PRIVACY & DATA SECURITY LAW JOURNAL

VOLUME 2 NUMBER 10 SEPTEMBER 2007

Homeland Security Information Sharing: Protections for Private Sector Information

JOE WHITLEY, GRACE MASTALLI, AND JUSTINA SESSIONS

"Information sharing underpins any true partnership and is necessary to mitigate the threat posed by a cunning, adaptive, and determined enemy."[1]

We must begin to think differently about national security and who is responsible for it.[2] Eighty five percent of the nation's critical infrastructure — the financial, transportation, telecommunications, energy, and emergency services we depend upon — is controlled by the private sector.[3] As the private sector and government have become increasingly interdependent, their abilities to assess vulnerabilities and mitigate the consequences of natural disasters, accidents, and terrorist attacks have become intertwined as well. Homeland security offi-

---

Joe Whitley, former General Counsel of the Department of Homeland Security, is a partner with Alston & Bird LLP. Grace Mastalli, former Director of the Homeland Security Department's Information Sharing and Collaboration Office, is president of Ethos International, Inc., in Washington, D.C. Justina Sessions is a student at the University of Michigan Law School. The authors are grateful to the members and staff of both the Interagency Working Group on SBU and the SBU Coordinating Committee for their efforts to improve government information management.

cials must be able to obtain and protect from public disclosure information on privately held infrastructure and other vulnerabilities. The safety of the nation depends on the ability of companies and government agencies to cooperate, share, and safeguard homeland security-related information.

Despite the benefits of information sharing, companies have been understandably reluctant to provide information to the government. Since much homeland security-related information is also proprietary and business sensitive, private entities are rightly concerned that such information could be disclosed either unintentionally or under compulsion by the courts or through open government laws.[4]

EXECUTIVE SUMMARY

In an effort to strike the necessary balance between "sharing the information that needs to be shared and protecting the information that needs to be protected,"[5] the federal government has developed a number of protection systems for sensitive but unclassified homeland security-related information. Three of the better-known regimes are Protected Critical Infrastructure Information (PCII), Sensitive Security Information (SSI) and Chemical-Terrorism Vulnerability Information (CVI). The Department of Homeland Security (DHS) has lead responsibility for all three of these information control, marking, and handling programs. PCII, SSI, and CVI are shielded from public disclosure under the Freedom of Information Act[6] (FOIA) and other laws and are subject to detailed procedures regarding how that information may be shared among government entities and with the general public. The specific requirements of the regulations governing these types of information are outlined in the table at the end of this article.

Although these safeguards and protections are significant, they are neither fail-safe nor permanent. Potentially, such information may be used in certain judicial and administrative proceedings. Also, data protections and security are only as good as the users' own compliant behavior. Moreover, Congress is reevaluating the disclosure protections given to these types of information and pressuring the Administration to issue its

final recommendations for reform of controlled unclassified information (CUI) pursuant to Guideline 3 of the President's December 16, 2005 Memorandum for the Heads of Executive Departments and Agencies.[7] The protections for SSI were significantly altered by Congress in 2006. In the coming months, it can be anticipated that Congress may consider elimination of the CVI category; amendment of FOIA may be proposed to cut back on the disclosure exemptions afforded PCII, SSI, and CVI; and the Guideline 3 Report recommendations applicable to homeland security, terrorism, and law enforcement CUI will be issued.

PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

The Critical Information Infrastructure Act of 2002[8] (the CII Act) created the PCII framework. It was designed to encourage the submission of Critical Infrastructure Information[9] (CII) to DHS by implementing handling safeguards, restrictions on distribution, and protections from disclosure of CII voluntarily submitted to DHS.

PCII Protections

The Department of Homeland Security regulation regarding CII (the "CII Final Rule") sets out specific physical and procedural safeguards against accidental disclosure of PCII and affords several protections against disclosure of information classified as PCII.[10] Once information is classified as PCII, it does not lose these protections unless a change of status is requested by the submitter and the PCII Office determines that the information was in the public domain at the time it was submitted.[11]

- **Marking and Handling.** PCII must be clearly marked as such, stored in a secure environment, and destroyed in a way that prevents retrieval.[12]
- **FOIA Exemption and Preemption of State and Local Open Records Laws.** PCII is exempt from disclosure under FOIA and from any similar state or local laws that require disclosure of information.[13]
- **Ex Parte Exclusion.** PCII is not subject to any rules or judicial doc-

trine regarding ex parte communications with decision-making officials.[14] Communications with DHS officials regarding PCII do not become public record.

- **Civil Liability Protection**. PCII cannot be used directly in any civil action by a third party, including government entities.[15] DHS interprets this to mean that PCII is neither discoverable nor admissible as evidence in civil litigation.[16]
- **Restrictions on Sharing and Use**. The CII Final Rule describes the circumstances under which DHS may share PCII with other government entities and with the general public. Disclosure of PCII must be authorized by the PCII Program Manager, the Under Secretary for Preparedness, and the Assistant Secretary for Infrastructure Protection.
  - *Sharing with the government*. PCII may be shared with federal, state, and local government entities for the purpose of protecting critical infrastructure and in furtherance of the investigation or prosecution of a criminal act.[17] State and local governments may not further disclose PCII except to parties already authorized to receive PCII.[18]
  - *Sharing with government contractors*. PCII may be shared with federal, state, and local government contractors only with the permission of the PCII Program Manager and only for appropriate purposes under the CII Act. Employees of government contractors who will handle PCII must sign individual nondisclosure agreements.[19]
  - *Sharing with the public*. PCII may be used to prepare warnings and alerts directed to companies, targeted sectors and the general public. When issuing these warnings, DHS must take care to protect from disclosure any information that is business sensitive or might be used to identify the submitting entity.[20]

Exceptions to PCII Protections

The CII Final Rule provides several exceptions to the disclosure protections.

- **Use in Criminal Proceedings**. PCII may be disclosed in furtherance of a criminal investigation or prosecution, when the disclosure is coordinated by a federal law enforcement official.[21]
- **Communication with Submitting Entities**. PCII may be disclosed in order to communicate with a person who has submitted PCII about that submittal.[22]
- **Congress and the Comptroller General**. PCII may be disclosed by an officer or employee of the United States (1) to either House of Congress and to committees thereof; or (2) to the Comptroller General, in the course of the duties of the General Accountability Office.[23]
- **DHS Inspector General**. PCII may be disclosed to the DHS Inspector General for the purposes outlined in the CII Act.[24]

SENSITIVE SECURITY INFORMATION

SSI is information related to transportation security, obtained or created by the Transportation Security Administration (TSA)[25] or the Department of Transportation (DOT). The rule governing SSI[26] (the SSI Interim Final Rule) was implemented to protect the confidentiality of SSI and reduce the ability of terrorists to obtain information regarding transportation security practices and vulnerabilities.

SSI Protections

The disclosure protections for SSI are significantly weaker than those for PCII. They consist primarily of a FOIA exemption and restrictions on the sharing and use of information. TSA[27] may determine at any time that information no longer meets the criteria for SSI.[28]

- **Marking and Handling**. SSI must be clearly marked as such, stored in a locked container, and destroyed in a way that precludes recognition or reconstruction.[29]
- **FOIA Exemption**. SSI is exempt from public inspection or copying under FOIA, the Privacy Act,[30] and other laws.[31] However, if a document contains information that is SSI and information that is not SSI, TSA may disclose the document with the SSI portion redacted.[32] Section 525 of the Homeland Security Appropriations Act of 2007[33] limited the SSI FOIA exemption in two ways:
  - *Automatic reexamination of status upon request for release.* When a request is made for a document containing SSI, "the document shall be reviewed in a timely manner to determine whether any information contained in the document meets the criteria for continued SSI protection" and "all portions that no longer require SSI designation [shall] be released."[34]
  - *Release after three years.* SSI that is three years old and is not incorporated into a current transportation security directive, contingency plan, or information circular and does not contain current information in particular sectors is subject to release unless the Secretary of TSA makes a written determination that there is a rational reason that the information must remain SSI.[35]
- **Restrictions on Sharing**. SSI may only be shared with persons with a "need to know." A person has a need to know SSI when the person (1) needs access to SSI to carry out transportation security activities, is in training to carry out such activities, and is supervising individuals carrying out such activities; or (2) needs SSI to provide technical or legal advice to a covered person[36] regarding transportation security requirements of federal law and needs the information to represent a covered person in connection with any judicial or administrative proceeding regarding those requirements.[37] DHS may also further restrict who has the need to know specific SSI.[38]
  - *Sharing with federal employees.* A federal employee has a need to know SSI if the employee requires access to the information for performance of official duties.[39]

– *Sharing with contractors.* A DHS or DOT contractor has a need to know SSI if the contractor requires access to the information for performance of the contract.[40]

Exceptions to SSI Protections

The SSI Interim Final Rule provides exceptions for disclosure to persons otherwise without a need to know SSI.

- **Civil Proceedings.** SSI will be disclosed to a party (or counsel) in a federal civil proceeding where the party demonstrates "substantial need of relevant SSI in the preparation of the party's case and that the party is unable without undue hardship to obtain the substantial equivalent of the information by other means," unless TSA or DHS can demonstrate that such disclosure presents a risk of harm to the nation.[41]
- **Administrative Enforcement Proceedings.** SSI may be provided to a person when access to SSI is necessary for the person to prepare a response to an allegation in a legal enforcement action document issued by TSA.[42]
- **Congress and the Comptroller General.** SSI may be disclosed to a committee of Congress authorized to have the information and to the Comptroller General.[43]
- **Conditional Disclosure.** TSA may disclose specific SSI when it determines that such disclosure would not be detrimental to transportation security.[44] For example, TSA discloses the requirement that airlines ask for identification upon passenger check-in, even though the information is SSI.

CHEMICAL-TERRORISM VULNERABILITY INFORMATION

DHS promulgated regulations relating to chemical facility anti-terrorism standards in April of 2007 (CFATS),[45] including a section on the protection of CVI. CVI is information relating to vulnerability and security

that is exchanged between DHS and facilities that produce or handle potentially dangerous quantities of chemicals.[46]

CVI Protections

The disclosure protections for CVI are similar to, but somewhat broader than, those afforded to SSI and include a FOIA exemption, restrictions on the sharing of information, and restrictions on the use of CVI in judicial proceedings.

- **Marking and Handling**. CVI must be clearly marked as such, stored in a secure container, and destroyed in a way that precludes recognition or reconstruction.[47]
- **FOIA Exemption**. CVI is exempt from public inspection or copying under FOIA, the Privacy Act, and other laws.[48] However, if a document contains information that is CVI and information that is not CVI, DHS may disclose the document with the CVI portion redacted.[49]
- **Restrictions on Sharing**. CVI may only be shared with persons with a "need to know." A person has a need to know CVI when the person (1) needs access to CVI to carry out chemical facility security activities, is in training to carry out such activities, or is supervising individuals carrying out such activities; (2) needs CVI to provide technical or legal advice to a "covered person" (each person with a need to know CVI or who otherwise receives or gains access to CVI) regarding chemical facility security requirements of federal law; or (3) is determined to have a need to know by DHS. DHS may also further restrict who has the need to know specific CVI.[50]
  - *Sharing with federal employees*. A federal employee has a need to know CVI if the employee requires access to the information for performance of official duties.[51]
  - *Sharing with contractors*. A DHS contractor has a need to know CVI if the contractor requires access to the information for performance of the contract.[52]

- **Restrictions on Use in Judicial Proceedings.** CVI is not available in any civil or criminal litigation, unless otherwise provided for by the Secretary of DHS.[53]

Exceptions to CVI Protections

CFATS provides a narrow exception for disclosure to persons without a need to know CVI, for use in the context of specific administrative and judicial enforcement proceedings. This disclosure is not mandatory — it is at the discretion of the Secretary of DHS.

- **Judicial and Administrative Enforcement Proceedings.** The Secretary of DHS may, in the context of a judicial or administrative enforcement proceeding of Section 550 of the Homeland Security Appropriations Act of 2007,[54] provide access to persons involved in the proceeding.[55]

INTERACTION AMONG PROTECTIONS

The interplay among these protections has not been tested and remains unclear. SSI or CVI that was voluntarily submitted to the government theoretically could also be designated as PCII. Information receiving a PCII and either SSI or CVI designation should be afforded the more stringent protections of PCII.[56] In practice, however, multiple designation markings may cause confusion in handling.

THE FUTURE OF HOMELAND SECURITY INFORMATION PROTECTIONS

Although the Homeland Security Act as initially enacted included a number of information-sharing and control initiatives, these and other information-protection provisions, have only recently garnered much public attention.[57] On the one hand, many — including Congress, businesses, and open government advocates — have focused on the disclosure exemptions for sensitive information. On the other hand, privacy advo-

cates, intelligence reform supporters, state and local officials, and Executive Branch agencies have been concentrating on the improved control of sensitive unclassified information.[58] Within the foreseeable future, Congress and the Executive Branch both are expected to further change federal policies related to safeguarding and protecting shared terrorism, law enforcement, and homeland security information.

- **SSI Has Been Significantly Weakened**. The Homeland Security Administration Appropriations Act of 2007 significantly weakened the protections afforded to SSI. A designation of information as SSI must be re-examined upon an FOIA request, and any information that no longer meets the SSI criteria is released. Information also loses its presumption of protection after three years and is no longer exempt from disclosure unless DHS makes an express determination that it must be exempt.[59]
- **CVI May Be Eliminated**. DHS's authority to regulate CVI expires in 2009, but significant changes to the chemical facility antiterrorism standards are likely to arise even before then. Representative Jackson-Lee of Texas has proposed the Chemical Facility Security Improvement Act of 2007,[60] which would eliminate CVI classification altogether and make chemical facility information SSI. Although the bill is currently in a subcommittee and may not survive, it is an indication that future changes to the CVI regime are likely.
- **FOIA May Be Modified**. Many Members of Congress perceive an erosion of FOIA and may attempt to limit the FOIA protections given to PCII. Recently, the Freedom of Information Act Amendments of 2007[61] passed in the House. The amendments impose tighter deadlines on agencies to respond to FOIA requests and require reports from the Comptroller General on the number of people who have submitted information under the CII program, the number of requests for access to information granted or denied, and an examination of whether nondisclosure of information has led to increased protection of critical infrastructure. The Senate passed a similar bill, the Openness Promotes Effectiveness in our National Government Act on August 3, 2007,[62] to which the Administration strongly objects.[63]

- **Controlled Unclassified Information ("CUI") Framework May Be Adopted**. CUI is the new federal designation to be given to certain data that by law or policy requires protection, safeguarding, and controls relating to access, distribution, or dissemination and that may not meet the standards for national security classification under Executive Order 12958,[64] as amended. The CUI recommendations are expected to propose a governance regime and policy framework for information within the scope of the Information Sharing Environment (ISE).[65] Congress is likely to consider more sweeping reforms than those recommended in the final Guideline 3 report. DHS will be one of many agencies required to implement the CUI framework, but by definition much of the Department's sensitive information, including CVI, SSI, and PCII, falls within the scope of the ISE.

CONCLUSION

Sharing of sensitive information regarding the security and vulnerability of critical infrastructures, such as financial, transportation, telecommunications, energy, health, and chemical facilities, is essential to homeland security. Companies can only be expected to provide this sensitive information voluntarily, however, if they are confident that it will be protected from public disclosure and will not be inappropriately shared. Presently, the PCII, SSI, and CVI programs provide some, but not absolute, protection for such sensitive information. The very complexity of these specialized information access and control regimes may limit their utility while at the same time making them vulnerable to criticism.

In the coming months, Congress will consider elimination of the CVI category; FOIA amendments will be proposed to cut back on the disclosure exemptions afforded PCII, SSI, and CVI; and the Administration's Guideline 3 Report[66] on standardizing marking and handling procedures applicable to shared homeland security, terrorism, and law enforcement CUI will be issued. The CUI recommendations are expected to propose a governance regime and policy framework initially mandated only for information within the scope of the ISE. Carefully designed and implemented CUI reforms have the potential of reducing costs while improving

the effectiveness of information control. DHS, although only one of many agencies to be covered by the CUI framework, will be among the most heavily involved in implementation.

Businesses possessing sensitive homeland security-related information must appreciate the complexity of the existing legal regimes and the dynamic policy environment in which changes will be made. Private sector stakeholders need to engage in the policy process to address FOIA-related legislative actions and other challenges to achieving the right balance among competing interests.

Information Protection Regulations

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520[67] and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
Definition: Designation			
Definition	Validated Critical Infrastructure Information[68] that is voluntarily submitted to DHS. (§29.2(g))	Information obtained or developed in the conduct of security activities, including research and development, including: (1) security programs and contingency plans; (2) security directives; (3) information circulars; (4) performance specifications; (5) vulnerability assessments; (6) security inspection or investigative information; (7) threat information; (8) security mea-	(1) Security Vulnerability Assessments;[69] (2) Site Security Plans;[70] (3) documents relating to DHS's review and approval of Security Vulnerability Assessments and Site Security Plans; (4) Alternative Security Programs;[71] (5) documents relating to inspection or audits; (6) any records required to be created or retained under §

Information Protection Regulations, cont.

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520 and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
		sures; (9) security screening information; (10) security training methods; (11) identifying information of certain transportation security personnel; (12) critical aviation or maritime infrastructure asset information; (13) systems security information; (14) confidential business information; (15) research and development; and (16) other information that TSA determines is SSI. (§ 1520.6(a);(b))	27.255; (7) sensitive portions of orders, notices, or letters; (8) information developed pursuant to §§ 27.200 and 27.205; and (9) other information developed for chemical facility security purposes that the Secretary determines is similar to other SSI. (§ 27.400(b))
Requirements for designation	Information must be: (1) voluntarily submitted; (2) submitted for protected use regarding the security of critical infrastructure or protected systems, analysis, warning, interdependency study, recovery, reconstitution, and other appropriate	Determination by TSA that the disclosure of the information would (1) constitute an unwarranted invasion of privacy; (2) reveal trade secrets or privileged or confidential information obtained from any person; or (3) be detrimental to the	Must fall into one of the categories above or be designated as CVI by the Secretary of DHS.

Information Protection Regulations, cont.

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520 and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
	purposes, including, without limitation, for the identification, analysis, prevention, preemption, disruption, defense against and/or mitigation of terrorist threats to the homeland; (3) the information is labeled with an express statement that it is submitted in expectation of protection from disclosure; (4) accompanied by a statement containing the submitting person's or entity's contact information and certifying that the information being submitted is not customarily in the public domain. (§ 29.5(a))	security of transportation. (§ 1520.5(a))	
Protection while under consideration for designation	All information submitted under the proper procedures will be treated and protected as PCII until a final deter-		

Information Protection Regulations, cont.

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520 and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
	mination to the contrary has been made. (§ 29.6(b))		
Marking	"This document contains PCII. In accordance with the provisions of 6 C.F.R. Part 29, this document is exempt from release under the Freedom of Information Act (5 U.S.C. 552(b)(3)) and similar laws requiring public disclosure. Unauthorized release may result in criminal and administrative penalties. This document is to be safeguarded and disseminated in accordance with the CII Act and the PCII Program requirements." (§ 29.6(c))	"WARNING: This record contains Sensitive Security Information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed 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 the U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520." (§ 1520.13)	"WARNING: This record contains Chemical-terrorism Vulnerability Information controlled by 6 C.F.R. 27.400. Do not disclose to persons without a 'need to know' in accordance with 6 CFR 27.400(e). Unauthorized release may result in civil penalties or other action. In any administrative or judicial proceeding, this information shall be treated as classified information in accordance with 6 C.F.R. 27.400(h) and (i)." (§ 27.400(f)(3)).

Information Protection Regulations, cont.

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520 and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
Change of status	Status changes may only take place when the submitting person or entity requests in writing that the information no longer be protected under the CII Act; or when the PCII Program Office determines that the information was, at the time of the submission, customarily in the public domain. (§ 29.6(g))	TSA or the Coast Guard may determine in writing that information is no longer SSI (§ 1520.6(c)). Sensitive security information that is three years old and not incorporated in a current transportation security directive, security plan, contingency plan, or information circular; or does not contain current information in particular SSI categories shall be subject to release upon request unless: (1) the secretary or his designee makes a written determination that identifies a rational reason why the information must remain SSI; or (2) such information is otherwise exempt from disclosure under applicable law. (H.R. 5441 § 525(a)(2))	

Information Protection Regulations, cont.

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520 and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
Relationship with Other Protections			
Relationship with other protected information	If classified as PCII, information will enjoy that protection regardless of other classifications.	In the case of information that both is SSI and has been designated as critical infrastructure information under Section 214 of the Homeland Security Act, any covered person who is a federal employee in possession of such information must comply with the disclosure restrictions and other requirements applicable to such information under Section 214 and any implementing regulations. (§ 1520.9(d))	In the case of information that is CVI and also has been designated as critical infrastructure information under Section 214 of the Homeland Security Act, any covered person in possession of such information must comply with the disclosure restrictions and other requirements applicable to such information under Section 214 and any implementing regulations. (§ 27.400(d)(8))
Use of Information			
Use of information by regulatory and other federal, state, and local agencies	An agency that receives PCII may use the PCII only for purposes appropriate under the CII Act, including securing critical		

Information Protection Regulations, cont.

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520 and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
	infrastructure or protected systems. (§ 29.3(b))		
Safeguards and Handling			
Responsibility for safeguarding	Each person who works with PCII is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it. (§ 29.7(a))	A covered person[72] must comply with the handling requirements of § 1520.9.	A covered person[73] must comply with the handling requirements of § 27.400(d).
Handling and storage	When PCII is in the physical possession of a person, reasonable steps shall be taken, in accordance with the procedures prescribed by the PCII Program Manager, to minimize the risk of access to PCII by unauthorized persons. When PCII is not in the physical possession of a person, it shall be stored in a secure environment. (§ 29.7(c))	A covered person must take reasonable steps to safeguard SSI in that person's possession or control from unauthorized disclosure. When a person is not in physical possession of SSI, the person must store it in a secure container, such as a locked desk or file cabinet or in a locked room. (§ 1520.9(a)(1)) Subject to the	A covered person must 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. (§§ 27.400(d)(1) and (2))

Information Protection Regulations, cont.

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520 and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
Disposal and destruction	Documents and material containing PCII may be disposed of by any method that prevents unauthorized retrieval, such as shredding or incineration. (§ 29.7(e))	requirements of the Federal Records Act, DHS destroys SSI when no longer needed to carry out the agency's function (§ 1520.19(a)). A covered person must destroy SSI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the SSI to carry out transportation security measures. (§ 1520.19(b))	Subject to the requirements of the Federal Records Act, the DHS destroys CVI when no longer needed to carry out the agency's function. A covered person must destroy SSI completely to preclude recognition or reconstruction of the information when the covered person no longer needs the CVI to carry out security measures. (§ 27.400(k))
Disclosure			
Generally; FOIA exemption	Information is exempt from FOIA and any state or local law requiring disclosure of records or information. (§ 29.8(g))	Information is exempt from FOIA, the Privacy Act, and other laws; released only to persons with a need to know. (§ 1520.5) But, when a FOIA request is made, the document shall be	Information is exempt from FOIA, the Privacy Act, and other laws; released only to persons with a need to know. (§ 27.400(g)(1))

Information Protection Regulations, cont.

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520 and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
		reviewed to determine whether any information contained in the document meets the criteria for continued SSI protection. All portions that no longer require SSI designation shall be released. (H.R. 5441 § 525(a)(1))	
Sharing with federal government employees	The PCII Program Manager or the PCII Program Manager's designees may provide PCII to an employee of the federal government, provided that such information is shared for purposes of securing the critical infrastructure or protected systems, analysis, warning, interdependency study, recovery, reconstitution, and for another appropriate purpose including, without limitation, the identification,	SSI may only be disclosed to a covered person with a need to know. A federal employee has a need to know SSI if access to the information is necessary for performance of the employee's official duties. (§ 1520.12(b)(1))	CVI may only be disclosed to a person with a need to know. A federal employee has a need to know CVI if access to the information is necessary for performance of the employee's official duties. (§ 27.400(e)(2)(i))

Information Protection Regulations, cont.

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520 and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
	analysis, prevention, preemption and/or disruption of terrorist threats to the homeland. (§ 29.8(b))		
Collateral regulatory purposes	PCII may not be used, directly or indirectly, for any collateral regulatory purpose. (§ 29.8(b))		
Sharing with state and local government	PCII may be provided to a state or local government entity for the purpose of protecting critical infrastructure or protected systems and in furtherance of an investigation or the prosecution of a criminal act. (§ 29.8(b))	Person must have a need to know.	A person, including a state or local official, has a need to know CVI when: (1) the person requires access to specific CVI to carry out chemical security activities, is in training to do so, or the information is necessary for the person to supervise or manage individuals carrying out such activities; (2) the person needs the information to provide technical or legal advice to a covered person, who has a

Information Protection Regulations, cont.

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520 and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
			need to know the information, regarding security requirements of federal law; or (3) DHS determines that access is required under §§ 27.400(h) or 27.400(i) in the course of a judicial or administrative proceeding. (§ 27.400(e))
Disclosure to government contractors	May be disclosed to contractors when necessary for an appropriate purpose under the CII Act. The contractor's employees who will be handling PCII must sign individual nondisclosure agreements to receive PCII. (§ 29.8(c))	A person acting in the performance of a contract with or grant from DHS or DOT has a need to know SSI if access to the information is necessary to performance of the contract or grant. (§ 1520.12(b)(2))	A person acting in the performance of a contract with or grant from DHS has a need to know CVI if access to the information is necessary to performance of the contract or grant. (§ 27.400(e)(2)(ii))
Disclosure to others	PCII may be used to prepare advisories, alerts, and warnings to relevant companies, targeted sectors,	A person has a need to know SSI when: (1) the person requires access to specific SSI to carry out aviation	A person has a need to know CVI when: (1) the person requires access to specific CVI to carry out chemical

Information Protection Regulations, cont.

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520 and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
	governmental entities, information sharing and analysis organizations, or the general public regarding potential threats and vulnerabilities to critical infrastructure as appropriate pursuant to the CII Act. (§ 29.8(e))	or maritime transportation security activities, is in training to do so, or the information is necessary for the person to supervise or manage individuals carrying out such activities; or (2) the person needs the information to provide technical or legal advice to a covered person regarding security requirements of federal law and needs the information to represent a covered person in a judicial or administrative proceeding regarding those requirements. (§ 1520.12(1))	security activities, is in training to do so, or the information is necessary for the person to supervise or manage individuals carrying out such activities; (2) the person needs the information to provide technical or legal advice to a covered person, who has a need to know the information, regarding security requirements of federal law; or (3) DHS determines that access is required under §§ 27.400(h) or 27.400(i) in the course of a judicial or administrative proceeding. (§ 27.400(e))
Ex parte communications	PCII is not subject to any agency rules or judicial doctrine regarding ex parte communications with a decision-making official. (§ 29.8(h))		

Information Protection Regulations, cont.

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520 and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
Use in judicial proceedings	PCII shall not, without the written consent of the person or entity submitting such information, be used directly by any federal, state, or local authority and by any other third party, in any civil action arising under federal, state, local, and tribal law. (§ 29.8(i))	In civil proceedings in the United States district courts, where a party seeking access to SSI demonstrates that the party has substantial need of relevant SSI in the preparation of the party's case and that the party is unable without undue hardship to obtain the substantial equivalent of the information by other means, the party or party's counsel shall be designated as a covered person under 49 CFR 1520.7 in order to have access to the SSI at issue in the case (H.R. 5441 § 525(d))	Access to CVI shall not be available in any civil or criminal litigation unrelated to the enforcement of Section 550. (§ 27.400(i)(6))
Exceptions to Disclosure Rules			
Use in judicial or administra-	CII may be used or disclosed in furtherance of an investi-	TSA or the Coast Guard may provide SSI to a person in	DHS may provide CVI to a person governed by

Information Protection Regulations, cont.

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520 and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
tive proceedings	gation or the prosecution of a criminal act by the federal government and by a state, local, or foreign government, when such disclosure is coordinated by a federal law enforcement official. (§ 29.8(f)(1)(a)).	the context of an administrative enforcement proceeding when access to the SSI is necessary for the person to respond to allegations in a legal enforcement action document issued by TSA or the Coast Guard. (§ 1520.15(d))	Section 550, and his counsel, in the context of an administrative enforcement proceeding of Section 550 when access to the CVI is necessary for the person to respond to allegations in a legal enforcement action document issued by DHS (§ 27.400(h)). CVI may be provided to any person necessary for the conduct of a judicial enforcement proceeding of Section 550. (§ 27.400(i))
Communication with submitting entities	CII may be used or disclosed in order to communicate with a submitting person or an authorized person on behalf of a submitting entity. (§ 29.8(f)(1)(b))		
Disclosure to Congress	CII may be disclosed by any offi-	SSI may be disclosed to a commit-	

Information Protection Regulations, cont.

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520 and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
	cer or employee of the United States to either House of Congress. (§ 29.8(f)(1)(C)(1))	tee of Congress authorized to have the information. (§ 1520.15(c))	
Disclosure to the Comptroller General	CII may be disclosed by any officer or employee of the United States to the Comptroller General in the course of the performance of the duties of the General Accountability Office. (§ 929.8(f)(1)(C)(2))	SSI may be disclosed to the Comptroller General and to any authorized representative thereof. (§ 1520.15(c))	
Disclosure to the DHS Inspector General	PCII may be disclosed to the DHS Inspector General. (§ 29.8(f)(2))		
Partial disclosure under FOIA		If a record contains both SSI and information that is not SSI, TSA or the Coast Guard may disclose the record with the SSI redacted, provided the record is not other-	If a record is marked to signify both CVI and information that is not CVI, DHS may disclose the record with the CVI redacted, provided the record is not

Information Protection Regulations, cont.

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520 and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
		wise exempt from disclosure under FOIA or the Privacy Act. (§ 1520.15(b))	otherwise exempt from disclosure under FOIA or the Privacy Act. (§ 27.400(g)(2))
Other disclosure		TSA may authorize a conditional disclosure of specific SSI upon the written determination by TSA that disclosure of such information would not be detrimental to transportation security. (§ 1520.15(e))	
Violations			
Reporting	Persons authorized to have access to PCII shall report any suspected violation of security procedures, the loss or misplacement of PCII, and any suspected unauthorized disclosure of PCII immediately to the PCII Program Manager. (§ 29.9(a))	When a covered person becomes aware that SSI has been released to unauthorized persons, the covered person must promptly inform TSA or the applicable DOT or DHS component or agency. (§ 1520.9(c))	When a covered person becomes aware that CVI has been released to persons without a need to know, the covered person must promptly inform the Assistant Secretary. (§ 27.400(d)(7))

Information Protection Regulations, cont.

	PCII (6 C.F.R. 29)	**SSI** (49 C.F.R. 15; 49 C.F.R.1520 and H.R. 5441-27)	**CVI** (6 C.F.R. 27)
Notification	The submitting entity shall be notified unless providing such notification could reasonably be expected to hamper the relevant investigation or adversely affect any other law enforcement, national security, or homeland security interest. (§ 29.9(c))		
Penalties	Fine or imprisonment for up to a year; removal from office or employment. (§ 29.9(d)(1))	Civil penalty, enforcement, or corrective action by DHS, appropriate personnel actions for federal employees. (§ 1520.17). Civil penalty of up to $50,000 for each violation of 49 C.F.R. 1520 by persons provided access to SSI under H.R. 5441. (H.R. 5441§ 525(d))	Civil penalty, enforcement, or corrective action by DHS, appropriate personnel actions for federal employees. (§ 27.400(j))

NOTES

[1] White House, The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets 12 (2003).

[2] 148 Cong. Rec. S11,562-03 (daily ed. Nov. 19, 2002) (statement of Sen. Bennett).

[3] Nat'l Comm'n on Terrorist Attacks Upon the U.S., The 9/11 Commission Report 317 (2004).

[4] *See* Securing our Infrastructure: Private/Public Information Sharing: Hearing Before the S. Comm. on Governmental Affairs, 107th Cong. 78 (2002) (statement of John S. Tritak, Director, Critical Infrastructure Assurance Office, U.S. Department of Commerce).

[5] The Over-Classification and Pseudo-Classification of Government Information: The Response of the Program Manager of the Information Sharing Environment: Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the H. Comm. on Homeland Security, 110 Cong. (2007) (Statement of Dr. Carter Morris, Director of Information Sharing and Knowledge Management for the Office of Intelligence and Analysis at the Department of Homeland Security).

[6] 5 U.S.C. § 522 (2007).

[7] Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment, 41 Weekly Comp. Pres. Doc. 1874 (Dec. 26, 2005).

[8] Homeland Security Act §§211-215, 6 U.S.C. §§ 131-134 (2007).

[9] Critical Infrastructure Information is defined in the CII Act as:

> [I]nformation not customarily in the public domain and related to the security of critical infrastructure or protected systems — (A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates federal, state, or local law, harms interstate commerce of the United States, or threatens public health or safety; (B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk man-

agement planning, or risk audit; or (C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

Homeland Security Act § 212(3).

[10] In order to be classified as PCII, information must be: (1) voluntarily submitted; (2) submitted for protected use regarding the security of critical infrastructure or protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other appropriate purposes including, without limitation, for the identification, analysis, prevention, preemption, disruption, defense against, and/or mitigation of terrorist threats to the homeland; (3) labeled with an express statement; (4) accompanied by a statement containing the submitting person or entity's contact information and certifying that the information being submitted is not customarily in the public domain. Procedures for Handling Critical Infrastructure Information; Final Rule, 6 C.F.R. § 29.5(a) (2007).

[11] *Id.* at § 29.6(g).

[12] *Id.* at §§ 29.7(a), (c), (e) and 29.6(c).

[13] *Id.* at § 29.8(g).

[14] *Id.* at § 29.8(h).

[15] *Id.* at § 29.8(i).

[16] See Procedures for Handling Critical Infrastructure Information; Final Rule, 71 Fed. Reg. 52,264 (Sept. 1, 2006) (supplemental information section).

[17] 6 C.F.R. § 29.8(b). PCII may be provided to an employee of the federal government for the purposes of "securing the critical information infrastructure or protected systems, analysis, warning, interdependency study, recovery, reconstitution or other appropriate purposes including, without limitation, for the identification, analysis, prevention, preemption, disruption, defense against and/or mitigation of terrorist threats to the homeland." *Id.*

[18] *Id.* at § 29.8(d).

[19] *Id.* at § 29.8(c).

[20] *Id.* at § 29.8(e).

[21] *Id.* at § 29.8(f)(1)(A).

[22] *Id.* at § 29.8(f)(1)(B).

[23] *Id.* at §§ 29.8(f)(1)(C)(1) and (2).

[24] *Id.* at § 29.8(f)(1)(2).

[25] SSI is defined as:

> [I]nformation obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA [or the Secretary of the Department of Transportation] has determined would (1) constitute an unwarranted invasion of privacy....(2) reveal trade secrets or privileged or confidential information obtained from any person; or (3) be detrimental to the security of transportation.

Protection of Sensitive Security Information, 49 C.F.R. § 1520.5(a) (2007). SSI consists of: (1) security programs and contingency plans; (2) security directives; (3) information circulars; (4) performance specifications; (5) vulnerability assessments; (6) security inspection or investigative information; (7) threat information; (8) security measures; (9) security screening information; (10) security training methods; (11) identifying information of certain transportation security personnel; (12) critical aviation or maritime infrastructure asset information; (13) systems security information; (14) confidential business information; (15) research and development; and (16) other information that TSA determines is SSI. *Id.* at § 1520.5(b).

[26] Separate regulations for TSA and DOT govern SSI, but they are identical. The TSA regulation appears at 49 C.F.R. § 15, and the DOT regulation at 49 C.F.R. § 1520. Unless otherwise stated, references herein will be to the TSA regulation.

[27] References to TSA also include the Coast Guard and DOT, as applicable.

[28] 49 C.F.R. § 1520.6(c).

[29] *Id.* at §§ 1520.9(a)(1), 1520.13, and 1520.19(b).

[30] 5 U.S.C. § 552a (2007).

[31] 49 C.F.R. § 1520.15(a).

[32] *Id.* at § 1520.15(b).

[33] Homeland Security Appropriations Act of 2007, H.R. 5441 § 525, 109th Cong. (2006).

[34] *Id.* at § 525(a)(1).

[35] *Id.* at § 525(a)(2).

[36] Defined at 49 C.F.R. § 1520.7.

[37] *Id.* at § 1520.11(a).

[38] *Id.* at § 1520.11(d).

[39] *Id.* at § 1520(b)(1).

[40] *Id.* at § 1520(b)(2).

[41] H.R. 5441 § 525. This reflects the changes to SSI disclosure requirements

enacted by H.R. 5441.

[42] 49 C.F.R. § 1520.15(d).

[43] *Id.* at § 1520.15(c).

[44] *Id.* at § 1520.15(e).

[45] Chemical Facility Anti-Terrorism Standards, 6 C.F.R. § 27 (2007).

[46] CVI is comprised of: (1) Security Vulnerability Assessments; (2) Site Security Plans; (3) documents relating to DHS's review and approval of Security Vulnerability Assessments and Site Security Plans; (4) Alternative Security Programs; (5) documents relating to inspection or audits; (6) any records required to be created or retained; (7) sensitive portions of orders, notices, or letters; (8) information developed to determine security risk; and (9) other information developed for chemical facility security purposes, at the Secretary of DHS's discretion. *Id.* at § 27.400(b).

[47] *Id.* at §§ 27.400 (d), 27.400(f)(3), and 27.400(k).

[48] *Id.* at § 27.400(g)(1).

[49] *Id.* at § 27.400(g)(2).

[50] *Id.* at § 27.400(e).

[51] *Id.* at § 27.400(e)(2)(i).

[52] *Id.* at § 27.400(e)(2)(ii).

[53] *Id.* at § 27.400(i)(6).

[54] This section provides for the regulations establishing the CVI program.

[55] *Id.* at §§ 27.400(h)(1) and (i)(1).

[56] *Id.* at § 1520.9(d) and § 27.400(d)(8).

[57] *See* Gina Marie Stevens, Congressional Research Serv., Report on Homeland Security Act of 2002: Critical Infrastructure Information Act (2003) ("The Homeland Security Act was approved by the House and Senate expeditiously, with relatively little focus on its FOIA-related provisions.").

[58] H.R. 5441, at § 525(a).

[59] H.R. 1530, 110th Cong. (2007).

[60] H.R. 1309, 110th Cong. (2007).

[61] S. 849, 110th Cong. (2007).

[62] *See* Ralph Lindeman, *Leahy Backs Minor Change in FOIA Bill but Resists Others Sought by Opponents*, BNA Daily Report for Executives, June 4, 2007, at A-23.; *see also* 153 Cong. Rec. H2,504 (daily ed. March 14, 2007) (Statement of Administration Policy).

[63] Exec. Order No. 12,958, 60 Fed. Reg. 19,825 (Apr. 20, 1995).

[64] Memorandum on Guidelines and Requirements in Support of the

Information Sharing Environment, 41 Weekly Comp. Pres. Doc. 1874 (Dec. 26, 2005).

[65] Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment, 41 Weekly Comp. Pres. Doc. 1874 (Dec. 26, 2005).

[66] The DOT regulation is at 49 C.F.R. 15, and the TSA regulation appears at 49 C.F.R. 1520. The regulations are identical. Section references in this chart refer to the TSA regulation.

[67] As defined in Section 2 of the Homeland Security Act of 2002.

[68] An assessment required of chemical facilities designated as high-risk, which includes (1) an identification and characterization of potential critical assets and identification of hazards and consequences of concern for the facility; (2) a description of possible internal, external, and internally assisted threats; (3) an identification of potential security vulnerabilities and existing countermeasures and their level of effectiveness in reducing identified vulnerabilities; (4) a determination of the relative degree of risk to the facility in terms of the expected effect on critical assets and the likelihood of success of an attack; and (5) strategies that reduce the probability of a successful attack or reduce the probable degree of success. § 27.215(a).

[69] Plans for site security that (1) address each vulnerability identified in the site's Security Vulnerability Assessment and describe the security measures to address such vulnerability; (2) identify and describe how security measures selected by the facility will address applicable risk-based performance standards and potential modes of terrorist attack; and (3) identify and describe how security measures will meet or exceed each applicable risk-based performance standard for the appropriate risk-based tier for the facility. § 27.225(a).

[70] Security programs submitted by covered facilities in lieu of Security Vulnerability Assessments, Site Security Plans, and both. Alternative Security Programs must be approved by DHS. § 27.235(a) and (b).

[71] (1) Airport and aircraft operators; (2) indirect air carriers; (3) owners, charterers, and operators of vessels required to have security plans under federal or international law; (4) owners or operators of maritime facilities required to have security plans; (5) persons performing the function of a computer reservation system or global distribution system for airline passenger information; (6) persons participating in national, area, and port security committees; (7) industry trade associations that represent covered persons and have entered

into nondisclosure agreements with DHS and DOT; (8) DHS and DOT; (9) persons conducting research and development activities that relate to transportation security and approved or directed by DHS; (10) persons with a need to know SSI; (11) employees or agents of covered persons; (12) persons for whom a vulnerability assessment has been created or that have prepared vulnerability assessments for DOT or DHS; and (12) persons provided access to SSI by DHS.

[72] Each person who has a need to know CVI and each person who otherwise receives or gains access to what they know or should reasonably know constitutes CVI.

[73] Such disclosure is not a public release of information under FOIA. (§ 1520.15(g))