

# Commercial Operations Advisory Committee

## Comments On

### Department of Homeland Security's Draft Report

#### *“Strategy to Enhance International Supply Chain Security”*

May 15, 2007

### **Background**

On March 29, 2007, the Department of Homeland Security (DHS) provided the Commercial Operations Advisory Committee (COAC) with a draft of its “Strategy to Enhance International Supply Chain Security”, a document intended to meet the requirements of Sections 201 and 202 of the SAFE Port Act. That Act calls for DHS to obtain COAC comments on this document.

DHS requested COAC to provide comments by May 4. However, the full COAC could not accept our comments until May 15. The following comments are in response to that request. COAC hopes that these comments will be useful to the Department in addressing this very challenging issue.

### **SUMMARY OF COMMENTS**

A majority of COAC members having considered the draft recommends the following be considered.

1. We do not believe the plan is actionable. A good plan should provide a clear set of instructions that are specific as to roles, responsibilities and actions to be taken. It should be a blue print that can be referred to in both planning and execution. The plan as written is general and very high level in describing roles and responsibilities. Until the detail is populated, we do not believe the plan is useful.

2. The international supply chain environment is interdependent as to modalities of transportation and supporting industries. The maritime environment does not exist in vacuum. Yet the plan is almost entirely focused on the maritime environment and therefore fails to recognize these co-dependencies. Recognition and a broader focus on the totality of the environment was recommended in COAC's preliminary comments that were provided in January.
3. COAC's preliminary recommendations indicted that clear lines of command and control are essential to a good plan. The plan does not specify exactly who is in charge at each level or how that authority cascades and there are also no recommendations "regarding legislative, regulatory and organizational changes necessary to improve coordination among the entities or to enhance the security of the international supply chain" [Sec 201 (b) (3)]
4. While the plan describes at a high level the relationship between departments of the government, it does not specify what interlocking agencies are expected to do in detail sufficient to enable coordinated guidance. It is merely a compendium of agency high-level departmental responsibilities and a historical recap. Moreover, there is no discussion of the "gaps and unnecessary overlaps in the roles, responsibilities, or authorities " and what is going to be done to address them [Sec 201 (b) (2)].
5. Key to minimizing chaos in the event of a terror incident or disaster is keeping the trade informed. This was a key recommendation of the COAC in its earlier comments. The plan does not require 24x7 communication with the trade nor does it provide that any agency is charged with this responsibility. This is a major weakness.
6. Key to resuming the flow of goods is identifying available alternative pathways. The plan does not provide for intelligence to the trade on port conditions as recommended in our original comments.
7. The law requires a protocol for resuming the economy in the event of a disaster but the plan does not provide tactical protocols that specify what discrete steps the government will take to restore the flow of goods and materials into the US economy.
8. There is no mention of addressing potential requests of foreign governments for export information in order to help secure their own borders.
9. The plan does not speak to the exchange of information with other domestic and international law enforcement agencies that may have actionable intelligence. Other than a brief discussion of the Office of Intelligence and Analysis there is little mention of the "process for sharing intelligence and information with private sector stakeholders to assist in their security efforts [Sec 201 (b) (8)].

10. The SAFE Ports Act requires that the government set measurable goals, objectives and timetables to implement a national strategy. But the plan does not provide these important benchmarks.
11. The plan does not make any legislative proposals as provided in the Act. We believe legislative proposals, such as establishing the principles of Federalism, are indicated.
12. A key to the layered approach to national security, has been voluntary participation in CTPAT. Recognizing this the Act calls for incremental benefits for participation in voluntary programs. The plan does not speak to this.
13. Insofar as COAC is to advise CBP, there is no mention of specific CBP plans, which COAC would presumably have particular insights to. For example, the redeployment of CBP assets.
14. The plan does not speak to costs versus benefits or even how analysis of marginal costs\benefits can be approached. Programs such as the “advanced data initiative” will require re-engineering of the global business process. But there is no requirement that the program be demonstrated to achieve significant benefit.

We would like to submit the following specific comments, which have been endorsed by COAC.

Finally, we also respectfully request that the Department continue to consult with COAC as subsequent iterations of this Strategy and tactical plans are developed, up through and including the final strategy that is not due to Congress until late 2009.

## **General**

A good strategic plan should identify the overall objective that you are trying to achieve, where you currently are and what you need to do to get there or close the “gap.” Such a strategic plan should also clearly identify who is responsible for what. The draft strategy is an excellent compilation of the existing regulations, programs, plans and relationships but it fails to address how these pieces fit together, does not identify what further action needs to be taken and what plans are in place or under development to address these needs, not does it clearly identify who is responsible for what future action.

Finally, the scope of the document should be clearly articulated upfront. While “international supply chain security” presumably includes non-containerized cargo, export cargo and international cooperation, the document is almost exclusively focused on containerized import cargo.

## **Part II. Purpose**

### **“Problem Definition” Section**

Page 6: Line 32: The term “push our borders out” may be unnecessarily provocative in other countries. COAC fully supports the development and expansion of effective security strategies beyond the limits of the nation’s territorial jurisdiction. Borders, however, are not mobile, and they should be respected. Foreign nations have shown willingness to cooperate with the United States on supply chain security initiatives. CSI is a good example; however, protecting their national sovereignty is an understandable objective. As a stylistic recommendation, we believe these words could be dropped with no detracting from the concept being presented.

Line 33: For some aspects of maritime commerce, the U.S. government performs risk assessment before a conveyance, person, or cargo arrives in the U.S. For containerized import cargo – the most substantial part of the international supply chain security challenge, however, the U.S. government’s stated strategy has been that risk assessment should be conducted before a container is loaded aboard a vessel destined for the U.S., not before it reaches the U.S. This is the premise of the “24 Hour Rule” and CSI. This Draft Strategy is notably less clear and specific about that, which should be changed. While the 24 Hour Rule should not necessarily be extended to non-containerized cargoes not already covered, the document should clearly restate this principle for inbound containerized cargo. We recommend that the following text be inserted prior to the period at the end of the sentence “, and for international containerized cargo, before it is loaded onto vessel destined for the United States”. Second, we note here and in several subsequent observations that it is very odd for a document explaining DHS’s international supply chain security strategy to mention not a single word about the Secure Freight Initiative or CBP’s pending “10 plus 2” initiative, which are designed to enhance the present strategy.

Lines 34-35: The Strategy states: “The global supply chain is bidirectional, requiring domestic efforts to ensure the integrity of both inbound and outbound cargo.” While a correct statement, the Strategy does not discuss outbound supply chain security strategy, gaps or measures to be taken.

### **“The International Cargo Supply Chain” Section (pages 7-9)**

Figure 1 and its accompanying text are described as depicting “intermodal supply chains; Figure 2 is described as a modification “to accommodate non-containerized cargo results”, yet Figure 2 continues to use containers in its flow chart. We do not see that Figure 2 adds any value to Figure 1. If a non-containerized trade depiction is desired, further effort may be appropriate.

As a more general comment, there appears to be a discrepancy between the Draft Plan’s foreword, quoting the SAFE Port Act language requiring that the Plan should be “specific to containerized cargo”, and subsequent parts of the Draft that includes other types of cargo. The causes some confusion in places, such as Chapter VIII’s inclusion of a discussion of air cargo, but only for the U.S. domestic transport movements.

The Department may wish to choose between drafting a plan for all types of cargo in international supply chains and include balanced descriptions for air, rail and truck movements, or focus on maritime cargoes (and perhaps specifically on containerized maritime cargoes as required in the SAFE Port Act).

### **“Securing the Supply Chain” Section (pages 9-10)**

The Largest Perceived Threat: Page 9, lines 10-12 state: “The largest perceived threat to the international supply chain today is the potential for a terrorist to use a maritime cargo container as a conveyance for a weapon of mass destruction.” Is this correct? We recommend that DHS make sure that this is the Department’s view, as some senior Department officials have expressed different opinions on this issue, and as later parts of the Strategy state that the threat of such weapons “is not limited to containerized cargo, but includes bulk, break-bulk and roll-on, roll-off (RORO) cargo as well.” (page 11, lines 18-19)

Page 10, lines 12-13, state that the greatest threat is “the use of the maritime transportation system to deliver a nuclear weapon”, which is a considerably broader description than the use of a maritime container, particularly of the “system” is defined to include small vessels, fishing vessels, and recreational vessels.

Supply Chain Financial Flows: Line 32 on page 10 states that the government’s supply chain security program requires that “the financial flows” between supply chain “trade partners” must be “tracked”. The document nowhere else discusses what the government strategy, program; plan or intent is in this regard.

## **Part III. Scope**

### **“Relationship to Other Plans” Section (pages 15-20)**

The Draft Strategy to Enhance International Supply Chain Security should clearly explain the relationship between itself and the array of plans that have already been developed for maritime security, including the eight maritime security sub-plans under HSPD-13, the HSPD-7 Maritime Modal Plan under the National Infrastructure Protection Plan (NIPP), and the National Maritime Transportation Security Plan under MTSA.

The Draft Strategy document fails to do this.

The Executive Summary (page 5) states that the Strategy is “built on and complements” the other strategies. Figure 4 on page 15 provides a visual listing of all the various directives, strategy documents, and plans, but fails to inform how they relate. For example, how does the National Response Plan under HSPD-5 relate to the Maritime Modal Plan under HSDF-7 or the Maritime Operational Threat Response Plan under HSPD-13? There is no apparent linkage or relationship between the Maritime Modal Implementation Plan under HSPD-7 and any of the eight maritime plans issued under HSPD-13. For example, it not clear what the relationship is between the Maritime Modal Implementation Plan of the Transportation Sector Specific Plan and the Maritime Appendix of National Strategy for Transportation Security. For example, the Draft Strategy appears as a new plan under the SAFE Port Act with no defined relationship to the other plans. Clearly, the text of the Draft Strategy borrows from other plans, but one is left wondering: Do all the plans retain equal, unchanged, present validity? How they relate to one another?

The plethora of plans creates confusion regarding who is supposed to do what, when and how.

Figure 5 provides no enlightenment in this regard. For example, it identifies twelve (12) different “plans” and eight (8) additional “systems” or “strategies” that apply to U.S. ports of entry.

Figure 5 also does not accurately reflect the beginning and end points for a number of the plans and programs. For example MTSA does not address the Port of Origin through Shipment Deconsolidation, nor does the AMSP cover Shipment Deconsolidation.

The narrative text in these five pages lists and describes these many plans, but again provides no real enlightenment. It is confusing.

Finally, a “plan” should be a document that when read describes who is responsible to do what, under what circumstances. It also should define what further actions and improvements need to be undertaken, and by whom. In fact, the terms of Section 201 of the SAFE Port mandating this document appear to require such detailed clarity. Much of this Draft Strategy, like many of the other plans listed in Figure 4, is a general narrative of what various DHS entities are doing, rather than being a clear plan.

## **Part IV. Guiding Principles**

### **“Guiding Principles” Section**

General : COAC believes that information sharing among various agencies and reciprocity with trusted trading partners should be added as guiding principles.

Page 22, Line 12: As noted above, the present strategy for international import containers is to obtain and analyze accurate advance data, and perform risk assessment, *before vessel loading* in the foreign port, not before “it *approaches* the U.S.” This important distinction should be retained for import containerized cargo.

Page 22, Lines 8-13: Information sharing amongst U.S. government agencies and with the governments of our trading partners is equally critical. A common set of desired data elements will help minimize duplicate requests for information being made from different trading partners to the same supply chain constituent.

Same page, lines 33 onwards: The text should not characterize the IMO, WCO and ISO at the same level. The first two are intergovernmental organizations; the latter a NGO. The text creates an impression that these organizations work products have the same value/standing as “standards”. The ISPS Code is a mandatory, uniform set of requirements. The WCO’s Framework is a very high level, voluntary framework of guidelines, not specific standards, developed by government authorities. The ISO’s are voluntary industry standards with little or no government input or even support.

### **“Economic Impact” Section**

Page 23, lines 28-29: Consistent with the Maritime Infrastructure Recovery Plan (MIRP) and Maritime Commerce Security Plan, the draft Strategy’s stated assumption is that the maritime transportation system should not be automatically shut down in response to an incident. That is an important assumption. It is a fundamental principle of building the necessary resiliency into the international transportation system. A system shutdown would create potentially disastrous economic consequences – consequences that could easily exceed the damage caused by the transportation security incident itself. This Strategy document, however, provides no real insight into how this objective will be achieved.

### **‘All-Hazards Planning’ Section**

Page 24: There is clearly merit in all-hazard incident management planning. There are significant differences within maritime sectors and amongst maritime security threats, however, which require different planning in order for effective response to be applied. For example, planning for the oil transportation sector will involve issues different from the cruise industry. Further, different sectors have different government agencies responsible for portions of their sector’s security, necessitating segmented strategic planning.

Containerized maritime cargo, which is a main component of the international maritime supply chain security challenge and this Strategy, requires distinct planning

efforts, not only because it cuts squarely across Coast Guard and CBP and foreign jurisdictions' authority and competence, but because a terrorist incident involving a container will very possibly mean hundreds of thousands of separate conveyances (containing billions of dollars of goods) in or on their way to U.S. ports may become subject to security concerns that cannot be effectively addressed until the cargo containers are allowed to be unloaded. These scenarios require plans that go far beyond an "all-hazards" plan.

## **"Concepts of Prevention, Response and Recovery" Section**

Page 27: lines 10-40 indicate that there are three phases of recovery "initial," "long term" and "restoration." In the aftermath of Hurricane Katrina, the USCG formed a Maritime Recovery and Restoration Task Force. That Task Force identified just two phases of recovery; "recovery" and "restoration." The Task Force recommendations eventually became Area Instructions and were incorporated in AMSP's around the country. The Area Instructions also required the creation of "MTS Recovery Units" in each port. The Strategy should be brought into alignment with other guidance from the USCG.

## **Part V. Considerations and Assumptions**

On page 29, the fifth bullet point (lines 17-18) states: "Expansion of trade will result in expansion of infrastructure to accommodate the cargo flow." At one level, this statement is obviously correct. The implications the Strategy document seeks to draw from this statement are not clear, however. Planners should recognize that the intermodal transportation system does not generally operate with significant excess capacity in its various components, and it will have limits on how efficiently it can handle major, sudden shifts in cargo volumes. Thus, for example, even if Puget Sound ports could accommodate calls from the vessels normally scheduled for Los Angeles, there would not be adequate rail capacity, chassis, truck capacity, or terminal space to handle the cargo, and thus the vessels could not be serviced in any kind of normal operation, affecting export as well as import commerce.

Planners should also recognize that, for a number of reasons, expansion of trade would need to be accommodated by increased efficiency of existing infrastructure; that is, more cargo will be run through the existing infrastructure. Accordingly, actions that impair the ability of the infrastructure to handle cargo volumes efficiently will have even greater adverse effects in the future as freight volumes grow.

The seventh bullet point (lines 23-25) states: "Enhanced delivery of security data (e.g., imaging and scanning data) will enable more informed targeting of cargo." It is more than a little odd and disconcerting that a DHS "Strategy to Enhance International Supply Chain Security" would not define or even discuss the Department's "Secure Freight Initiative" or its principal components, namely the enhanced overseas radiological and radiographic inspection of containers (as strongly advocated by the

Congress) or CBP's announced "10 plus 2" Initiative. They are nowhere even mentioned, and their roles in the Strategy are nowhere discussed. This is a fundamental problem, as these efforts are presumably significant parts of the Department's "Strategy to Enhance International Supply Chain Security".

The Maritime Commerce Plan and the SAFE Port Act recognize that advance electronic cargo information is critically important to before vessel loading security screening for containerized cargo, and that DHS needed to "develop a plan to obtain additional advance electronic information to support cargo risk assessments". (See page 14 of the Maritime Commerce Plan. See also Section 203(b) of the Act.) In response, CBP has undertaken its "10 plus 2" initiative, has worked closely with the trade and with COAC.

Because the DHS strategy in dealing with international supply chain security is based on risk assessment, and because the "10 plus 2" initiative and the Secure Freight Initiative are important advancements in the Department's improvement of its risk assessment capabilities, this Strategy document needs to address them and their role.

In the tenth bullet point (line 36), "ensuring" should be replaced with "enhancing".

### **Additional Considerations and Assumptions**

Operating Port Facilities at MARSEC Level III: An important factor relevant to Considerations and Assumptions is that in planning for trade resumption, the Coast Guard and DHS must recognize that at MARSEC Level III, container port facilities can operate only at an extremely limited basis, will be ineffective at handling normally scheduled operations, and are unlikely to be able to handle any significant level of operations that may be diverted to them. Thus for planning purposes, MARSEC Level III should not be considered a security level at which ports can handle significant cargo volumes.

The Supply Chain "Pipeline": DHS Strategy must recognize and address the fact that at any given moment, huge quantities of import cargo are loaded on vessels destined for the U.S. On any given day, roughly some 370,000 containers of cargo are on board vessels on their way to United States ports. This means that approximately *one-third of all the vessel capacity* serving U.S. international containerized commerce is already loaded and at some point on its voyage to the U.S. Should substantial restrictions be placed on that transportation's capacity to deliver its cargo according to the scheduled service (including the ability to discharge cargo in port), the "knock-on" consequences to the entire transportation network and the cargo throughout the thousands of import and export supply chains could be very significant. It is for this reason, amongst others, that DHS's enhancement of its pre-vessel loading risk assessment and screening capabilities is so important.

## **Part VII. Roles, Responsibilities and Authorities**

### ***Federalism and Preemption***

The text on lines 27-28 on page 32 states: “And finally upon release by CBP, the cargo becomes subject to State and local jurisdictions.”

On page 54, the Strategy document has an excellent discussion of federalism and preemption of state action when *the Coast Guard* takes action pursuant to this plan. Those principles are no less important and no less applicable with respect to *Customs and Border Protection* decisions on cargo admission and release under this plan, and it is essential that the Strategy document make this clear. Once DHS, presumably via CBP, has completed its security review of containerized cargo and determined that cargo security questions have been properly addressed, and has determined to allow that interstate or foreign transportation of the goods to continue, that decision must not be countermanded by state and local officials. The same arguments, which led to the “Federalism” statement for Coast Guard/DHS decision-making, apply to CBP/DHS decision-making regarding the permissible flow of import foreign commerce. If the federal government’s view is that state and local governments can stop a container from moving through their jurisdiction after DHS has cleared it for movement, this Strategy document’s attempt to articulate a workable framework for the continuity of commerce and transportation system resiliency is an empty shell and could be rendered meaningless in the event of a transportation security incident.

We recognize that the Draft Strategy states that: “The authorities of federal agencies, other than the Coast Guard, may also preempt state action....”; however, it goes on to say: “All questions concerning specific agency authority to preempt state action must be referred to competent counsel.” (page 55, lines 1-2) This reflects the absence of a plan or a strategy for how to address this issue, and is thus incompatible with an effective and workable international supply chain security strategy. It is fundamentally important that this Strategy document address state preemption with respect to DHS cargo release decisions with clarity equal to what is used in addressing preemption with respect to DHS decisions affecting vessels and ports.

It is entirely appropriate for federal officials to consult with state and local authorities in both developing and implementing this security strategy and related plans; however, once the federal government has made a decision under the plan and exercised its authority about the permissibility of the continued transportation of interstate and foreign commerce, that decision must be binding on all governmental units within the United States.

## *Other Comments*

Spheres of Influence: Figure 8's depiction of "spheres of influence" is not helpful. It does not really describe the "interrelationships between the various responsibilities" (page 33, line 13), and fails to provide clear information or meaning. It makes the government look less coordinated than it presumably is, and fails to distinguish decision-makers in the implementation of this strategy from non-decision-makers.

Who Decides What Cargo Comes into U.S. Ports? Consistent with the MIRP and the Maritime Commerce Security Plan, the document states that CBP "screens and evaluates cargo, crew, and passenger movements into and out of the United States" and "Authorizes lading and unlading of cargo" (page 37, lines 21-22, and 26), and that the Coast Guard "supports U.S. Customs and Border Protection in the screening and evaluating of cargo movement into and out of the United States", and "controls vessel traffic, movement and anchorage ... and controls access to and operations of " port facilities. (page 36, lines 7, 9-10 and 28-29) The DHS Strategy should clearly address this issue of responsibility and decision-making for the decision to permit or exclude containerized cargo entry into U.S. ports and to permit its release from the port. The industry's experience to date is that this issue is still awkwardly addressed or avoided.

In the event that there is a transportation security incident caused by something that has been secreted into a container, we may face a situation where the "first" defenses of cargo screening and CSI have not prevented the incident, C-TPAT may not have prevented the incident, and we may not have sufficient intelligence or forensics to isolate the cause or give complete confidence in all arriving containers, which arrive at U.S. ports at roughly the rate of 36,000 per day. On average, roughly 370,000 containers are on board vessels that are sailing for U.S. ports on any given day.

It is fine to say that the Coast Guard controls vessel traffic and movement and access to port facilities, and regulates port facilities, and that CBP screens the cargo, but the Strategy seems best summed up by saying: "CBP and Coast Guard will work jointly to make initial cargo and vessel movement decisions and to execute those decisions in a coordinated fashion". (page 81, lines 33-34) How will this happen? How will the system be managed under such difficult circumstances? DHS should have pre-planned clarity on this issue. Furthermore, there will also be non-DHS departments who may want to play a decision-making role at such times, including the Department of Defense and the FBI. A clear pre-planned DHS unity of action will be necessary.

If this kind of planning has taken place within DHS, it is not evident from this Strategy document or the other plans listed in Figure 4. In fact, Part VII of the document could be read to imply that it has not been done. An effective international supply chain security strategy would seem to require that this planning be done and clear to all participants -- including carriers, port facility operators, government agencies, and foreign governments -- in advance, and that it would shape the strategy of what additional security measures need to be taken (e.g., the "10 plus 2" initiative).

Crew Screening: The Strategy states that it is CBP's responsibility to screen and evaluate vessels' crew. It is important that CBP, ICE and the Coast Guard agree on this and act in a coordinated, unified fashion. It would be helpful if the plan identifies how this coordination will occur.

MARAD: The text describing MARAD's responsibilities states that the agency "determines services and routes necessary to develop and maintain American foreign commerce and requirements of ships necessary to provide adequate service on such routes". (pp. 42-43, lines 35-1). This text describes an extinct operating differential subsidy program functionality applicable to U.S. flag vessels. It is no longer applicable.

DOC: The text states that the Department of Commerce "can provide expertise in the management of cargo". We are not aware of such expertise within DOC.

Subject Matter Experts: The text reiterates the concept identified in the MIRP that the private sector may be asked to participate in the efforts to facilitate restoration of commerce: "When requested by the National Maritime Security Advisory Committee (NMSAC) during planning for recovery...provide experts for advising on recovery management..." DHS should clarify its expectations regarding "subject matter experts". In February 2006, NMSAC responded to a request from the Coast Guard and provided a list of subject matter experts (SMEs) for this purpose; however, NMSAC recommended at that time that the Coast Guard/DHS contact these recommended parties at its earliest convenience in order to:

- 1) confirm with them whether the Coast Guard/DHS has accepted them as SMEs,
- 2) confirm and obtain any necessary elaboration of the party's contact information to meet Coast Guard/DHS needs,
- 3) as clearly as possible, *identify what the Coast Guard/DHS expects of SMEs*, and
- 4) *inform each such person selected as a SME what kind of information the Coast Guard/DHS would be likely to seek from them so that such persons can make arrangements in advance to try to obtain, or be able to quickly obtain, that desired information.*

To the best of our knowledge, neither the Coast Guard nor DHS has ever contacted these SMEs, or informed them of what the Department's expectations may be. In fact, during the discussions with DHS leading to the formation of the Maritime Security Coordinating Council (MSCC), the function and even the intended use of these SMEs was left in doubt, as this function was described by DHS representatives as one that the

MSCC would undertake. This confusion is not helpful and should be addressed. Furthermore, any such persons, if they are to be used for the stated purpose, should be contacted well in advance of a crisis to inform them of what they may be requested and expected to do to be of assistance at such times.

Federalism: Regarding the “Federalism” section on page 54, please refer to the discussion above immediately under the heading of Roles, Responsibilities and Authorities.

MSCC: Regarding Sector Coordinating Councils (page 55, lines 30-39), the role and function of the Maritime Sector Coordinating Council remain unclear and undeveloped.

Understanding How Much Cargo is Coming: A substantial portion of the maritime transportation capacity serving the United States will at any given time be loaded with cargo and sailing for U.S. ports. For example, it can take roughly 8-17 days for a TransPacific service, depending on the service and load port, a week or more for a North Atlantic Service, and more than two weeks for an U.S.-Australian-New Zealand service. A very rough estimate is that one-third of all vessel capacity at any given time is loaded and underway for the U.S. Thus, if there were a transportation security incident that required substantial restriction of U.S. port access or U.S. port closure, it would be important for DHS to quickly be able to assess how much cargo is scheduled to arrive at which U.S. ports when. CBP has container cargo manifests for all arriving vessels 24 hours before vessel loading, and the Coast Guard (and CBP) have Notices of Arrival (NOA) 96 hours prior to vessel arrival. But, NOAs do not show how many containers are planned for discharge at each U.S. port of arrival, and we are unaware of whether CBP extracts this data from its AMS system in a routine or timely manner.

The Strategy states that the Coast Guard “monitors maximum vessel, cargo and intermodal throughput” (page 36, lines 24-25), and that CBP does the same (page 37, lines 19-20)”. We are unaware that the agencies do this, and are not clear how they do this. But if, for example, the Port of Charleston were closed, would the DHS management structure know how much containerized cargo was due to arrive in Charleston in the next four days? Would DHS know how much excess capacity a port currently has? Such information would be relevant in response and recovery planning and implementation. If this information is not currently available to DHS, then it represents the kind of issue that we would hope the Strategy document could identify as “work to be done”, and which the industry would be pleased to work with DHS to address.

## **Part VIII. Concept of Operations**

General: The Concept of Operations is a long run on text and would be easier to follow if it was bulleted or numbered.

### **“Origination to Port of Origin” Section (Page 58)**

As indicated in the comments about the Guiding Principles, international cooperation is critical, however there is no mention of it in the ConOps.

### **“CSDs (Container Security Devices)” Section (page 59)**

We commend and fully support the effort of CBP, DHS Policy and S&T to develop technical and operational requirements for the employment of CSDs. It will be important that the maritime industry have the opportunity to comment on such requirements before they are finalized.

The requirements need to address, inter alia, the following issues:

- What specific security function must the device accomplish? Is the CSD limited to just “door opening and removal” (page 59, line 34) or “six-sided security as envisioned by the ACSD program?
- What is the permissible rate of false positives and negatives?
- What is the technology to be used? RFID? GPS? This is critical to know what kind of device reading infrastructure would be required.
- What radio frequencies must the devices operate within? The devices must be able to operate and be read throughout the world if they are to be useful.
- What are the power standards and battery life requirements?
- What are the *devices*’ safety standards? If carriers are going to be transporting containers with electronic devices in them, including in containers with goods such as fireworks, flammable, dangerous and hazardous cargoes, there must be effective standards protecting carriers and cargo against the risk of device leakage, electrical discharge, fire or explosion.
- What are the standards that protect against amendment and manipulation of the data in a device? As most vendors call for reusable devices, many people around the world are likely to have access to devices that allow them to amend the data in a CSD. This presents security vulnerabilities that should be addressed in the standards.
- Data storage and transmission standards.
- Data reader standards. (RFID devices are worthless without a global reading infrastructure.)

The standards must be operational globally – as that is where the containers will be traveling.

It would be unacceptable if the only way a CSD reading can be obtained is through a proprietary information system owned or controlled by the device provider.

Finally, and even more importantly, it is essential that such standards must ensure the application and utilization of non-proprietary, open architecture technology.

Regarding the Strategy document's discussion of the potential use of CSDs as part of Tier III of C-TPAT, we recognize that the concept of developing CSDs for C-TPAT Tier III participants is a concept found in the SAFE Port Act. A necessary precursor to the consultations that the Strategy says DHS anticipates with industry, however, will be clarity on who will be expected to read the CSDs, at what points, and what the protocols will be with respect to those readings. How and by whom will the CSD's be "qualified" (page 61, line 4)?

Figure 9: In line with our comments about Figure 5, Figure 9 also does not accurately reflect the beginning and end points for a number of the plans and programs. For example MTSA and TWIC do not necessarily apply to Storage and Shipment Deconsolidation.

### **“ATS (Automated Targeting System)” Section (page 63)**

We do not understand how a Strategy to Enhance International Supply Chain Security can discuss the Department's advance containerized cargo screening strategy without a single reference to CBP's "10 plus 2" initiative, particularly in light of Section 203(b) of the SAFE Port Act's requirement to enhance the capability of Automated Targeting System.

As noted in discussions above under "Problem Definition", it is also important that this document not be read to deviate from existing CBP import container screening strategy that cargo evaluation is intended to be done before vessel loading in the foreign port, not "before arrival" as stated on line 28 , page 63. If the security question does not involve high risk, it is acceptable to inspect a particular container in the U.S. port of discharge, but the strategy should be to perform the risk assessment and to inspect any and all "high risk" containers before vessel loading.

We recommend that the Strategy document be revised to address these points.

### **“CBP Cargo Screening” Section (page 69)**

We recommend that this section of the Strategy document, as well as the NII and Radiation Screening Technology section immediately following it on page 70, should address the Department's Secure Freight Initiative pilot programs, and how it intends to address the high profile Congressional interest in higher levels of overseas container inspection.

The quantitative descriptions of DHS's technology deployments on page 69 differ from those provided on page 70. One consolidated, reconciled listing would be appropriate.

### **“Lead Agency Mission Execution” Section (page 75)**

**FBI**: The Strategy document states: “For terrorist incidents, the Attorney General, acting through the FBI, executes the primary responsibilities for coordinating and conducting all federal law enforcement and criminal investigation activities”. The document goes on to state that the FBI “works in conjunction with the PFO (Principal Federal Official)”. (page 77, lines 34-36, 38-39)

We note that the U.S. Department of Justice Inspector General's March 2006 report, entitled “*The Federal Bureau of Investigation's Efforts to Protect the Nation's Seaports*”, Audit Report 06-26, among other things, stated:

- “overlapping responsibilities between [the FBI and the Coast Guard have] the potential to confuse the respective responses of the FBI and the Coast Guard to a maritime-based terrorism incident.”
- “The Maritime Operational Threat Response (MOTR) plan ... issued in October 2005 ... does not clearly delineate the respective roles of the Coast Guard and the FBI...a lack of jurisdictional clarity in the MOTR could hinder the ability of the FBI and the Coast Guard to coordinate an effective response to a terrorist threat or incident in the maritime domain. Specifically, we are concerned about how confusion over authorities will affect the two agencies' ability to establish a clear and effective incident command structure.”
- “To ensure an effective federal government response to maritime terrorism, the overlapping responsibilities, jurisdictions, and capabilities of the FBI and the Coast Guard need to be sorted out before an incident occurs and not during an incident. Unfortunately, the MTSA and MOTR plan have not eliminated the potential for interagency conflict and confusion in the event of a terrorist incident at a seaport or elsewhere in the maritime domain.”

While the report stated that the “relationship between the FBI and CBP is better defined”, it would seem that the same jurisdictional questions would be likely if the security incident involved a threat coming from the supply chains being handled by the maritime industry as by a direct attack on maritime assets.

We also note that the “MOTR” is nowhere explained in the Strategy document, other than through an otherwise unexplained reference on page 79, lines 39-40. If the issues identified in the Department of Justice's Inspector General report have been addressed, the document should explain that. If they have not been addressed, we believe that the situation requires serious attention.

**NROM and the Need for Exercises:** The Strategy states: “CBP and the Coast Guard will jointly activate the [National Response Options Matrix]. The NROM will provide the Commandant and the Commissioner with a menu of immediate, pre-planned security response options to implement throughout the maritime transportation system.” (page 82, lines 20-22) Industry has little insight into the NROM or its implications for commercial operations. To the extent the options would have significant operational ramifications for ocean carriers, terminal operators, or shippers, we would strongly recommend interagency exercises involving the industry. As the Department of Justice Inspector General report mentioned above notes:

“Such exercises are important to identify and resolve any problems or misunderstandings over jurisdiction, incident command, communications, tactical operations, or other matters that might impede the swift and effective resolution of a maritime terrorist incident.”

We also recommend that such exercises involve appropriate governmental authorities of the United States’ foreign trading partners.

## **Protocols and Factors for Prioritization of Resumption of Trade**

The discussion under this section (pages 86-90) is quite important, but also unclear.

### **Prioritization for cargo or commodity movement (page 87)**

The first factor for cargo prioritization is: “Is the conveyance, cargo or commodity cleared for entry based on established or incident specific screening procedures?” This is confusing for several reasons:

- For containerized cargo, is the “conveyance” the ship transporting the container or the container that holds the cargo? If it means the ship and its clearance for entry, then this has no application to the prioritization of cargo, as there could be 4,000 or more containers on a ship. If it means the container, then there is some confusion about what is intended by the term “cleared for entry”. Normal commercial and Customs practices and law do not require goods to be cleared for entry before they are allowed to be unladen from a vessel, and in some cases (such as “in bond” shipments) entry may occur 10 days after delivery at an inland destination.

If merchandise entry were to be required for cargo to be allowed to be unladen or released, then the Strategy would need to be very clear about this, as it is a very substantial change from current law and practice and would have enormous operational ramifications for the transportation of cargo.

If the term “entry” does not mean merchandise entry in the normal sense, the text should clarify its intent.

- Another factor in the Strategy document relating to priority for cargo movement is whether “the conveyance [is] operated by a trusted partner, such as a validated participant in C-TPAT. (page 87, lines 11-12). Again, clarity on the definition of “conveyance” is needed. It would appear that this language confuses an already awkward provision of the SAFE Port Act (Section 202(c)(2)), which at least makes clear that the “conveyance” is the container, and would require the importer to be a validated C-TPAT participant.

The term “operated” is unclear. It could be interpreted to mean that it is a container involving a C-TPAT importer’s cargo. It could be interpreted to mean a container that is being transported by a carrier, although the term “operate” is not normally used in this manner. As all significant liner shipping companies are C-TPAT participants, *carrier* C-TPAT participation would not produce any significant prioritization. The text should be modified to make it clear whether the conveyance in this context means the container, and whether it means that the cargo in the container is from a C-TPAT importer.

- More fundamentally, both this section of the Strategy and Section 202(c) of the Act speak to giving “preference” to cargo controlled by C-TPAT importers but nowhere describes what is meant by such “preference”. Does this mean quicker release from the U.S. discharge port? Vessels will have validated C-TPAT importers’, non-validated C-TPAT importers’, and non-C-TPAT importers’ cargo on the same vessel, so it is simply impractical to discriminate amongst C-TPAT containers and non-C-TPAT containers in so far as vessel entry and vessels’ cargo discharge are concerned. Further, the preference cannot reasonably relate to permission to unlade only such containers at U.S. discharge ports, as vessel operations cannot function that way with mixed status containers aboard.

If the “preference” means that only C-TPAT cargo may be loaded aboard vessels destined for the U.S. at foreign ports of lading, the plan will need to be very clear about this, as this would present numerous, substantial issues, including 1) the ability of CBP’s AMS system to promptly issue carriers Do Not Load Messages to all non-validated C-TPAT shipment filings pursuant to the 24 Hour Rule immediately upon the occurrence of a transportation security incident that might trigger such a preference, 2) the development in advance of protocols for all the vessels that are already loaded and underway to the U.S. (roughly a third of all container vessel capacity serving U.S. commerce) with tens of thousands of loaded containers aboard, and 3) clarity

on what the non-validated C-TPAT supply chains would need to do to become acceptable.

- The text on page 87-88 goes on to discuss “Commodity Needs” and “commodity priorities”. We fully understand that energy supplies, for example, might need to take priority over other types of cargo. Military cargoes might be another example of a higher priority type of cargo warranting different treatment. We also understand that validated C-TPAT importers might receive more expeditious release of their cargo. We strongly urge DHS, however, to avoid trying to distinguish between commercial priorities amongst the many thousands of containers of cargo on a ship or in a port. Only in highly unusual situations should the government try to determine how to address competing requests for expedited release from the many different commercial interests involved in containerized shipments based on the relative “importance” of their cargo. The most expeditious handling of these cargoes is likely to result from allowing the industry to work out the most expeditious handling and onward transportation of such cargoes.
- Page 87, line 31: Insert “ocean carriers” after “TSA Federal Security Director”. It is the ocean carriers that manage much of the logistics, coordinate with truckers and rail service providers, etc.

### **Vessel Prioritization (page 88)**

The text under this section of the report describes existing tools to assess vessel security risk and regulatory compliance, but provides little insight into how vessel prioritization in the event of a crisis would be considered. The terms of Section 202(b) of the SAFE Port Act are similarly unhelpful.

For example, having an “approved security plan” or a valid international ship security certificate is regulatory requirement for all vessels above 300 tons trading internationally, and provides no meaningful basis for vessel prioritization. The vast majority of vessels approaching U.S. ports are highly likely to have a good “history of compliance with safety and security regulations”, an “approved security plan” and no identified crew concerns. (page 88) It would thus appear that all such vessels would be treated equally, which would be logical.

Several aspects of Figure 10 appearing on page 89, however, warrant comment. First, DHS obviously knows that possession of a TWIC will be of very limited utility in this regard, as TWICs for seagoing personnel are only to be issued to U.S. seafarers, and less than 3% of U.S. maritime commerce is handled by U.S.-flag ships using U.S. seafarers.

Second, the C-TPAT cargo questions and considerations may not be applicable to the non-liner shipping portion of the industry.

Third, the C-TPAT and cargo considerations included in Figure 10, when applied to containerized cargo vessels, confusingly appear to combine vessel prioritization with cargo prioritization. For containerized cargo, Figure 10 also poses questions about whether containerized cargo is part of a validated C-TPAT participant's supply chain and whether it is somehow highly urgent cargo. We understand that DHS may give validated C-TPAT importers and essential commodities preference for Customs release from a U.S. port; however, container ships will contain a wide mixture of varying types of C-TPAT cargo (e.g., Tiers I, II, III, validated/non-validated), non-C-TPAT cargo, and cargoes with varying levels of "necessity", and they must be allowed to discharge all their scheduled container loads, if they are to have any hope of maintaining any semblance of commercial efficiency or maintaining export transportation services. Accordingly, it would be problematic if container *vessel* prioritization or permitted vessel/stevedoring operations were affected by such C-TPAT questions.

### **“Information Sharing and Communication” Section (pages 90-92)**

The difficulty with this section of the Strategy is that, while it recognizes the importance of information sharing and communication, it does not identify who has the responsibility within the government for such communication functions. This is a major point that needs to be addressed as a ‘plan’ requires the clear assignment of responsibility.

The Strategy on page 91 seems to identify Area Maritime Security Committees “as the primary means to communicate with the private sector” (p.91). We are certain that AMSCs could play an important role in communication, but we question whether this description is adequate, particularly when implementing the directives of a joint command, and when the government needs to speak with a consistent, single voice in a time of crisis. AMSCs by their nature are local organizations and not suited for national-level communication. We also question whether AMSCs have been informed that this would be their role, and whether adequate planning and resources have been assigned, or whether most AMSCs have undertaken sufficient drills to perform this task.

During the preliminary discussions about the Maritime Sector Coordinating Council (MSCC) information sharing and communication in the aftermath of an incident was also identified as a potential function of the MSCC. This needs to be resolved.

A number of information elements that were included in COAC's preliminary comments were excluded from the draft and should be included, namely: the MARSEC levels at all effected ports and the wait times at border crossings.

### **“Performance Measures” Section (pages 92-94)**

This section of the document reiterates the identity of existing DHS programs. It does not provide “performance measures” to assess how these programs are performing, nor does it identify any gaps in existing capabilities or how any of the programs should or will be improved. It also does not identify any real incentives (benefits) for voluntary private sector measures.

For example, as noted earlier, any discussion of “performance measures” relating the Automated Targeting Systems should logically address the Secure Freight Initiative and CBP’s “10 plus 2” initiative and how they fit into a plan to improve performance.

For example, the document on page 95 discusses the WCO SAFE Framework, but does not address what DHS believes the standards and implementation or enforcement requirements will need to occur for “mutual recognition” of AEO programs to occur.

For example, the document on page 95 refers to the fact that the ISO has developed a set of standards for supply chain security, but fails to state in this Strategy document what role, if any, the U.S. government has identified for the ISO standards, and specifically whether it has any intention to “recognize” or “adopt” these standards.

## **“Implementation Schedule, Priorities, and Milestones” Section**

General: While the legislative language provides three years before the final *Strategy to Enhance International Supply Chain Security* to be delivered to Congress, what does DHS expect to change in the interim and why cant it be delivered sooner?

Failure to include the Secure Freight Initiative and the “10 plus 2” initiative in this section (pages 95-96) is an omission that should be addressed.

---

## **Typographical Errors**

1. Page 6, line 20: “cargos” should be “cargo’s”.
2. Page 6 line 22: “it’s” should be “its”.
3. Page 22, line 33” “four” should be “three”
4. Page 76, line 35, “it’s” should be “its”.
5. Page 92 line 3: “port of facility” should read “port or facility”