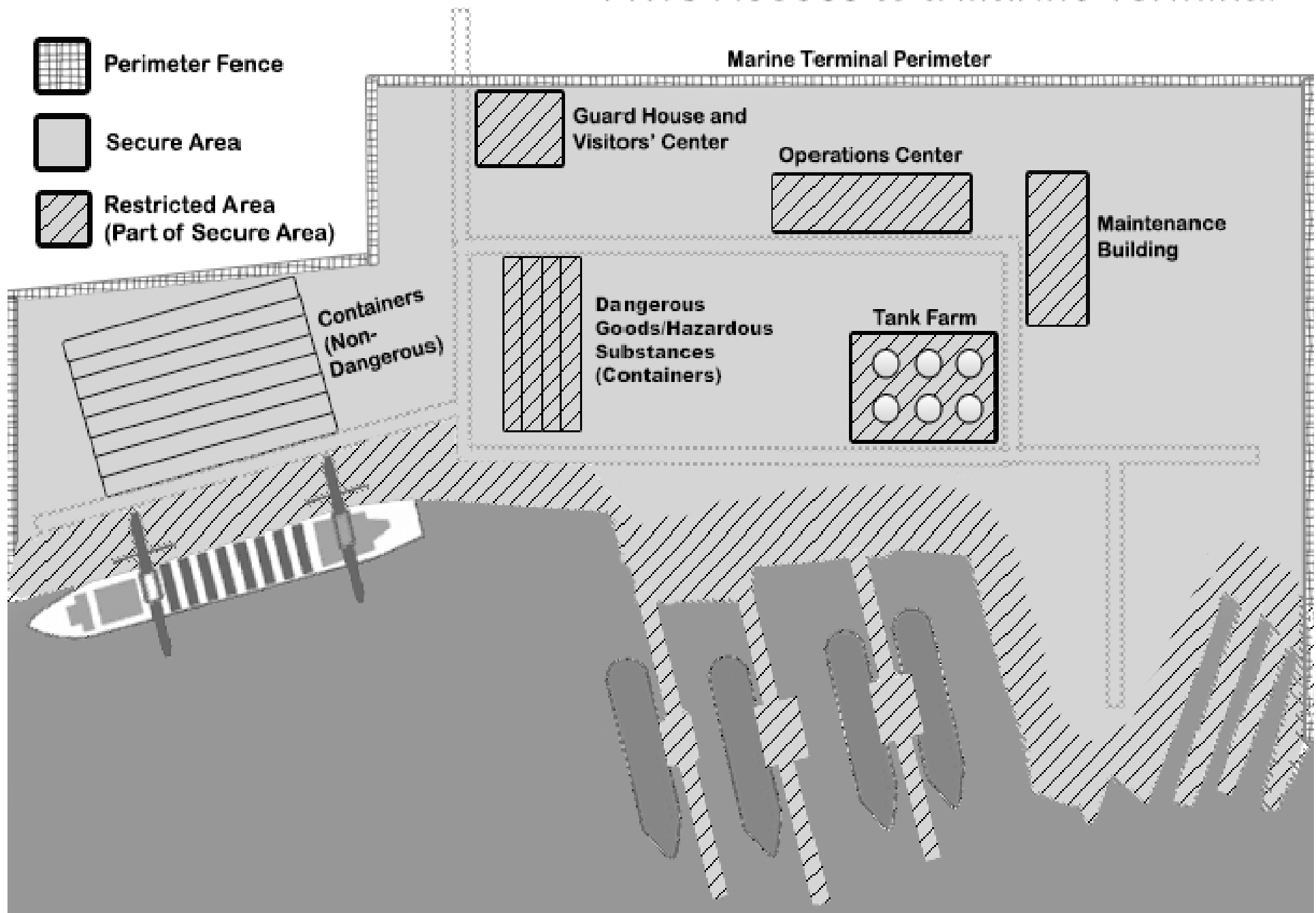
49 CFR § 1570.5 Fraud and intentional falsification of records. No person may make, cause to be made, attempt, or cause to attempt any of the following:

(a) Any fraudulent or intentionally false statement in any record or report that is kept, made, or used to show compliance with the subchapter, or exercise any privileges under this subchapter.

49 CFR § 1572.17 Applicant information required for TWIC security threat assessment.

(e) The applicant must certify the following statement in writing: As part of my employment duties, I am required to have unescorted access to secure areas of maritime facilities or vessels in which a Transportation Worker Identification Credential is required; I am now, or I am applying to be, a credentialed merchant mariner; or I am a commercial driver licensed in Canada or Mexico transporting hazardous materials in accordance with 49 CFR 1572.201.

TWIC Access to a Marine Terminal



TWIC/MTSA POLICY ADVISORY COUNCIL

January 7, 2008

Redefining Secure Areas and Acceptable Access Control 01-08

Background: The TWIC final rule allows facility owners and operators to redefine their secure areas for purposes of TWIC. However, it is unclear which facilities may redesign their secure areas, and how much of the previously included facility area can be excluded through redesignation.

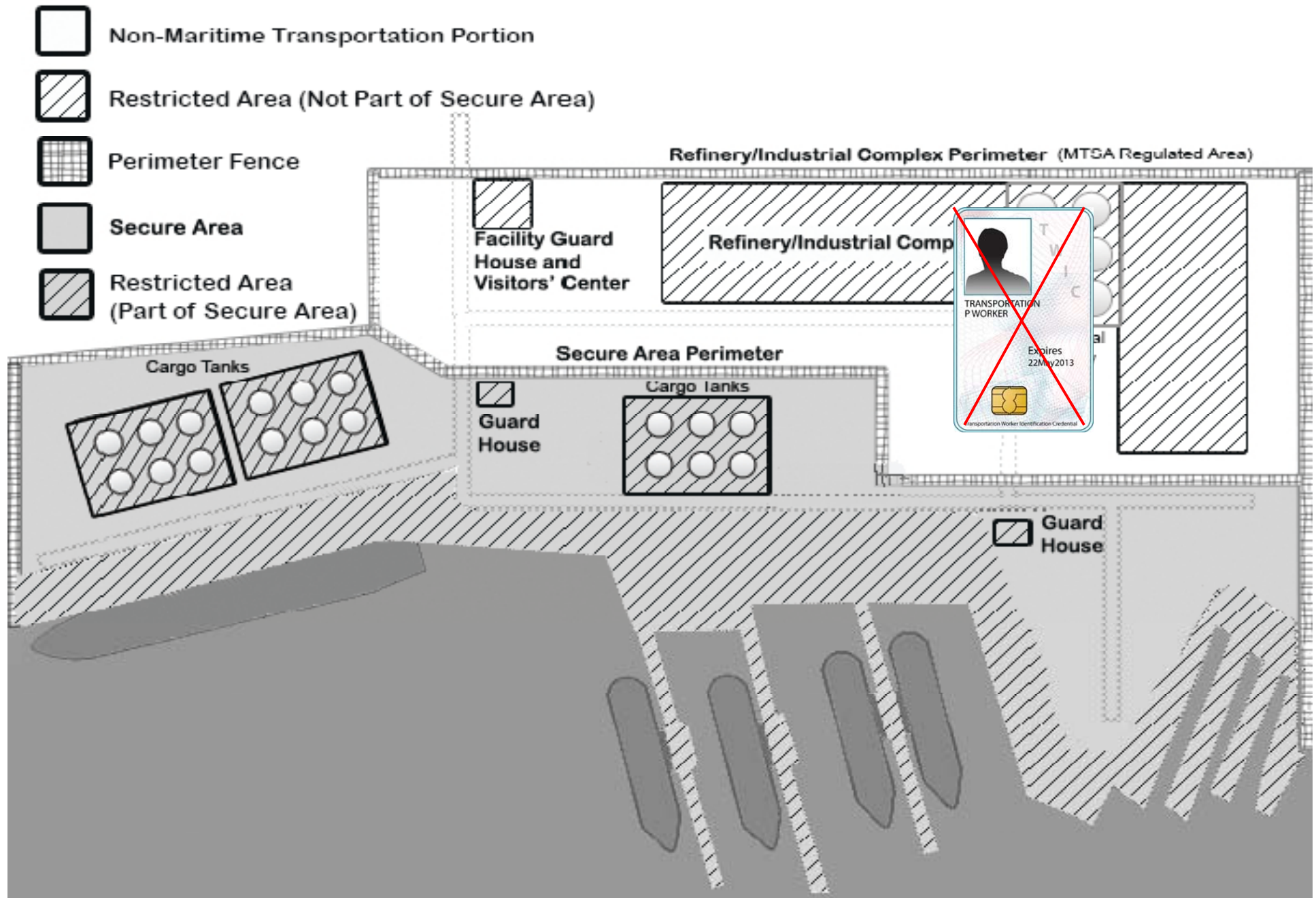
Issues:

- If certain mixed-use MTSA facilities are allowed to redefine their secure area for TWIC purposes, what guidelines should they use during their redesignation?
- What measures will be expected/accepted by the USCG for access control to these newly defined secure areas?

TWIC/MTSA Policy Advisory Council discussion: The USCG employs a 3-step process for determining whether to approve amendments to a Facility Security Plan:

1. Does the facility have a significant non-maritime transportation related portion?
 1. Yes → proceed to Step 2
 2. No → deny the request
2. Is the area to be excluded non-maritime transportation related?
 1. Yes → approve the request
 2. No → deny the request
 3. Yes and no → proceed to Step 3
3. Is the area to be excluded at risk of a TSI (transportation security incident)?
 1. No → approve the request
 2. Yes → deny the request and/or ask for differently defined secure area

TWIC Access to Marine Terminal in a Refinery/Industrial Complex

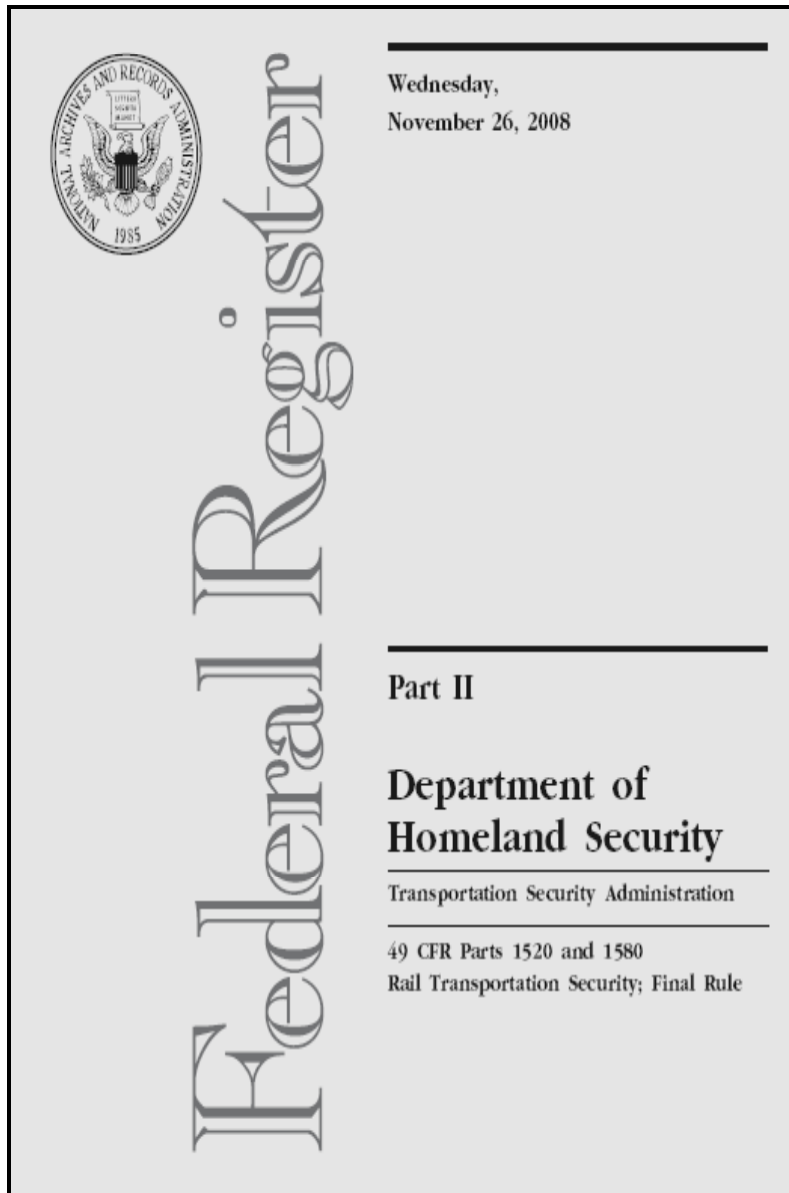


Rail Hazmat

Rail Security Considerations – Toxic Inhalation Hazards (TIH) – Regulation Took Effect on 12/26/08

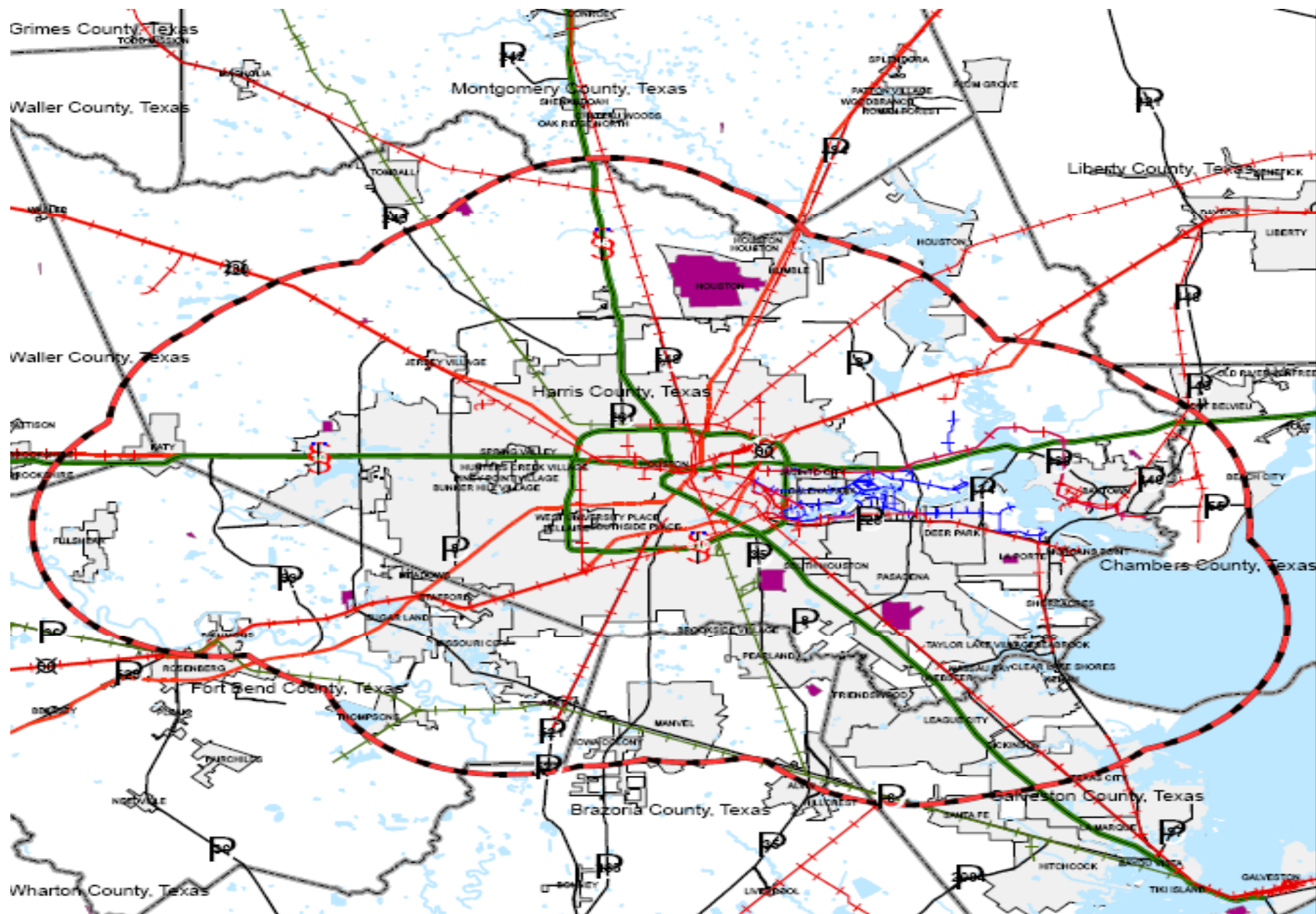


TSA Rail Regulations




- Applies to rail as well as select facilities that ship and receive certain classes and quantities of hazmat → Could include a facility within a port complex.
- New security obligations include the appointment of a Rail Security Coordinator, chain of custody & control procedures, and the reporting of significant security concerns, among other things.
- Designates 46 High-Threat Urban Areas.

Houston HTUA



SSI: MTSA and Rail Applicability



Federal Register

Wednesday,
November 26, 2008

Part II

**Department of
Homeland Security**

Transportation Security Administration

49 CFR Parts 1520 and 1580
Rail Transportation Security; Final Rule



Chapter XII—Transportation Security Administration, Department of Homeland Security

PART 1520—PROTECTION OF SENSITIVE SECURITY INFORMATION

1. The authority citation for part 1520 continues to read as follows:

Authority: 46 U.S.C. 70102–70106, 70117; 49 U.S.C. 114, 40113, 44901–44907, 44913–44914, 44916–44918, 44935–44936, 44942, 46105.

2. In § 1520.3, add definitions of “Rail hazardous materials receiver,” “Rail hazardous materials shipper,” “Rail facility,” “Rail secure area,” “Rail transit facility,” “Rail transit system,” “Railroad,” and “Railroad carrier,” amend the definition of “Vulnerability assessment” to read as follows, and insert in alphabetical order:

Homeland Security Laws and Regulations: Current and Anticipated Issues for the Port Attorney and Risk Manager

Presented to the:



April 17, 2009