HOMELAND SECURITY ADVISORY COUNCIL

PRIVATE SECTOR INFORMATION SHARING TASK FORCE

ON

HOMELAND SECURITY INFORMATION SHARING BETWEEN GOVERNMENT AND THE PRIVATE SECTOR

AUGUST 10, 2005

Table of Contents

Introduction

"We will build a national environment that enables the sharing of essential homeland security information. We must build a 'system of systems' that can provide the right information to the right people at all times. Information will be shared 'horizontally' across each level of government and 'vertically' among federal, state, and local governments, private industry, and citizens."

— The President's National Strategy for Homeland Security

Origin of Report; Authorship. Because the Private Sector controls the great majority of the Nation's critical infrastructure, effective cooperation between the Federal Government – particularly the Department of Homeland Security – and the Private Sector is essential to protecting those assets from terrorist attack. Nowhere is that cooperation more vital than in the area of information sharing. And yet that cooperation has been hampered by a variety of legal and procedural obstacles. The Homeland Security Advisory Council charged its Private Sector Information Sharing Task Force on March 21 to understand the nature of those obstacles and to propose solutions to them. The Task Force concluded that the best way to understand these obstacles – which could be real or perceived – was to ask the Private Sector about them. Accordingly, the Task Force assigned several of its members, led by Rick Stephens, to reach out to lawyers and others representing private sector critical infrastructure companies and associations. This ad hoc Group of Subject Matter Experts comprises aeronautics, banking, chemicals, commercial aviation, electric power, refining, telecommunications, broadcasting, food products, and state and local government. (See Attachment A for the roster of the Task Force and its Subject Matter Experts.)

Scope of Report. The Task Force concluded that the question of which legal obstacles impair information sharing could not be addressed in isolation from the channels by which information flows from government entities to private ones and vice-versa. The Task Force's report therefore evaluates, and makes recommendations regarding, the requirements and processes for information sharing between government and private entities.

It then discusses at length the legal and related obstacles that have impeded information flow in existing channels and, unless effectively addressed, will continue to do so in the proposed architecture. Finally, the report addresses the role of the media in this process.

In conducting this analysis, the Task Force defined "government" to include Federal, State and local entities. While the focus of this report is information sharing between government and private sector critical infrastructure entities, we also recognize that state and local governments operate some critical infrastructure, and hence may find themselves on the "private," as well as the "government," side of the equation.

The Task Force recognizes that some office and/or agency names and responsibilities referred to in the report may change with pending 2SR implementation.

Methodology of the Work. The Task Force determined that its work encompassed four key issues:

- Information collection and sharing **requirements** (up and down)
- Public/private information sharing **process/flow**
- **Laws, rules, policies** that affect public/private information sharing
- **Partnering with the communications media** on an ongoing basis

The Task Force assigned members to lead work on each of these key issues and decided to defer a fifth issue, **training** the private and public sector on the collection, analysis, dissemination, and use of homeland security information.

The Task Force divided its work into two phases:

- Phase I (Current State) -- Determining the "as-is" environment of information sharing between government and the Private Sector. In this connection, Task Force members:
  - Conducted numerous interviews of Federal and Private Sector officials;
  - Met and spoke with representatives from DHS offices (e.g., Information Analysis and Infrastructure Protection Directorate, Homeland Security Operations Center, National Infrastructure Coordination Center) and the Private Sector; and
  - Reviewed studies and reports (e.g., GAO's July 2004 report on information sharing,[1] the draft Interim National Infrastructure Protection Plan).
- Phase II (Future State/Recommendations) -- Defining requirements, roles, and responsibilities of the Private Sector and DHS for effective information sharing. In this phase, the Task Force:
  - Expanded its membership to include Federal, State, and local representatives and Subject Matter Experts from the Private Sector; and
  - Received input from key stakeholders through Task Force meetings and conference calls.

Role of DHS Participants. Several representatives from DHS provided the Task Force with helpful factual information regarding DHS, its current information sharing processes, and its views regarding particular legal issues. This assistance was vital to our work, and we appreciate it. We emphasize, however, that these DHS representatives did not participate in the Task Force's deliberations, and that the analysis and recommendations presented here are entirely those of the Task Force's non-Federal participants.

Categorization of Recommendations. This report provides concrete recommendations to address each of the issues we identified. These recommendations are classified by the type of change they call for, in order to provide some perspective regarding how easily and quickly they could be implemented:

- L (legislative): Changes to the U.S. Code. This would require Congressional action, and is thus the most difficult and time-consuming to accomplish.
- R (regulatory): Changes to the Code of Federal Regulations. This would require DHS or another agency to conduct rulemaking. While rulemaking is within a given agency's control, it nonetheless requires time and resources for compliance with the Administrative Procedure Act and other requirements.
- M (mechanical): This refers to guidelines, policies or other explicit procedures that do not require rulemaking.
- A (attitudinal): These are changes in attitude or organizational culture, rather than particular agency processes. They can best be effected by clear statements from the Secretary and other senior leaders.

Appreciation for DHS's Work to Date. The Task Force emphasizes that its recommendations, while critical at times of DHS processes, are not intended to be critical of DHS personnel or their motives. DHS staff have worked extremely hard, in good faith and with the best of intentions, to stand up new processes in uncharted areas. They have worked under intense time pressures, stringent budget and personnel limitations, and impatient public scrutiny. The report respects that service. But we would dishonor it if we were not completely frank regarding the legal and other challenges that confront information sharing. For the same reason, we have not compromised or hedged our recommendations for how those obstacles should be overcome.

[1] GOVERNMENT ACCOUNTABILITY OFFICE, "CRITICAL INFRASTRUCTURE PROTECTION: IMPROVING INFORMATION SHARING WITH CRITICAL INFRASTRUCTURE SECTORS," GAO-04-780 (July 9, 2004).

Information Sharing with the Broader Public. The Task Force emphasizes that the purpose of this report is not to promote the greatest possible withholding of private security-related information from release by the government. The Task Force recognizes that DHS, like all Federal agencies, must effectuate long-standing principles of open government. As discussed below, the Task Force believes that the government overclassifies or otherwise restricts from disclosure information that should be provided to Private Sector entities which own or operate critical infrastructure.By extension, some government information that is "security-related" likely could safely be made public without jeopardizing the security of private sector infrastructure – especially if it is summarized or abstracted in a way that does not create undue risks. On the other hand, while different people will draw the line at different places, ultimately all (or virtually all) observers would agree that there are circumstances in which security-related information provided by private entities to the government must be protected from unrestricted public release. Further, the government needs to listen carefully to the Private Sector to understand the sensitivities that are at stake when the government is considering disclosing information about private entities. These issues are among those that the Task Force will consider further in the context of "responsible information sharing," a future work item.

Coordination with Other Entities. Consistent with its charter to address and provide recommendations on the spectrum of Homeland Security issues, the Homeland Security Advisory Council (HSAC) has created a Critical Infrastructure Task Force (CITF). The CITF is focused on the transformation and advancement of national critical infrastructure policy. This transformation is intended to go beyond protection to provide for the resilience and continuity of operation of the Nation's critical infrastructure. The recommendations of this Task Force and the CITF have been closely integrated. That integration must continue.

Executive Summary

Because the Private Sector controls the great majority of the nation's critical infrastructure, effective cooperation between the Federal Government – particularly the Department of Homeland Security – and the Private Sector is essential to protecting those assets from terrorist attack. Nowhere is that cooperation more vital than in the area of information sharing. And yet that cooperation has been hampered by a variety of legal and procedural obstacles. The Homeland Security Advisory Council charged its Private Sector Information Sharing Task Force on March 21 to understand the nature of those obstacles and to propose solutions to them.

The Task Force concluded that the best way to understand these obstacles – which could be real or perceived – was to ask the Private Sector about them. Accordingly, the Task Force assigned several of its members to reach out to numerous private sector critical infrastructures, as well as State and local government.

The Task Force during its deliberations reached the following general findings:

1. Significant information sharing activities and work are underway in DHS and in the public and Private Sectors. But it is not clear that there is an aligned "architecture" or clear understanding of who has the responsibility to create one. Such an architecture should address:
   - Organizational accountabilities and relationships with other organizations
   - Systems and information flow (processes, information systems and data)
   - Other Federal Agency information resources, requirements and needs

2. Significant work is required to align relationships between DHS and the Private Sector.

3. Different considerations apply for sharing threat information and vulnerability information.

4. The Task Force supports the State and Local Information Sharing Working Group's principal finding: State, Local and Tribal Governments – and the Private Sector – require homeland security threat and indications and warning (I&W) information that, to the maximum extent possible, is UNCLASSIFIED, timely, actionable/tailored and updated frequently.

5. Intelligence/information sharing between DHS and the Private Sector involves policy, process, and technology and the creation and maintenance of a trusted partnership between all concerned.
   - A number of statutory, regulatory, policy and attitudinal improvements are needed.
   - It will be difficult or impossible to make significant progress on many other topics until these obstacles can be overcome.

6. A stronger working relationship between DHS and the media will increase the likelihood that preparedness, threat and crisis information provided to a diverse public is accurate, timely, actionable and in context.
   - Provide a reassuring sense that government, business and civic leaders are working well together.
   - Improve service to the public in a crisis.
   - Refinements in the Homeland Security Advisory System are needed.
   - A national community-based threat and preparedness campaign.

7. Relationships and interaction between the Private Sector and state and local agencies are less problematic and, therefore, the focus of the Task Force was on the DHS/Private Sector relationship.

The Task Force issued the following recommendations:[2]

1. ***DHS and the Private Sector should work in collaboration to develop a formal, and objectively manageable, homeland security intelligence/information requirements process.***
   - *The process should place a premium on, and leverage, superior Private Sector information resources, expertise in business continuity planning, and understanding of the operations of infrastructure sectors. (M/A)*
   - *The process must recognize the diversity of the Private Sector. (A)*
   - *DHS should partner with the Private Sector in developing an integrated architecture for information collection and sharing. The Task Force understands that this is how Homeland Security Information Network (HSIN) is being developed and how HSIN-CI (Critical Infrastructure) (with 40,000+ members) operates. The Task Force supports that approach. (M/A)*
   - *The Private Sector and DHS need to integrate and align their requirements for information collection and sharing. (M/A)*
   - *Information Sharing & Analysis Centers (ISACs), Sector Coordinating Councils (SCCs) and other Private Sector organizations and stakeholders must coordinate their efforts and define Private Sector requirements for DHS so that specific Private Sector entities can formally request, track and receive only that information requested. This will require doing a better job of articulating what types of information they want from government and with what frequency. (M/A)*
   - *Information Sharing & Analysis Centers (ISACs), Sector Coordinating Councils (SCCs) and other Private Sector organizations and stakeholders must coordinate their efforts and define Private Sector requirements for DHS so that specific Private Sector entities can formally request, track and receive only that information requested. This will require doing a better job of articulating what types of information they want from government and with what frequency. (M/A)*
   - *The process should include a greater bias toward disseminating more information in unclassified form. The solution should not primarily be to investigate more people and issue more clearances. (M/A)*
   - *Where information must be classified,*
     - *DHS and other agencies should work harder to produce unclassified versions. (M/A)*
     - *The President should continue to implement on a timely basis the provisions of the Intelligence Reform law designed to expedite the clearance process. (M)*

2. **DHS should adopt a tiered approach to infrastructure vulnerability information sharing.**
   - Carefully consider the known and potentially exploitable vulnerabilities of database technologies, and the consequences of compromise of a "national asset database" of vulnerabilities. (L/M)
   - Maintain appropriate Federal information at the DHS level, State information at the State level, local information at the local level, and Private Sector information at the Private Sector level. (L/M)
   - To enhance the security of vulnerability information, maintain public sector infrastructure information at the city and municipal level and Private Sector information with trusted third party/non-governmental entities. (L/M)
   - Establish an appropriate organization or process for cross-sector and government information exchange. (M)

[2]Highest priority recommendations are italicized.

3. **DHS needs to be flexible and responsive in accommodating diversity within and among Private Sector critical infrastructure sectors.**
    - HSPD-7 calls for two functions: information sharing and sector coordination.
    - Sector Coordinating Councils in every sector may not be able to perform all the functions DHS desires. At a minimum, DHS must allow each sector to determine the nature, functions, and rules of its council and its relationship with its ISAC and SSA (Sector Specific Agency). (M/A)

4. **DHS should continue to develop a network integrated information model for information flow.**
    - Significant work is required:
        - DHS should employ a "hub and spoke model" for information flow, as used in HSIN and HSOC. (M)
        - Information should flow from the Private Sector and other government sources to the DHS hub for analyses, and then be distributed back to the Private Sector on a targeted basis. (M)
        - DHS needs Private Sector input and presence at the hub. (M/A)
    - As a national priority, build a resilient/survivable Homeland Security Operations Center (HSOC) and Homeland Security Information Network (HSIN). (M)
        - In their current condition, both are single points of DHS operational failure – an unacceptable circumstance.
    - Leverage the unparalleled success of, and invest in expanding, HSIN-CI. (M)
        - HSIN-CI is a trusted and proven model for effectively gathering and sharing information.
    - Statewide intelligence/information fusion centers should be integrated into national information sharing efforts. (M/A)
        - *DHS should hold regular collaborative sessions (start monthly) with each Private Sector coordinating organization (e.g., SCCs, ISACs). (M)*
        - *DHS should hold regular, detailed threat briefings with each sector.*
        - *Representatives of IA and IP should meet with selected security and continuity of operations personnel of critical infrastructure service providers. (M)*
        - *These sessions should be held more often than every six months, and should be held separately for each sector. (M)*
        - *They should involve more specific information than is currently presented in classified sector briefings. (M)*
        - *They should be oriented less toward presentation and more toward dialogue. (M/A)*

5. ***DHS should promptly and decisively revise its rules and policies for information sharing.***
    - *Regard Private Sector critical infrastructure facilities, companies and their associations as partners with legitimate interests in policy formulation and implementation – and as the only entities capable of implementing most policy in the subject area. (A)*
    - *Respond to Private Sector concerns about liability risks associated with sharing security information with DHS*
        - *DHS should ensure that critical infrastructure information is only used to protect or ensure the operational resilience of critical infrastructure. (R)*
        - *Critical Infrastructure Information Act (CIIA) regulations must be simple and broadly agreed-upon before they will be used. (R)*
        - *Educate potential submitters regarding the protections afforded by all existing laws and potential risks. (M)*
    - *Fully implement the Critical Infrastructure Information Act (CIIA):*
        - *Do not require all CIIA submissions to be validated. (R)*

- *Declare that information submitted by SCCs and ISACs and maintained on HSIN by sector representatives will be deemed CII. (R/M)*
- *Allow "class" CIIA determinations in advance of submittal. (R/M)*
- *Allow "indirect" and electronic submission under CIIA. (R/M)*
- *Roll out the CIIA program as quickly as possible to all DHS entities, to other sector-specific agencies, and to states willing to execute memoranda of agreement (on behalf of themselves and local governments within the State). (M)*
- *Authorize all personnel of its Information Analysis & Infrastructure Protection Directorate who interact with critical entities to be CIIA portals. (M)*

- *In consultation with DOJ and the Private Sector, adopt broad, Department-wide positions regarding the applicability of the confidential business information and law enforcement sensitive exemptions under the Freedom of Information Act (FOIA). (M)*
- *Resolve questions about how the Federal Advisory Committee Act (FACA) applies to SCCs and ISACs.*
  - *The ongoing Private Sector/Government operating relationship is critical to an effective homeland security operation and is hobbled by FACA issues.*
  - *SCCs and ISACs are not covered by FACA because they are not "utilized" by the Executive Branch and are primarily operational, rather than advisory. (M)*
  - *If challenged, DHS should use one of three possible authorities to exempt SCCs and ISACs from FACA. If this requires amending the CIIA rules, DHS should do so promptly. (R/M)*
  - *Given the above, under no circumstances should DHS employ FACA "work arounds" like treating SCCs as subgroups of the National Infrastructure Advisory Council or seeking only the views of individual companies. (M)*
- DHS offices and staff should identify coordination needs with DHS, with other Federal agencies and with State and local governments, and should undertake such coordination as early as necessary, without waiting for affected entities to initiate it. (M/A)
- DHS should determine if it needs particular information to do its job, or whether some other governmental or private entity is doing that job adequately. DHS should not request information because it can, or because it would be "nice to know," but only where it is necessary to enable DHS entities to perform essential functions. (M/A)
- The Sensitive Security Information (SSI) rulemaking conducted by the DHS Transportation Security Administration (TSA) should encompass all modes of transportation. (R)

6. ***DHS should pro-actively invest in a better-informed and more engaged media through specific targeted programs aimed at developing a stronger working relationship between the government, the media and the Private Sector in major incidents. (M/A).***
   - *Upon completion of an assessment, the government and local media should scale their existing National Academies of Science media engagement program into a sustained campaign in all UASI (Urban Areas Security Initiative) media markets.*
   - *Government officials at both the national and local levels should conduct a systematic program of background briefings for members of local media including, among other things, the National Response Plan and National Incident Management System, potential threat and response scenarios, scientific information regarding biological, chemical and radiological materials, a glossary of homeland security and citizen protective actions, and other FAQs.*
   - *Local elected officials and trusted authorities (public and Private Sector) should be trained on how to conduct press briefings during an incident in order to provide (1) timely and actionable information and protective action recommendations to the Private Sector and the public and (2) contextual material needed to maintain public order and confidence.*

- *DHS, local elected officials and national and local media should develop protocols for the timely confirmation or correction of unconfirmed information or rumors during the course of an incident.*

7. ***The Homeland Security Advisory System should be refined to provide more specific guidance to the Private Sector and to the public, including changes in warning levels. (M).***
   - *Warning levels should be adjustable on a sector-specific, geographic or time-limited basis (or on another basis, as appropriate).*
   - *Warning level changes should include a specific advisory to the public regarding the purpose for the change and the steps, if any, that the public is expected to take as a result of such a change.*
   - *DHS, State and local officials and the Private Sector should meet, confer and develop common understandings and expectations regarding the readiness or preparedness levels associated with different warning levels.*
   - *Any refinement of the Advisory System should be accompanied by a clear, easy-to-understand public communications plan.*

The Task Force identified the following next steps:

- The Task Force urges DHS to reach out to Private Sector entities that represent critical infrastructure (i.e., Sector Coordinating Councils and Information Sharing & Analysis Centers) to establish joint DHS/Private Sector teams to work on the highest priority recommendations.
- In consultation with these teams, DHS should build an action plan, with milestones, to address all the recommendations discussed below.
- Task Force members stand ready to support this effort.
- In the future, the Task Force will address the issue of training the private and public sector on the collection, analysis, dissemination, and use of homeland security information.
- Additionally, the Task Force will review, and determine whether to develop recommendations regarding, the following issues:
  - Creation of a domestic counterpart to the Overseas Security Advisory Council.
  - Ensuring implementation of a formal intelligence requirements process for the Private Sector, including both physical mechanisms and educating stakeholders.
  - Ensuring *responsible* information sharing, so as to satisfy legitimate public right-to-know goals without creating even greater risks to the public through the release of information that could assist terrorists.
  - Supporting the State and Local Information Sharing Working Group's initiatives, particularly Private Sector roles and responsibilities in state and local fusion centers.

Discussion

PART ONE: ESTABLISHING NEW INFORMATION SHARING REQUIREMENTS AND PROCESSES

I. The Imperative for Creating a Formal and Objectively Manageable Homeland Security Intelligence/Information Requirements Process

A huge amount of information currently flows in both directions between private sector critical infrastructure entities and the Federal Government. Attachment B to this paper is an outline of the most important of these flows. (It does not include the great volume of information moving in each direction in the form of press releases, briefings, and general public affairs campaigns.) Much of the information described in Attachment B is part of the process of legal and regulatory enforcement (but not the promulgation of rules or regulations); much falls into the definition of "critical infrastructure information." Despite – or perhaps because of – the sheer volume of this information, it is not clear that there is an aligned "architecture" for sharing it, nor a clear understanding of who has the responsibility to create one.

Members of private sector critical infrastructure have a wide variety of requirements regarding information that they want from government and information that they are willing to share with government. As a general rule, the Private Sector wants information (both from government and other Private Sector sources):

- to change business behavior when necessary;
- on things which would affect businesses; and
- to respond/react/initiate resilience.

A. Requirements regarding threat information

The Private Sector generally views information coming from DHS as primarily about threats, and information coming from the Private Sector as primarily about vulnerabilities.

Reflecting the wide-ranging differences among them, different industries and companies want varying levels of threat information. Many smaller companies want only specific, actionable information concerning immediate threats that affect them individually. Some companies and industries desire government assessments of security and business-continuity capabilities, but only when and as requested. Some want information that is a bit more general, but which nonetheless is refined by time, region or sector, or focused on threat trend and technique analyses.

Some, however, want almost all information available — the broad spectrum of threat and risk information.

These companies (or industries) view themselves as fully able to decide whether it is relevant to them and how to respond. While recognizing that the Private Sector is a source of and has a responsibility to provide information to the Government, until the government's new information dissemination and sorting methods are refined, these companies want DHS to spend more effort on the process of getting information out to the Private Sector, letting the Private Sector sort through applicability and share information across sectors or within regions. Even with this group, however, there was a desire that shared information be as specific, timely and actionable as possible, so that it assists those responsible for adjusting their security and operational continuity measures to respond accordingly.

The Private Sector also needs to be able to get threat information from State and local sources, as well as from DHS. To avoid confusion, especially during times of crisis, this will require Federal-State cooperation and coordination.

Too often threats and warnings seem based on sector rather than geography.

B. Requirements regarding criticality/ vulnerability

The process of determining which infrastructure elements within a given sector are "critical" or "vulnerable" needs to be better defined and made only with the input of Private Sector expertise. While DHS has made progress in building its organizational and oversight capacity regarding the Private Sector, the fact is that, by necessity, the Private Sector will always understand its operations better than DHS (or other government agencies). As the government learned during the Y2K transition, empowerment of and trust in the Private Sector's superior knowledge of its own infrastructure and inclusion of its expertise will produce optimal decisions and objectively sustainable results. Exclusion of that expertise, or dictation to those holding it, will assure the continuation of suboptimal decisions, expenditures of resources, and effects. For example, DHS's National Communications System (NCS) maintains a database about network configuration entitled the "Network Design & Analysis Capability" (NDAC). The data comes to DHS by purchase from companies under nondisclosure agreements, from public sources such as the Local Exchange Routing Guide (LERG), and by voluntary submissions.

Analysis of the data, however, should always be reviewed by the company (usually under the terms of the NDA) to avoid incorrect conclusions. In one instance where such review was not obtained, a government analyst's assumption that a telecommunications cable crossed a bridge (when in fact it was buried under the stream crossed by the bridge) led him to erroneously conclude that destroying the bridge would destroy connectivity.

C. Requirements regarding unclassified and classified information

The Private Sector, recognizing it has its own "insider" security concerns, needs information — unclassified to the maximum extent possible — that is actionable; i.e., enabling it to respond in the best way based on local trusted relationships. As discussed below, Congress and the Government Accountability Office (GAO) have emphasized the need for DHS and other agencies to issue more security clearances to State, local and private individuals, and such clearances are clearly needed by many who do not have them. But DHS should not proceed on the basis that issuing more clearances will resolve this obstacle. There are simply too many people in the tens of thousands of critical infrastructure entities for DHS to clear them all – and new people go to work for these businesses and governments all the time. Equally problematic, for homeland security information to produce the intended benefits, recipients of it need to be able to relay its substance to colleagues within their own organizations and sectors, within interdependent sectors, and within State and local governments. It is not very helpful if cleared people cannot tell non-cleared people what they know.[3]

[3]This was the clear consensus of participants in a panel convened by the American Bar Association's Section of Administrative Law and Regulatory Practice on the new "information sharing environment." Participants in the March 16, 2005 event were William Leonard, Information Security Oversight Office, National Archives & Records Administration; William Dawson, Deputy Intelligence Community CIO and Special Assistant for Information Sharing to the Director of Central Intelligence; Larry Halloran, Staff Director and Counsel of the House Government Reform Committee's Subcommittee on National Security, Emerging Threats and International Relations; and Mary DeRosa, Senior Fellow, Technology Program, Center for Strategic and International Studies and a consulting expert to the Markle Foundation's Task Force on National Security in the Information Age. Audio available at http://www.abanet.org/adminlaw/calendar.html.

The primary solution to this obstacle needs to be giving people unclassified, timely and actionable information to clear them all – and new people go to work for these businesses and governments all the time.

In particular, the Private Sector feels that government should trust it and provide access to "Law Enforcement Sensitive" and "For Official Use Only" information. Those and similar restrictions some-times lead law enforcement or other sector-specific agencies to prevent Private Sector access, even though many within the critical infrastructure security organizations understand how to handle sensitive data.(Indeed, such companies are equally if not more concerned about this information being publicly released.) DHS should explore the value of nondisclosure agreements as a means of limiting subsequent dissemination of information it provided to selected critical entities. Such agreements are mandatory when classified information is shared, and could be useful for sharing unclassified information as well.

The Task Force is not alone in its belief that DHS should share more information with the Private Sector. Congress has twice acted since 9/11 to encourage greater information sharing. Before discussing the obstacles to such information sharing, it is worth discussing these two Congressional directives which, in the Task Force's view, have received insufficient attention.

First, when Congress enacted the Homeland Security Act, it created the "Homeland Security Information Sharing Act" (HSISA), a free-standing law intended to promote the distribution of such information, whether classified or unclassified, to the public and private owners and operators of critical infrastructure.[4]

HSISA declares the sense of Congress that Federal agencies should share, to the maximum extent practicable, information that:

- Relates to terrorist threats;
- Relates to the ability to prevent or disrupt terrorist activity;
- Would improve the identification or investigation of suspected terrorists; and
- Would improve response to terrorist attacks.[5]

Essentially, HSISA instructs the President to develop homeland security information sharing systems to promote the sharing of both classified and sensitive but unclassified information.[6]

While the President has issued Executive Order 13311 delegating the relevant authority to the Secretary of DHS,[7] the Task Force is unaware that any further steps have been taken explicitly to implement the law.

[4]While HSISA speaks of sharing such information with "State and local personnel," that term is defined to include "employees of private sector entities that affect critical infrastructure, cyber, economic or public health security, as designated by the Federal government in procedures developed pursuant to [HSISA]." 6 U.S.C. § 482(f)(3)(F).

[5]*Id.* §§ 481(c), 482(f)(1).

[6]These systems are to have the capability to limit distribution to specific subgroups of people based on geographic location, type of organization, position of recipient within an organization, and need to know. *Id.* § 482(b). They may also condition distribution on limitations on redistribution. *Id.* The procedures can include issuing additional security clearances for classified information or entering into nondisclosure agreements for sensitive but unclassified information. *Id.* § 482(c). The law clarifies that information distributed through these procedures remains under the control of the Federal Government and may not be released under state open records laws. *Id.* § 482(e).

[7]68 Fed. Reg. 45149 (July 31, 2003). *See* esp. § 1(f).

Second, the Intelligence Reform and Terrorism Prevention Act, passed in December 2004, requires the President to establish an "information sharing environment" (ISE) within the Federal Government to facilitate sharing of information about terrorists, and the threats they may pose, "among all appropriate Federal, State, local, and tribal entities, and the Private Sector."[8] The ISE is intended to "promote a culture of information sharing."[9] Compliance with the ISE is mandatory on Federal agencies that possess or use terrorism information.[10] The law establishes a series of milestones for implementation of the ISE.[11]

The Task Force calls on the Administration to implement HSISA and the Intelligence Reform law. In doing so, and in other ways, DHS should take clear steps to increase the amount of homeland security information that it shares with Private Sector owners and operators of critical infrastructure. To do so, DHS will need to overcome the following legal obstacles. The discussion below identifies the Task Force's recommendations in these regards.

1. Sensitive But Unclassified Issues

Where information has not been classified, the Task Force believes that DHS has been overly reluctant to share it with owner/operators of critical infrastructure. In the two Congressional enactments just discussed (HSISA and the Intelligence Reform law), Congress emphasized the need for the Federal Government to more broadly disseminate unclassified information, as well as classified information. Unfortunately, the culture of the classified world still adversely influences handling of unclassified information.[12]

- *"Need to know" attitude.* Much, if not most, unclassified security information is still restricted to those that the possessor of the information determines have a need to know, often not including the Private Sector. The problem with this way of thinking is that the possessor of information may not know who else may find information useful or why.[13]
- *Need for originator permission for broader dissemination.* This constraint makes further dissemination of information much more difficult. The Task Force believes that voluntary private submitters of sensitive information to the Federal Government ought to be able to condition or limit subsequent dissemination of that information, since they bear the risk if information is misused. But information that the government originates should not be subject to continuing originator control.

[8]Pub. L. No. 108-458, 6 U.S.C. § 485(b)(2) (emphasis added).

[9]*Id.* § 485(d)(3). [10]*Id.* § 485(i).

[11]The ISE is to be run by a program manager designated by the President. *Id.* § 485(f). (The President designated John Russack on April 15, 2005.) It is to be overseen by the "Information Sharing Council," a new name for the "Information Systems Council" established by the President last August to strengthen sharing of terrorism information. *Id.* § 485(a)(1), (g). The Program Manager was supposed to issue an initial report on establishment of the ISE by June 15, 2005, containing among other things "a description of the technological, legal, and policy issues presented by the creation of the ISE, and the way in which these issues will be addressed." By September 13, 2005, the President is due to "leverage all ongoing efforts consistent with establishing the ISE" and issue guidelines for promoting information sharing. The guidelines must "ensure that information is provided in its most shareable form, such as by using tearlines to separate out data from the sources and methods by which the data are obtained"; and "reduc[e] incentives to information sharing, including over-classification of information and unnecessary requirements for originator approval . . . and . . . providing affirmative incentives for information sharing." *Id.* § 485(d). By the end of 2006 and annually thereafter, the President must report on "the extent to which . . . information from owners and operators of critical infrastructure is incorporated in the ISE, and the extent to which individuals and entities outside the government are receiving information through the ISE." *Id.* § 485(h)(2)(G).

[12]This section of the report applies to all unclassified security-related information that warrants being safeguarded, regardless of precise label used to describe it (i.e., "sensitive but unclassified," "for official use only," etc.).

[13]*See* National Commission on Terrorist Attacks upon the United States, 9/11 COMMISSION REPORT 417 (2004).

- *Bias against disclosure to private owner/operators.* Because classified information is rarely provided to members of the Private Sector, many persons within the government charged with managing unclassified information are reluctant to share it readily with private personnel.
- *Indiscriminate use of FOUO, SBU labels.* "For official use only" and "sensitive but unclassified" are labels that provide a basis for safeguarding information (i.e., managing it carefully). Many within government do not understand that these labels are not, however, a legal basis for withholding information from private persons.[14]

These legacy issues continue to be a problem. For example, representatives of the natural gas utility industry were given the initial list of DHS "protective security advisors," but were told that the list could not be disseminated within the industry, nor shared with other interdependent sectors (e.g., the electric utility industry).

The Intelligence Reform law[15] and the 9/11 Commission Report[16] both urge greater reliance on trusted information sharing networks where, once individuals or organizations are accredited members of the network, they are trusted to determine who else can see information. Part of this solution may be broad acceptance of definitions of FOUO and SBU that affirmatively urges sharing within such networks.

2. Classification Issues

A. Perception that too much information is classified

There is a widely shared perception, by Task Force members and others, that the current classification system results in too much information being classified by the government. This perception is not new or exclusive to private businesses. For example, the 9/11 Commission Report found that "[c]urrent security requirements nurture overclassification and excessive compartmentalization of information among agencies."[17] The official in charge of classification policy across the Federal Government has made the same point.[18] Incentives to overclassification were also highlighted in the Intelligence Reform law.[19]

In large measure, the obstacle arises from the fact that, pre-9/11, terrorist threat information was generally classified and of interest to very few people outside the Federal Government. Now, however, that information is vitally necessary to representatives of critical private entities. They need this information in order for their vulnerability assessments to be well-informed and their security measures targeted. They also need it for both these efforts to be an efficient use of resources, rather than a blunderbuss approach.

A second reason for this obstacle is that a number of the individuals who originally were detailed to the White House Office of Homeland Security and who were involved in the creation of DHS came from the military, law enforcement and intelligence communities. All of these communities are experienced in adversary tactics and are highly disciplined. Thus, they have been heavily trained on national policies regarding classification and clearances, and are used to operating on a need-to-know basis.

[14] *See* James W. Conrad, Jr., "Protecting Private Security-Related Information from Disclosure by Government Agencies," 57 ADMIN. L. REV. _ (Summer 2005) (in press) (Attachment C), at 17-18.

[15] *See* 6 U.S.C. § 485(d)(3).

[16] *See* 9/11 COMMISSION REPORT at 418.

[17] *Id.* at 417.

[18] J. William Leonard, Director, Information Security Oversight Office, National Archives & Records Administration, "Information Sharing and Protection: A Seamless Framework or Patchwork Quilt?" Remarks at the National Classification Management Society's Annual Training Seminar, Salt Lake City, Utah (June 13, 2003), available at http://www.fas.org/sgp/isoo/ncms061203.html. *See* also Markle Foundation, PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE 14 (Oct. 2002).

[19] *See* 6 U.S.C. § 485(d).

While the best at what they do, these communities do not have long traditions of regulating or otherwise interacting with the Private Sector on a regular basis. Those practices and attitudes, while useful in their original applications, are not conducive to effective information sharing with critical Private Sector entities.

B. Disseminating unclassified summaries

Where information must be classified, DHS and other agencies should work harder to produce unclassified versions. In some cases, information will continue to need to be classified. In such cases, government staff should be trained to maximize the amount of that information that can be shared in an unclassified manner, by "writing for release," producing abstracts or digests, use of tear sheets that do not reveal sources and methods, etc. Again, these are fundamentally attitudinal and cultural issues, but may need to be implemented via new policies.

C. The slow clearance investigation and adjudication process

Congress, the GAO and others have repeatedly found that the Federal Government – especially outside DHS -- has been too slow in issuing security clearances to enable critical infrastructure owners and operators to have access to classified information. This was a principal finding of the Intelligence Reform Act.[20] The GAO came to the same conclusion recently in its examination of information sharing in the maritime security context, in which it concluded that "[t]he major barrier hindering information sharing has been the lack of security clearances for nonfederal members of [area maritime security] committees or [interagency operational] centers."[21]

To varying degrees, Task Force members and their organizations have experienced this problem first hand.

Recommendations

1. ***DHS and the Private Sector should work in collaboration to develop a formal, and objectively manageable, homeland security intelligence/information requirements process.***
   - *The process should place a premium on, and leverage, superior Private Sector information resources, expertise in business continuity planning, and understanding of critical infrastructure sector operation and resiliency. (M/A)*
   - *The process must recognize the diversity of the Private Sector. (A)*
   - *DHS should partner and collaborate with the Private Sector in developing an integrated architecture for information collection and sharing. The Task Force understands that this is how HSIN is being developed and how HSIN-CI (with 40,000+ members) operates. The Task Force supports that approach. (M/A)*
   - *The Private Sector and DHS need to integrate and align their requirements for information collection and sharing. (M/A)*
   - *Information Sharing & Analysis Centers (ISACs), Sector Coordinating Councils (SCCs) and other Private Sector organizations and stakeholders must coordinate their efforts and define Private Sector requirements for DHS, so specific Private Sector entities can formally request, track and receive only that information requested. This will require doing a better job of articulating what types of information they want from government and with what frequency. (M/A)*
   - *The process should include a greater bias toward disseminating more information in unclassified form. The solution should not primarily be to investigate more people and issue more clearances. (M/A)*

[20] *See* 50 U.S.C. § 435b.

[21] GAO, MARITIME SECURITY: NEW STRUCTURES HAVE IMPROVED INFORMATION SHARING, BUT SECURITY CLEARANCE PROCESSING REQUIRES FURTHER ATTENTION, "What GAO Found" (GAO-05-394) (April 2005).

- *Where information must be classified,*
    - *DHS and other agencies should work harder to produce unclassified versions. (M/A)*
    - *The President should continue to implement on a timely basis the provisions of the Intelligence Reform law designed to expedite the clearance process. (M)*

II. Different Considerations for Threat Information and Vulnerability Information

A. Vulnerability Information Is Uniquely Sensitive

The Private Sector makes a key distinction between threat and indications and warning (I&W) information and vulnerability information. The former, absent sources and methods, is more important and should be less problematic to share. As a philosophical matter, Government has a clear Constitutional duty to "provide for the common defense" and, implicitly, to warn citizens about and protect them from hostile forces, both foreign and domestic.

As to the latter, while the Homeland Security Act sets out broad mandates for DHS's Information Analysis & Infrastructure Protection Directorate (IAIP) (or its 2SR successor), it is clear that the most effective manner of complying with those mandates has not yet been developed, and unclear that IAIP must or can perform all aspects of this task itself.

The government continues to ask industry to provide a vast array of information, up to and including all possible information concerning its critical facilities. Attachment D is a summary list of desired information, but interested readers should review any of several official DHS 'requirements' documents, all of which are tens of pages long and seek enormous amounts of information.[22] (These documents are not attached because they are labeled "For Official Use Only.") Many within the Private Sector, however, are reluctant to comply with such requests, for the following reasons:

- It is still uncertain on what basis such information can or will be kept confidential, and few companies are willing to risk the legal, business, or other consequences from an inappropriate disclosure. See Part Two, § II below.
- Neither DHS nor any other agency could properly store, much less even begin to analyze, the vast amount of information it would receive if it got everything it is seeking.
- The data being requested changes too often and too quickly for DHS (or any other agency) to create a stable, useful database.
- DHS already knows, or should know, where to get specific, detailed industry information when it is truly needed, but does not (or does not appear to) do so, do so consistently, or appropriately share such information it may receive with relevant offices within DHS.

In general, the risks of sharing such information seem to outweigh the benefits. Risks identified by members of the Private Sector include:

- Vulnerability information provided to the government might be used against companies in other contexts. For example, the government might decide not to contract with a company that it determines is too vulnerable in some respect.
- Companies are not confident that government will help industry fix any problems that are found.

[22] E.g., "Terrorist Threats to the U.S. Homeland – Reporting Guide for Critical Infrastructure and Key Resource Owners and Operators," forwarded under a January 24, 2005 memorandum from Under Secretary Frank Libutti; "Priority Intelligence/Information Requirements, January 2005-July 2005," forwarded under a January 7, 2005 memorandum from Assistant Secretary Patrick Hughes.

- Knowledge of vulnerabilities could lead to inappropriate government interference with business operations. For example, some vulnerabilities do not warrant remediation under any reasonable cost/benefit analysis of the probability they will be exploited, the consequences if they were, and the cost of remediation.
- Although some vulnerabilities may need Federal involvement, most are regional or local and need, at most, only state or local government involvement. Even there, state sunshine/openness laws create disincentives for the Private Sector to share information, and for government-owned entities to assess or review their own vulnerabilities.

B. National Asset Database vs. Other Means of Storing Vulnerability Data

As the portions of the emerging NIPP and the Sector Specific Plans (SSPs) dealing with vulnerability assessment are being rewritten, the respective roles and responsibilities of the Private Sector and IAIP (and of specific components within IAIP and elsewhere in DHS) need to be carefully re-evaluated to deploy public and private resources most efficiently and economically — and to avoid creating greater risks. The Task Force is particularly concerned about the wisdom and feasibility of creating and maintaining a "national asset database" of critical infrastructure assets and key resources:

- Exploitable vulnerabilities in cheaply produced, foreign-written software and the level of attack sophistication grow daily. Databases of all varieties are compromised continually. National asset and vulnerability databases will become the number one target of terrorists and hostile nations (either to access or disable). While one can understand Congress' intent in directing the creation of such databases, it obviously did so with the assumption that such databases could be completely secure and thus not become principal instruments of the Nation's destruction. This is not a sound assumption. Accordingly, a growing number of decision makers within the Private Sector simply do not want to assist in the creation of what could become a "target list" featuring them.
- How can the currency of such a large database possibly be maintained, given the number of facilities covered and the fact that their vulnerabilities change over time as the facilities and their operations change?
- Is the creation of this massive data base seen as an end in itself? Such a database is not useful to the Private Sector, members of which as a matter of sound business practice constantly conduct their own risk analyses as part of operational continuity programs.

The Task Force recognizes that the statutory responsibilities of the Under Secretary for Information Analysis and Infrastructure Protection include "carry[ing] out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructures of the United States [and] integrat[ing] relevant information, analyses and vulnerability assessments (whether . . . provided or produced by the Department or others) in order to identify priorities for protective and support measures by the Department . . . and other entities."[23] On the other hand, however, it is unclear that the most effective manner of complying with those mandates has yet been developed, or indeed that IAIP must or can perform all aspects of this task itself. At a minimum, the Task Force believes that the bolded language quoted above signals Congress' intent that DHS allow this work to be carried out by those critical entities where they have the capability and willingness to do so.

Understanding that DHS is, in part, responding to Congressional directives, the Task Force suggests (a) a review of the government's Y2K transition information sharing success and (b) a legislative effort to relieve DHS of some of the vulnerability data-gathering and maintenance requirements imposed on it by the Homeland Security Act.

[23] 6 U.S.C. § 121(d)(2), (3).

Recommendations

2. **DHS should adopt a tiered approach to infrastructure vulnerability information sharing.**
    - Carefully consider the known and exploitable vulnerabilities of database technologies, and the consequences of compromise of a "national asset database" of vulnerabilities. (L/M)
    - Maintain appropriate Federal information at the DHS level, state information at the state level, local information at the local level, and Private Sector information at the Private Sector level. (L/M)
    - To enhance the security of vulnerability information, maintain public sector infrastructure information at the city and municipal level and Private Sector information with trusted third party/non-governmental entities. (L/M)
    - DHS devote a substantial effort to establishing an appropriate organization or process for cross-sector and government information exchange. (M)

III. Diversity Within the Private Sector

The Private Sector is not monolithic. There are significant differences both across and within sectors. In addition, there are often crucial differences between roles and capabilities of trade associations and those of owner/operators. DHS must respect these differences as it develops a process for sector coordination.

The Task Force understands that, from government's point of view, given competing demands and limited resources, "one stop shopping" for information exchanges with the Private Sector is a desirable goal. However, as DHS rewrites the National Infrastructure Protection Plan, it must carefully reconsider how feasible or desirable such a goal is in light of the divergent evolution of Sector Coordinating Councils, Information Sharing & Analysis Centers and similar bodies.

Paragraph 25 of Homeland Security Presidential Directive/HSPD-7 mandates that DHS and other Sector-Specific Agencies (SSAs) "collaborate with appropriate Private Sector entities and continue to encourage the development of information sharing and analysis mechanisms." In addition, that paragraph provides that sector coordination mechanisms should " a) identify, prioritize and coordinate the protection of critical infrastructure and key resources; and b) facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices." It is thus understandable that, in drafting the NIPP, DHS would attempt to combine these functions (and more) in a symmetrical array of "Sector Coordinating Councils" (SCCs), each paired with a "Government Coordinating Council." A recent presentation by the Director of IAIP's Infrastructure Coordination Division (ICD) listed the following roles for SCCs:

- serving as a "single forum into sector for entire range of HS issues,
- institutionalizing the sector's coordination of policy development, sector wide strategy and planning,
- program promulgation and implementation,
- monitoring of progress,
- provision of best practices and guidelines,
- requirements for information sharing, research and development,
- point of cross sector coordination."

It is not clear that a single entity will (or should) be able to perform all these functions — which go beyond the role prescribed in HSPD-7 — for a critical sector in an effective, efficient, and expeditious manner. The scope outlined by ICD includes a broad array of policy, operational, strategic and tactical functions, many of which can only be performed by those who own and operate specific Private Sector infrastructure elements. As discussed in Part Three, moreover, there are significant benefits to limiting SCCs (and ISACs) to primarily operational issues.

Different sectors have organized themselves in a variety of ways to accomplish the information sharing and coordination functions described in HSPD-7:

- The Food and Agriculture SCC, for example, includes two representatives and one alternate from each of seven sub-councils, and has a six-page statement of governing principles and procedural rules. Its decisions must be by consensus of representatives of all sub-councils, rather than by a majority of all members. Most of the members are trade associations.
- The Financial Services SCC was founded by the Treasury Department, while the Financial Services ISAC predates it and was founded by the banking and finance industry itself. The majority of the Financial Services SCC members are trade associations; the majority of the Financial Services ISAC members are individual banks and financial institutions.
- The IT and Communication Infrastructure (formerly telecommunications) Sectors are still in the process of forming and have just formed their SCCs, although each sector already has its own ISAC and dedicated DHS component (NCSD and NCS, respectively).

These last two sectors offer some interesting contrasts.

- The Communications Infrastructure sector, with a relatively small number of companies and four associations (wire line carriers, wireless carriers, equipment manufacturers, and now internet service providers) has a long history of cooperation and National Security/Emergency Preparedness (NS/EP) coordination under the NSTAC and the NCS in the Defense Department. The Communications Infrastructure SCC makes it very clear that it will address policy matters only, that operational matters will be handled by the Communications Infrastructure ISAC, and that while they will coordinate, they will remain separate.
- The IT sector includes hardware and software manufacturers, internet service providers, network providers, telecomm companies, cable companies, data security companies, and service companies. In general, there are many more companies than trade associations. Indeed, information technology is so pervasive in our economy that the sector is still debating criteria for inclusion (e.g., whether the majority of a company's income comes from producing IT components — hardware, software, or services — the extent in which IT is used in a company). The sector is also considering membership in the context of funding. The IT/ISAC requires funding to operate and, as such, membership is limited to those who contribute (with some exceptions). However, many feel that the IT SCC should be more broadly based and free.

This diversity highlights the need for DHS to provide flexibility for the different sectors.

Recommendations

3. **DHS needs to be flexible and responsive in accommodating diversity within and among Private Sector critical infrastructure sectors.**
   - HSPD-7 calls for two functions: information sharing and sector coordination.
   - Sector Coordinating Councils in every sector may not be able to perform all the functions DHS desires. At a minimum, DHS must allow each sector to determine the nature, functions, and rules of its council and its relationship with its ISAC and SSA. (M/A)

IV. Developing a Resilient and Integrated Network for Information Sharing

A. Range of Views Regarding Need

The Private Sector has varying desires regarding the best communication mechanisms for receiving threat information.

- Some feel the need for a new communication mechanism similar to the State Department's OSAC. They feel that the new Homeland Security Information Network—Critical Infrastructure (HSIN-CI) will be able to serve that function (especially to the extent that it can operate across sectors within regions, similar to how some InfraGard chapters and Area Maritime Security Committees function at the local level).

- Others appear to be better at communicating with DHS, and believe they get sufficient information through existing mechanisms, whether formal or informal. Private Sector representatives who are already comfortable with existing mechanisms are concerned that new mechanisms could lead to new turf battles. Similarly, most feel that sharing with State and local constituencies seems to work well, and where it works there is felt to be no need for new mechanisms.

Whether or not they felt new procedures are necessary, most Private Sector representatives believe that existing communication mechanisms are defective to some degree, or at least inconsistent. Many feel that IAIP has not sufficiently focused on the interoperability/interdependence of critical infrastructure elements, and instead has become too organized by sector "stovepipes." Information must flow in the most effective and efficient manner. How that task is accomplished is ultimately DHS' job, but the current organization is duplicative and confusing. In the telecommunications sector, for example, the Network Design & Analysis Capability is maintained by the National Communications System, but under the current interim Sector Specific Plan for the telecommunications sector, it is unclear whether that data will also be maintained by IAIP's Protective Services Division or put in the National Asset Database.

B. Satisfaction with Existing Arrangements Outside DHS

Many critical infrastructure sectors currently communicate among themselves about security issues through means to which the Federal Government has limited access (e.g., via ISACs). The existence of such capability creates reluctance within those sectors to move to a Federally-operated or overseen system (e.g., the Homeland Security Information Network). It also means that systems like HSIN are redundant to that extent. If DHS hopes to encourage entities within these sectors to switch to a Federally-sponsored or operated system, it will need to explain why its system will serve the sector's needs better and why the prospect of Federal access does not create a less attractive proposition.

Businesses with many critical infrastructure sectors already have trusted relationships with other sector-specific agencies, FBI field offices, and State & local governments (especially law enforcement and emergency response). The path of least resistance in such cases would be for DHS to work with those other governmental units rather than initiating a new relationship directly with the business. For any new relationships, DHS would need to show why that relationship was not redundant, why it added value to the business and why it was equally trustworthy.

C. Importance of Trust and Personal Relationships

Several groups examining the question of information sharing have emphasized how much the process relies on trusted personal relationships. In many cases these arise from people having previously worked together, or for the same organization (e.g., the Coast Guard). In other cases, they simply have to grow out of an extended period of association. By and large, members of Private Sector critical entities already have these relationships with State and local governments, and, to a lesser extent, with their sector-specific agencies. By and large, they do not have them with DHS or its contractors, except in those cases where a Private Sector individual worked with a DHS employee in some prior capacity, or both worked for the same organization. DHS simply has not been around long enough in stable form for trusted relationships to have developed in a great many cases. That problem has been exacerbated by frequent reorganizations within DHS and high turnover or transfer of DHS staff.

In a growing number of cases (e.g., the DHS sector specialist for the chemical sector), the private and public personnel involved have worked long and closely enough together that these sorts of trust relationships have been established. Time and stability should produce additional such relationships.

However, and despite the foregoing, many in the Private Sector feel there is too much reliance on preexisting personal relationships rather than on the creation of effective mechanisms (i.e., that there is often more willingness to rely on existing trusted personal relationships, rather than attempting to build trust in some new, untested communication mechanism). Whatever the case, it is clear that any new model for information sharing will need to address the trust issue (as HSIN-CI has done), and not simply assume that people will use a new and untested system because the Federal Government created it.

D. General Design Considerations

The Task Force identified several other considerations relevant to design of a new model for information flow:

- As explained above, DHS needs to include the Private Sector in the "intelligence cycle" – especially the requirements definition process – in order to better enable government to collect information for analysis and timely dissemination that will permit it to provide tailored, actionable answers to industry's questions.

- A means must also be created to allow greater State, local and tribal involvement in filtering or analyzing data. It is simply too massive a job for, and beyond the capabilities of, the Federal Government alone.

- As the amount of information goes up, the need for specialized communication mechanisms increases.

- New mechanisms may be more appropriate for future increases in threat level if suicide bombing, etc., moves into the U.S.

- DHS needs to regularize processes and strive for high level consistency in processes, while maintaining flexibility in quantity and type of information.

- There needs to be a free flow in both directions, and among all constituencies, regardless of the source of data, or who undertook the analysis.

- There is a crucial time element at play in information exchanges involving both threat, indications and warning data and vulnerability data. This element spans the spectrum between near real time transmittal of threats from government at all levels and the Private Sector to deliberative policy advice or regulatory comments from the Private Sector which can take weeks or months to prepare, discuss and finalize. A comprehensive model or vehicle for transmission of all types of information would need to encompass this range of data and operational need.

Clearly there is much that the Private Sector should do as well to improve the process, and to help forge a meaningful two-way partnership.

E. The Need for Regular, Interactive Threat Discussions

DHS and critical sectors must develop a meaningful process to have real time, detailed discussions about threats. Currently, IP conducts a single classified threat briefing semiannually for the combined electrical, energy and chemical sectors. Such briefings are somewhat instructive and are very much appreciated. However, every six months is too infrequent, and lumping three sectors into one briefing results in long sessions much of which is not relevant to two-thirds of attendees. Most problematic, the presentations still are frustratingly hypothetical, illustrative and general.

We believe that IAIP's Information Analysis Division would be willing to conduct a dialogue and share certain more detailed threat information with selected individuals in the security departments of critical infrastructure companies, but a mutually satisfactory vehicle for doing so must be developed. The Infrastructure Protection Division, as the primary interface with members of critical sectors, should arrange such interactions (e.g., a question and answer session and discussion in some detail of the ability of terrorists to disrupt the generation and/or transmission of electric power in the Southeastern United States). These sessions should be held more often than every six months, and should be held separately for each sector.

Recommendations

4. **DHS should continue to develop a network integrated information model for information flow.**

- Significant work required:
  - DHS should employ a "hub and spoke model" for information flows, as used in HIN and HSOC. (M).
  - Information should flow from the Private Sector and other government sources to the DHS hub for analyses, and then be distributed back to the Private Sector on a targeted basis. (M)
  - DHS needs Private Sector input and presence at the hub. (M/A)
- As a national priority, build a resilient/survivable Homeland Security Operations Center (HSOC) and Homeland Security Information Network (HSIN). (M)
  - In their current condition, both are single points of DHS operational failure – an unacceptable circumstance.
- Leverage the unparalleled success of, and invest in expanding, HSIN-Critical Infrastructure (CI). (M)
  - HSIN-CI is a trusted and proven model for effectively gathering and sharing information.
- Statewide intelligence/information fusion centers should be integrated into national information sharing efforts. (M/A)
- *DHS should hold regular collaborative sessions (start monthly) with each Private Sector coordinating organization (e.g., SCCs, ISACs). (M)*
- *DHS should hold regular, detailed threat briefings with each sector.*
  - *Representatives of IA and IP should meet with selected individuals in the security departments of critical infrastructure companies. (M)*
  - *The sessions should be held more often than every six months, and should be held separately for each sector. (M)*
  - *They should involve more specific information than is currently presented in classified sector briefings. (M)*
  - *They should be oriented less toward presentation and more toward dialogue. (M/A)*

The second part of this report analyzes the legal and related issues that the Task Force identified as impeding better information sharing between government and critical infrastructure entities. In many cases, it will be difficult or impossible to make significant progress on the preceding recommendations until these obstacles can be overcome.

I. Regarding Private Sector Representatives as Partners

As noted earlier, many within DHS come from intelligence, military, or law enforcement backgrounds where they have had little regular, official contact with the Private Sector. By contrast, most other sector-specific agencies engage continually with Private Sector and other non-governmental stakeholders through rulemaking, permitting and other interactive processes. Because of their background, these DHS personnel often are not accustomed to viewing critical infrastructure owners and operators as real partners or customers. This has effects at two levels:

- *At the level of policy implementation.* As an example, on occasion DHS staff has not provided advance notice to corporate headquarters of a planned visit to a corporate facility. This has caused delay, as the facility awaits direction from headquarters, and may have engendered resentment or distrust.

- *At the level of policy formulation.* DHS staff may not consult with companies (or their trade associations) in the development of a policy that affects them. As a result, the policy is likely to be less effective and potentially even counterproductive. This point is particularly significant, because a small amount of up-front consultation may avert a great deal of delay and confusion later.

The lack of Private Sector involvement at both levels plays a large and ongoing role in all the other legal issues discussed in this part of the report. Building trust by recognizing Private Sector representatives as partners, and consulting with them early on and throughout the policy formulation process, would allow those entities to point out problems and concerns and to suggest workable solutions. Conversely, leaving them out of the process means that DHS may have to reverse course or undo earlier decisions, as it has had to do in the creation of the National Infrastructure Protection Plan. DHS's Office of Private Sector Liaison has been very helpful at undoing these kinds of problems, but an effective strategy of partnership to prevent them must be a Department-wide effort.

II. Liability Concerns

More than anything else, the issue that most affects private entities' willingness to share sensitive information with the Federal Government is the concern that this information will somehow be used against them in some subsequent governmental enforcement case or private civil action.

- *Enforcement.* Companies fear that information provided to DHS may somehow, whether advertently or inadvertently, be obtained by some other governmental agency that may use the information for enforcement of other, non-security-related laws or rules. EPA and OSHA are most commonly mentioned in this connection, but any Federal agency that has oversight over any critical sector (Treasury, FCC, DOE) is potentially a source of concern, as are foreign, State and local governments. It was not generally clear to the Task Force how information of the sort sought by DHS might indicate noncompliance with some other laws or rules, but this fear is quite widespread, strong, and possibly growing.

- *Litigation.* Companies similarly fear that information provided to DHS may come into the hands of private litigants – whether injured parties or shareholders -- who might use it against the company in the event that a terrorist attack does occur (or in other circumstances). Companies are concerned that vulnerability assessments or security plans may be used to show knowledge of a risk and lack of due care in response to it. Of course, the conduct of a vulnerability assessment, and implementation of security measures, can also be probative of due care, whereas the failure to take either step may show lack of the same. Nonetheless, many businesses feel that the likelihood of such information becoming available to and being used by adverse litigants is increased by sharing it with the government.

To some degree, these anxieties appear to be based on misunderstanding of existing law and procedure, and will be reduced when people understand how those laws and procedures actually work.

On the other hand, these fears cannot be completely assuaged by anything DHS does, for two reasons:

- *Legal uncertainty.* Part of companies' concern is the inherent uncertainty that attaches to any legal rule – one never knows for sure how a court will interpret it. This is particularly true with many legal authorities in the homeland security field, which are new and untested in court.

- "*Falling through the cracks".* People are also afraid that, even if applicable laws, rules and policies on their face would not allow information to be released to another agency or a potential litigant, mistakes may occur that have this result. These concerns grow when DHS is able to share information with foreign, State or local governments, since the question very logically then includes the adequacy of those entities' information security and protection capabilities.

These anxieties are heightened by the fact that bills are regularly introduced to weaken existing protections (e.g., OPEN Government Act, Restore FOIA Act), even in the face of known threats of enemy exploitation of publicly available information and growing vulnerabilities of information systems and networks.

As a general matter, DHS should always consider, address as necessary, and explain to potential submitters of information how it has addressed, the prospect of disclosure by any potential means. These include:

- FOIA requests from public to DHS,
- access by other Federal agencies (and for what purposes),
- FOIA requests to those other agencies,
- access by foreign, State and local governments (and for what purposes),
- FOIA-like requests to those other governments,
- civil discovery against any of the foregoing,
- criminal investigations (Federal or State).

In particular, the Critical Infrastructure Information Act (CIIA) provides that information submitted pursuant to it may be used by Federal employees, and State and local government agencies, only "for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act."[24] While that last proviso will concern some, this language should prevent a Federal agency using this information to pursue a civil enforcement action based on other laws. DHS should (a) maximize the opportunities for information to be submitted pursuant to that act, (b) should ensure that other agencies and governments afforded access to this information abide by this restriction, and (c) publicize the restriction and DHS's commitment to honoring and enforcing it.

[24] *Id.* § 133(a)(1)(D), (E).

It would also be helpful if DHS would publicly commit to following CIIA submitters' instructions regarding limitations on use and dissemination of information. DHS should not by default incorporate submitted information into major databases accessible to anyone within DHS.

III. Implementing the Critical Infrastructure Information Act

The Critical Infrastructure Information Act is a powerful law that offers unparalleled protections to private information submitters. In essence, it allows private owners and operators of critical infrastructure, or organizations representing them, to voluntarily submit information to DHS regarding threats, vulnerabilities and protective measures (critical infrastructure information, or CII), with assurances that the information will be protected from public disclosure. To promote integrated protection of critical assets, the law allows DHS to share this information with State and local governments for such purposes without fear that these other governments might have to disclose it. To protect this information, the law:

- Effectively codifies the *Critical Mass* decision nationwide,[25]
- Preempts state open records laws,[26]
- Blocks use by the government of protected information in civil litigation, and[27]
- Creates criminal penalties for Federal employees who knowingly disclose protected information.[28]

Besides classification, no other federal program offers such protections. Yet the law is not widely understood, and is regarded suspiciously by some for various reasons. One of these reasons is that the statute has not yet been tested in court. DHS obviously cannot do anything about that now. DHS can, however, do something about how the statute has been implemented, which is not as Congress intended – a point noted in a May 25 letter to Secretary Chertoff from Tom Davis, Chair of the House Committee on Government Reform. Three problems have dogged the CIIA's implementation: it has been slow, it has not been well-coordinated, and it has embodied narrow legal interpretations.

1. Slow pace of implementation

The process of implementing the CIIA has been frustratingly slow. The statute merely required DHS to issue "procedures" within 90 days of enactment, or by February 23, 2003. Nor did the statute condition its effectiveness upon issuance of those procedures. DHS instead chose to proceed through notice and comment rulemaking, a process that took over a year. An "interim" rule was not published until February 2004. DHS sought comments at that time on an eventual final rule.

The rule described a phased rollout:

- Phase I: information would be shared only within IAIP
- Phase II: information would be shared elsewhere within DHS
- Phase III: information would be shared with other Federal agencies and, pursuant to memoranda of agreement, with State and local governments

The rules provided initially for submission only on paper or other tangible media, but promised eventually to allow electronic submission.

[25] Critical Mass holds that where information is *voluntarily* supplied to an agency, the only question the agency need ask, in deciding whether the information is protected as confidential business information under FOIA, is whether the information is "of a kind that would customarily not be released to the public by the person from whom it was obtained." *Critical Mass Energy Project v. NRC*, 975 F.2d 871, 879 (D.C. Cir. 1992)(en banc). *Critical Mass* is only binding in the D.C. Circuit, whereas the CIIA applies nationwide.

[26] 6 U.S.C.§ 133(a)(1)(E).

[27] *Id.* § 133(a)(1)(C).

[28] *Id.* § 133(f).

[29] *Id.* § 133(e)(1).

[30] 69 Fed. Reg. 8074 (Feb. 20, 2004).

Almost 18 months later, DHS has apparently made little progress. (DHS claims to be constrained in describing the full state of current implementation due to the pendency of a final rule, a position the Task Force does not understand.) It is unclear to what extent DHS has allowed sharing of CII beyond IAIP but within DHS. There is no evidence, however, that DHS has rolled the program out to other Federal agencies. This been a problem for sectors whose sector specific agency is not DHS (e.g., electricity, whose sector specific agency is DOE).

Nor is there any evidence that DHS has rolled the program out to State or local governments, even though DHS has had a model MOA since February 2004.[31] This has led to problems in several States. For example, the New York State Office of Homeland Security has been trying to establish a mechanism whereby it can get access to vulnerability information to be submitted by facilities to DHS under DHS's Risk Analysis and Management for Critical Asset Protection (RAMCAP) program;[32] but does not yet have an approved MOA with IAIP even though it submitted the paperwork six months ago. Similarly, critical infrastructure businesses in California have been seeking enactment of a state counterpart to the CIIA so that they can confidently share security information with that State's Office of Homeland Security, since the State has apparently been unable to conclude an MOA with DHS. Maryland's Emergency Management Agency shares the same frustration.

Finally, DHS appears still not to be accepting CII electronically, even though the ISAC and HSIN mechanisms it has promoted with critical sectors for sharing of threat and incident data are all electronic systems.[33]

2. Poor coordination within DHS

The slow pace of CIIA implementation has been compounded by a consistent lack of coordination among the various components of DHS. At least initially, these components did not understand the relationship of the CIIA and other information protection regimes. For example, the preambles to the CIIA rule and the sensitive security information (SSI) rules issued by TSA and DOT both made erroneous statements about the other rules.[34] Implementation of the CIIA has not been well-coordinated even within IAIP. There is as yet no intake capability for CII among the three major programs within IAIP's Protective Security Division: its Protective Security Advisors, its Buffer Zone Protection Plan (BZPP), or its RAMCAP program. It would be quicker and administratively simpler for facilities who want to do so to submit information in the field, directly to their PSAs or to visiting PSD staff administering the BZPP or RAMCAP programs. Instead, they still have to submit paper copies to IAIP's central "PCII Program Office," and then all concerned must wait for that office to validate and forward it to the intended recipients.

3. Narrow legal interpretations

The third difficulty with implementation of the CIIA has been a series of conservative legal decisions by DHS:

- *No indirect submissions.* Most frustrating to critical infrastructure sectors whose sector specific agencies are not DHS, the CIIA rule does not allow "indirect" submission via agencies besides DHS. So, for example, financial institutions cannot submit CII to the Treasury Department, but must instead

[31]It is an appendix to the DHS PCII PROCEDURES MANUAL (Feb. 17, 2004).

[32]RAMCAP stands for "Risk Analysis and Management for Critical Asset Protection."

[33]The one exception to this statement is that DHS provides PCII protection for information that the telecommunications industry has been submitting electronically for years to the National Communications System.

[34]The CIIA preamble stated that SSI, unlike CII, "ordinarily will not be voluntarily submitted," see 69 Fed. Reg. 8076, which is incorrect, since much information is submitted voluntarily to the Coast Guard as SSI by facilities regulated under the Maritime Transportation Security Act either directly or indirectly (because they are located in regulated ports). Similarly, the preamble to the SSI rules asserted that the CIIA "generally prohibits disclosure of properly designated CII outside the Federal Government," see 69 Fed. Reg. 28069, which is also wrong since, as noted above, the CIIA explicitly anticipates CII being provided to state and local governments.

send it to DHS, which is then supposed to send it to Treasury (except that such interagency sharing is not yet occurring to the Task Force's knowledge).

- *"PCII."* The CIIA rule invented the concept of "pro- tected critical infrastructure information" or "PCII" – a phrase not in the statute. This concept only confuses things, in the Task Force's view, because now there can be "critical infrastructure information" that is not protected by the CIIA. (It would be simpler to conclude that information not meeting the definition of CII is not CII.)
- *Validation of all CII claims.* The CIIA rule requires DHS to review and "validate" all submitted CII. This approach is in contrast to the way Federal agencies have implemented the closely analogous FOIA exclusion for "trade secrets and commercial or financial information [that is] privileged or confidential" – a.k.a. "confidential business information" or CBI.[35] Under that practice, agencies simply note a CBI claim and treat the information accordingly, but do not evaluate the merits of the claim unless and until someone submits a FOIA request for that information. Validating every CII claim up front could become an administrative problem if the program ever gets busy.
- *No "class validations."* The CIIA rules do not provide for (although they do not exclude) the notion that particular categories of information could be deemed, in advance of submission, to be CII. This is peculiar, because the TSA/DOT rules regarding "sensitive security information" establish several 'categorical inclusions' – if information falls into one of these categories, it is automatically SSI.[36] The concept of class determinations regarding the applicability of FOIA exclusions (e.g., CBI) is also well-established at agencies like EPA.

The last issue is particularly problematic for Sector Coordinating Councils (SCCs), ISACs and similar bodies that represent critical infrastructure sectors. DHS has thus far been unwilling to determine up-front that all or some of the information supplied by such entities to DHS is CII. This refusal is frustrating because protecting such sharing is exactly what the CIIA was intended to facilitate. (Several Task Force members were closely involved in Congressional consideration of the CIIA and its predecessor bills over the course of several years.) There is no evidence that DHS has considered what proportion of SCC communications to DHS would qualify as CII, or whether their charters could be amended to clarify when their communications to DHS would be considered CII.

IV. DHS's Caution, Lack of Clarity Regarding Other Freedom of Information Act Exemptions

Outside the CIIA, DHS has also not taken clear, firm positions on applicability of other FOIA exemptions to information that private critical infrastructure entities might submit to DHS. Most prominent among these are the (b)(4) exemption for CBI and the (b)(7) exemption for law enforcement information the release of which "could reasonably be expected to endanger the life or physical safety of any individual."[37] Both of these exemptions would seem to be broadly applicable to security information submitted by private entities and potentially strongly defensible.[38] For example, the (b)(7) exemption could be sweepingly applied if all of DHS were a "law enforcement" agency, which is a reasonable interpretation of an obscure provision of the Homeland Security Act.[39] Notably, when the FBI ran the National Infrastructure Protection Center (NIPC), it took the position that information submitted to it via ISACs would be protected from

[35]U.S.C § 552(b)(4).

[36]These include "vulnerability assessments . . . directed, created, held, funded, or approved by the DOT [or] DHS, or that will be provided to DOT or DHS in support of a Federal security program," 49 C.F.R. §§ 15.5(b)(5), 1520.5(b)(5), and "any information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure," id. §§ 15.5(b)(7), 1520.5(b)(7).

[37]5 U.S.C § 552(b)(7)(F).

[38]*See* Attachment C at 11-16.

[39]*See* 6 U.S.C. § 122(c) (stating that the Secretary of Homeland Security "shall be deemed to be a Federal law enforcement . . . official").

release by both of these exemptions. The Task Force is not aware of any statement by DHS regarding how ISAC data is protected from release now that the NIPC has become the National Infrastructure Coordination Center and is housed within IAIP.

DHS has not reached out to the Private Sector — or the public — for comment on these very important questions. Rather, its decision process is opaque and apparently closely-held. Moreover, the positions that DHS components or staff do communicate on these issues seem to be ad hoc and uncoordinated. This lack of clarity regarding what need not be disclosed appears to have led to unfortunate disclosures of private information that need not have been disclosed. All the foregoing undermines the confidence of the Private Sector in DHS's judgment and its willingness and ability to address and resolve issues regarding nondisclosure under FOIA. These questions are not simple ones, but they are too important not to answer.

DHS, in consultation with the Department of Justice, should adopt broad, Department-wide positions regarding applicability of (b)(4) and (b)(7)(F) exclusions (at least). DHS (and DOJ) should state their intent to assert these positions aggressively so as to effectuate the purposes of the Homeland Security Act. DHS should train and test its personnel on these interpretations.

V. Federal Advisory Committee Act Issues

Virtually all critical sector interaction with DHS is slowed down and complicated by DHS staff concerns about compliance with the Federal Advisory Committee Act (FACA). FACA requires that "advisory committees . . . established or utilized" by a Federal agency must meet in open session, after prior notice in the Federal Register, and must make associated written materials public unless a FOIA exemption (other than the deliberative privilege exemption) applies.[40]

Like FOIA, FACA serves important and long-standing open government goals, and should not be evaded. On the other hand, neither should it impede vital communication between DHS and critical sectors of information that should not be made public. This is particularly problematic in the case of Sector Coordinating Councils, but the same problem arises with ISACs or any other sector-representative group with which DHS wants to consult or otherwise exchange information.

As discussed below, DHS has ample reason to take the position that SCCs, ISACs and similar bodies are exempt from FACA. Alternatively, or additionally, it has at least three means for exempting them from FACA. DHS should not, however, adopt FACA "work arounds" that treat these entities as subgroups of advisory committees, or that regard members of these entities as independent actors. These points are explained below.

1. Non-Federal critical infrastructure coordination entities are not advisory councils

There are at least two reasons why non-Federal critical infrastructure coordination entities are not advisory councils within the meaning of FACA – they are not "utilized" by DHS or other Federal agencies, and their activities are "primarily operational." Each is discussed below.

   a. SCCs and ISACs are not "utilized" by the government

A group including Private Sector representatives is an "advisory committee" subject to FACA only if it is "established or utilized" by a Federal agency.[41] SCCs, ISACs and similar bodies have been established by private entities, and so are not subject to FACA on that basis. But neither should they be subject to it on the theory that they are "utilized" by DHS or other sector specific agencies. The leading Supreme Court decision on this issue recognized that the Executive Branch "utilizes . . . in one common sense of the term" an American Bar Association committee for evaluating potential Federal judges.[42] However, the Court concluded that

[40] *5 U.S.C. App. 2, §§ 3(2), 10.*

[41] *Id.* § 3(2)(C).

[42] Public Citizen v. U.S. Dept. of Justice, 491 U.S. 440, 452 (1989).

Congress intended this term only to reach entities that are "utilized . . . in the same manner as a Government-formed advisory committee," and are "the offspring of some organization created or permeated by the Federal Government."[43] The Court noted three factors as particularly relevant in this determination: whether an entity was forme privately, rather than at the government's prompting, whether it receives Federal funds, and whether it is "amenable to . . . strict management by agency officials" along the lines imposed by an earlier Executive Order regarding advisory committees.[44]

Interpreting this decision, the D.C. Circuit has focused on the last of those three factors, declaring that "utilized . . . is a stringent standard, denoting something along the lines of actual management or control of the advisory committee," and only "encompass[ing] a group so closely tied to an agency as to be amenable to strict management by agency officials."[45] Even where government officials sit on a body and hence influence it, the D.C. Circuit noted, "influence is not control."[46] District courts employing this demanding standard have regularly and recently found FACA inapplicable to a wide variety of private groups.[47]

SCCs and ISACs generally have been formed privately; indeed, many ISACs predate DHS. Most do not receive any Federal funding. But most important, neither DHS nor other sector specific agencies strictly manage or control these private critical infrastructure sector entities. While the specific facts of each group differ, these bodies determine their own memberships, set their own agendas, and decide what recommendations or other information they will or will not provide the Federal Government. Indeed, many of these bodies are spiritedly independent of DHS, to DHS's frustration in some cases. The Task Force is not aware of any SCC, ISAC or similar group that is controlled by DHS or any other Federal agency.

In conclusion, the D.C. Circuit has observed that "the government has a good deal of control over whether a group constitutes a FACA advisory committee .... [I]t is a rare case when a court holds that a particular group is a FACA advisory committee over the objection of the executive branch."[48] The Task Force emphatically believes that this is not one of those rare cases.

b. SCCs' and ISACs' functions are "primarily operational"

[43] *Id.* at 463-64 (quoting H.R. Rep. No. 91-1731, at 9-10 (1970)).

[44] *Id.* at 457-58.

[45] *Washington Legal Foundation v. U.S. Sentencing Comm'n*, 17 F.3d 1446, 1450-51 (D.C. Cir. 1994) (internal citations and quotations omitted).

[46] *Id.* at 1451.

[47] *See, e.g., Washington Toxics Coalition v. EPA*, 357 F. Supp. 2d 1266, 1273-74 (W.D. Wash. 2004) (task force composed of representatives of pesticide manufacturers not covered by FACA, even though EPA consulted with it on test methods for developing data and used data compiled by it to determine whether pesticides may be registered); *Physicians Committee for Responsible Medicine v. Horinko*, 285 F. Supp. 2d 430, 445-46 (S.D.N.Y. 2003) (trade association and environmental group collaborating with EPA to design high production volume chemical testing program not subject to FACA; no evidence that EPA "was the driving force behind . . . meetings or that it exerted any control over who attended and what was discussed"); *American Soc. of Dermatology v. Shalala*, 962 F. Supp. 141, 147 (D.D.C. 1996) (although HHS sent an observer to each meeting of one American Medical Association group and had a panel position on the other, the AMA groups were run by the AMA, which appointed their members, provided staff, set the agenda, recorded the minutes, and maintained records), aff'd mem. 116 F.3d 941 (D.C. Cir. 1997); *Huron Env'tl Activist League v. EPA*, 917 F. Supp. 34, 40 (D.D.C. 1996) (even though EPA determined the schedule for a group's meetings and made other logistical arrangements for them, provided the meeting rooms, and spent public funds to retain a consultant to attend and assist with the meetings, "[n]othing in this case suggests that the working group is subject to actual management or control by the EPA, or that the industry representatives are so closely tied to the executive branch of the government as to render it a functionary thereof").

[48] *Association of Am. Physicians & Surgeons, Inc. v. Clinton*, 997 F.2d 898, 914 (D.C.Cir.1993).

The General Services Administration's rules implementing FACA provide that entities whose functions are "primarily operational" rather than "advisory" are exempt from FACA.[49] The rules define "operational functions" as "those specifically provided by law, such as making or implementing Government decisions or policy."[50] The Homeland Security Act (HSA or the Act) specifies a long list of functions for the Under Secretary of Information Analysis and Infrastructure Protection (IAIP), and that list repeatedly establishes roles for "Private Sector entities" – as opposed to "the public" -- to play. Under the Act, these entities have distinct roles in:

- providing "intelligence . . . and other information" for analysis;[51]
- taking "protective and support measures"[52];
- "in cooperation with" IAIP, "recommend[ing] measures necessary to protect the key resources and critical infrastructure of the United States";[53]
- receiving "warning information, and advice about appropriate protective measures and countermeasures," as part of the Homeland Security Advisory System;[54]
- receiving "information analyzed by the Department . . . in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States";[55]
- "consult[ing] with [IAIP] to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States";[56]
- providing "additional information . . . relating to threats of terrorism"; and[57]
- "coordinat[ing] with elements of the intelligence community and with Federal, State and local law enforcement agencies . . . as appropriate."[58]

The operational partnership spelled out in the Act has been implemented by the President via Homeland Security Presidential Directive/HSPD-7. That document instructs the Secretary of DHS to "coordinate protection activities for [listed] critical infrastructure sectors."[59] HSPD-7 also requires DHS and other sector specific agencies generally to "collaborate with appropriate Private Sector entities . . . ."[60] In particular, it requires them to "continue to encourage the development of information sharing and analysis mechanisms," and "to continue to support sector coordinating mechanisms," whose functions it specifies as "(a) to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and (b) to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices."[61]

[49] 41 C.F.R. § 102-3.40(k).
[50] *Id.*
[51] *See* 6 U.S.C. § 121(d)(1).
[52] *Id.* § 121(d)(3).
[53] *Id.* § 121(d)(6).
[54] *Id.* § 121(d)(7)(B).
[55] *Id.* § 121(d)(9).
[56] *Id.* § 121(d)(11).
[57] *Id.* § 121(d)(13).
[58] *Id.* § 121(d)(17).
[59] Homeland Security Presidential Directive/HSPD-7, § 15 (Dec. 17, 2003).
[60] *Id.* § 25.
[61] *Id.*

Based on the foregoing, DHS has ample basis to, and should, take the position that SCCs, ISACs and similar bodies are primarily operational in nature. The Homeland Security Act and HSPD-7 have clearly established a range of functions that private critical infrastructure sectors are intended to serve, in cooperation with DHS and other agencies. These functions are not primarily about providing DHS or the President with broad "advice or recommendations on issues or policies" – to quote the FACA regulations.[62] As discussed above, some of these bodies may also serve broader policy functions, but that function should be seen as secondary to fulfilling their statutory roles. Moreover, as one court has just noted, "[a]s long as a committee is not a Federal advisory committee under the legal standard delineated [by the Supreme Court], the Court does not find anything in the statute to indicate that Federal agencies may not consult with such committees regarding policy issues without subjecting those committees to FACA regulations."[63] SCCs and ISACs are certainly not intended to be stakeholder bodies in the way that advisory committees are generally understood to be, and the touchstone for their constitution is representativeness or inclusion, not "balance."[64]

Fundamentally, the challenge of ensuring the resilient/reliable operation of critical infrastructure is unique, as it requires close communication and coordination between critical private sector entities and the Federal agencies charged with regulating them. Those communications, moreover, must remain non-public in order for those functions to be served. As specified in statute, these communications are to involve intelligence and law enforcement information, and are to serve warning, preventive and protective functions.

Disclosing this sort of information would defeat the purpose of those communications by giving our nation's enemies information they could use to most effectively attack a particular infrastructure and cause cascading consequences across multiple infrastructures.

In coordination with the FACA Committee Management Secretariat, managed by GSA, DHS should officially determine that SCCs, ISACs and similar bodies exercising functions under the HSA provisions referenced above are not advisory committees under FACA.

Alternatively, or in addition, DHS should also act to exempt SCCs, ISACs and similar bodies from FACA. It could do so in any of three ways, listed below in rough order of preference from the Task Force's perspective.

2. "Communications of critical infrastructure information."

Subtitle II of the HSA has two subtitles. Subtitle A, just discussed, describes the functions of the IAIP Directorate and the roles of the Private Sector in those functions. Subtitle B is the CIIA – demonstrating the important linkage between the roles of critical sectors and the CIIA as a means of effectuating those roles. The CIIA includes a FACA exemption intended to enable "information sharing and analysis organizations" (not necessarily "ISACs") to share "critical infrastructure information" with DHS.[65] This exemption was enacted precisely to enable the coordination purposes of Subtitle A. Moreover, the exemption is analogous in function to a comparable FACA exemption in the Maritime Transportation Security Act, currently being used by the Coast Guard to allow it to interact confidentially with Area (i.e., port) Maritime Security Committees.[66]

[62] *See* 41 C.F.R. § 102-3.25.

[63] *Washington Toxics Coalition v. EPA,* 357 F. Supp. at 1274.

[64] *Cf.* 5 U.S.C. App. 2, § 5(b)(2) (requiring advisory committees to be "fairly balanced in terms of the points of view represented and the functions to be performed by the advisory committee").

[65] *See* 6 U.S.C. § 133(b)("No communication of critical infrastructure information to [DHS] made pursuant to [the CIIA] shall be considered to be an action subject to the requirements of [FACA].").

[66] 46 U.S.C. § 70112(g)(1)(B)). This exemption references those committees, rather than referring to the type of information being communicated, as the CIIA FACA exemption does. This difference is not significant, however. The MTSA references the precise entities to which it applies because the MTSA also created those entities. By contrast, when the CIIA was enacted (in 2002, as part of the Homeland Security Act), it was unclear – as it remains today -- exactly what entities would be serving as representatives of critical infrastructure sectors. The CIIA exemption permits the diversity of approaches sought by the various sectors by focusing on type of information being communicated, rather than on name of the entity doing it.

The statutory definition of "CII" is quite broad, and encompasses the topics covered in HSA Subtitle A and HSPD-7, and of greatest importance to critical sectors and DHS.[67] Therefore, DHS can and should rely on the CIIA's exemption to free SCCs and ISACs from FACA provisions. This approach has the virtue of simultaneously solving both of the problems created by FACA: open meetings and public disclosure of documents.

The Task Force understands that some within DHS are concerned that its "PCII" rules and procedures now make it administratively complicated to rely on this exemption. In response, the Task Force notes first that the exemption is written in terms of "communications" of CII rather than "submissions," a word used elsewhere in that section of the Act, suggesting that Congress intended the FACA exemption to operate as broadly as possible and not to be constrained by whatever procedures DHS developed to implement that section.[68] The Task Force also notes that the section only called for "procedures," not regulations, and that Congress may not have intended the complex submission and validation process established by current rules.[69] Finally, the Task Force contends that, if this is a problem, the right solution is to go back and amend those rules.

3. Generic FACA Exemption

Section 871 of the Homeland Security Act provides simply and generically that the Secretary of DHS may establish and use the services of advisory committees, and may exempt such committees from FACA.[70] Consistent with the default rule established by FACA,[71] such committees expire by law after two years, but the Secretary may extend their existence in additional two-year increments indefinitely.[72] This approach would have the advantage that it would not be based on the substance of the communications involved. The Task Force understands that this exemption authority has never been exercised, apparently due to some sort of understanding between Congress and the Administration, struck at the time the law was enacted, that it would only be used in extraordinary cases, if at all. The Task Force believes any such understanding should be renegotiated or abrogated and that DHS should use the discretion it has under this provision to take such actions as it reasonably deems necessary and appropriate to protect and ensure the resilient operation of the Nation's critical infrastructure and key resources.

---

[67] The full definition is "information 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 other 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 management 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."
6 U.S.C. § 131(3). "Protected system--
(A) means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and
(B) includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage."
Id. § 131(6).

[68] Compare *id.* § 133(a) (information "submitted") with § 133(b) ("communication" of information).

[69] *See id.* § 133(e)(1).

[70] 6 U.S.C. § 451(a). The Secretary must publish a notice in the Federal Register announcing the establishment of the committee and identifying its purpose and membership. *Id.*

[71] *See* 5 U.S.C. App. 2, § 14(a)(1).

[72] 6 U.S.C. § 451(b).

4. Defense Production Act

The third way to provide SCCs and similar entities with a FACA exemption is through the Defense Production Act of 1950 (DPA). The DPA was enacted to enable the Federal Government and industry representatives to jointly develop preparedness programs to assure the availability of capacity and supply of resources and products critical to national defense at levels beyond those required by civilian demand.[73] The DPA creates a process whereby members of an industry sector and designated government officials may establish a "voluntary agreement," which can then be implemented by a "plan of action."[74] The DPA further provides that activities conducted under a voluntary agreement or plan of action are exempt from FACA when conducted in compliance with the DPA, its implementing rules, and the provisions of the agreement or plan.[75] The CIIA provides that the President or the Secretary of DHS may designate a component of DHS as a "critical infrastructure protection program,"[76] and that the President may delegate to that program the authority to enter, along with representatives of the Private Sector, into a voluntary agreement or plan of action, as those terms are defined under the DPA.[77]

> The DPA establishes elaborate procedural requirements for the establishment of these agreements and plans, as well as for meetings associated with carrying them out. These requirements are highly burdensome. For example, the meetings to establish a voluntary agreement must be attended by representatives of the Department of Justice and the Federal Trade Commission (to avoid antitrust violations), be noticed in the Federal Register and be transcribed verbatim.[78] Implementation of plans and agreements must be rigorously overseen by DOJ and the FTC, with documents made public unless certain FOIA exemptions apply.[79] The DPA approach may be the least preferable option for this reason.

5. DHS should not devise "work arounds"

Instead of determining that FACA does not apply to critical sector organizations under HSPD-7, or availing itself of any of the three exemption options discussed above, DHS is instead pursuing two other, ill-advised approaches.

The Interim National Infrastructure Protection Plan (NIPP) envisions the dozen or so SCCs communicating with a "NIPP Leadership Council" made up of various Federal entities. DHS's current FACA "work around" is proposing a "Sector Partnership Model" under which the NIPP Leadership Council would become a FACA advisory committee, and the SCCs would be treated as subgroups of that committee. This would allow SCC meetings to be exempted from FACA on the basis of judicial decisions holding that, while advisory committees must comply with FACA, subgroups of advisory committees do not need to do so.[80] DHS's Infrastructure Protection Division has requested the National Infrastructure Advisory Council (NIAC) – a body whose Designated Federal Officer is a DHS Employee — to evaluate an interim approach under which the NIAC would serve as this FACA body, and the various SCCs would be "study groups" of the NIAC. This is a bad idea for several reasons:

[73] 50 U.S.C. App. § 2158(c)(1).

[74] *Id.* § 2158(b)(2).

[75] *Id.* § 2158(n).

[76] 6 U.S.C. § 132. Section 29.4(a) of the CIIA rules designates the IAIP Directorate as responsible for directing and administering the "critical infrastructure protection program." *See* 6 C.F.R. § 29.4(a); *see also* 68 Fed. Reg. 18524 (April 15, 2003).

[77] 6 U.S.C. § 133(h). The President delegated his powers under DPA to the Secretary of DHS in Section 24 of Executive Order 13286 (Feb. 28, 2003).

[78] 50 U.S.C. App. § 2158(e).

[79] *Id.* § 2158(h).

[80] *See, e.g., National Anti-Hunger Coalition v. Executive Committee of President's Private Sector Survey on Cost Control,* 711 F.2d 1071 (D.C. Cir. 1983).

- As explained above, SCCs and ISACs are intended by HSPD-7 to be operational bodies, serving to facilitate two-way communication between their respective sectors and DHS.
- SCCs and ISACs were never intended to interface with the NIAC. These entities must be able to have real-time or very fast turnaround communications with DHS. Having to communicate through the NIAC frustrates that considerably.
- Most problematic, running SCC and ISAC communications through the NIAC means that these communications would, as a general rule, have to be made public at the NIAC sessions. To prevent release of sensitive information, therefore, these communications would have to be scrubbed before they officially reached DHS. Such an arrangement would substantially defeat the purpose of SCCs and ISACs.[81]

DHS's second FACA "work around" is to ask the various constituent companies or associations making up an SCC or other critical sector body to respond to DHS documents or questions individually, on their own behalves, rather than providing the consensus views of the sector. While this approach may indeed avoid the application of FACA,[82] it fundamentally defeats the purpose of HSPD-7 and the sector bodies it calls for, which is precisely to ensure that DHS can obtain (to the extent it exists) the views of a sector, not just the views of individual sector members. There is little point (or efficiency, from DHS's perspective), to creating sector bodies if DHS is going to studiously avoid using these bodies to cultivate and communicate a sector position.

VI. Lack of Coordination Within DHS and Between DHS and Other Agencies

Beyond implementation of the CIIA, DHS has generally shown a disappointing lack of coordination within itself and with other agencies. In some cases it appears to be due to simple oversights attributable to doing too much with too little, or not fully establishing or understanding priorities. In many other cases, however, the Not Invented Here Syndrome and claiming and protecting turf seems like the most likely explanation. These problems happen at all levels.

- *Within DHS:* Companies represented by group members, in various sectors, have all reported cases where a DHS contractor showed up, without any prior notice to the plant or its corporate headquarters, to validate their National Asset Database data. The Science & Technology Directorate typically initiates research projects on matters that are the purview of other directorates without any prior consultation. A good example is a grant to the National Academy of Sciences to prioritize research needs for the chemical sector, initiated without any consultation with chemical sector specialists at IAIP (or the sector itself).

- *Between DHS & other Federal agencies:* Critical sector groups experienced great difficulty getting DHS and FBI to collaborate on defining terrorist threat reporting triggers, and agreeing on who to call and in what order. The FBI held three national workshops on the triggers issue, in which DHS participated only after much effort. While the FBI staff working on the workshops were distilling their results, all concerned were stunned by the release of the "Terrorist Threat Reporting Guide" under the signatures of the FBI Director and the Under Secretary for IAIP. Staff of both agencies and the sector are still working to reconcile these efforts.

[81]The head of the agency being advised by a FACA committee can close meetings and limit release of documents when a FOIA exemption would apply. *See* 5 U.S.C. App. 2, § 10(b), (d). As noted earlier, DHS has not yet taken definitive positions on when these exemptions would apply in the critical infrastructure context.

[82]GSA's FACA regulations provide that FACA does not apply when an agency expressly does not seek the consensus views of a group. See 41 C.F.R. § 102-3.40(e).

- *Between DHS and State/local governments:* As noted earlier, several states have complained about their inabilities to execute MOAs allowing them to receive CII.

Private critical sector entities spend much of their time introducing DHS to itself, and bringing about coordination that should have happened earlier. As a result, this coordination usually takes place under great time pressures or after the fact. This lack of coordination inspires further lack of confidence on the part of the Private Sector. Again, the Office of Private Sector Liaison has been helpful in this regard, but should not have to fix problems that could have been averted.

VII. Requirement for Clearer Justification for Information

Frequently critical infrastructure entities receive multiple requests from different DHS offices for the same or similar information. The justification for these requests is not always clearly stated, and in some cases does not always sound plausible to the Private Sector. Repeated requests for information, especially where the need for the information is unclear, raise concerns about how that information will be used and how well it will be safeguarded. In this connection, the Task Force urges DHS to seriously consider the following questions:

- What specifically does DHS intend to do with information besides hold and share it?
  - Beyond implementation of the Stafford Act, will the information be used to develop Federal response plans to mitigate existing vulnerabilities or to provide assets to remediate the consequences of infrastructure failures?

- Whether in fact information that DHS really needs is being shared, and whether the mere existence of the PCII Program Office is creating a misleading expectation that more information could or should be shared.

- Whether the simple existence of IAIP, and the PCII program in particular, is the basis for these requests or expectations. That is, have staff adopted the view that, because IAIP has the statutory responsibility to assess vulnerabilities and security measures, therefore it should simply ask for any and all information on these topics from all critical sectors, without regard to the criticality of this information and DHS's ability to understand and assess it?

- Whether existing mechanisms for gathering information, especially via State and local entities, are adequate? Wherever possible, DHS should obtain that information from other entities that have collected it, not ask the original source to supply it again.

- Given the success of the Y2K Transition information sharing construct, whether DHS itself needs particular information, or can it rely on (a) other sector specific agencies or (b) the sector itself to supply either the information itself or a less sensitive version of the information.

VIII. Completion of SSI Rulemaking

The TSA/DOT rules regarding sensitive security information (SSI)[83] are proving to be very useful in the aviation and maritime contexts. Some of these SSI rules apply to all transportation modes (including land modes), but others do not, reportedly due to bureaucratic issues involving OMB. This is a serious shortcoming, as it means that some sensitive information regarding the security of land transportation is not being adequately protected from public release. It has been over a year since these rules were substantially revised, and these agencies should act quickly to expand the SSI rules to reach all transportation modes.

[84] *Id.* §§ 15.13(c), 1520.13(c).

The only really controversial aspect of the SSI rules is their marking requirements, which are highly burdensome (they require a lengthy footer for every page).[84] TSA and DOT have indicated that they may relax this requirement in a forthcoming rulemaking. They should do so when they revise the rules to encompass land modes. It would be sufficient for the rules to require printing a warning legend once on the document, and then just require a simple "Sensitive Security Information" header or footer on subsequent pages.

Recommendations

5. ***DHS should promptly and decisively revise its rules and policies for information sharing.***
    - *Regard Private Sector critical infrastructure facilities, companies and their associations as partners with legitimate interests in policy formulation and implementation — and as the only entities capable of implementing most policy in the subject area. (A)*
    - *Respond to Private Sector concerns about liability risks associated with sharing security information with DHS*
        - *DHS should ensure that critical infrastructure information is only used to protect or ensure the operational resilience of critical infrastructure. (R)*
            - *Critical Infrastructure Information Act (CIIA) regulations must be simple and broadly agreed-upon before they will be used. (R)*
            - *Educate potential submitters regarding the protections afforded by all existing laws and potential risks. (M)*
    - *Fully implement the Critical Infrastructure Information Act (CIIA):*
        - *Do not require all CIIA submissions to be validated. (R)*
        - *Declare that information submitted by SCCs and ISACs and maintained on HSIN by sector representatives will be deemed CII. (R/M)*
        - *Allow "class" CIIA determinations in advance of submittal. (R/M)*
        - *Allow "indirect" and electronic submission under CIIA. (R/M))*
        - *Roll out the CIIA program as quickly as possible to all DHS entities, to other sector-specific agencies, and to states willing to execute memoranda of agreement (on behalf of themselves and local governments within the state). (M)*
        - *Authorize all personnel of its Information Analysis & Infrastructure Protection Directorate who interact with critical entities to be CIIA portals. (M)*
    - *In consultation with DOJ and the Private Sector, adopt broad, Department-wide positions regarding the applicability of the confidential business information and law enforcement sensitive exemptions under the Freedom of Information Act (FOIA). (M)*
    - *Resolve questions about how the Federal Advisory Committee Act (FACA) applies to SCCs and ISACs.*
        - *The ongoing Private Sector/Government operating relationship is critical to an effective homeland security operation and is hobbled by FACA issues.*
        - *SCCs and ISACs are not covered by FACA because they are not "utilized" by the Executive Branch and are primarily operational, rather than advisory. (M)*
        - *If challenged, DHS should use one of three possible authorities to exempt SCCs and ISACs from FACA. If this requires amending the CIIA rules, DHS should do so promptly. (R/M)*

[84] *Id.* §§ 15.13(c), 1520.13(c).

- *Given the above, under no circumstances should DHS employ FACA "work arounds" like treating SCCs as subgroups of the National Infrastructure Advisory Council or seeking only the views of individual companies. (M)*

- DHS offices and staff should identify coordination needs with DHS, with other federal agencies and with state and local governments, and should undertake such coordination as early as necessary, without waiting for affected entities to initiate it. (M/A)

- DHS should determine if it needs particular information to do its job, or whether some other governmental or private entity is doing that job adequately. DHS should not request information because it can, or because it would be "nice to know," but only where it is necessary to enable DHS entities to perform essential functions. (M/A)

- The Sensitive Security Information (SSI) rulemaking conducted by the DHS Transportation Security Administration (TSA) should encompass all modes of transportation. (R)

PART THREE – PARTNERING WITH THE MEDIA

I. Findings

It is vital to the health and safety of the American public that it receive **timely**, **accurate** and **actionable** information during times of crisis. Erroneous information, false rumors or exaggerated reports of the geographic, economic and human impact of an incident risk loss of life and serious adverse economic, social and national security consequences.

The government and the media, while not "partners" in the normal sense of that term, each have a responsibility during a crisis for addressing this public interest and can, consistent with their independent roles in our constitutional system, work together to serve the public.

It is critical to our national interest that the government and the media clearly understand their respective responsibilities, roles and operational relationships in a crisis so that each can execute its responsibilities to the public with full knowledge of how the other will behave.

The media is regarded by the public, the Private Sector and most elements of the public sector as their primary source of information in a crisis – and should be regarded by the government as a reliable participant in disseminating timely, accurate and actionable information. Information can be as critical as food and water to potential victims in a crisis, and the media play a central role in the homeland security information system.

There is too little exchange of crisis information between the government and the media before an incident takes place:

- Public officials tend to regard the media as a potentially hostile or disruptive element in crisis communications.
- The media tend to regard public officials as trying to "hide the ball" regarding threat information or emergency preparedness planning and resource allocations.
- This shared perception deprives the media of important subject matter expertise and relationships important to it in communicating with the public during an incident.
- And this shared perception diminishes the ability of government to use the media as effectively as it might to communicate accurate, timely and actionable information to the public during an incident.

Pre-incident communications are needed in order to improve public communications in a crisis.

- News organizations need coverage plans before an incident so that they can get the story right.
- News organizations need emergency plans and protective gear to protect their own first responder personnel.
- News organizations need contingency plans to continue operating if their broadcasting, publishing or server capacities are damaged or destroyed.
- News organizations need ready-to-use, off-the-shelf access to scientific, emergency management and other expertise critical to reporting on an incident.
- Government public information officials need to know which reporters will cover which element of an incident.
- Government public information officers need to know logistical needs of the media in order to provide public updates.
- Government public information officers need to have a fully-informed, responsive media in order to provide actionable information to the public.

The government and the media are neither "partners" nor "adversaries" in crisis communications; the relationship is subtle and dynamic.

- During an incident, the media play both an informational and accountability role.
- At the outset of an incident, the media report information concerning the incident and its immediate causes; as the incident progresses, the media report on the failures in the prevention system that allowed the incident to occur; at some point, the media begin to investigate who is to blame for the breakdown in the prevention system.
- Both the government and the media must understand that each of these roles is distinct and valuable, but that during a crisis, communication to the public of accurate, timely and actionable information is critical to life and property and takes priority.
- After-action reports, whether by the government in its self-improvement role or by the media in its investigatory and accountability roles, are valuable tools as well.

Different media have different roles, staffing, skills, and training in crisis communications:

- Local broadcast media carry lion's share of role in informational period, but are least prepared or staffed
- National broadcast media play secondary role in information phase, but are most staffed and skilled
- Print media play greater role in later stages
- National 24-hour cable media are faster but, with more time to fill, tend to "fill" with speculation
- Talk radio, relying on listener input, are sometimes source of unfounded rumors

If an "official" government spokesperson cannot or does not have a prompt answer to a media inquiry, the media will find some "unnamed source" or "outside expert" to provide it.

Government public information officers need a clear system to monitor press reports and correct erroneous reports or unconfirmed rumors.

As a consequence, government and the media find it difficult to work together in communicating consistent, accurate, timely and actionable information to the public during an incident.

Yet, media and media personnel are "civic minded" and may be "force multipliers" in engaging public in preparedness and incident response and recovery.

Failure of a well-understood working relationship between government and media may leave the public:

- less prepared prior to crisis,
- more anxious during a crisis and thus less responsive to government protective action recommendations, and
- slower as consumers, employees and families to recover from the effects of an incident.

A well-understood working relationship between the Government and a well-informed media can provide timely, accurate and actionable information to the public and a reassuring sense that Government and business leaders are working well together to manage the response to an incident and its consequences.

II. From "Media and First Response Program" to a Sustained Partnership

The Government and local media should transform their current limited "media and first response program" into a sustained campaign in all of the top UASI media markets to enable key officials and local media personnel to better understand their respective roles and behaviors in providing information to the public during a crisis.

- Doing so will develop working relationships between government and media personnel that will enable a more trusted sharing of information during the early stages of an incident, including the better understanding and handling of ambiguous threat or incident information and of information that may be sensitive and important.
- This campaign should include table-top exercises, editorial board briefings, background sessions with on-air anchors, writers, general and beat reporters, traffic and weather reporters, assignment editors, bookers, producers, local public health officials, first responders, elected officials, local FBI personnel, others responsible for local emergency operations.

To assure that those relationships are sustained and that media expertise and readiness is maintained, this program should put in place a local team in each market to maintain a continuing series of exchanges between government and local media.

- Complacency is a powerful force undermining continuing readiness.
- Continuing attention to proper government/media relationships can also extend to "all-hazards" events.

III. Need for Regular Background Briefings

Government officials, at both the national and local levels, should conduct regular, ongoing background briefings for members of the media.

- Background briefings should include: potential scenarios regarding man-made or natural disasters, means by which any available threat or warning information will be delivered, default preventive and protective measures to be taken by the public, consistent terminology for alternative protective action measures (e.g., shelter-in-place versus evacuation; in-place quarantine versus "see doctor"), scientific background information and known experts in the relevant fields, logistics of government briefings during crisis, possible technologies available to the media for the receipt and display of crisis-related information and protective measures for first-responding media personnel.
- During these briefings, the media should identify its needs for logistical information, subject matter expertise and personal protective requirements in various crisis scenarios.

IV. Role of Local Officials and Trusted Authorities

Regular press briefings should be scheduled by local elected officials and trusted authorities (public and private) immediately upon learning of an incident.

- Communications to the public should be a critical priority in incident response activities.

Even if information is ambiguous, unconfirmed or incomplete, government and Private Sector officials should be briefing the press on what is known, what is not known, what is being done by emergency response personnel to respond to the incident and what protective action, if any, is being recommended to the public.

- Public information officials should be included as a senior member in all aspects of incident planning and response activities.
- Local elected leaders should undergo continuing crisis communications training.

The ability to sustain public trust and to set appropriate public expectations in a crisis is critical to increasing the prospect of a predictable public response to recommended protective actions and to minimize economic and social impacts of an incident through rapid recovery and resiliency.

- Working with the media, professional standards should be developed for "confirmed" and "unconfirmed" tags in crisis reports, and clear "rumor control" protocols should be developed to assure the accuracy and timely delivery of actionable information to the public.
- During and after a crisis, the government should issue regular updates on the consequences of the incident, including deaths, injuries, economic and foreign policy impacts.

After-action reports following an incident should include an assessment of the nature, quality and management of public communications regarding the incident, including findings regarding the public awareness, understanding and assessment of the incident, the protective actions the public understood it was to take during the incident and the timeliness, accuracy and action-orientation of the information that was communicated to the public.

V. Refining the Homeland Security Advisory System

The color-coded threat notification system should be significantly modified because it does not provide actionable information to the public.

- Available threat information important to the public should be made public, but it should also be made clear what actions should be taken by elected officials and first responders, businesses in potentially-impacted sectors or regions or by the public.
- If no action is to be taken by the public, it should be made clear why the warning level is being changed.

The Department should organize and support a national community-based threat and preparedness campaign, working with local media partners, to engage employers and citizens in reporting local suspicious activity and in enhancing their own preparedness.

- Locally-executed campaigns, using local media and local community organizations, are more likely to change behavior than a national media campaign alone.
- Locally-reported suspicious activity, carefully crafted to avoid privacy concerns, can be better quality-assessed by local law enforcement and will relieve overburdened national hotlines.

Recommendations

6. ***DHS should pro-actively invest in a better informed and more engaged media through specific targeted programs aimed at developing a stronger working relationship between the government, the media and the Private Sector in major incidents. (M/A)***
   - *Upon completion of an assessment, the government and local media should scale their existing National Academies of Science media engagement program into a sustained campaign in all UASI (Urban Areas Security Initiative) media markets.*
   - *Government officials at both the national and local levels should conduct a systematic program of background briefings for members of local media including, among other things, the National Response Plan and National Incident Management System, potential threat and response scenarios, scientific information regarding biological, chemical and radiological materials, a glossary of homeland security and citizen protective actions, and other FAQs.*
   - *Local elected officials and trusted authorities (public and Private Sector) should be trained on how to conduct press briefings during an incident in order to provide (1) timely and actionable information and protective action recommendations to the Private Sector and the public and (2) contextual material needed to maintain public order and confidence.*
   - *DHS, local elected officials and national and local media should develop protocols for the timely confirmation or correction of unconfirmed information or rumors during the course of an incident.*

7. ***The Homeland Security Advisory System should be refined to provide more specific guidance to the Private Sector and to the public, including changes in warning levels. (M)***
   - *Warning levels should be adjustable on a sector-specific, geographic or time-limited basis (or on another basis, as appropriate).*
   - *Warning level changes should include a specific advisory to the public regarding the purpose for the change and the steps, if any, that the public is expected to take as a result of such a change.*
   - *DHS, State and local officials and the Private Sector should meet, confer and develop common understandings and expectations regarding the readiness or preparedness levels associated with different warning levels.*
   - *Any refinement of the Advisory System should be accompanied by a clear, easy-to-understand public communications plan.*

GLOSSARY OF ACRONYMS

2SR	Second Stage Review
AMA	American Medical Association
APA	Administrative Procedure Act
APRSAC	Academe, Policy and Research Senior Advisory Committee
BZPP	Buffer Zone Protection Plan
CBI	Confidential Business Information
CBP	Customs and Border Protection
CDC	Centers for Disease Control and Prevention
CEII	Critical Energy Infrastructure Information
CI/KR	Critical Infrastructure/Key Resources
CII	Critical Infrastructure Information
CIIA	Critical Infrastructure Information Act
CIO	Chief Information Officer
CIPO	Critical Infrastructure Programs Office
CITF	Critical Infrastructure Task Force
C-TPAT	Customs-Trade Partnership Against Terrorism
CWC	Chemical Weapons Convention
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOE	Department of Energy
DOJ	Department of Justice
DOT	Department of Transportation
DPA	Defense Production Act
EAS	Emergency Alert System
EPA	Environmental Protection Agency
ERSAC	Emergency Response Senior Advisory Committee
FAA	Federal Aviation Administration
FACA	Federal Advisory Committee Act
FAQ	Frequently Asked Question
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FIG	Field Intelligence Group
FinCEN	Financial Crimes Enforcement Network
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FTC	Federal Trade Commission
GAO	Government Accountability Office
GCC	Government Coordinating Council
GSA	General Services Administration
HSA	Homeland Security Act
HHS	Health and Human Services
HSAC	Homeland Security Advisory Council
HSAS	Homeland Security Advisory System
HSIN	Homeland Security Information Network
HSIN-CI	Homeland Security Information Network-Critical Infrastructure
HSISA	Homeland Security Information Sharing Act
HSOC	Homeland Security Operations Center
HSPD-7	Homeland Security Presidential Directive 7
I&W	Indications and Warning
IA	Information Analysis
IAIP	Information Analysis and Infrastructure Protection
ICD	Infrastructure Coordination Division
IP	Infrastructure Protection
ISAC	Information Sharing and Analysis Center
ISE	Information Sharing Environment
ISP	Internet Service Provider
IT	Information Technology
JRIES	Joint Regional Information Exchange System
JTTF	Joint Terrorism Task Force
LERG	Local Exchange Routing Guide
MTSA	Maritime Transportation Security Act

MOA	Memorandum of Agreement
NAWAS	National Warning System
NCAS	National Cyber Alert System
NCC	National Coordinating Center
NCS	National Communications System
NCSD	National Cyber Security Division
NDA	Non-Disclosure Agreement
NDAC	Network Design and Analysis Capability
NIAC	National Infrastructure Advisory Council
NICC	National Infrastructure Coordinating Center
NIMS	National Incident Management System
NIPC	National Infrastructure Protection Center
NIPP	National Infrastructure Protection Plan
NOAA	National Oceanic and Atmospheric Administration
NRP	National Response Plan
NS/EP	National Security/Emergency Preparedness
NSIE	National Security Information Exchange
NSTAC	National Security Telecommunications Advisory Committee
OMB	Office of Management and Budget
OSAC	Overseas Security Advisory Council
OSHA	Occupational Safety and Health Administration
PCII	Protected Critical Infrastructure Information
PSD	Protective Security Division
PSO	Private Sector Office
PVTSAC	Private Sector Senior Advisory Committee
RAMCAP	Risk Analysis and Management for Critical Asset Protection
RSPA	Research and Special Projects Administration
SAV	Site Assistance Visit
SBU	Sensitive But Unclassified
SCC	Sector Coordinating Council
SIOC	Strategic Information and Operations Center
SLSAC	State and Local Officials Senior Advisory Committee
SSA	Sector Specific Agency
SSI	Sensitive Security Information
SSP	Sector Specific Plan
TSA	Transportation Security Administration
UASI	Urban Areas Security Initiative
USCERT	United States Computer Emergency Response Team
WAWAS	Washington Area Warning System
Y2K	Year 2000

Attachment A

PRIVATE SECTOR INFORMATION SHARING TASK FORCE

Chair, Mayor Patrick McCrory
(HSAC)
Vice Chair, Herb Kelleher
(HSAC, PVTSAC)
Mayor Karen Anderson
(SLSAC)
Dick Andrews
(HSAC, ERSAC)
Sheriff Michael Carona
(ERSAC)
James Dunlap
(SLSAC)
Donna Finn
(SLSAC)
Chief Michael Freeman
(ERSAC)
Ellen Gordon
(ERSAC)
Steve Gross
(PVTSAC)
Dr. Doug Huntt
(PVTSAC)
Chief Phil Keith
(ERSAC)
Monica Luechtefeld
(PVTSAC)
Paul Maniscalco
(ERSAC)
Commissioner Karen Miller
(SLSAC)
Mayor Donald Plusquellic
(SLSAC)
Jack Reall
(ERSAC)
Rick Stephens
(PVTSAC)
George Vradenburg
(PVTSAC)
Jack Williams
(PVTSAC)

HSAC STAFF

Daniel Ostergaard
Executive Director, HSAC
Candace Stoltz
Director, Private Sector Information Sharing Task Force
Jeff Gaynor
Mike Miron
Katie Knapp

SUBJECT MATTER EXPERTS

Drew Arena
Verizon Communications
Laurence W. Brown
Edison Electric Institute
Barbara Cochran
Radio-Television News Directors Association
John Cohen
Office of the Governor, MA
James W. Conrad, Jr.
American Chemistry Council
Greg Gwash
The Boeing Company
Neil Gallagher
Bank of America
Ava A. Harter
Dow Chemical

Dick Ketler
Southwest Airlines

Maurice McBride
National Petrochemical & Refiners Association

Susan Neely
American Beverage Association

Tom Prince
Blackwell Sanders Peper Martin, LLP

Frank Sesno
School of Public Policy/ George Mason University

Steve Wheeler
Lockheed Martin Aeronautics Company

Attachment B

PUBLIC/PRIVATE INFORMATION SHARING PROCESS

Below is an outline that attempts to map existing channels for security-related information flows. Included information covers: the flow of information in both directions between government and the Private Sector on warnings, threats or reports of manmade or natural emergencies, accidents, criminal acts, and attacks, as well as information on design, location, and function of elements of the nation's critical infrastructure. Not included is information flowing in either direction regarding rulemaking and the promulgation of regulations, nor that contained in press releases, briefings and other aspects of general public affairs activities.

For each entry, the qualitative or quantitative sense of the number of reporting/disseminating entities; the frequency and volume of reports/releases; and whether they are mandatory or voluntary in nature will all vary. In addition, certain restrictions are placed by statute/rule/Executive Order/policy on the information's use by the recipient entity (public or private) and the ability of that entity to share it further.

I. From Government to Private Sector

A. From State to Local Governments

B. From Federal Government

i. Department of Homeland Security

1. IAIP
   - ISACs, USCERT.
   - HSIN (HSIN has multiple customers at different levels. i.e. JRIES is for Law Enforcement and State Homeland Security Advisory, while HSIN-CI's primary mission focus is the Private Sector).
   - Warnings/Threat level.

2. FEMA
   - Emergency Alert System (EAS): dissemination of alert and warning messages, Presidential messaging to the nation, and state/local use. EAS operates at the national level through 34 Primary Entry Point broadcast stations.
   - National Warning System (NAWAS): created to rapidly notify emergency management officials of impending or threatened attack or accidental missile launch on the United States. The three types of civil warnings supported by NAWAS are: (1) natural and technological emergency warning; (2) attack warning; and (3) fallout warning.
   - Washington Area Warning System (WAWAS): a 24-hour alert and warning system for the Washington DC area that coordinates federal and city emergency operations in the Nation's Capital.
3. U.S. Secret Service; Financial Crimes Task Force
4. U.S. Coast Guard
   - Local Area Maritime Security Committees composed of federal and non-Federal port partners.
   - Local Command Centers.
   - Captains of the Ports.
   - Liaison at interagency operations centers.
   - Electronic bulletins.
   - 3 Interagency command centers located at San Diego, Norfolk and Charleston (SC).
5. Private Sector Office
   - HSIN-CI: Established and continued expansion to private sector members.

- HSAS: Provided outreach/notification and coordination of private sector leaders to changes in level.
- Ready-Business: Shaped content, messaging, outreach and partnerships for campaign to enhance private sector preparedness and business continuity.
- US-Visit: Fostered information and issue exchanges for the transportation communities on the rollout, impact and benefits of the Program.

ii. Department of Commerce
National Oceanic and Atmospheric Administration (NOAA) encompasses the National Weather Service.

iii. Department of Justice
- FBI: InfraGuard is part of HSIN-CI.
- https://www.swern.gov/ privatesector/InfraGard.php.
- Wanted lists; Joint Terrorism Task Forces.
- HSIN-CI, HSOC is currently sending Joint FBI/DHS Sector.
- Bulletins via HSIN-CI.

iv. Department of Transportation
Federal Aviation Administration (FAA)

v. Department of Energy

vi. Department of Health and Human Services
Centers for Disease Control (CDC)

vii. Nuclear Regulatory Commission

II. From Private Sector to Government

A. To State & Local Governments

i. Emergency Management Agencies

ii. Utility Regulators

B. To Federal Government

i. Department of Homeland Security

1. IAIP
- Infrastructure Analysis (IA): analyzes intelligence from the United States Private Sector entities for information regarding homeland security. IA also collaborates with the Private Sector by: ensuring that the appropriate threat information with homeland security implications reaches Private Sector officials that protect the American citizenry and critical infrastructure; and producing threat related information bulletins and advisories for Private Sector critical infrastructure owners and operators.
- Infrastructure Protection (IP): in partnership with IA and the Private Sector, protects America's critical infrastructure through the following:
- Infrastructure Coordination Division (ICD)—serving as the hub of infrastructure expertise by sustaining core sector capabilities, maintaining operational awareness, and fostering work-level relationships with the Private Sector, and State and local governments.
  - National Infrastructure Coordinating Center (NICC): a 24x7 watch operation center that maintains operational and situational awareness of the nation's critical infrastructure key resources (CI/KR) sectors. The NICC provides a centralized mechanism and process for information sharing and coordination between and among government, Sector Coordinating Councils (SCCs), Government Coordinating Councils (GCCs), and other industry partners.
  - Infrastructure Coordination and Analysis Office: comprised of Sector Specialists who have expertise and/or established contacts in the CI/KR sectors. Additionally, Sector Specialists analyze operational and situational information that is provided by the National Infrastructure Coordinating Center (NICC) to determine incident-related impacts to the CI/KR sectors.
  - Critical Infrastructure Programs Office (CIPO): supports information sharing and collaboration through sector partnership models. The owners and operators of the CI/KRs form the cornerstone of the Sector Partnership Model. These stakeholders own, operate, build, and invest in the assets that provide the vital functions of the sector.

- Sector Coordinating Councils (SCCs): Under the National Infrastructure Protection Plan (NIPP), there are 17 SCCs that assemble all the different actors in the Private Sector to instill information sharing. DHS personnel work with asset owners and operators to identify vulnerabilities and provide options for consideration.
- Information Sharing and Analysis Centers (ISACs): created in the identified critical infrastructure sectors to coordinate industry and industry-government sector data sharing and analysis regarding vulnerabilities and incidents.
- Protected Critical Infrastructure Information (PCII) Program: allows DHS to receive protected and qualifying information from disclosure and to be used by DHS, other agencies, State and local governments for securing critical infrastructure.

- Protective Security Division (PSD)—reduces the nation's vulnerability to terrorism by developing and coordinating plans to protect critical infrastructure and denying use of our infrastructure as a weapon. PSD is also the Sector Specific Agency (SSA) for five sectors: Commercial, Nuclear, Chemical, Dams, and Emergency Services.
  - National Asset Database: the repository of U.S. assets among the 17 CI/KR sectors.
  - Sector Specific Plan (SSP): each SCC develops a SSP.
  - Buffer Zone Protection Programs (BZPPs) and Site Assistance Visit (SAV): performs SAV site specific write-ups called Common Characteristics and Vulnerabilities Reports for a particular sector or segment of that sector.
- National Communication System (NCS)—assists in the planning for, and provision of, national security and emergency preparedness communications for the Federal Government under all circumstances.
  - National Security Telecommunications Advisory Committee (NSTAC): provides industry-based advice and expertise to the President on issues and problems related to implementing national security and emergency preparedness (NS/EP) communications policy. NSTAC is composed of up to 30 industry chief executives representing the major communications and network service providers and information technology, finance, and aerospace companies.
  - National Security Information Exchange (NSIE): established as a forum in which Government and industry share information in a trusted and confidential environment.
  - National Coordinating Center (NCC): a joint industry-government operation encompassing the U.S. telecommunications industry and Federal Government organizations involved in responding to the Federal Government's NS/EP telecommunications service requirements. The operational arm of the NCC is its 24 x 7 watch and analysis operation, the "NCC Watch."
  - Communications-ISAC: facilitates voluntary collaboration and information sharing among its participants in the communications sector.
- National Cyber Security Division (NCSD)—acts as the single national point of contact for the public and Private Sector regarding cyber security issues, including outreach, awareness, training, and the National Asset Database.
  - USCERT: partners between DHS and the public and Private Sectors to protect the nation's Internet infrastructure. US-CERT coordinates defense against and responses to cyber attacks across the nation.
  - The National Cyber Alert System: US-CERT established a National Cyber Alert System in January 2004 to provide information to the public and the Private Sector.

- The US-CERT Portal: a secure, web-based collaborative system that allows US-CERT to share sensitive cyber-related information with government and industry members.
- The US-CERT Control Systems Center: plays a vital role in most critical cyber systems in the nation's infrastructure.
- US-CERT Public Website: serves as a critical function to provide government, Private Sector organizations, and the public with information they need to improve their ability to protect their information systems and infrastructures.
- The National Cyber Alert System (NCAS): an operational part of the US-CERT Response System that delivers targeted, timely, and actionable information about incident and threats in a series of periodic "cyber tips," "best practices," and "how-to" guidance messages.

2. National Emergency Management National Response Plan
3. HSIN-CI: uses the FBI's TIPs program on all websites, where members and the general public can submit information to both DHS (HSOC) and FBI (SIOC) via this internet tool. The FBI then sends the report to JTTF and FIGs for investigation, while DHS coordinates with IA; and the following web link: https://www.swern.gov.
4. Transportation Safety Commission
5. U.S. Coast Guard Local Command Centers; Captains of the Port National Response Center 1-800-424-8802
6. DHS Law Enforcement Agencies U.S.
7. Private Sector Office
   - Initiated exchanges of economic data from multiple private sector groups and companies as well as Federal Departments (Commerce, Labor, Agriculture) to assist PSO analyses on the economic impact of DHS policies and regulations (i.e. air transit program; advance passenger information systems, border wait times, etc).

ii. Department of Justice
   1. U.S. Attorney's Office; Grand Jury Investigations
   2. Infraguard; JTTFs
   3. Bureau of Alcohol Tobacco & Firearms
      Firearms and Explosives Info

iii. Department of Energy
iv. Department of Transportation
   1. FAA

v. Department of the Treasury
   1. FINCEN Suspicious transaction reporting; Bank Secrecy Act

vi. Department of Health and Human Services
vii. Federal Communication Commission
viii. Nuclear Regulatory Commission
ix. Environmental Protection Agency
   Releases/spills toxic materials

Attachment C

PROTECTING PRIVATE SECURITY-RELATED INFORMATION FROM DISCLOSURE BY GOVERNMENT AGENCIES

JAMES W. CONRAD, JR.[1]

TABLE OF CONTENTS

[1]Assistant General Counsel, American Chemistry Council. The author very much appreciates the helpful comments he received on earlier drafts of this article from Dion Casey, Transportation Security Administration; Daniel Metcalfe, Department of Justice; and James O'Reilly, University of Cincinnati College of Law. Staff of the Department of Homeland Security's Protected Critical Infrastructure Information Program declined to comment officially. All opinions and any errors contained herein are exclusively the author's.

C. Sensitive Security Information

1. Background

2. Scope

3. Operation

a. SSI is partially self-implementing

b. SSI can be submitted voluntarily to the federal government

c. Persons able to obtain SSI

d. The SSI rules bind private persons

Conclusion

INTRODUCTION

Most of this nation's critical infrastructure is privately held. It has become commonplace to describe information about the security of these businesses – i.e., their vulnerabilities and the security measures they have taken – as a roadmap to terrorists. And yet this characterization is apt. Security vulnerability assessments and security plans are among the most sensitive documents that could ever be prepared about a facility, whether that facility is a chemical plant, a dam or railroad storage yard. Comparable information about transportation modalities like trucking or rail may pose even greater risks, given their ubiquity and the great distances over which shipments may be vulnerable. Security vulnerability assessments and plans generally describe the worst possible consequences that could result from an attack; where, when and how to attack to produce those consequences; and what steps the business has taken to deter or delay such an attack, or to minimize the consequences. A terrorist planning such an attack could not have a more useful guide.

In some cases federal, state or local law may require a privately-held business to prepare these sorts of reports. In other cases, the business owner or operator may have done so voluntarily, pursuant to an industry initiative such as the chemical industry's Responsible Care®, Security Code.[2] Finally, the owner or operator may have independently recognized that its facilities or distribution methods could be an attractive target, and that potential legal liability or simply common sense impelled it to take protective measures.

Another familiar mantra is that security is a shared responsibility between the public and private sectors. In order to discharge this responsibility, both sectors need to share information with each other. Indeed, security planning – particularly in the area of response – cannot be conducted effectively unless each sector is aware of the other's capabilities and has cooperated in defining scenarios, roles and actions. This means that a government agency with responsibility for the security of a particular type of infrastructure is likely to want to be able to review and discuss security documents prepared by those businesses. It might also want to obtain a copy for its files – and it may have the power to do so. Finally, effective security planning may require that the federal government be able to share this information – in a controlled fashion – with state or local governments, or even with other private actors involved in securing the asset in question.

This article addresses what sorts of legal protections may exist to prevent the public release of a private business's security documents once they are in the possession of an executive branch agency of the federal government. It also notes:

- when these protections may impose obligations on the business submitting the information, not just the government; and
- when these protections envision the government sharing information with certain non-Federal governments or private entities for homeland security purposes, while not releasing it to the public at large. This concept requires a major cultural shift from the traditional binary notion that information is either publicly released or held only by government -- but this shift may be crucially important for ensuring security.

The article focuses on legal protections available at the federal level, though it also points out when these protections extend to documents in the hands of state or local agencies. As the discussion reveals, this area of the law is particularly complicated, not only because of the number and complexity of laws involved, and their interactions, but also by the distracting pervasiveness of labels that have some practical, though not consistent, meaning within government agencies, but yet provide no legal basis for withholding information from disclosure.

[2] *See* http://www.rctoolkit.com/security.asp.

The article begins by discussing the Freedom of Information Act, which provides the overall framework for deciding when the federal government may or must protect information from public disclosure. It focuses particularly on several exemptions from disclosure under FOIA. The next part of the article addresses a variety of labels that may appear to justify withholding information but really do not. Finally, the article explains at varying lengths a number of statutes that give the government the ability to protect certain types of security information from public release. This part of the article focuses on two recent and controversial programs regarding "critical infrastructure information" and "sensitive security information."

This article does not attempt to provide an exhaustive description of every program or authority it discusses. Readers interested in how they may be affected by the topics discussed below are encouraged to review the underlying laws or rules before making important decisions about them.

Finally, let me emphasize that the purpose of this article is not to promote the greatest possible withholding of private security-related information from release by the government. The 9/11 Commission,[3] the official in charge of classification policy across the federal government,[4] and commentators writing in this journal[5] all have expressed concern that the government overclassifies or otherwise restricts from disclosure information that safely could — and should — be disclosed to the public in order to effectuate longstanding principles of open government. Certainly some privately-generated information is "security-related" and yet could be made public without jeopardizing the security of the generator or others. And in most cases, the government can "write for release" by summarizing sensitive information or abstracting from it in a way that does not create undue risks. (Indeed, critical infrastructure representatives frequently complain that the government should do this more often with threat information that it possesses.) On the other hand, while different people will draw the line at different places, ultimately all (or virtually all) observers would agree that there are circumstances in which security-related information provided by private entities to the government must be protected from unrestricted public release. This article addresses whether and how well that purpose can be served under existing law.

I. EXECUTIVE SUMMARY

FOIA. The Freedom of Information Act is the starting point for any analysis of whether an executive branch agency must or may withhold a particular document from public disclosure. FOIA requires an agency to release a record in its possession upon request by any member of the public unless an exemption applies. Five FOIA exemptions are potentially applicable to business security information:

"**Other Laws**" (exemption (b)(3)): FOIA does not apply where another law prohibits an agency from disclosing a document or establishes particular criteria for withholding that type of information. Several of these laws are potentially applicable to business security information, and are summarized under "Other Statutes" below. A business concerned about the security of its information in the hands of the government should always check to see whether one or more of these laws applies.

[2] *See* http://www.rctoolkit.com/security.asp.

[3] National Commission on Terrorist Attacks upon the United States, THE 9/11 COMMISSION REPORT 417 (2004).

[4] J. William Leonard, Director, Information Security Oversight Office, National Archives & Records Administration, "Information Sharing and Protection: A Seamless Framework or Patchwork Quilt?" Remarks at the National Classification Management Society's Annual Training Seminar, Salt Lake City, Utah (June 13, 2003), available at http://www.fas.org/sgp/isoo/ncms061203.html.

[5] Christina E. Wells, "National Security Information and the Freedom of Information Act," 56 ADMIN. L. REV. 1195, 1198-1205 (2004).

National Security (exemption (b)(1)): Documents classified for national security reasons are exempt from disclosure under FOIA. There is no formal process for a business to request that information it submits to the government be classified, however, and access to classified documents is strictly limited. This exemption is unlikely to be useful to most businesses in most cases.

Law Enforcement (exemption (b)(7)(F)): FOIA exempts from disclosure information generated for civil or criminal law enforcement purposes the release of which could jeopardize the life or physical safety of a person. This exemption may well be applicable to business security information submitted to the government, provided that the information can be said to have been generated for purposes of enforcing some law, federal or state. This proviso is most easily accomplished where the agency in question has the authority to enforce some law relevant to homeland security. There may be some question whether all components of the Department of Homeland Security (DHS) have this authority.

Confidential Business Information (exemption (b)(4)): Between FOIA and the Trade Secrets Act, it is a crime for a government employee to release confidential commercial information about a business. For the most part, information about the security of a business should fall into that category. Moreover, the federal government's position – and the law in the D.C. Circuit – is that business information that is voluntarily submitted to an agency will be protected from release so long as it is the kind of information the business would not customarily release. Thus, this exemption should be broadly useful in protecting business security information from being released by a federal agency. However, this conclusion is not free from doubt in any given case, and a business would do well to determine if any other grounds exist for the government withholding the business's security information from release.

"Risk of Circumvention" (exemption (b)(2)): Most federal jurisdictions protect government information whose effectiveness requires that it be maintained confidential. The government is relying on this exemption to protect security-related information that it generates, whether about public or private infrastructure. It is questionable, however, whether this exemption would be of any use to protect documents that are generated privately and submitted to the government, especially if the substance of the report has not been integrated into a government document.

Protections that Aren't. The federal government maintains different levels and types of safeguards for various categories of information, depending principally on the agency in question. Common example categories are "sensitive but unclassified" (SBU) and "for official use only" (FOUO). While agencies may in fact handle such information carefully to avoid inadvertent release, these labels do not provide a basis for an agency to withhold a document from release in response to a FOIA request. Information must fall into a FOIA exemption to be withheld.

Other Statutes. Numerous statutes provide a basis, under the (b)(3) exemption noted above, for agencies to withhold business security-related information from public disclosure.

Specific statutory exemptions exist for:

- Larger public drinking water systems;
- Facilities and vessels regulated under the Maritime Transportation Security Act;
- Shippers and carriers of hazardous materials required to prepare security plans; and
- Facilities regulated under the Chemical Weapons Convention Implementation Act.

While it does not have a special basis for withholding information from release, the Federal Energy Regulatory Commission has established innovative rules for managing FOIA-exempt information submitted by facilities it regulates.

Two other programs, established by statute, provide a basis for exempting security-related information across a wide range of businesses. Businesses should always consider the possible applicability of these programs:

Critical infrastructure information (CII). This program, administered by DHS, protects security-related information about critical infrastructure when it is voluntarily submitted to DHS. This program provides an unprecedented level of protection, although partly as a result it has been slow to get up and running. It has great potential, however, to enable federal, state and local governments to share, in a secure fashion, information about the assets they need to protect. This law has been strongly challenged by those who believe it will lead to undue secrecy or even immunity from enforcement under other laws. In fact, however, the law and its implementing rules have been carefully crafted to avoid those outcomes.

Sensitive Security Information (SSI). This program, administered by both the Department of Transportation and the Transportation Security Administration, enables these agencies to protect from disclosure information they obtain or generate the release of which could jeopardize the safety or security of transportation. Private sector representatives may be able to have access to SSI on a need-to-know basis under a nondisclosure agreement. The SSI rules are also self-implementing, meaning that classes of information are SSI by definition, without anyone having to apply for such treatment. As with classified information, private entities possessing SSI have legal obligations to protect it – even if it is their own information.

II. THE FREEDOM OF INFORMATION ACT

The starting point for any analysis of whether an executive branch agency may or must release information in its possession is the Freedom of Information Act or FOIA.[6] This law provides the overarching framework for deciding whether a federal agency may refuse to publicly disclose a document. Enacted in 1966, and sparking a series of other "open government" laws, FOIA generally embodies a Congressional policy decision that all government "records" should be made publicly available – some automatically, and the rest (including, potentially, private security records) upon request by any person.[7]

Assuming a federal agency comes into possession of a business's security report, therefore, the default position is that the report is available to a FOIA requester, unless the report is covered by one of FOIA's exemptions from disclosure. FOIA has nine exemptions, of which five are potentially relevant to businesses' security information.[8] Each is discussed below. How useful any of them may prove to be in a given case is uncertain, however, for several important reasons:

[6] 5 U.S.C § 552. All federal agencies have issued regulations governing their implementation of FOIA. FOIA does not apply to the legislative or judicial branches of the federal government (or, thus, to entities within those branches like the Government Accountability Office (GAO)).

[7] "Any" person in this case really means any person, whether or not a U.S. citizen, and without any requirement to provide, much less substantiate, a need for the record. See U.S. DOJ, FOIA GUIDE AND PRIVACY ACT OVERVIEW 44-47 (2004 edition), available at http://www.usdoj.gov/oip/foi-act.htm. This comprehensive document is issued every other year by the Justice Department's Office of Information & Privacy, which coordinates the development and implementation of, and compliance with, FOIA policy throughout the executive branch. It provides useful insight into the government's position on FOIA issues. Much of this article's discussion of FOIA is derived from it. Another valuable reference is JAMES T. O'REILLY, FEDERAL INFORMATION DISCLOSURE (Thomson West 3d. ed 2000).

[8] FOIA also contains three "exclusions" that flatly forbid release of information, but they are unlikely to be relevant to private security information. (Two concern criminal investigations or proceedings and the third addresses certain classified information possessed by the FBI. See 5 U.S.C. § 552(c).)

- First, the exemptions are from FOIA's mandate to disclose, meaning that the government retains the discretion under FOIA to disclose exempt information, unless some other legal authority affects the agency's power to release it.[9] Many such authorities exist in the security area, fortunately, and are noted below where relevant.
- Second, most FOIA exemptions have been construed narrowly by agencies and courts in their efforts to effectuate Congress's openness policy. Agencies now in the business of obtaining or reviewing private security information generally have indicated an intention to apply relevant FOIA exemptions aggressively, and the Justice Department has stated its intent to defend exemption decisions "unless they lack a sound legal basis."[10]
- Still, whether an agency will protect a given document is its decision to make, and whether a court will agree is obviously uncertain. This difficulty is compounded by the fact that different federal circuits can and do construed FOIA differently, and a lawsuit seeking to compel disclosure of a business's security information could be filed by a plaintiff anywhere he or she resides.[11]
- Finally, each exemption has its own peculiarities, deriving from statutory language and years of evolving (and divergent) agency practice and judicial interpretations.

As a practical matter, it seems reasonable to assume that a court, faced with deciding whether to release information that the federal government argues should be protected to avoid facilitating a terrorist attack, would find some FOIA exemption to apply. Nonetheless, the upshot is that FOIA and its exemptions alone are not, in the view of many, an ideal solution to concerns about protecting business security information. For this reason, since 9/11 Congress has enacted or amended several other statutes, and federal agencies have issued several regulations, to provide greater measures of protection for some kinds of security-related documents. These other statutes and regulations are summarized in Part A immediately below and discussed in Part V of this article.

A. The "Other Laws" Exemption

The most reliable FOIA exemption potentially relevant to private security information is the "(b)(3)" exemption, which exempts from FOIA's disclosure mandate any information the release of which is controlled by another federal law. In essence, this exemption ensures that FOIA does not override any other law that either "(A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld."[12] A multitudeof statutes come in through this door. Some of these are outright prohibitions on release, using unambiguous language like "shall not be disclosed," and many include civil or even criminal penalties for government employees who violate them.[13] Others speak of documents "being exempt from disclosure" under FOIA, and may allow disclosure under certain circumstances. A business concerned about protecting information it might provide to the government should first determine whether any of these laws apply. Several of them are applicable to private security information, and are discussed in Part V below.

---

[9] Even more exasperating, only some of these other authorities flatly forbid the federal government from releasing certain information under any circumstances. Many of them merely provide that information "is exempt" from disclosure under FOIA, and in the view of the Justice Department, at least, such a law does not necessarily deprive the government of the discretion to disclose the information outside of FOIA if the other statute permits such discretionary disclosure. See FOIA GUIDE, supra note 9, at 229-31 and 683-91, esp. p. 684. This may be an academic point, since agencies generally treat a statute saying that information is "exempt" from disclosure under FOIA as a flat prohibition on disclosure in all cases.

[10] Memorandum from John Ashcroft, Attorney General, for Heads of all Federal Departments and Agencies (Oct. 12, 2001), available at http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm.

[11] *See* 5 U.S.C. § 552(a)(4)(B).

[12] *Id.* § 552(b)(3).

[13] *See*, e.g., the Trade Secrets Act and the Chemical Weapons Convention Implementation Act, discussed respectively in footnotes 42 and 72 and accompanying text.

B. National Security Exemption

FOIA exempts from disclosure documents that have been properly classified for reasons of national defense or foreign policy.[14] Thus, government records that are "top secret," "secret" or "confidential" need not be disclosed under FOIA – and in fact other authorities establish a range of sanctions if they are.[15] While on first blush this "(b)(1)" exemption might seem an ideal way for the government to protect privately-generated "homeland security" documents like vulnerability assessments from release while in the government's possession, classification actually has a number of serious limitations:

- *Only some federal agencies can classify a document.* The only way a document can become classified is if a federal agency that has "original classification authority" affirmatively acts to classify it.[16] While the Department of Homeland Security (DHS) and most other federal agencies have this authority, some do not.[17] A private entity cannot classify its own document. Nor is there any established process for private entities to request an agency to classify a document.

- *Access to classified documents is very tightly controlled.* Once a document has been classified, the only people who can see it are those who have:
  - an active security clearance at the requisite level (e.g., "secret" level for documents that have been classified at the secret or confidential level)
  - a need to know; and
  - signed a nondisclosure agreement (NDA).[18]
- *No one else can see the document – even the person who prepared it.* That means that if a private person without a security clearance prepared a vulnerability assessment of his facility and submitted it to a government agency, and the agency classified the document, the submitter could not get it back. Obviously, this is not conducive to effective security or information sharing.

And meeting the first two access requirements is not easy or quick. First, there is a tremendous backlog of persons seeking security clearances: more than three years after 9/11, federal agencies with classification authority still do not have adequate resources or budgets to process the many applications that they have accepted. And the requisite background checks – the source of most of the delay – will always take some degree of time.[19] Many applications have languished for long periods of time. And even if a person does have a clearance from one federal agency, other federal agencies have often been disinclined to accept them readily, even though they have been legally bound by executive order[20] – and now a federal statute[21] – to grant such "reciprocity."

[14] 5 U.S.C. § 552(b)(1). The current authorities governing the classification of documents are Executive Order 12958, as amended by E.O. 13292 (68 Fed. Reg. 15315, March 28, 2003), and rules issued pursuant to those orders by the National Archives & Records Administration's Information Security Oversight Office, located at 32 C.F.R. Part 2001. E.O. 12958 explicitly references information that "reveal[s] current vulnerabilities of systems, installations, infrastructures, or projects relating to national security." *Id.* § 3.3(b)(8).

[15] Sanctions for unauthorized disclosure of classified documents are discussed in Sections 4.1(b) and 5.5 of E.O. 12958. Criminal penalties exist for certain disclosures of classified information. E.g., 18 U.S.C. §§ 641, 793(d), 798; 50 U.S.C. § 783.

[16] E.O. 12958, § 1.1(a)(1).

[17] For example, EPA only recently received this authority.

[18] E.O. 12958, § 4.1(a).

[19] The statute enacted last year to implement some of the 9/11 Commission's recommendations contains provisions intended to improve the number and timeliness of security clearances. See 50 U.S.C. § 435b. An inherent part of the delay is that, among the federal law enforcement personnel who conduct or manage the process, doing background checks is often regarded as boring, low-status work compared with the more results-oriented work most of them signed up expecting to do.

[20] *See* E.O. 12968 (1995).

[21] *See* 50 U.S.C. § 435b(d).

Second, it is not necessarily easy or simple to get a federal agency to agree that you have a need to know. As the 9/11 Commission and other critics have pointed out, the classified world has evolved over the years into one where individual agencies are loathe to share information with each other, much less with private-sector individuals.[22] (The Commission's report calls for a new, "need to share" culture, and the statute passed by Congress last December to implement many of those recommendations contains provisions intended to create an "information sharing environment."[23])

Third, agency rules and procedures regarding access to classified documents are quite burdensome and cumbersome. Someone who meets the three requirements for access listed above has to construct an appropriately secure facility where the documents must remain at all times, with access controls and record-keeping requirements.[24] People cannot even discuss classified information over the telephone unless they have secure telecommunications capabilities, which are expensive and time-consuming to install.[25]

Finally, persons who violate these rules, or the terms of their NDA, can face very serious consequences – even if they are famous, as individuals such as Sandy Berger and John Deutsch have demonstrated.[26]

It should thus be obvious that classification is a very poor tool for promoting the security of private businesses.

C. Law Enforcement Exemption

Another FOIA exemption of partial use in protecting private security documents is the one covering information compiled for civil or criminal law enforcement purposes (conventionally referred to as "law enforcement sensitive" information). This exemption applies to a half-dozen categories of documents, but one is of particular relevance to the facility security predicament: records the release of which "could reasonably be expected to endanger the life or physical safety of any individual."[27] While this "(b)(7)" exemption was originally crafted to protect law enforcement personnel, it has been broadly interpreted to justify agencies' refusing to disclose law enforcement records whenever their release could reasonably be expected to result in harm to *any* person.[28] In the homeland security context, a federal court recently held that Bureau of Reclamation "inundation maps" detailing areas that might be flooded if the Hoover or Glen Canyon Dams failed catastrophically were covered by this exemption because disclosure of the maps "could reasonably place at risk the life or physical safety of . . . individuals," communities, or infrastructure downstream of the dams.[29] A business's security vulnerability assessment could well fall into this category also, and indeed federal agencies have made known their intention to assert this defense where relevant.[30]

[22] 9/11 COMMISSION REPORT, *supra* note 3, at 416-419.

[23] *Id.*; see also 6 U.S.C. § 485.

[24] *See* 32 C.F.R. §§ 2001.41(b), 2001.43. These are often referred to as "secure compartmentalized information facilities" or "SCIFs."

[25] *Id.* §§ 2001.41(c), 2001.49. These are often called "secure telecommunications units" or "STUs."

[26] *See* note 15 *supra. E.g.,* "Berger Will Plead Guilty to Taking Classified Paper," *Washington Post,* A1 (April 1, 2005).

[27] 5 U.S.C § 552(b)(7)(F).

[28] FOIA GUIDE, *supra* note 7, at 660 n. 20.

[29] See *Living Rivers, Inc. v. United States Bureau of Reclamation,* 272 F. Supp. 2d 1313, 1321-22 (D. Utah 2003).

[30] For example, when the FBI housed the National Infrastructure Protection Center (NIPC), it stated that it would assert this defense, among others, if anyone sought information supplied by private facilities regarding threats or similar incidents.

The problem with this exemption is that it can only be asserted when the private information in question could plausibly be argued to be have been generated or compiled in connection with some law enforcement purpose. This is likely to be only sporadically true in the security context. Most notably, the FBI has general authority to investigate violations of federal law, and so could plausibly assert this exemption in a range of cases. Another prominent example is the Coast Guard, which has authority to enforce the Maritime Transportation Security Act (MTSA), applicable to facilities and vessels that may be involved in a maritime transportation incident.[31] The Coast Guard is mandated to receive, review and approve security plans (which include vulnerability assessments) under the MTSA, and thus could reasonably assert this exemption, particularly to the extent it was using the report as part of an investigation or enforcement action under the law. Other types of businesses whose security is subject to enforceable federal authority include:

- Larger public drinking water systems (regulated by EPA under the Safe Drinking Water Act);[32]
- Shippers and carriers of hazardous materials required to prepare transportation security plans (regulated by DOT's Research and Special Projects Administration (RSPA) under the Hazardous Materials Transportation Act);[33]
- Facilities manufacturing or storing certain drug precursors (regulated by the DOJ's Drug Enforcement Administration under the Controlled Substances Act);[34] and
- Facilities manufacturing or storing certain chemical weapons precursors (regulated principally by the Commerce Department's Bureau of Industrial Security under the Chemical Weapons Convention Implementation Act).[35]

(Apart from the law enforcement context, these laws often also provide an independent basis for the government to withhold information from disclosure, as discussed in Part IV.A below.)

U.S. Customs & Border Protection (CBP), located within DHS, has authority to enforce a host of customs and foreign trade-related statutes. While none of these laws directly authorize it to regulate the security of trade-related facilities or distribution mechanisms, CBP administers a voluntary program (the "Customs-Trade Partnership Against Terrorism" or C-TPAT) through which participants obtain preferential treatment under these laws (e.g., reduced inspections) in exchange for submitting to CBP detailed information about their security programs (which CBP protects from disclosure) and acceding to CBP verification of those programs.[36]

On the other hand, many facilities whose security could be important are not subject to any of the laws referenced above, and many federal agencies do not have law enforcement authority associated with facility security. Most problematic, the Department of Homeland Security (DHS)'s Directorate of Information Analysis and Infrastructure

[31]The MTSA is 46 U.S.C. §§ 70101-70117. The Coast Guard's implementing rules are located at 33 C.F.R. Parts 101-106.

[32]*See* 42 U.S.C. § 300i-2.

[33]DOT's authority to regulate hazardous materials transportation security is found at 49 U.S.C. § 5103(b). The security plan rules are located at 49 C.F.R. Part 172.

[34]The Controlled Substances Act is codified at 28 U.S.C. §§ 801-971, and DEA's rules are codified at 21 C.F.R Parts 1300-1316.

[35]The CWCIA is found at 22 U.S.C. §§ 6701- 6771. BIS's rules are at 15 C.F.R. Parts 710-722

[36]*See* http://www.customs.gov/xp/cgov/import/commercial_enforcement/ctpat/.

Protection (IAIP), the federal office broadly charged with securing the nation's critical infrastructure and key resources – and the lead or "sector-specific" agency for the chemical, transportation, emergency services, postal and shipping sectors,[37] has no specific authority to investigate or enforce any law. There is some basis to argue that all DHS components are law enforcement agencies, but that conclusion is not assured.[38] If IAIP were not viewed as a law enforcement agency, it could only assert the law enforcement sensitive exemption to the extent the information in question had been compiled for purposes of enforcing a law, like those listed above, that some other governmental entity had authority over. This is not an ideal arrangement for the agency that is most commonly in the position of receiving (or requesting) facility security documents.

Importantly, however, the (b)(7) exemption applies in connection with the enforcement of any law — federal, state or local. Clearly, all levels of government have important roles to play in enforcing laws that protect private operations from the actions of terrorists or other criminals. To the extent that a federal entity like IAIP possesses information that is also possessed by state or local law enforcement — or is able to share information with such entities — the federal agency may be able to assert the (b)(7) exemption premised on the enforcement of state or local laws. IAIP is reportedly exploring the usefulness of this approach in connection with "Buffer Zone Protection Plans" that it is developing, in coordination with state and local authorities, for especially critical facilities.

D. Confidential Business Information Exemption

1. The exemption

Although much maligned by some, one FOIA exemption *does* offer potential protection to any private business: the "(b)(4)" exemption for "trade secrets and commercial or financial information [that is] privileged or confidential" – a.k.a. "confidential business information" or CBI. The landmark *Critical Mass* case interpreting this exemption holds that where the information in question is *voluntarily* supplied to the agency, the only question an agency need ask is whether the information is "of a kind that would customarily not be released to the public by the person from whom it was obtained."[40] Since no business in its right mind would customarily release actionable security information to the public, this means that voluntarily submitted private security information should categorically be covered by this exemption. And, as noted above, all information submitted to DHS's IAIP is voluntarily submitted, since IAIP has no power to compel the submission of information.

[37] *See* Homeland Security Presidential Directive/HSPD-7 (Dec. 17, 2003), § 11, available at http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.

[38] The Homeland Security Act provides that the Secretary of Homeland Security "shall be deemed to be a Federal law enforcement . . . official," but it is unclear whether that grant is universal or limited to the three statutes referenced in that provision, and whether it automatically flows down to all DHS components. *See* 6 U.S.C. § 122(c).

[39] 5 U.S.C § 552(b)(4).

[40] *Critical Mass Energy Project v. NRC*, 975 F.2d 871, 879 (D.C. Cir. 1992)(en banc). *See generally* FOIA GUIDE, *supra* note 7, at 281-84. The Justice Department and most courts have concluded that information can be voluntarily submitted even where an agency has the power to require its submittal, if the submission was not made in response to exercise of that authority. *See* FOIA GUIDE at 284-99.

Pursuant to Executive Order, all federal agency FOIA regulations provide that the agency will notify a submitter if someone has requested information provided by the submitter for which the submitter has claimed CBI protection, giving the submitter a reasonable period of time to object. If the agency determines to release the information notwithstanding an objection, the agency must notify the submitter in advance of a specified release date so the submitter can file a "reverse FOIA" lawsuit to block release.[41]

2. Concerns about the exemption

While the (b)(4) exemption, as construed in *Critical Mass*, would seem to provide clear protection for voluntarily-submitted business security information, many representatives of private interests have expressed skepticism about whether this is really the case. As discussed below, some of these concerns are probably unfounded or overwrought, but others have at least some merit.

a. Is it really discretionary?

Some representatives of potential CBI submitters note with concern the seemingly discretionary nature of the CBI exemption – meaning that an agency may, but is not required to, refuse to disclose information covered by that (or any other) FOIA exemption. While this is technically true, looking only within the four corners of FOIA, it is also true that courts have construed the federal Trade Secrets Act[42] to be coextensive with the CBI exemption.[43] This means that if information falls within the scope of the CBI exemption, it is a federal crime – a felony, in fact – for a federal employee to release it under FOIA. So the "discretionary" nature of the (b)(4) exemption should not be a basis for concern among would-be submitters – but it is, in the author's experience, by some who do not appreciate the Trade Secrets Act angle.

b. Will courts follow *Critical Mass*?

A second basis for concern is that the *Critical Mass* decision, while of great persuasive precedential value, is only binding precedent within the D.C. Circuit. While other federal district courts and one circuit have followed it,[44] it is not necessarily the law of the entire homeland. Indeed, district courts in California, Maine, New York, and Virginia have refused to follow it absent its adoption by their respective circuit courts.[45] As noted earlier, a lawsuit seeking to compel disclosure of a business's security plan could be filed by a plaintiff anywhere he or she resides.[46]

Thus it is entirely possible that a court somewhere in the U.S. would decline to follow *Critical Mass* and instead direct the agency to follow prior law, which required agencies to assay whether disclosure would likely "impair the Government's ability to obtain necessary information in the future" or "cause substantial harm to the competitive position of the person from whom the information was obtained."[47] Needless to say, many are

[41] *See* Executive Order 12600 (June 23, 1987), 52 Fed. Reg. 23781 (June 25, 1987).

[42] 18 U.S.C. § 1905. Many environmental statutes have similar protections for CBI (e.g., 7 U.S.C. § 136h (FIFRA), but it is questionable whether business security information would be covered by one of those statutes. The federal hazardous waste regulations require access control at hazardous waste treatment, storage and disposal facilities (see 40 C.F.R. §§ 264.14, 265.24), but beyond that, environmental laws and rules do not to the author's knowledge address security.

[43] E.g., *CNA Financial Corp. v. Donovan*, 830 F.2d 1132, 1151 (D.C. Cir. 1987). See generally FOIA GUIDE, supra note 7, at 358-60.

[44] *See* FOIA GUIDE, supra note 7, at 284-304. The Tenth Circuit adopted the Critical Mass distinction between voluntary and involuntary submission in Utah v. U.S. Dep't of Interior, 256 F.3d 967, 969 (10th Cir. 2001), although both sides in that case agreed that the submission involved was an involuntary one.

[45] *See* FOIA GUIDE, supra note 7, at 299-300.

[46] *See* 5 U.S.C. § 552(a)(4)(B).

[47] *National Parks & Conservation Ass'n v. Morton,* 498 F.2d 765, 767 (D.C. Cir. 1974).

uncomfortable risking the disclosure of vital information on outcome of such subjective tests.

c. Is security information really "commercial or financial"?

A third basis may be that potential submitters do not think of security-related information as "commercial" or "financial" information, since for the most part it does not involve cost or price data, product formulas, or other sorts of information that would typically be regarded as valuable to competitors. Obviously, information regarding security measures a business has taken could well be competitively sensitive, as could data on process modifications a plant made to reduce the inherent hazard it presents. More generally, most courts have concluded that "commercial" information covers anything "pertaining or relating to or dealing with commerce."[48] However, one federal district court has concluded that "factual information [supplied to the FAA by airlines] regarding the nature and frequency of in-flight medical emergencies" was not commercial information.[49] The uncertainty about how such cases might apply to threat information, and potentially some vulnerability information, is a cause for concern.

d. The culture of disclosure

Finally, some potential submitters are no doubt put off by associations that they have with the (b)(4) exemption deriving from their experience with it in other contexts. Many agencies, especially EPA, have zealously followed judicial admonitions to interpret exemptions from FOIA narrowly. Persons who are familiar with these agencies' policies and practices likely will impute them to DHS or other agencies and be reluctant to trust those agencies with such sensitive information. This concern is heightened by FOIA's requirement that agencies release "reasonably segregable portion[s] of a record."[50] A submitter cannot therefore assume that an entire document will be withheld from disclosure just because one or more portions of it contain CBI. Indeed, in such a case, the submitter may anticipate arguments with the agency – if such a document is requested under FOIA – about portions whose CBI status is debatable.

For all these reasons, the (b)(4) exemption is both (a) potentially applicable to a broad range of business security information but (b) of somewhat uncertain reliability.

E. "Risk of Circumvention" Exemption

A somewhat unlikely FOIA exemption that may have limited utility in protecting private security documents is the "(b)(2)" exemption protecting records "relating solely to the internal personnel rules and practices of an agency."[51] Over the years, many courts have interpreted this exemption to cover not only ministerial agency papers (so called "low 2" materials), but also "high 2" materials: i.e., those "predominantly internal" records that are effective only if they remain confidential.[52]

[48] *American Airlines, Inc. v. Nat'l Mediation Bd,* 588 F.2d 863, 870 (2d Cir. 1978). *See generally* FOIA GUIDE, *supra* note 7, at 271-73

[49] *Chicago Tribune v. FAA,* No. 97 C 2363, 1998 WL 242611, at *3 (N.D. Ill. May 7, 1998).

[50] 5 U.S.C § 552(b).

[51] *Id.* § 552(b)(2).

[52] *See* FOIA GUIDE, *supra* note 7, at 204-26, U.S. DOJ, FOIA Update, Vol. X, No. 3, at 3-4 ("OIP Guidance: Protecting Vulnerability Assessments Through Application of Exemption 2.").

Immediately after 9/11, the Justice Department advised other federal agencies that this exemption is "well-suited for application to the sensitive information contained in vulnerability assessments," and that agencies should "avail themselves of the full measure of Exemption 2's protection for their critical infrastructure information as they continue to gather more of it, and assess its heightened sensitivity, in the wake of the September 11 terrorist attacks."[53]

DOJ's interpretation of Exemption 2 applies clearly to vulnerability assessments and other security information that a government agency generates itself, and would seem to apply even if the critical infrastructure that is the subject of the report is privately owned. Since 9/11, DHS and other agencies from time to time have been requesting information from private entities that the agencies can roll up or incorporate into sectoral or regional analyses the agencies are preparing, and this exemption should be useful in protecting that information when supplied for such purposes. This exemption would also seem applicable to analyses developed by federal agencies regarding a single facility; e.g., a Buffer Zone Protection Plan prepared by DHS or a DHS contractor regarding a privately-held oil refinery.

On the other hand, not all circuit courts have adopted the "high 2" concept, and a district court recently refused to apply it to "inundation maps" prepared by the Bureau of Reclamation illustrating areas below the Hoover and Glen Canyon Dams that could be affected by catastrophic failures of the dams.[54] Moreover, it is not at all clear whether this exemption could apply to a report developed by a private business. Since cases have interpreted the exemption as applying to reports that are "predominantly internal" to the government, the exemption might apply if the substance of the private report was integrated into a government report. It may also be that a facility owner could prepare a report in sufficient cooperation or partnership with the government that the exemption would apply. However, establishing agreement among the relevant government officials – and their counsel – on the legal defensibility of this approach, and the mechanics of making it work, could be long and involved process. Thus this exemption is not likely to be of reliable use in protecting privately-generated assessments.

III. PROTECTIONS THAT AREN'T, REALLY

Understanding the rules for when government agencies can withhold information is complicated by the existence of several labels that, while frequently referenced by government agencies seeking to protect information, do not actually authorize those agencies to withhold records from release under FOIA.

Many government documents are prominently captioned "For Official Use Only," or "FOUO," and contain legends like this one:

> Warning: This document is FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with [agency] policy related to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized [agency] official. No portion of this document should be furnished to the media, either in written or verbal form.

[53] U.S. DOJ, FOIA Post (Oct. 15, 2001), available at http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm. *See also* FOIA GUIDE, *supra* note 7, at 214-15, 223-26.

[54] *See Living Rivers, supra* note 29, 292 F. Supp. 2d at 1317 (maps not sufficiently related to Bureau's "internal personnel rules and practices").

> While this language sounds gravely important and may trigger visions of locked file cabinets and armed guards, FOUO does not represent a category of information that is exempt from release under FOIA. If no FOIA exemption applies, an FOUO document would have to be produced in response to a FOIA request that adequately describes it.

A similarly intimidating but legally ineffectual label that is commonly used in and out of government is "Sensitive But Unclassified," or "SBU." As described in Part II.B above, there are three types of classified information: top secret, secret, and confidential. A document properly classified at one of these levels is exempt from disclosure under FOIA thanks to the (b)(1) exemption. But there is no "sensitive but unclassified" exemption to FOIA – an "SBU" document that does not fall into a real FOIA exemption is just as releasable under FOIA as an office holiday party announcement.

FOUO, SBU and similar labels are basically intra- or intergovernmental tools for "safeguarding" documents; i.e., ensuring that they are closely held and not disseminated more broadly than intended.[55] These labels have originated in a variety of ways,[56] and have neither any government-wide definition or any agency whose job it is to interpret them.[57] These labels typically trigger a set of agency rules or procedures – which could include sanctions for employees who violate them – to physically or practically limit access to information. But they are not themselves a *legal* basis for denying access to the documents under FOIA, if someone asks for them.[58]

Many documents that *are* exempt from FOIA are labeled FOUO or SBU so that government employees don't inadvertently release them. But many FOIA-releasable documents are also labeled FOUO or SBU. This is not necessarily bad, but it is confusing. And many, perhaps most, government employees do not understand these distinctions, adding to the confusion.[59]

[55]Other common labels that do not necessarily correlate with any FOIA exemption are: "Official Use Only" (OUO), "Sensitive Homeland Security Information" (SHSI), "Limited Official Use" (LOU), "Safeguarding Information" (SGI), "Unclassified Controlled Nuclear Information" (UNCI), and "restricted data."

[56]For example, "sensitive but unclassified" appears to have first been used, by Congress at least, in the Computer Security Act of 1987. See 15 U.S.C. § 278g-3(d)(4); see generally Wells, *supra* note 5, at 1209-1212.

[57]A post-9/11 memo jointly issued by the National Archives' Information Security Oversight Office (ISOO) and the Justice Department urges all federal departments and agencies to "maintain and control" "sensitive but unclassified information," balancing "[t]he need to protect such sensitive information from inappropriate disclosure" and "the benefits that result from the open and efficient exchange of scientific, technical and like information." Memorandum from Laura Kimberly, ISOO and Richard Huff and Daniel Metcalfe, DOJ, regarding "Safeguarding Information Regarding Weapons of Mass Destruction and other Sensitive Records Related to Homeland Security" (March 21, 2002), available at http://usdoj.gov/oip/foiapost/2002foiapost10.htm. The memorandum provides no guidance, however, regarding what constitutes SBU information.

[58]*See* FOIA GUIDE, *supra* note 7, at 190-191.

[59]Wells, *supra* note 5, argues that increased use of labels like SBU will lead to overwithholding, 56 ADMIN. L. REV. at 1212, and to overclassification, id. at 1211, and expresses concern that courts will "defer to . . . government claims" when "'sensitive but unclassified' withholdings are made in the name of national security," id. at 1212. It does seem likely that an agency faced with a FOIA request for a document that is labeled SBU will be more inclined than otherwise to look for a plausible basis for withholding it. This is intentional, and as a result agencies should exercise some judgment and not apply such labels routinely. On the other hand, an agency still must identify a defensible FOIA exemption before withholding an "SBU" document, since there is no "SBU" exemption. It seems unlikely, moreover, that an agency would choose to classify a document that it has already determined is unclassified. And a court cannot "defer to . . . 'sensitive but unclassified' withholdings," since as just noted SBU is not a basis for withholding a document from disclosure.

III. OTHER LAWS THAT MAY PROTECT A BUSINESS'S SECURITY INFORMATION

As noted earlier, the (b)(3) exemption from FOIA protects documents from being released when some other statute governs their disclosure. A number of these are specifically designed to protect security-sensitive information. Because these laws largely were enacted after 9/11, rules implementing them are still new or not yet complete, and the responsible agencies in most cases are still struggling to determine their scope and operation – as are organizations that generate or may possess covered information. Part A below summarizes information protections applicable to particular types of facilities or operations. Parts B and C describe two much more broadly applicable regulatory programs for protecting two kinds of information: "Critical Infrastructure Information" and "Sensitive Security Information."

A. Laws Applicable to Particular Classes of Business Activities

As Part II.C above explained, the "law enforcement" exemption from FOIA may apply where particular agencies have the ability to regulate security at particular types of facilities or transportation modalities. The laws granting such authority often contain their own information protections applicable to information generated pursuant to their authorities.[60] One can safely expect that future such laws – e.g., chemical facility security legislation – will also have detailed information protections.[61] This part of the article discusses four such laws, as well as two innovative programs for managing security sensitive information related to energy infrastructure

1. Larger public drinking water systems

The Safe Drinking Water Act requires these systems to certify to EPA that they have conducted vulnerability assessments, and to provide it with those assessments.[62] The identity of a facility submitting an assessment and the date of the certification must be made public.[63] Otherwise, however, EPA must develop protocols to ensure that these assessments, and information derived from them, are kept in a secure location, and EPA is prohibited from making this information "available to anyone other than an individual designated by the [EPA] Administrator.[64] (Designated individuals need not be government employees.) Criminal penalties are provided if such an individual knowingly or recklessly releases the information in an unauthorized fashion.[65] The law further provides that covered drinking water systems do not have to provide these assessments to a state or local entity "solely by reason of the requirement" that they submit them to EPA[66]

[60] Neither the Controlled Substances Act nor DEA's implementing regulations (see footnote 35 and accompanying text) contain particular information protections. Since DEA is part of the Department of Justice, security-related information supplied to DEA would be subject to DOJ's FOIA regulations and procedures and protected to the extent it fell into one of the FOIA exemptions above in Parts III.B-E above (national security, law enforcement, CBI or anticircumvention).

[61] For example, S. 994, the "Chemical Facilities Security Act" reported by the Senate Environment & Public Works Committee on May 11, 2004 contained protections possibly exceeding those provided by any other statute for unclassified information. See §§ 3(i), 4(e), 7(c).

[62] *See* 42 U.S.C. § 300i-2(a)(2).

[63] *Id.* § 300i-2(a)(3).

[64] *Id.* § 300i-2(a)(5).

[65] *Id.* § 300i-2(a)(6)(A). Such an individual can disclose the information (i) to another designated individual, (ii) for purposes of conducting inspections or taking actions in response to imminent hazards, or (iii) in administrative or judicial enforcement actions under the act. *Id.*

[66] *Id.* § 300i-2(a)(4). This provision was designed to preempt state or local laws that say, in effect, 'you must submit to us anything you have to submit to EPA.'

— but it does not prevent state or local entities from passing enactments that specifically require submission of these assessments. The law also authorizes designated individuals who are government employees to "discuss the contents of a vulnerability assessment" with state or local officials.[67]

2. Facilities and vessels regulated by the Maritime Transportation Security Act

The MTSA declares that, "[n]otwithstanding any other provision of law, information developed under [it] is not required to be disclosed to the public, including . . . facility security plans, vessel security plans . . . port vulnerability assessments; and . . . other information related to security plans, procedures or programs for vessels or facilities authorized under [it].[68] Scattered provisions of the Coast Guard's MTSA rules flesh out this declaration (which does not require regulations to be effective) by stating that various types of information generated under the MTSA are "sensitive security information" ("SSI") under regulations jointly published by the DOT and the Transportation Security Administration (TSA).[69] The SSI rules – which impose obligations on the generators of this information, not just agencies – are discussed in Part IV.C below.

3. Shippers and carriers of hazardous materials required to prepare security plans

Shippers and carriers of certain hazardous materials required by DOT/RSPA rules to prepare transportation security plans are not required to submit those plans to DOT. DOT has stated that it "[g]enerally . . . will not collect or retain security plans," and that its

> Inspectors . . . generally will not take copies with them or require companies to submit security plans.[70] In the rare instance that RSPA enforcement personnel identify a need to collect a copy of a security plan, or if a company voluntarily submits a copy of its security plan, we will analyze all applicable laws and Freedom of Information Act exemptions to determine whether the information or portions of information in the security plan can be withheld from release. Prior to submission of a security plan to DOT in these unusual instances, companies should follow the procedures in 49 CFR 105.30 [the DOT FOIA rules] for requesting confidentiality. Under those procedures, a company should identify and mark the information it believes is confidential and explain why. We will then determine whether the information may be released or protected under the law.[71]

Obviously this language is not terribly reassuring to hazmat businesses. However, there is a compelling argument that hazmat security plans obtained by or provided to DOT as described above are currently protected by the SSI rules referenced in the previous section (discussing the MTSA). Also, DOT and TSA intend to propose amendments to those rules to expressly reference land modes of transportation. Both these issues are discussed in Part IV.C below.

[67] *Id.* § 300i-2(a)(6)(B).
[68] 46 U.S.C. § 70103(c)(7).
[69] E.g., 33 C.F.R. § 105.400(c) (stating that facility security plans are SSI).
[70] 68 Fed. Reg. 14517 (March 25, 2003).
[71] *Id.*

4. Facilities regulated under the Chemical Weapons Convention Implementation Act

The Chemical Weapons Convention Implementation Act provides that any "confidential business information" supplied to or otherwise acquired by the United States government under the Act or the Convention "shall not be disclosed" under FOIA.[72] "Confidential business information" is defined under the Act to include CBI as defined under FOIA (see Part II.D above), and specifically also includes "any plant design process, technology, or operating method," which could well include plant security practices or procedures.[73] Exceptions to this prohibition allow the government to supply CBI:

- to the CWC Technical Secretariat or other states who are parties to the Convention (which has its own "Annex on the Protection of Confidential Information");[74]
- to Congressional committees and subcommittees, upon written request of the chair or ranking member (though committees and staff are prohibited from disclosing this information except as required or authorized by law);[75]
- to other federal agencies for enforcement of any law, or when relevant to any proceeding under any law (but in either case must be managed "in such a manner as to preserve confidentiality to the extent practicable without impairing the proceeding");[76] or
- when the government determines it is in the national interest to do so.[77]

5. Activities regulated by the Federal Energy Regulatory Commission

Shortly after 9/11, the Federal Energy Regulatory Commission (FERC) initiated two innovative, though controversial, approaches for managing information related to the security of energy infrastructure.[78] Unlike the authorities discussed above, these approaches do not provide a separate basis for withholding information from disclosure. However, they are worth discussing in the interest of completeness.

First, FERC has established special FOIA rules for "Critical Energy Infrastructure Information" (CEII), defined as information about critical infrastructure that:

- relates to the production, generation, transportation, transmission or distribution of energy;
- "could be useful to a person in planning an attack on critical infrastructure";
- is exempt from disclosure under FOIA; and
- does not simply give the location of the infrastructure.[79]

The CEII program does not expand the scope of information exempt from FOIA, since it only applies to information that already falls into a FOIA exemption (usually, the (b)(4) exemption for CBI). In fact, the purpose of the CEII rules is actually to facilitate the limited, but not general, disclosure of information that FERC could simply refuse to release to anyone.

[72] 22 U.S.C. § 6744(a).

[73] *Id.* § 6713(g). BIS's rules implementing these provisions are at 15 C.F.R. Part 718.

[74] 22 U.S.C. § 6744(b)(1).

[75] *Id.* § 6744(b)(2).

[76] *Id.* § 6744(b)(3).

[77] *Id.* § 6744(b)(4).

[78] *See* 18 C.F.R. §§ 388.112 & .113

[79] *Id.* § 388.113(c)(1). FERC's definition of "critical infrastructure" closely tracks the definition in DHS's Critical Infrastructure Information Act rules. *See* note 91 infra.

Under the rules, a person submitting information to FERC – whether voluntarily or not – who believes its information qualifies as CEII must file, along with the information, a statement justifying special treatment of the information.[80] Persons who can substantiate why they need particular CEII (typically, to participate in a ratemaking or similar FERC proceeding involving the infrastructure in question) can be given access to it, provided they provide FERC with personally identifying information and, at the discretion of FERC's CEII Coordinator, sign a nondisclosure agreement.[81] As with any FOIA request for CBI, FERC will provide the submitter of information with five day's notice of the request (in case the submitter wants to object) and five days notice of a decision to release (in case the submitter wants to sue).[82] The CEII rules do not require a person claiming CEII treatment for information to abide by any safeguarding or similar obligations. Presumably, if a CEII submitter made that information widely available, FERC would not protect it as CEII if someone later requested it.

Second, FERC has created the category of "non-Internet public" information for "maps or diagrams that reveal the location of critical energy infrastructure . . . but do not rise to the level of CEII."[83] A submitter must request "non-Internet public" treatment as it would CEII treatment.[84] FERC treats "non-Internet public" like any other public information, except that it does not include it in its online "Federal Energy Regulatory Records Information System."[85]

B. The Critical Infrastructure Information Act

1. Background

As the nation prepared for Y2K, the federal government sought to persuade computer-dependent "critical infrastructures" like banking, telecommunications and electric power to share information with it about their vulnerabilities and preparedness. These sectors had expressed reluctance about doing so, however, due to concerns about release of information under FOIA and state open records laws. The government's need for such information grew dramatically after 9/11, and so legislation first drafted before that date found its way into the Homeland Security Act.

The "Critical Infrastructure Information Act of 2002" (CIIA)[86] attempts to encourage critical infrastructure sectors to share security-related information with DHS by providing the information with an unprecedented type of protection. While the CIIA merely required DHS to "establish uniform procedures" for implementing it by February 2003,[87] DHS chose to go through rulemaking. As a result, final CIIA rules were not issued until a year later.[88]

[80] *Id.* § 388.112(b).
[81] *Id.* § 388.113(d)(2).
[82] *Id.* §§ 388.112(d), (e).
[83] *Id.* § 388.112(a)(3).
[84] *Id.* § 388.112(b)(1).
[85] *Id. See* 68 Fed. Reg. 46457 (Aug. 6, 2003).
[86] 6 U.S.C. §§ 131-34.
[87] *Id.* § 133(e).
[88] 69 Fed. Reg. 8074 (Feb. 20, 2004). The website for the PCII Program is www.dhs.gov/pcii.

As things are turning out, the very protections offered, particularly criminal liability for government employees, have slowed implementation of the law,[89] driven a very cautious approach to implementation, and (as a result) led many to question its usefulness. In view of the substantial protections the law offers, however, business owners and operators should carefully consider seeking its protections in applicable situations.

The CIIA has engendered a small storm of controversy, but in the author's judgment its critics are either mistaken or at least overwrought, as discussed below. Their criticisms are all the more remarkable, moreover, given how slowly the statute has been implemented and how little it is apparently being used.

2. Scope

The CIIA applies to *"critical infrastructure information"* that is *"voluntarily"* submitted to the "Protected Critical Infrastructure Information (PCII) Program" at DHS/IAIP.

- *"Critical infrastructure information"* basically means information not customarily in the public domain regarding threats, vulnerabilities and related problems or solutions affecting critical infrastructure or the physical or cyber resources that support it.[90] "Critical infrastructure" is defined very obliquely in the law and DHS's rules,[91] but the President has identified about a dozen critical sectors, most of which are privately held.[92]
- *"Voluntarily"* means not in response to DHS's exercise of its power to compel access to or submission of the information.[93]

[89]A trade press article reported that DHS had received only six CII submissions in the first three months the program was operative. "Response slow to DHS protected info sharing," GOVERNMENT COMPUTER NEWS, May 24, 2004.

[90]The full definition is "information 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 other 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 management 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."

6 U.S.C. § 131(3). "Protected system--

(A) means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and

(B) includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage."

Id. § 131(6).

[91]The statutory definition references the USA PATRIOT Act definition, which does not mention any industry by name. See 6 U.S.C. § 101(4), referencing 42 U.S.C. § 5195c(e). The CIIA rules define "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the[ir] incapacity or destruction . . . would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." 6 C.F.R. § 29.2.

[92]They are: information technology; telecommunications; chemicals; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; postal and shipping; agriculture and food; public health and healthcare; drinking water and water treatment systems; energy, including oil and gas and electric power; banking and finance, the defense industrial base; and national monuments and icons. See HSPD/7, supra note 37, at 3-4.

[93]6 U.S.C. § 131(7)(A).

- The Homeland Security Act does not give DHS any general power to do this, though various elements of DHS (e.g., the Coast Guard) have that power.

The rules carefully distinguish between "critical infrastructure information" and "protected critical infrastructure information" (PCII), but in the author's view this distinction is more confusing than helpful and is not perpetuated in this article.

3. Information Protections

The law creates a variety of protections applicable to critical infrastructure information that is submitted to DHS, including the identity of the submitter. (DHS is also applying these protections to transmittal documents.) The protections encompass:[94]

- *FOIA exemption*. The information is exempt from disclosure under FOIA. Criminal penalties are established for federal employees who "knowingly" release the information.[95]
- *Preemption of state and local open records laws*. The information is also exempt from disclosure under any state or local 'FOIA' or "sunshine" laws.
- *Ex parte exclusion*. The information is not subject to disclosure by operation of any rules about "ex parte" communications with agency officials.
- *Civil liability protection*. If submitted in "good faith," the submitted information cannot itself be used "directly" in any federal, state or local civil enforcement action, or in any private civil lawsuit, in federal or state court. (It could be used in a criminal action.) Presumably, the same "information," in the sense of facts or data, could be used "indirectly" in a governmental or private civil case if the plaintiff obtained the information independently; i.e., in some way besides getting it from DHS.[96] (For example, a plaintiff may be able to obtain a copy of the same document, through discovery, directly from the submitting party.[97])
- *No waiver of privilege*. The submitter cannot be held, by the act of submitting information, to have waived any privileges or protections supplied to it by law (e.g., attorney-client privilege, work-product doctrine, trade secret protection).
- *Restrictions on sharing and use*. DHS can share the information within the federal government and with state and local government — and contractors working for them — but all of these entities can only use it for purposes of:
  - infrastructure protection; or
  - investigating or prosecuting crimes.

[94]All of these bullets are derived from 6 U.S.C. § 133(a)(1) unless otherwise noted. Explicitly (or, presumably, implicitly) all of these protections can be waived by the consent of the submitter. See note 111 infra.

[95]*Id.* § 133(f).

[96]This is DOJ's interpretation of the issue. *See* USDOJ, FOIA Post (2/27/94), available at http://www.usdoj.gov/oip/foiapost/2004foiapost6.htm ("What must be remembered is that the same industry information can exist in two counterpart forms, identical in whole or in part. . . .").

[97]*See* note 123 *infra* and accompanying text.

DHS can also give it to Congress or the GAO, presumably upon request.

The CIIA rules also lay out detailed physical and procedural protections regarding safeguarding of the information.[98] These protections do not apply to information submitters, who remain free to release or otherwise handle their CII as they choose.[99]

The CIIA was also intended to enable members of a critical infrastructure sector to meet and share sensitive information frankly among themselves and with DHS, whether through Information Sharing & Analysis Centers (ISACs) or otherwise. It does so in two ways not further discussed in this article: an exemption from the Federal Advisory Committee Act[100] and an oblique antitrust exemption.[101] The author is unaware of either provision being relied upon to date.

4. Implementation Issues

The Act and DHS's rules establish a complex and rigid process for submitting and sharing CII:

- At present, information must be submitted in hard copy or on tangible electronic media. E-mail and oral submission is not generally allowed now, though such "eSubmissions" capability is imminent, according to PCII Program staff.[102] DHS has worked out an arrangement to receive electronic data on a continuing basis from one critical sector.
- DHS's rules at present require information to be submitted directly to the PCII Program; they do not allow "indirect" submissions through other components of DHS or other federal agencies, though DHS has stated its intent to allow this in the future.[103] Private entities can submit information through an "information sharing and analysis organization," like an ISAC[104]
- To be eligible for protection, information must be accompanied by an "express statement" referencing the CIIA.[105]

[98]6 C.F.R. §§ 29.7, 29.8.

[99]As noted below (*see* note 112 *infra* and accompanying text), DHS will stop protecting CII if it becomes publicly *available* through legal means.

[100]Communication of critical infrastructure information to DHS does not trigger the Federal Advisory Committee Act. 6 U.S.C. § 133(b). Thus groups of industry sector representatives could meet with DHS to communicate CII without becoming subject to the open meetings or other requirements of FACA. DHS does not seem to set much store by this provision, however. In part, the constricted process that DHS has created for accepting and "validating" CII has undercut its ability to use this FACA exemption.

[101]The CIIA does not explicitly create an exemption from the antitrust laws. However, it does provide an indirect means of accomplishing that goal via a reference to the Defense Production Act of 1950 (DPA), 50 U.S.C. app. § 2158. *See* 6 U.S.C. § 133(h). The DPA process is quite innovative, but also highly burdensome (in order to assure that the antitrust defense the DPA provides is not abused).

[102]69 Fed. Reg. 8077.

[103]*Id.* at 8075.

[104]6 U.S.C. § 131(7)(A).

[105]Written information must be marked with language "substantially similar to the following: 'This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002.'" *Id.* § 133(a)(2). The statute allows oral information to be protected if such a written statement is provided within a reasonable period. *Id.*

- Once the information is submitted, DHS reviews the information and "validates" it as protected CII.[106] (It protects the information presumptively as CII pending that determination.) DHS will notify the submitter of its determination. A source can withdraw the information while the determination is pending. DHS may ask the submitter for more information to substantiate its CII claim, in which case the submitter has 30 days to respond. If DHS determines that the information does not qualify as CII, DHS says it will, at the submitter's direction, either maintain it without protection or destroy it in accordance with the Federal Records Act.[107] (But DHS will not return the information to the submitter at that point.)
- If DHS determines that information, though not qualifying as CII, could be withheld under another FOIA exemption, it will do so in response to a FOIA request.[108] It may also retain (and safeguard) information that it considers to be law enforcement sensitive or that it believes should be classified. This latter assertion of authority has worried some, although it probably should not be surprising.
- Where a submission contains portions that qualify as CII and portions that likely do not, DHS does not require submitters to "portion mark" the CII-candidate sections (as many agencies require when people submit information that is partially protected by other FOIA exemptions — for example, CBI). Rather, DHS will safeguard, and in the event of a FOIA request withhold from disclosure, the entire submission.[109]
- The default generally established by the rules is that CII will be maintained within DHS. The rules authorize DHS to share CII with other federal agencies, and with state and local governments, that agree to provide the information with the same degree of protection (state and local governments must sign a standard memorandum of agreement to this effect).[110]
- DHS is considering piloting a process of "class" validations that could be issued in advance of any particular submission and that would then automatically apply to all submissions falling within that class.
- The CIIA and rules do not discuss scenarios under which DHS could share protected CII with any nongovernmental entity besides the submitter, even under a nondisclosure agreement, for purposes of critical infrastructure protection.[111] While this may be

[106]Unless otherwise noted, this bullet is drawn from 6 C.F.R. § 29.6(e).

[107]Under that act, destruction by agencies of records in their possession is governed by schedules promulgated by the National Archives & Records Administration. *See* 44 U.S.C. § 3303a.

[108]6 C.F.R. § 29.3(b).

[109]69 Fed. Reg. 8078. PCII Program staff informally encourage portion marking of CII in large submissions, but they do so to expedite the validation process, not because only the marked portions will be protected.

[110]6 C.F.R § 29.8(b).

[111]The statute and rules do, somewhat inconsistently, speak of the ability of CII to be disclosed with the consent of the submitter (e.g., 6 U.S.C. §§ 133 (a)(1)(C), (D), & (E)(ii); 6 C.F.R. §§ 29.3(c), 29.8(d)(1), (f)(1)(i), (k)), but the rules never discuss the circumstances under which such consent might be sought. PCII Program staff generally express an intention never to disclose CII to nongovernmental entities for any purpose.

reassuring for most purposes, it does limit the ability of DHS and critical infrastructure entities to work collaboratively. As discussed below, the rules regarding "sensitive security information" do contemplate such sharing and as a result are potentially much more useful for public/private partnership.

- DHS will stop protecting CII if it determines that the information was customarily in the public domain, was required by law to be submitted to DHS, or "is publicly available through legal means." (Presumably "is" means "is" and not "is capable of becoming.") DHS will inform the submitter if it makes this determination.[112]
- The CIIA provides that "nothing in this [Act] may be construed to create a private right of action for enforcement of any provision of this Act."[113] Whatever this language means, it does not mean that a submitter is prevented from filing a lawsuit to block DHS from disclosing information that it has determined does not qualify as CII. In establishing the right to file analogous lawsuits to block imminent disclosures under FOIA (so-called "reverse FOIA" lawsuits), the Supreme Court made clear that the ability to file them arises not as a result of some private right of action under FOIA or the statute that supposedly prevents disclosure, but under the Administrative Procedure Act,[114] which generally authorizes judicial review of any final agency action not otherwise reviewable.[115]

The complexity of the foregoing process has undoubtedly discouraged use of the statute. Also, DHS entities who might ask private entities to provide them with information meeting the definition of CII have generally failed to coordinate adequately with the PCII Program Office, further limiting the statute's use. The program's rollout has been excruciatingly slow, with little apparent action throughout all of 2004. Finally, many potential submitters remain unconvinced that the statute really offers any protection over and above what might already be available under other authorities. This skepticism appears to be grounded less in any identifiable shortcomings of the law or rules than in two consequences of the their novelty: the lack of any judicial decisions upholding DHS decisions to withhold, and lack of longstanding, personal trust relationships between would-be submitters and DHS officials. Only time can address these factors. Notwithstanding all of the above, in the author's view the CIIA, appropriately implemented, remains a potentially powerful tool and one that potential submitters should consider thoughtfully.

[112] 6 C.F.R. § 29.6(f). The rules do not clearly explain what happens after DHS decides to stop protecting CII that it has formerly been protecting. Arguably, it must follow the submitter's prior instructions regarding destruction vs. maintenance subject to release under FOIA. *Id.* § 29.6(e). The DHS PCII PROCEDURES MANUAL (Feb. 17, 2004) says if the PCII Program concludes that a protected document did not really warrant protection at the time of the Program's initial determination, the Program will ask the submitter what it should do with the information *if it was never used*. If the information has been used, the Program will simply stop protecting it. *Id.* at 6-5 to 6-6.

[113] 6 U.S.C. § 134.

[114] *Chrysler v. Brown*, 441 U.S. 281, 293-94, 316-18 (1979). The Court expressly held that the statute assertedly blocking disclosure in that case –- the Trade Secrets Act –- did not afford a "private right of action," but the Court nonetheless authorized judicial review under the APA. *Id.* at 316-18.

[115] *See* 5 U.S.C. § 704.

5. No "Polluter Secrecy"

Partly as a result of its facial potential, the CIIA has been roundly denounced by the open-government and environmental communities as "likely to cause excessive secrecy regarding information only tangentially related to national security"[116] and as possibly leading to "a radical reversal of common law tort liability and open government requirements."[117] Bills have been introduced in both the 108th and 109th Congresses that would substantially curtail it.[118] These critics assert that its protections will allow organizations to hide embarrassing information or worse. These claims are generally wrong or hyperbolic, for the reasons discussed below, and suggest that those involved are less concerned about the CIIA itself as they are about using the CIIA to make larger political points.

- *Continued requirements to report.* Regulated entities must continue to report to the Federal government any information that they are required to report under any other law.[119] Information submitted or relied upon for permitting decisions or in regulatory proceedings is also not covered by the CIIA.[120] Any information so provided to those other agencies could be used by them in enforcement actions, since it would have been obtained independently of the CIIA.[121]
- *Government access to information.* Federal, state and local agencies will continue to have all their existing powers under other laws to obtain records and other information that regulated entities are required to make available to them.[122] This would seem to include information that states or local agencies – but not the federal government – require to be reported. Again, it would seem that these documents (and the information they contain) could be used in enforcement actions because they were independently obtained.
- *Private access to information.* While the issue is less clear, it appears that private litigants also retain under the CIIA whatever powers they have under other authorities to obtain critical infrastructure information directly from submitters and to use it in lawsuits.[123]

[116]Wells, *supra* note 5, at 1214.

[117]Rena Steinzor, "Democracies Die Behind Closed Doors: The Homeland Security Act and Corporate Accountability," 12 KANSAS J. LAW & PUB. POL'Y 641, 643 (Spring 2003).

[118]See S. 622, 109th Cong., 1st Sess. (2005); S. 609, 108th Cong., 1st Sess. (2003).

[119]6 U.S.C. § 133(d). The rules also clarify that submitters may not try to claim CII protections in required submissions they make to other agencies. *See* 6 C.F.R. § 29.3. The rules do allow DHS to treat a document as CII even when the same document is also submitted to one of other agencies (see the last sentence of § 29.3) — but those other agencies would not be bound by any CIIA prohibitions and could freely use that document in any otherwise authorized fashion, including releasing it publicly. *See* 6 U.S.C. § 133(c), 6 C.F.R. § 29.3(d).

[120]6 U.S.C. § 131(7)(B)(ii). The CIIA also does not protect information contained in registration statements filed with the SEC or federal banking regulators or in disclosures associated with the sale of securities. *Id.* § 131(7)(B)(i).

[121]*Id.* § 133(c).

[122]*Id.*; see also 6 C.F.R. § 29.3(d).

[123]That seems to be DHS's interpretation of 6 U.S.C. §§ 133(c). *See* 6 C.F.R. § 29.3(d). If this is true, however, one wonders why Congress included the words "or any third party" in part of the CIIA that prohibits DHS, "any other Federal, State or local authority, or any third party" from "directly" using CII in any civil action (*see* 6 U.S.C. § 133(a)(1)(C)) — especially since non-governmental parties have no lawful way to obtain CII from any government entity. Perhaps this language captures the prospect of third parties obtaining CII accidentally or improperly.

- *Protections not applicable to public (or customarily public) information*. Information that has already been disclosed lawfully to the public cannot be "pulled back" or otherwise protected under the law.[124] Information that is "customarily in the public domain" is also not protected.[125]
- *Linkage to critical infrastructure*. In order to be eligible for the protections of the CIIA, DHS must determine (through the validation process) that the information fits the definition of "critical infrastructure information."
- *Good faith requirement.* For the civil liability protections to apply, the information must be submitted in good faith.[126] DHS dropped a proposal to make submitters certify that a submission was made in good faith, but DHS noted that false representations to it are a federal crime.[127]
- *Whistleblower protection*. The CIIA rules clarify that the PCII program does not supersede the Whistleblower Protection Act,[128] and thus federal employees can disclose CII without penalty if they reasonably believe it evidences, among other things, a specific danger to public health or safety.[129]

Business groups have also raised concerns about how the CIIA will affect business transactions. For example, if company A wants information from company B, company B might require company A to agree not to submit that information as CII. Some have predicted that companies might also assert PCII status as a reason for not supplying information to other companies in transaction or in discovery, although in the latter case this defense would seem unavailing.

B. Sensitive Security Information

1. Background

In 1974, the Federal Aviation Administration was given the power to prohibit the disclosure of information that, if released, could jeopardize the safety of passengers in air transportation. This authority has been revised and expanded twice since that date. At present, both DOT and TSA have statutory authority to issue regulations "[n]otwithstanding [FOIA]" that "prohibit[] disclosure of information obtained or developed in ensuring security" [DOT] or "in carrying out security" [TSA] under authorities they administer, if the Secretary of Transportation or the Assistant Secretary of Homeland Security for Transportation Security Administration decides that "disclosing the information would . . . reveal a trade secret or privileged or confidential information; or . . . be detrimental to transportation safety" [DOT] or "transportation security" [TSA].[130]

[124] *See* 6 U.S.C. §§ 133(c); *see also* 6 C.F.R. § 29.6(f).

[125] 6 U.S.C. § 131(3).

[126] *Id.* § 133(a)(1)(C).

[127] *See* 69 Fed. Reg. 8077.

[128] 5 U.S.C. § 1213.

[129] 6 C.F.R. § 29.8(f)(3). This provision is evidently premised on a savings clause in the Homeland Security Act stating that nothing in that act (which includes the CIIA) overrides the Whistleblower Protection Act. *See* 6 U.S.C. § 463(2).

[130] *See* 49 U.S.C. §§ 114(s)(1) (TSA), 40119(b)(1) (DOT). While the DOT language refers to transportation "safety" rather than "security," the difference is probably not legally significant. These two statutes also protect information the disclosure of which would "[b]e an unwarranted invasion of privacy." *Id.* §§ 114(s)(1)(A), 40119(b)(1)(A).

The two agencies have jointly issued rules implementing this authority.[131] For reasons not worth discussing here, the current rules largely address aviation security (regulated by TSA) and maritime security (regulated by the Coast Guard under the MTSA – *see* Part IV.A.2 above). Land modes of transportation (e.g., rail and truck) are not expressly referenced in the rules, but a few of the rules are written so generally that they apply in any transportation setting. (This is TSA and DOT's view, as well as the author's.) TSA and DOT intend to propose amendments that will expand these joint regulations to apply to all modes.

The rules are substantially different than the CII rules, both in scope and operation.

2. Scope

The rules have both general and particular applicability. In general, they track the statutes by defining "sensitive security information" as "information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA [or the Secretary of DOT] has determined would . . . [r]eveal trade secrets or privileged or confidential information obtained from any person; or . . . be detrimental to the security [or safety] of transportation."[132]

The rules also identify several 'categorical inclusions' – if information falls into one of these categories, it is automatically SSI. Two of these categories are not limited to aviation or maritime transportation:

- *Vulnerability assessments* . . . directed, created, held, funded, or approved by the DOT [or] DHS, or that will be provided to DOT or DHS in support of a Federal security program."[133]
- *"Threat information*. Any information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure."[134]

The other categorical inclusions are restricted to aviation and maritime security. The rules list over a dozen, including:

- "*Security programs and contingency plans* . . . issued, established, required, received, or approved by DOT or DHS." ("Security programs," at least, are largely limited to aviation and maritime operations.[135]) These specifically include vessel and maritime facility security plans.[136]
- *"Security inspection or investigative information* . . . . Details of any security inspection or investigation of an alleged violation of aviation or maritime transportation security requirements of Federal law that could reveal a security vulnerability . . . ."[137]
- *"Security measures.* Specific details of aviation or maritime transportation security measures, both operational and technical, whether applied directly by the Federal government or another person . . . ."[138]

[131] 49 C.F.R. Parts 15 (DOT) and 1520 (TSA), published at 69 Fed. Reg. 28066 (May 18, 2004).

[132] 49 C.F.R. §§ 15.5(a)(2) & (3), 1520.5(a) (2) & (3). As with the statutes authorizing the rules, the regulatory definition of SSI also generally includes information the disclosure of which would "[c]onstitute an unwarranted invasion of privacy." *Id.* §§ 15.5(a)(1), 1520.5(a)(1).

[133] *Id.* §§ 15.5(b)(5), 1520.5(b)(5) (emphasis in original).

[134] *Id.* §§ 15.5(b)(7), 1520.5(b)(7) (emphasis in original).

[135] *Id.* §§ 15.3, 1520.3. They also include "transportation-related automated system[s] or network[s] for information processing, control and communications." *Id.*

[136] *Id.* §§ 15.5(b)(1), 1520.5(b)(1) (emphasis in original).

[137] *Id.* §§ 15.5(b)(6), 1520.5(b)(6) (emphasis in original).

[138] *Id.* §§ 15.5(b)(8), 1520.5(b)(8) (emphasis in original).

- *"Security training materials.* Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out any aviation or maritime transportation security measures required or recommended by DHS or DOT."[139]
- *"Critical aviation or maritime infrastructure asset information.* Any list identifying systems or assets, whether physical or virtual, so vital to the aviation or maritime transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is —
  (i) Prepared by DHS or DOT; or
  (ii) Prepared by a State or local government agency and submitted by the agency to DHS or DOT."[140]
- *"Trade secret information . . . and [c]ommercial or financial information* . . . obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public."[141]

The rules authorize DOT or DHS to determine that information has stopped meeting the definition of SSI.[142] Even more interesting, the rules enable either of these agencies to determine that information is not SSI, even though it appears to fall into one of the categorical inclusions listed above, if it concludes that the information the information may be released in the interest of public safety or in furtherance of transportation security.[143]

3. Operation

a. SSI is partially self-implementing

As noted above, the SSI rules define over a dozen categories of information that are automatically SSI. As a result, information that clearly falls into these categories is SSI by definition, and qualifies for automatic protection. Information not falling in these categories can be SSI if DOT or TSA determines that it meets the statutory criteria for SSI; i.e., that improper disclosure of the information would be detrimental to transportation security. (Note: The DHS rules speak of TSA making these determinations on behalf of DHS, but in practice the Coast Guard can and does make SSI determinations as well.)[144]

b. SSI can be submitted voluntarily to the federal government

The preamble to the SSI rules attempts to distinguish the CII rules by saying that SSI "for the most part . . . is created by TSA or the Coast Guard or is required to be submitted to" the federal government, and that "information constituting SSI generally is not voluntarily submitted . . . ."[144] While these statements may be true in part, it is also true that information constituting SSI can be, and has been, submitted voluntarily to DOT or DHS. And the SSI rules do not prohibit this.[146]

[139] *Id.* §§ 15.5(b)(10), 1520.5(b)(10) (emphasis in original).
[140] *Id.* §§ 15.5(b)(12), 1520.5(b)(12) (emphasis in original).
[141] *Id.* §§ 15.5(b)(14), 1520.5(b)(14) (emphasis in original).
[142] *Id.* §§ 15.5(c), 1520.5(c).
[143] *Id.* §§ 15.5(b), 1520.5(b).
[144] As noted in Part IV.A.2 above, the Coast Guard has its own independent statutory authority to protect MTSA-related information, but uses the SSI rules to implement that authority.
[145] 69 Fed. Reg. 28069.
[146] The rules do provide that if information is properly submitted to the PCII Program and validated as PCII, the more restrictive CII rules will apply, even if the information also qualifies as SSI. *See* 49 C.F.R. §§ 15.10(d), 1520.10(d).

c. Persons able to obtain SSI

The SSI rules have been purposefully designed to facilitate the protection by the federal government of privately-held or operated activities such as commercial aviation and maritime commerce. As a result, the rules allow DOT and DHS to make SSI available to the relevant players in these areas. In the maritime security context, these "covered persons" include:

- owners, operators and charterers of vessels required to have a security plan;
- owners and operators of facilities required to have a security plan;
- persons participating on national, area or port security committees;
- industry trade associations representing the foregoing (if they have entered into a non-disclosure agreement with DOT or DHS);
- DHS and DOT; and
- persons employed by, contracted to or acting for any of the above.[147]

Apart from transportation mode, the rules also provide that SSI can be made available to any person for whom a vulnerability assessment has been "directed, created, held, funded, or approved by DHS or DOT," or who provides an assessment to either department.[148]

In any case, access to specific SSI is limited to persons with a "need to know" that SSI. Under the SSI rules, these include the following private sector actors:

- persons carrying out, in training to carry out, or supervising, any transportation security activities approved, accepted, funded, recommended or directed by DHS or DOT;
- persons providing technical or legal advice to a covered person regarding any federal transportation security requirements; and
- persons representing covered persons in connection with any judicial or administrative proceeding regarding those requirements.[149]

Federal employees can have access to SSI whenever it is necessary for performance of the employee's official duties. Federal contractors and grantees can have access if it is necessary to performance of the contract or grant.[150]

d. The SSI rules bind private persons

Like the procedures for classified information, but unlike all the other information protection authorities discussed in this article, the SSI rules impose obligations on private sector persons who possess SSI — including the persons who generate the information in the first place. These include:

- Taking reasonable steps to safeguard it from unauthorized disclosure (this includes storage in a secure container, such as a locked desk or file cabinet or in a locked room);

[147] *See* 49 C.F.R. §§ 15.7(c), (d), (f), (g), (h) & (k), 1520.7(c), (d), (f), (g), (h) & (k).

[148] *See* 49 C.F.R. §§ 15.7(l), 1520.7(l).

[149] *See* 49 C.F.R. §§ 15.11(a), 1520.11(a). These two subsections originally spoke only of aviation and maritime activities, *see* 69 Fed. Reg. 28081, 28084-85, but that restriction was eliminated through a technical amendment, see 70 Fed. Reg. 1379 (Jan. 7, 2005).

[150] *See* 49 C.F.R. §§ 15.11(b), 1520.11(b).

- Disclosing it only to covered persons who have a need to know, unless otherwise authorized in writing by TSA, the Coast Guard or the Secretary of DOT;
- Complying with marking requirements; and
- Reporting unauthorized disclosures to the applicable DOT or DHS component.[151]

Many have complained that the marking requirements are overly burdensome, as they require a lengthy footer for every page.[152] TSA and DOT have indicated that they may relax this requirement in a forthcoming rulemaking.

The rules provide that violations of the SSI rules by private actors are "grounds for a civil penalty and other enforcement or corrective action" by the relevant agency. Notably, each agency with authority regarding SSI is responsible for policing the SSI rules. So, for example, the Coast Guard interprets and enforces compliance with the SSI rules at MTSA-regulated facilities.

CONCLUSION

Security-related information supplied by a business to a federal executive branch agency may be protected from public release under a number of FOIA exemptions, as well as one or more other statutes or regulations, depending on the type of business, the subject matter of the information, the reason it was prepared, the agency to which it was submitted, whether it was submitted voluntarily, and a host of other factors. DOT/TSA "sensitive security information" rules impose obligations on submitters regarding their handling of the same information. A number of authorities envision controlled sharing of information between the federal government, on the one hand, and state and local governments and similarly-situated private entities, on the other – a relatively unusual concept but one that can be valuable in promoting protection of private infrastructure.

Several of the potentially applicable authorities provide an unprecedented level of protection for private information in government hands. How well these protections will work, and in particular how courts will interpret them, remains to be seen. To effectively secure the nation's private critical infrastructure, it will be crucial that all involved parties work together to maximize the effectiveness of these legal measures. This work will require reconciliation of three competing goals: (a) protecting sensitive information from public release; (b) sharing sensitive information, where appropriate, among the relevant public and private entities, and (c) ensuring that the first two goals do not lead to unnecessary withholding of truly nonsensitive and properly public information.

[151] *See* 49 C.F.R. §§ 15.9(a)(1), (2), (4) & (c), 1520.11(a)(1), (2), (4) & (c).
[152] *See* 49 C.F.R. §§ 15.13(c), 1520.13(c).
[153] *See* 49 C.F.R. §§ 15.17, 1520.17.

Attachment D

CATEGORIES OF SECURITY-RELATED INFORMATION SOUGHT BY GOVERNMENT FROM PRIVATE CRITICAL INFRASTRUCTURE ENTITIES

1. Cyber Threats to U.S. Infrastructure

2. Terrorism

3. Biological Weapons of Mass Destruction
    1. Biological Weapons (BW) and dual-use or controlled technology transfers
    2. Criminal, terrorist, and foreign government BW research and development capabilities, programs and infrastructure
    3. Methods of finance and exchange and transfer networks

4. Chemical Weapons of Mass Destruction
    1. Chemical Weapons (CW) and dual-use or controlled technology transfers
    2. Criminal, terrorist, and foreign government CW research and development capabilities, programs and infrastructure
    3. Methods of finance and exchange and transfer networks

5. Nuclear Weapons of Mass Destruction
    1. Nuclear Weapons and dual-use or controlled technology transfers
    2. Criminal, terrorist, and foreign government nuclear weapons research and development capabilities, programs and infrastructure
    3. Methods of finance and exchange and transfer networks

6. International Organized Crime
    1. Alien smuggling and human trafficking
    2. Money laundering and financial transactions in support of illegal activities
    3. Other crime with homeland security implications, i.e. conspiracy with terrorists, illegal arms trafficking, explosives theft

7. Illicit Drugs
    1. Production, storage, movement and transfer of illicit and illegal drugs, and precursor materials and equipment

8. Economic Stability and Trade
    1. Efforts to circumvent U.S. restrictions on the trade of controlled technologies, equipment, munitions and dual-use items

9. Energy Security
    1. Indications and warnings of targeting or attacks on U.S. energy infrastructure

10. Money Laundering
    1. Financial transactions in support of criminal activities, terrorism, drug trafficking, rogue states and groups.

11. Demographics, Migration, and Population Movements
    1. Immigration pressures on governments
    2. Identity, origins, locations and characteristics of refugee and migrant groups
    3. Surging population growth
    4. Foreign governments reactions and policies toward such groups

12. Environmental and Natural Resources
    1. Production, development, transport, and consumption of strategic natural resources, especially oil and natural gas and resources
    2. Production, release, illicit sale and disposal of pollutants and hazardous materials including their potential human health effects

13. Agriculture and Food Security
    1. Infectious disease of crops and domesticated animals
    2. Research, development, testing and development of agriculture and food science technologies, including genetically
       modified organisms

14. Infectious Disease and Health
    1. Location and status of infectious diseases that threaten U.S. national security, economic interests

15. Humanitarian Disaster and Relief