Moving Freight After 9/11: Compliance Dashboards to Keep Clients Current

With a low-key start right after 9/11, the U.S. Department of Homeland Security is now making substantial demands of companies that move freight. Between such new rules and the U.S. Department of Transportation requirements of longstanding, client businesses now face a bewildering and fast-changing regulatory landscape. Lawyers need a fresh approach to compliance counseling commensurate with this dynamic environment.

By Joel Webber

Homeland security-inspired constraints on logistics have become confusing to those who send and receive the goods on which our economy runs. Multiple agencies are making numerous new demands—some going to the very basics of long-standing supply chain processes. Lawyers should consider integrating these often-disconnected requirements into a "dashboard" template for clients. By marshalling otherwise isolated and fast-changing rules into a unified and coherent display, counsel can recast ad hoc regulatory constraints into actionable business intelligence.

Because of the way in which homeland security demands have developed in the last two years, lawyers must help their clients with what is actually a management challenge. This is a compliance task that is distinctive in three ways, and it calls for greater vigilance of the changing rules as well as more direct involvement with the client employees who must implement responses to these rules.

First, companies that move goods must adapt quickly to sweeping new business process demands. Of course, a federal agency's imposition of specific constraints on a company's operations is not a new phenomenon. But recent mandates by the U.S. Department of Homeland Security (DHS) are marked by their novelty, broad scope, and serious questions about feasibility. For instance, businesses that import goods into the United States have been subject to physical searches and documentation rules at ports and borders since the birth of the republic. But machine scans of cargo and tighter procedures have clogged border crossings to an extent that some trucking firms have ceased doing cross-border business with our most prolific trad-

ing partner (Canada), and those firms that are still in this business experience substantially longer waiting times than they did before.

The second way in which homeland security requirements differ from other federal regulations involves the need to comply with mandates issued by more than one federal agency. After 9/11, Congress designated a new department to protect against asymmetric attack; as a result, those who design and operate supply chains of goods must answer to two sheriffs: both DHS and the legacy agencies that regulated transportation prior to the creation of DHS, and continue to do so. For example, a chemical company that uses rail tank cars to move chlor-alkali products has long had to comply with regulations issued by U.S. Department of Transportation (DOT) agencies like the Federal Railroad Administration (FRA) and Pipeline and Hazardous Materials Safety Administration (PHMSA). Now both the legacy DOT agencies and the newer DHS are finalizing rules about such chemical tank car moves and they are doing so simultaneously. For the most part, the legacy DOT agencies and DHS are acting separately from one another and under distinct and independent legislative authorities.

The third distinction is the pace of current regulatory change, which is without recent precedent. Whenever Congress believes that federal agencies are moving too slowly, it legislates business process constraints of its own. As an example, from the time of its founding, DHS has taken the position that machine screening of cargo carried in belly holds of scheduled passenger airliners (roughly 70 percent of domestic air cargo) is commercially impossible; therefore, the department advanced its "Known Shipper" credentialing program as the main substitute for direct physical interaction with such freight. In the 9/11 Commission Implementation Act passed in August 2007, Congress simply required that *all* freight whose weight exceeds 16 ounces must be subjected to machine scans prior to loading it on scheduled aircraft that carry passengers; Congress set an implementation deadline of three years.

With the convergence of these three factors—(1) fast-paced and wholesale new government constraints on the supply chain, (2) multiple agencies acting under independent statutory authorities, and (3) Congress' expediting implementation when it believes that federal agencies deliberate too long—this new supply chain regulatory context calls for two types of contributions from lawyers.

First, lawyers need to integrate the new DHS-mandated rules with the decades-old regulations issued by legacy agencies, and they need to do so with constant vigilance. These days, the shelf life of supply chain legal knowledge is short, as each day's *Federal Register* has the potential to alter in basic ways the way that a firm moves its goods. "Dashboard" formats lend themselves better to this task than more traditional lawyer-client communications tools do.

Second, lawyers need to help their clients integrate these new rules into their firms' business processes. Briefing top management is only a first step. The agencies and Congress are both making demands that will fundamentally change the way front-line employees do their jobs. Counsel should draw on business process analysis methodologies to enable *all* personnel in their clients' firms who must incorporate these new and ad hoc agency demands into coherent business processes.

For reasons on which political scientists can speculate, the homeland security demands of the supply chain have shifted from minimal to tangible during the last year or two. Whether viewed as a function of the change in Congress' Democratic/Republican composition or because DHS agencies have now had time to sort out their massive new roles, this regulatory environment has an air of urgency that was markedly lacking earlier.

The New Regulatory Environment

After the terrorist attacks, the public said that 9/11 changed everything. But that was not immediately true for the regulation of freight flows. The impact of 9/11 right after the attacks was confined mostly to (1) heightened passenger security at airports by the new Transportation Security Administration (TSA), and (2) greater cargo scrutiny at ports and borders by U.S. Customs and Border Protection (CBP). Apart from greater CBP paperwork burdens on import activities that had long been document-intensive, firms that moved goods faced few new demands from the federal government.

To the degree that DHS asked anything of those moving freight, the department usually used the language of suggestion. Many regulations referred to "making the business case" for homeland security measures—for example, stating that securing cargo was necessary because there were thieves as well as terrorists who might get at the freight. Whatever requirements were issued tended to be in the form of security plans whose details were prepared by individual companies' managements, and were not dictated by agencies. In such a setting it was hard for businesses to get into trouble, and therefore unlikely that homeland security considerations would drive substantive business decisions bearing on people, operations, or the flow of goods and data.

"Safety" Versus "Security"

In spite of a modest start in the task of ensuring the security of the supply chain, in the first two years after 9/11 federal agencies addressed the question of how terrorists might make use of dangers *inherent* in activities that were otherwise perfectly legal. Agencies considered the issue in two settings.

First—and quite apart from any activity related to logistics—an agency was presented with the question of whether or not the public could demand protection from terror under pre-9/11 law. The agency said "no," the federal court of appeals said "yes," and the U.S. Supreme Court denied certiorari thereafter. *San Luis Obispo Mothers for Peace v. Nuclear Regulatory Comm'n*, 449 F.3d 1016 (9th Cir. 2006), *cert. denied,* 127 S. Ct. 1124 (2007).

That case involved the California's Pacific Gas and Electric company's application for a license to allow it to build a facility for storage of spent fuel from operations of its Diablo Canyon nuclear power plant. In two petitions to

the Licensing Board of the Nuclear Regulatory Commission (NRC), a citizens' group raised contentions under the National Environmental Policy Act (NEPA) against granting the needed license. The group's specific concerns related to the environmental impact that might arise as a result of a terrorist attack on the storage facility for which a license was requested.

The NRC Licensing Board rejected all environmental contentions related to terrorism, and NRC affirmed the rejection, relying on four pre-9/11 NRC decisions ruling that the NEPA review at issue need not be considered in terms of terrorist contingencies. The Ninth Circuit Court of Appeals reversed the decision, holding that NRC should have considered the environmental effects of a terrorist attack in conducting its NEPA review. The U.S. Supreme Court declined to grant certiorari.

One question remains otherwise unresolved: Broadly speaking, what do pre-9/11 laws designed to promote public safety require of agencies after 9/11 with respect to the possibility of asymmetric attack?

The second setting in which DHS and DOT addressed terrorist use of dangers inherent in otherwise legal activities was the transportation of hazardous materials. DOT and DHS debated ways in which to protect the American public from terrorists' use of hazardous chemicals against populations. Now that purposeful human activity was a policy factor, what changes—if anything—should be made in the way government secures the public against harmful release of a chlor-alkali or sulphur dioxide, for instance? Should the DOT continue to have jurisdiction as it had for decades under its Pipeline and Hazardous Materials Administration that promulgated the Hazardous Materials Regulations (HMR)? Or should DHS have this responsibility instead, reasoning that the threat to public safety from terrorists is different from the threat posed by inherent dangers? The answer given by federal agencies and Congress was: "Both should have responsibility."

From 2002 to 2004 the interagency debate between PHMSA—the legacy agency—and DHS focused on two terms of art: "safety" and "security." Even though the connotation of these terms might seem similar to those who are not familiar with this heretofore arcane debate, each term then and now reflects a very different source of legal authority and administrative reach.

For decades HMR's stated goal was called "safety," and, under this term of art, PHMSA (both then and under its earlier name, Research and Special Programs Administration) addressed those dangers inherent in chemicals that PHMSA had specified in that HMR. PHMSA and its partisans argued that this body of learning possessed by PHMSA and its DOT modal agency counterparts (such as the Federal Aviation Administration, Federal Motor Carrier Safety Administration, and Federal Railroad Administration) made PHMSA uniquely suited to secure the nation against terrorist uses of substances specified in HMR.

DHS argued against DOT that dangers arising from asymmetric attacks on hazardous chemicals related to a threat vector quite different from dangers inherent in such materials themselves. PHMSA's "safety" focus in HMR historically addressed dangers built into the materials themselves and not related to 9/11-style human intervention. The thought processes and protocols of preventing purposeful behavior were different from those related to accident prevention. And, in 2002, DHS had been chartered by Congress for this homeland security effort, and the interagency vernacular designated it as "security."

Overlapping Legal Authority and Agency Jurisdiction

The executive branch resolved the debate by leaving traditional "safety" regulation to the purview of PHMSA and its modal counterparts within DOT and by assigning "security" regulation of hazardous materials and other terrorist-caused dangers to TSA. Congress has since ratified this allocation of duties.

The case of hazardous materials transported by rail serves as a good example of the overlapping legal authority and agency jurisdiction following this role allocation of "safety" versus "security" between DOT and DHS. Since the executive branch meted out "safety" to PHMSA and other DOT agencies and "security" to DHS and its TSA unit, each has pursued parallel but distinct rulemaking in this area:

- On Dec. 21, 2006, PHMSA and FRA released a notice of proposed rulemaking on the routing of "poisonous by inhalation" hazardous material carried by rail. On April 16, 2008, the two agencies announced that this rule would get final status on June 1, 2008, as "Hazardous Materials: Enhancing Rail Transportation Safety and Security for Hazardous Material Shipments" (*Fed. Reg.* vol. 73, no. 74).
- Spelling out 27 criteria on how carriers should select routes for such hazardous material, the rule is directed to carriers but should have an impact on all shippers and recipients of the affected chemicals. Note in particular that the text references both "safety" and "security" as the goals of the regulation despite its issuance from the legacy "safety" agencies—PHMSA and FRA.
- Also on Dec. 21, 2006, DHS through its TSA agency released a notice of proposed rulemaking that also addressed "poisonous by inhalation" hazardous material carried by rail. But this rule was directed not at routing but at operational details of handling such hazardous material in rail tank cars. And rather than being directed solely to rail carriers, the TSA's regulation is directed to shippers, recipients, and other parties that handle such chemical freight. As this article goes to press, this proposal still has not been given notice for final status in the *Federal Register*, but the TSA's Office of Freight Rail Security has informed the author that the agency intends to issue the regulation in some final form.
- Meanwhile, in 2005, Congress responded to an incident involving the release of chlorine in Graniteville, S.C., by conferring jurisdiction over rail tank car "safety" to PHMSA and FRA (SAFETY-LU, 49 U.S.C. § 20155). As this article goes to press, this legislation has resulted in a proposal by PHMSA and FRA that is pending final status and would retire within five years most rail tank cars carrying "poisonous by inhalation" hazardous material that were

built before 1989 and would retire within eight years *all* such cars in favor of new ones built to prescribed heightened structural requirements (April 1, 2008: "Hazardous Materials: Improving the Safety of Railroad Tank Car Transportation of Hazardous Materials").

- Although the Graniteville incident that sparked the enabling legislation for this proposal was viewed as an accident and not as the result of terrorism, much of the debate surrounding this proposal has focused on the potential for an asymmetric attack on the specified hazardous material carried in rail tank cars.
- In a separate action, Congress passed the Implementing Recommendations of the 9/11 Commission Act of 2007 (H.R. 1), which conferred jurisdiction over rail tank car "security" to DHS. Other provisions of the act further complicate the question of who does what among federal agencies in cases of hazardous material that is transported by rail. Three aspects stand out:
    1. In § 1519, Railroad Tank Car Security Testing, H.R. 1 expressly confers on DHS jurisdiction for "security" of what Congress expressly conferred in 2005 on PHMSA and FRA as to "tank cars" and their "safety" in SAFETY-LU. Each text directs distinct federal agencies—DHS in H.R. 1 and PHMSA and FRA in SAFETY-LU—to prescribe structural and operational requirements for rail tank cars carrying specified chemicals whose unplanned release could harm the public.
    2. The two statutes provide divergent definitions of the specified chemicals over which Congress expresses security concerns. The legislation passed in 2005, SAFETY-LU, simply adopted the traditional pre-9/11 definition—those chemicals included in HMR, in which they are called "hazardous materials"; whereas § 1501 (13) of H.R. 1, passed in 2007, prescribes a new category of "Security-Sensitive Materials." As to this new term of art, Congress empowered DHS to define it, albeit with reference to HMR, and "in consultation to the Secretary of Transportation."
    3. The legislative considerations involving H.R. 1 did not take place in a governmental vacuum; the rulemaking described above has been taking place simultaneously. In particular, the TSA's final proposal of the rail-borne hazardous material rule described above has been delayed partly because of efforts within TSA's Office of Freight Rail Security to include H.R. 1 requirements into the final version (TSA personnel's conversation with the author, February 2008). It should be noted that even though TSA's initial rule was proposed in December 2006 prior to the passage of H.R. 1 in August 2007, the subsequent enactment of H.R. 1 is shaping TSA's regulatory proposal in this regard.

Overlap Sanctioned by Statute

In 2007, Congress left no doubt that it intends to leave jurisdiction over the "safety" and "security" of the transportation of goods with two separate sets of agencies. Section 1310 of the Implementing Recommendations of the 9/11 Commission Act of 2007 provides the following: "The [s]ecretary of Homeland Security is the principal [f]ederal official responsible for transportation security." Even though this section of the act directs DHS to "confer" with DOT, ultimate legal authority for "transportation security" is given unequivocally to DHS.

The Lawyer's Initial Task: Creating a "Dashboard" of Legal Demands

Just identifying the full set of homeland security demands that pertain to a client firm's freight operations is a complex undertaking—and one that requires constant updating. Business process analysis and creation of a related "dashboard" could be vital to sure-footed compliance in this emerging area. Unlike more mature regulatory regimes, homeland security makes demands that are too basic, require too rapid a response, and change too frequently to leave to more traditional and less dynamic means of lawyer-client communication.

From Ad Hoc Demands to Management Direction

This dashboard step consists simply of identifying all homeland security demands that bear on a client's personnel, operations, flow of goods, and data collection and flow. This task, in turn, requires reference to statutes, regulations, and the lore and informal practice of federal agencies. But, unlike the lawyer's subjective knowledge—or its counterpart in the form of a "memorandum of law" to the client—comprehensive compilation must be accessible to all the employees who are needed to implement compliance and thereby be actionable at the business level.

Why are these features important? Unlike a more stable and mature regulatory regime that agencies modify incrementally, three distinctive drivers identified above mark homeland security governance of logistics processes:

- rapid-paced, broad and far-reaching new government demands,
- push for action by multiple agencies with overlapping powers, and
- congressional acceleration of agency actions.

In the business process analysis terms many business clients apply to their existing commercial processes, what the client firm needs from its lawyer at this stage is a "dashboard"—a tool that collects current and near-term government demands (statutes, regulations, and agency lore) and displays them to both senior management and line-operating employees in a coherent display.

The convergence described above has created a dynamic legal environment. With several agencies often announcing in the daily *Federal Register* new government demands that introduce basic changes in the way logistics operations are conducted, both the managers and line employees of client companies require a tool to collect and report this information in order to incorporate the changes into the firm's daily business processes.

As this article goes to press, the statutes, regulations, and agency lore or informal practices indicate the need for the company's dashboard to include the following elements in order to respond to homeland security demands. Any dashboard will, of course, need to be client-specific. But the broad outline of supply chain constraints should include the following areas of coverage:

- people,
- details of operations,
- flow of goods, and
- flow of data.

Dashboard Elements: People

One obvious example of this element is the Transportation Worker Identification Credential (TWIC). Issuance is straightforward—only TSA issues this credential. But enforcement as to access lies mostly with U.S. Customs and Border Protection (CBP). TWIC is required at seaports and at facilities considered extensions of seaports—such as intermodal rail yards that are located well inland. Its issuance has been marked by numerous delays on the part of TSA, and monitors that read TWIC cards at ports and other venues have not become operational as scheduled.

Another example of regulations focused on personnel is TSA's credentialing of personnel admitted to sensitive areas of airport passenger terminal facilities as well as air cargo venues. This area is marked by debate as to how the credential will be evidenced, and what biometric and other functionalities should be embedded in it.

Not all supply chain constraints on people stem from formal rules. For instance, some hazardous material facilities have begun to require drivers to have TWIC cards; the requirement is informal and is done on the facilities' private initiative, not because it is required by law. It turns out that the elements of TWIC credential screening are virtually identical to those used by most states for endorsing commercial drivers' licenses for truckers hauling hazardous materials. In each context, the business has to ask whether or not any of its personnel must be approved as to criminal record, citizenship status, and other criteria as a precondition to driving a truck or being physically present inside a facility.

Finally, some client firms may respond by simply declining the business for which a homeland security credential is required. For instance, at the border between the United States and Canada, numerous truck carriers have ceased cross-border operations rather than get credentials that would include all their drivers in a special program required for faster driver clearance at that border. (This program, known as FAST—Free and Secure Trade commercial driver program—is operated jointly by CBP and Canada's counterpart, the Customs and Border Security Agency.)

Dashboard Elements: Details of Operations

These elements tend to be related either to restricting access to particular venues or to handling methods and special equipment required for specified goods—notably, chemical hazardous materials. As far as access to particular venues is concerned, business processes that go through a CBP station at a port or a border crossing will, of course, be significantly affected by the sequence of interactions with that agency—for example, the substantial increase in the delays that have been experienced in crossing the Ambassador Bridge between Detroit and Windsor, Ontario, since 2002.

Another experience that is related to venues involves local truck carriers who bring freight into restricted cargo areas of airports and are experiencing delays because of restrictions; these carriers are finding that, in terms of TSA's regulations, they fall outside established legal categories. Freight forwarders and airlines each have direct guidance and status credentialing from TSA, with rules governing access to air cargo areas as well as limits on what they can do in those areas. But the truck carriers bringing such cargo to the aircraft are neither air carriers nor forwarders; as a result, they have faced operational impediments stemming from their ambiguous regulatory status.

As to the limits placed by homeland security operations that are tied to particular goods, business processes that are either related to specified types of freight or use particular equipment to carry that freight may be subjected to detailed requirements. The account above relating to chemical hazardous material and to the tank car equipment that carries it is an example.

Moreover, as with the example of trucking companies withdrawing from cross-border service rather than obtaining credentials for all their drivers for the U.S.-Canada FAST program, a similar withdrawal is rumored once the rules for tank cars and related hazardous materials are finalized. For instance, one Texas firm has gone on record stating that it may have to simply not serve particular sulphur dioxide customers in light of the anticipated costs of compliance with homeland security regulations once these rules are settled.

Dashboard Elements: Flow of Goods

When it comes to the flow of goods, there is much to cover by way of explicit regulation and there is no other approach but to simply go rule-by-rule through each requirement, asking if any rule applies to one's client's operations. Encyclopedic treatment of this issue would take too many words for this article.

From a homeland security perspective, the flow of goods is primarily the subject of CBP and TSA regulation, but again, it is not possible to generalize without missing large areas of significance. For instance, the importation of food since 2004 has been subject to increasing and refined restrictions related to homeland security and asymmetric threats in the food chain—notably, filings required under the Bioterrorism Act (involving the Federal Drug Administration and CBP). More recently, the Consumer Products Safety Commission and its enforcement powers have been applied to regulation of lead in toy imports from China.

Beyond these regulations, a plethora of demands can apply to all types of goods—including the new Marine Transportation Security Act (involving the U.S. Coast Guard), the Container Security Initiative (CBP), the Known Ship-

per Program (TSA and FAA), the Secure Freight Initiative (DHS, CBP, and the Department of Energy), and upcoming 100 percent machine scanning of containers on sea vessels coming into the United States (per Congress in H.R. 1).

In addition, there is an informal form of governance of the flow of goods embodied in the Customs-Trade Partnership Against Terrorism (C-TPAT), a voluntary program sponsored by CBP. From the standpoint of the Administrative Procedure Act, these are not rules at all. If one's client firm is C-TPAT-qualified as to specified security standards, CBP promises, that company's goods will be expedited at ports and at border crossings. Although membership in C-TPAT is not formally required, membership is regarded in many circles as a practical requirement. As a former CBP commissioner stated in encouraging firms to join the program and to conform to its security demands, "Good luck" if there is a problem at the border and you are not a C-TPAT member.

Dashboard Elements: Flow of Data

As with the elements discussed above, it is important not to be beguiled by summarization here. Demands related to supply chain data flow stemming from homeland security requirements are numerous, but two broad categories illustrate the challenge.

First, as required by the Trade Act of 2002, CBP finalized rules requiring filing of cargo manifests with CBP by carriers *in advance of the goods' arrival at U.S. ports from abroad*. Requirements varied according to the mode of transport, but the common demand was that carriers must tell CBP what the goods were before the goods reached the United States, then CBP had to decide whether or not to let those goods into the country without further examination.

Second, and more recently, in January 2008 CBP issued its much awaited "10+2" data filing requirement for all imported goods. For the first time, CBP would require the importers themselves to provide data sets—10 of the information elements specified in the notice of proposed rulemaking. Far from being restricted to those businesses that consider themselves part of the logistics industry, this demand is made of any firm sourcing goods from outside the United States (January 2, 2008: "Importer Security Filing and Additional Carrier Requirements"). Despite much protest in advance over feasibility questions, CBP has expressed a strong intention to adopt this requirement in some form.

Dashboard Perspective

These elements of the dashboard—people, details of operations, flow of goods, and flow of data—are illustrative of the basic components of a dashboard that helps a business comply with homeland security in the movement of goods. Such a template is needed for two reasons. First, it must accommodate the entirety of nettlesome and possibly vital details of the actual demands the government makes in the homeland security regulation of supply chains. Although each rule is not necessarily treated by DHS or the legacy agency as so vital that its violation would be met with tough sanctions, DHS has selectively chosen a handful of areas for purposes of showing that the department is serious about compliance. In other words, noncompliance can hurt a firm. One does not want to guess wrong about which rules will be met with a "do not load" order by CBP when it comes to goods at a harbor, a company's removal from an approved program like C-TPAT, or material levels of fines imposed by DHS' Office of Chemical Security for a failure under Chemical Facility Anti-Terrorism Standards regulations.

The second reason for the template—and there is no other way to put this—is that constant vigilance is required. Someone must be reviewing the sources of rules, statutes, and agencies' informal intentions in order to avoid noncompliance on the part of the business. After all, the respective dynamics of business management and rulemaking pull in opposite directions. The supply chain must be run as a well-organized sequence of commercial activities, whereas the demands that government puts on the supply chain—at least for the moment—consist of discrete and often narrowly focused demands that come from divergent sources.

Conclusion

Regulation of the movement of freight for the purpose of ensuring homeland security—at least during the last two years and for the next few—is both intensely dynamic in its evolution and complex in its impact on the personnel, operations, and flow of goods and data of a business. Unlike the immediate aftermath of 9/11, these rules make substantial demands on the business sector, and agencies that administer the regulations in both the Department of Transportation and the Department of Homeland Security can be counted on to be serious—selectively at least—about a company's noncompliance.

For years corporate managers have used business process analysis methodologies to deconstruct the mass of their operations into discrete activities suitable for analysis and then focus on those activities they want to control. Until the storm surrounding the regulations dealing with the logistics of homeland security calms down, companies involved in the movement of goods will need tools like compliance dashboards that can meet this new challenge effectively. **TFL**

Joel Webber practices business law and serves logistics clients with the firm of Couri and Couri in the Chicago area. He previously served as vice president of mergers and acquisitions for GE Rail.