PCII, SSI & CVI: Comparison of Important Issues from the Perspective of Private Owner/Operators

James W. Conrad, Jr.[1]

These three programs grow out of federal statutes and regulations and prohibit the federal government from releasing, under the Freedom of Information Act, specific types of security-related information.

Issue	**Protected Critical Infrastructure Information** 6 U.S.C. §§ 131-34; 6 C.F.R. Part 29; 71 FR 52262 (Sept. 1, 2006)	**Sensitive Security Information** 49 U.S.C. §§ 114(s)(1), 40119(b)(1); 49 C.F.R. Parts 15 (TSA) & 1520 (DOT); 69 FR 28066 (May 18, 2004) (mainly)	**Chemical-terrorism Vulnerability Information** 6 U.S.C. § 121 note; 6 C.F.R. Part 27; 72 FR 17688 (April 9, 2007)
Scope	Information *submitted to DHS* regarding threats, vulnerabilities, consequences, countermeasures regarding critical infrastructure.	Information whose disclosure would be detrimental to transportation security or safety.	"Information developed under" the statute authorizing CFATS.
Self-implementing?	No – information must be submitted to DHS; DHS must "validate" it as PCII. - Provisionally PCII once submitted. - Upfront "categorical inclusions" possible.	Yes – information is SSI upon creation if meets regulatory definition; e.g.: - Vulnerability assessments - Threat information - Security programs/contingency plans - Security inspection/investigation results - Security measures - Security training records	Yes – information is CVI upon creation if meets regulatory definition; e.g.: - Top-Screen information - Security Vulnerability Assessments - Site Security Plans - Docs re review/approval of above - Inspection/audit docs - Security training, mainte-

[1] Conrad Law & Policy Counsel, 1615 L St., NW, Suite 1350, Washington, D.C. 20036
202-822-1970/jamie@conradcounsel.com/www.conradcounsel.com

		(or if DOT/TSA says is SSI).	nance records (or if DHS says is CVI).
Who can have?	Federal, state & local gov't officials & contractors as approved by PCII Program Office (generally, for critical infrastructure protection purposes or criminal law enforcement – not for collateral regulatory purposes).	"Covered persons"; e.g. - DHS/DOT - Aviation/maritime/hazmat owners/operators req'd to have security plans - Their trade ass'ns - Their employees, contractors & agents with a "need to know"; i.e., to carry out security activities, be trained, supervise, or give technical/legal advice.	"Covered persons" with a "need to know"; i.e., persons needing CVI to carry out security activities, be trained, supervise or give technical/legal advice.
Are state/local open records laws preempted?	Yes, in statute.	Yes, say TSA/DOT.	Yes, by statute (at least when comes from DHS) and rule.
Can DHS use in enforcement litigation?	No.	Yes, but not disclose publicly.	Yes, but must be treated as classified information.
Can the information be used in private civil litigation?	Not directly; DHS says not discoverable.	Prospect of DOJ intervention.	Prospect of DOJ intervention.
Are there penalties if Fed employees disclose without authorization?	Misdemeanor criminal penalties.	Yes, in statute.	Rules say violation is grounds for civil penalty.
Are there penalties if state/ local employees disclose without authorization?	Not in statute, but PCII PO works with states to identify state/local enforcement regimes.	Yes, in statute.	Rules say violation is grounds for civil penalty.
Does program impose enforceable requirements on private holders of information?	No – only binds Fed agency personnel and contractors.	Yes.	Yes.

What are penalties if private person mishandles?	None.	Up to $25,000 civil penalty per violation of rules (DOT: $1,100 for indiv./small business.	DHS can issue compliance order. Up to $25,000 civil penalty if violate order.
Do you have to be an "authorized user" to receive?	No for anyone to receive copies from the submitter. Yes for gov't personnel/contractors to receive validated copies of PCII from PCII PO.	No. Any covered person with a need to know and understanding of restrictions may possess.	Yes. Must be a covered person with a need to know, but also must complete web-based DHS training (incl. signing nondisclosure agreement (NDA)), be issued "authorized user" number from DHS.
Do private parties have to inform Feds of unauthorized release?	No.	Yes.	Yes.
Does a private person have to notify Feds if gives to another?	No.	No.	Guidance will address release to state/local officials.
Does a private person have to sign NDA to receive from gov't?	No (private persons should not be able to get PCII from DHS)	USCG: Yes, but not required when giving person information about own facility. DOT: No, but needs to understand restrictions	Yes – part of DHS web-based "authorized user" training.
Does a private person have to sign NDA to receive from another private person?	No.	No, but needs to understand restrictions.	NDA is part of "authorized user" training.
Do private entities have to use tracking logs of who gets to have?	No.	Coast Guard guidance encourages tracking in some fashion.	Tracking log part of "authorized user" training.
Are there marking/labeling req'ts for private persons?	No.	Yes.	Yes.

Are there safeguarding req'ts (i.e., storage & transmission) for private persons?	No.	Yes.	Yes.
Are there disposal req'ts for private persons?	No.	Yes.	Yes.