

# Commercial Operations Advisory Committee

## Comments On

### National Strategy for Global Supply Chain Security Development Efforts

#### Background

COAC has been requested to provide feedback as part of its contribution to the Administration's efforts to develop its National Strategy for Global Supply Chain Security.

DHS indicates that "The Administration envisions a global supply chain system that:

- Is secure against threats that could cause large-scale death, destruction and/or disruption of the US economy;
- Is resilient in response to large-scale events; and
- Maintains the expeditious flow of lawful commerce."

Global Supply Chain Security (GSCS) scope includes:

- Efforts directly supporting Global Supply Chain (GSC) security, resilience and expeditious trade flow;
- All modes of commercial transport on conveyances across air, land and sea;
- All potential modes in the legitimate supply chain where commercial shipments are handled; and
- GSC from points of origin or manufacture to final destination
  - Import and export

Given the above, COAC was asked to:

1. Review *Strategy to Enhance International Supply Chain Security* ("Strategy") July 2007;
2. Respond to questions directed by the SAFE Port Act;
3. Respond to additional questions posed by DHS; and
4. Identify other questions to be considered by DHS.

### **Summary of some key COAC findings and recommendations discussed in this report**

- COAC's comments on the Strategy made in 2007 are still valid.
- The Strategy should focus more attention on air and surface transportation.
- Timely sharing of actionable intelligence among government agencies and the private sector should be a strategic priority.
- Increasing the number of large and small scale security exercises is key to improving and measuring resiliency.
- Collaboration on the U.S. Customs-Trade Partnership Against Terrorism (C-TPAT) minimum security criteria should continue through this subcommittee and other industry organizations to help ensure this partnership program remains efficient and reflects the ever-changing threats.
- The mandate for 100% scanning of maritime containers and the 100% screening of air cargo on passenger aircraft contained within *the 9/11 Commission Recommendations Act* should be re-evaluated in favor of risk-based measures that target high-risk shipments for physical inspections. Further the requirement to scan 100% of maritime containers prior to vessel load should be repealed.
- Coordinating supply chain security protocols both inside and outside of the Department should be a priority.
- 19CFR103.31 should be modified to protect certain sensitive information from being released to the public too early creating security vulnerabilities and negating effectiveness of some C-TPAT minimum security criteria.
- Container-centric technology solutions present little hope of reducing the risk of terrorists using containers as Weapons of Mass Destruction (WMD) delivery tools.

Part 1

**Commercial Operations Advisory Committee (“COAC”)**

**Comments On**

**Strategy to Enhance International Supply Chain Security**

(July 2007 document)

**General**

As the Strategy indicates, “...trade may be viewed as entering or departing the United States via one of three modalities: surface transportation (rail or vehicular), air transportation, or the maritime domain.” The Strategy also indicates that it is DHS policy that a terrorist incident will not automatically result in a shutdown of the Nation’s air, land, or seaports. The document goes on to indicate that elevated security activities triggered by modality specific threat conditions (e.g., Maritime Security (MARSEC) levels in the maritime domain, or an increase in the Homeland Security Advisory System (HSAS) for a transportation segment such as aviation) will be based on facts on the ground, available intelligence and associated risk.

COAC supports this approach and realizes that in order to succeed, both the public and private sector need to collaborate closely to ensure that the security of our Nation, including the health of our economy, is protected. COAC realizes that this is no small task and understands that politicians will be under pressure to take draconian actions that might, in the end, cause more harm to our economy than the actual event.

As COAC’s comments indicated in 2007, the Strategy is not actionable. It should be a blue print that can be referred to in both planning and execution. A strategy should set a concise number of core priorities that programs, initiatives, and operating procedures strive to attain. Development and implementation of programs, initiatives, and operating procedures should be driven by the strategy, not vice versa.

More generally, DHS should read the comments COAC provided to the draft of the existing report in 2007. The vast majority of those comments are still valid as related to the maritime environment.

Although the Strategy correctly highlights the importance of the three modalities, the overriding theme of the document is weighted toward maritime. Consequently, little is written about either the air or surface modes. COAC believes this is an important gap that needs to be addressed.

When the Strategy references highway security elements, the focus is on the domestic portion of the truck transport sector, not the border/import sector. International supply chain security starts at the final loading point in the shipping country for highway mode. There is no reference to the Free and Secure Transport (FAST) program or C-TPAT for highway carriers. There is no mention of details for getting goods from port to domestic customers via truck when vessels have to be rerouted from a US port to a foreign port such as Vancouver, Canada. This will require truck carriers that have proven safety and security import practices in place. The “Protocols and

Factors for Prioritization of Resumption of Trade” is almost void of truck considerations. This is a critical gap as the risk of port closures along the northern and southern borders due to both terrorism and natural disasters is extremely high and will require effective trade resumption efforts.

In the air mode, several examples help highlight the importance of the Strategy taking a multi-modal approach:

- In the immediate aftermath of Hurricane Katrina and the 2004 Tsunami, US commercial airlines experienced shortages of jet fuel in parts of the country. Local and regional aircraft fuel availability could be a critical component towards maintaining continuity of the air cargo supply chain.
- Another example is the 2010 E15 volcano ash which caused the cancellation of flights globally, but particularly in the European Union (EU). This caused the backup and ultimately closure of processing plants (loss of jobs) and the destruction of perishables such as fresh fruits and flowers destined for other areas of the world.
- During a pandemic or other global emergency, the delivery of vaccines and medications would need to be by air. This would require prioritization decisions involving the different modes. An effective strategic framework could help speed up the decision-making process helping to determine modal and cargo priorities.

In the air mode, the Strategy lacks clear guidelines as to who is responsible for conducting physical cargo screening. TSA is responsible for screening air cargo in the US at small airports with exceptions permitted based on individual TSA airport directors. At large airports in the U.S., airlines (not TSA) are responsible for screening air cargo. Exceptions at large airports are sometimes made when TSA canines are available. Overseas, the Strategy needs to address protocols that recognize the security value when “trusted countries” perform physical air cargo screening. Finally, the private sector and our trading partners require improved guidelines as to which screening methods are “approved”. Without clearer screening guidelines it is difficult for the various parties to allocate both human and capital resources.

### **Detailed Comments**

The following are specific comments and observations made related to pages 98 to 102 of the Strategy:

Page 98:

- The Strategy states that a response to an incident should not unreasonably hinder the free flow of trade. It goes on to say, “To accomplish this objective, it is critical that pre-existing data and screening systems include the necessary information to “fully screen cargo”, including cargo already in transit and requiring additional risk-based analysis in a post-incident environment.” What additional post-incident changes to targeting are under consideration? The term “fully screen cargo” should be defined to ensure common

understanding and alignment of the Federal government's expectation and with available resources and security capabilities. To be effective, security measures must be risk-based and sustainable for extended periods.

- DHS should define “screening” by the definition used in Section 2(13) of the SAFE Port Act: SCREENING.—The term “screening” means a visual or automated review of information about goods, including manifest or entry documentation accompanying a shipment being imported into the United States, to determine the presence of misdeclared, restricted, or prohibited items and assess the level of threat posed by such cargo.
- While maritime trade is very important, it does not represent “95% of the cargo tonnage that comes to the United States.” This statement omits NAFTA trade which represents a significant percentage of US imports.
- The Strategy document states that “...the USCG and CBP ...are responsible for the development and execution of tactical plans intended to foster business continuations and provide for elevated security conditions. Such tactical plans will be or have been developed with input of the trade community.” We are not aware of such plans or the trade community input process. If this refers to planning that may have been done within the various Area Maritime Security Committees (AMSCs), then such a clarification would be warranted. Also note that industry representation in the AMSCs varies considerably by area. Plans in which AMSCs Marine Transport System Recovery Unit (MTSRU) have been involved are not tactical. They also are based on the same prioritizations that are listed in the Strategy and need to be expanded to include all modalities.
- Setting local priorities of cargo movement is complex and will depend on the circumstances. Different modes will face different and changing challenges. For example, what is pertinent and somewhat unique to the air mode is whether the cargo is perishable, contains medical supplies, whether the aircraft transporting the cargo is also transporting high-value passengers such as medical response teams, etc. Therefore it is important to understand what factors CBP would consider in deploying and/or re-allocating cargo inspectors between air, land and sea ports of entry to accomplish trade resumption.

Page 98-99:

- The Strategy states that “DHS components and agencies with trade-related missions...are responsible for the development and execution of tactical plans:”. With some exceptions primarily in the maritime mode, Federal government agencies should not be leading tactical planning and operations. Rather, they should set strategies and develop programs and commit resources to provide capabilities that local/regional agencies private sector entities lack. More extensive integration and coordination with the private sector in developing tactical plans is recommended.

- Discussion of “Incident Commander or Unified Command” imparts a Federal focus to what will largely be a local/regional and private sector challenge. The structure discussed, requiring coordination of efforts of multiple senior Federal officials, would necessitate designation of a Federal executive as “Incident Commander.” The designation of the Federal “Incident Commander” should be required to be made in advance of any incident or threat as a standing appointment to the responsibilities – to ensure the most ample opportunities for advanced coordination with all affected stakeholders, both in government and the private sector. It is most important for all to understand who acts, when and where.
- The existing Strategy document, in discussing “the security status of the vessel,” notes that one factor that will be relevant is: “Is any of the cargo on the vessel suspect, or deemed “high risk” by CBP’s ATS...” The industry has worked closely with CBP to improve ATS by implementation of the Importer Security Filing (“10 plus 2”) regulations. If there is high risk cargo that would affect DHS’ decision to allow a vessel to enter a US port, CBP should issue “Do Not Load” messages prior to vessel lading. That is the purpose of providing this data before vessel loading. The only exceptions we can see to this would be where new intelligence was received by DHS after vessel sailing. The Vessel Prioritization on pages 101-102 is a subset of the “security status of the vessel” on page 99 and should be cross referenced.

When considering the prioritization of containerized cargo, DHS should in particular reconsider what COAC recommended in 2007, namely:

“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 interest 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.”

- One of the bullets asks: Is there CBP resource availability to clear cargo or commodities once landed? This is a key issue for air, as well as USDA/FDA due to the volumes of perishables transported by air requiring other agency clearance.

Page 100:

- One of the bullets identifies the need for the vessel to move cargo out of the port (e.g., grain shipments needed to be shipped in order to avoid shutting down other transportation modes such as railways). Similarly, this is a significant issue for airports. The FAA needs to be fully engaged from both ATC and airspace standpoints. Likewise, airports need to be involved (locally if not nationally) due to gate availability and aircraft parking capacity standpoints.
- The Strategy notes: “Complicating the assessment of cargo priorities is the issue of non-homogenous cargoes, where vessels are not loaded with strictly C-TPAT participant’s containers.” This problem is also equally complicating in the air mode and, perhaps to a lesser extent, in the land mode.
- The USG should establish appropriate criteria for identifying high-risk cargo, and subject to priority cargo as identified nationally, and to the extent practicable, facilitate the movement of low-risk cargo. Cargoes from C-TPAT members or AEO members from supply chain security programs that have received Mutual Recognition generally should be considered to be lower risk than comparable non-C-TPAT /non-AEO member cargo.

Page 100-101:

- The Strategy discusses segregation of “high priority cargo” in transit. This proposed role for CBP to focus on separating “priority goods” from other categories within shipments and containers is impractical.

Part 2

## Commercial Operations Advisory Committee

### Response to Questions Directed by the SAFE Port Act

What changes to protocols would the COAC envision and/or advise?

The Department of Energy (“DOE”) and CBP radiation scanning results should be integrated into CBP’s risk scoring just as C-TPAT status is incorporated.

Organizations including key private sector subject matter experts, should be identified in advance and mustered together after a catastrophic event for consultation, helping ensure effective mitigation responses are employed.

DHS should take the lead in designing a path forward in developing harmonized security protocols (i.e., mutual recognition) among various US agencies both inside and outside the Department.

If protocols expand to all modes, what differences would the COAC envision?

Recognizing that transportation modes have differing priorities and characteristics, the protocols should remain as similar as practicable. This would provide industry a clear understanding of the protocols and expected responses by the government. Deviations may cause confusion among the trade and industry partners.

What information would industry desire to have in order to develop mitigation plans/business continuity plans?

In advance of an incident?

The critical information would be a complete description of planned government responses to various incidents. While it is impossible to know the response for every incident that could impact a single port or area, it is important to understand the planned steps and procedures for government responses. This information will be critical as industry develops their disaster recovery and business continuity plans.

DHS will have to address how the government will communicate with industry, to whom and what types of incidents will trigger these emergency communication channels. Similarly, DHS will have to develop means in which industry can inform the government of major disruptions.

#### Post incident?

One of the hardest things to manage during an event are Points of Contact (POCs) (both government and industry) so the key will be to ensure primary and backup POCs on both the government and industry sides to greatest extent possible.

The most critical information is the operational status of the affected port(s) and the plan that the government has put in place to keep trade flowing. What is the status of strategic ports around the nation? What is the capacity of these ports to handle trade diversions? What will be the process for clearing cargo originally destined for the affected port? How will cargo be prioritized?

Part 3  
**Commercial Operations Advisory Committee**

**Response to Additional Questions Posed by DHS**

What are the key concerns regarding threats/vulnerabilities in the global supply chain?

This is a difficult question for the private sector to competently address without more information from the public sector. What does the national intelligence estimate indicate regarding the top supply chain threats? What are the associated risks? While industry does have some information, there is other information that the government should share to help industry bolster their supply chain security efforts.

While not having complete information, as discussed above, many in COAC believe one vulnerability that warrants additional attention is the role in the supply chain played by intermediaries who handle the material from sources, manufacturing, and suppliers (more often trucking and smaller regional airlines).

A concern for air cargo is that the 100% physical screening requirement at the individual carton level for large pallets and containers on passenger flights can actually result in the dilution of screening effectiveness. The analogy is that right now we are looking for a needle in a thousand haystacks using only our hands and eyes. We have a better chance of finding that needle if we can reduce the number of haystacks using risk assessment algorithms.

How well does the US reduce these threats/vulnerabilities?

The real question should focus on how does the USG reduce associated risks? The threats will not likely go away. Our collective task should be in developing countermeasures designed to mitigate risks.

In a general sense from a maritime perspective, the USG has done a good job in taking a risk-based approach by implementing initiatives such as the Container Security Initiative (CSI), C-TPAT, Automated Targeting System (ATS), the 24-hour advance manifest rule, radiation scanning at the port of entry and most recently the Importer Security Filing (ISF or “10 plus 2”). DHS and CBP have also successfully resisted political pressure in implementing 100% scanning prior to vessel load and in mandating Conveyance Security Devices (CSDs) - costly efforts that would have only created a false sense of security.

For the all-cargo freighter air carriers, USG has also done a fairly good job identifying the threats and implementing regulations to mitigate vulnerabilities. This enables freighter aircraft operators to use screening methods appropriate to the threat.

For passenger airlines, as a result of a Congressional legislative mandate in reaction to the 9/11 Commission, the USG has implemented commercially strangling 100% physical

screening requirements for cargo on passenger flights that are commensurate with baggage screening requirements. Transportation Security Administration (TSA) regulations require screening to occur at the smallest carton level as packaged by the shipper due to a USG interpretation that equates “commensurate” in the passenger baggage world with “smallest piece level” in the cargo world. Many security experts believe that 100% physical screening is less effective at reducing vulnerabilities than targeted risk assessment and screening of cargo posing a higher threat; the current 100% air cargo requirement is inconsistent with DHS’ risk assessment and targeting regimes.

What are some examples of industry best practices in reducing threats/vulnerabilities?  
How might the USG better leverage private sector interest and efforts to secure the global supply chain?

The work done through C-TPAT is a good example. However, the USG needs to leverage C-TPAT and other AEO security programs by encouraging them to expand to other domestic and international constituents (e.g., foreign manufacturers located outside Mexico or Canada) that fall outside their normal scope/jurisdiction. For example, developing a strategy to better incorporate trucking within the partnership programs would be an effort which might materially improve supply chain security.

While not a government partnership, the Transported Asset Protection Association (TAPA) is another example of the industry putting programs into place to improve supply chain security.

What are the different threats/vulnerabilities between and among modes of transportation and what are opportunities for improvement?

More consideration needs to be given to truck chain-of-custody issues as virtually all products that are not bulk loaded have to get to an airport, seaport or rail terminal on a truck. A strategy designed to mitigate these truck related vulnerabilities would be one focused on securing international cooperation from like-minded countries.

What assumptions that currently inform our policies and programs may be incorrect or dated?

Scope needs broadening to incorporate additional industry issues such as food, product safety and pharmaceuticals.

Are there opportunities for legislative/regulatory improvement?

The Strategy should set legislative priorities for each mode (air, maritime and surface).

The Strategy should attempt to develop a structure to reduce the risk of ill-advised reactions following a major event (e.g., 100% inspection of all maritime containers destined to the US).

Terminology with common definitions provided by a recognized authority such as the Data Model published by the World Customs Organization (WCO) should be adopted for risk assessment and targeting data elements (e.g., ultimate consignee, scanning, screening, etc. ) to help facilitate accuracy, consistency and management of trade and targeting data globally.

Similarly, clear definitions of “screening” and “scanning” are needed to help eliminate confusion whether the reference is made by USG (e.g. TSA, CBP or DHS personnel) or private sector personnel.

On a more granular level, one of the biggest issues that impacts both operational security and political friction is the 100% scanning mandate. The SAFE Port Act charges DHS for example, to work with the private sector and foreign governments to develop effective processes and to determine the probability of detection regarding 100% scanning. The SAFE Port Act also charges DHS with developing a set of “lessons learned” findings. Unfortunately the *Implementing the 9/11 Commission Recommendations Act*, mandating 100% scanning was passed before the SAFE Port Act pilots were completed. The 100% scanning mandate failed to account for the operational and political hurdles that needed to be addressed and evoked a strong negative response from many key US trading partners. Therefore COAC recommends that the 100% scanning mandate be repealed. Similarly, the 100% physical screening requirement in air mode should be eliminated in favor of targeted risk-based analysis and leveraging of CBP and TSA intelligence to identify higher-risk shipments requiring a physical screening process.

Another issue that adversely impacts security is public access of shipment information. More specifically 19CFR103.31 requires, *inter alia*, that the manifest data acquired from the Automated Manifest System (AMS) is made available to the public on CD-ROMs. This regulation requires that CD-ROMs be compiled daily and contain all manifest transactions within the last 24 hour period. Some of the required data elements include vessel name, vessel voyage, port of unloading, estimated arrival date, bill of lading number, foreign port of lading, description of goods, container number and seal number. As a consequence of this regulation vulnerabilities are created that would otherwise not exist. For example, in most major ports/marine terminals, no documentation is required for a truck driver to take delivery of a container. Only knowledge of the container number and B/L number is usually required. For example, C-TPAT requires the use of high security seals and mandates specific seal control procedures. 19CFR103.31 negates any security benefit of these C-TPAT requirements as the seal number is a data element made available through this regulation. Therefore COAC recommends that 19CFR103.31 be modified to protect this sensitive information.

How might we better measure and account for efforts to increase security?

From the CBP/DHS perspective, more quantitative and qualitative reporting could help measure and account for security efforts. For example, publishing statistics about how existing security programs are working would be helpful. What types of successes have resulted from the collection of ISF data? Feedback to the private sector on successes could assist in providing justification to senior management for maintaining or increasing investment in more expensive or effective security solutions.

DHS should establish a reporting conduit to assist industry in identifying security practices and protocols in a format that is easy to use while still maintaining confidentiality.

Incorporating similar methodologies employed by the Overseas Security Advisory Council (OSAC) is worth consideration.

How might we better measure and account for efforts to increase our collective operational resiliency?

The primary and most effective tool to better measure and account for our collective operational resiliency is through frequent security exercises – both live and tabletop in all key geographic locations. These exercises are critical to ensure all agencies involved know their roles if and when an incident occurs. It is also important to include members of the trade as part of the exercise so the government and the trade can understand how each will react through a series of lessons learned sessions.

Examples of areas that can be addressed in these exercises include determining chain of command and who is in charge; evaluating the communication with industry; and measuring the pace of response including the ability to make on-the-ground operational decisions (e.g., does a CBP or TSA inspector let the passengers off this plane?).

How are trade partnership programs enhancing global supply chain security or what additional role could they play?

There is a positive impact on supply chain security; however, areas could be strengthened which address certain vendors and providers in the global supply chain (e.g., trucking).

Trade partnership programs could play a much more robust role if there was an informal international forum available to allow for the exchange of ideas to help facilitate work being done at the United Nations (UN) level (e.g., International Civil Aviation Organization (ICAO), the World Customs Organization (WCO) (SAFE Framework of Standards) and the World Trade Organization (WTO) (expansion beyond customs considerations). A strategy incorporating private sector participation would be helpful in this regard.

Specifically, with regard to C-TPAT, threat/intelligence information sharing needs to be improved. The trade is left to determine threats to the supply chain with little assistance from the USG. Individual companies have independent programs to determine threats/vulnerabilities in order to focus resources to meet the criteria set forth by USG (C-TPAT in this case). The USG could streamline the process and help create a proper focus on areas where the USG sees threats to the supply chain by sharing appropriate information.

Collaboration on C-TPAT minimum security criteria (reviews, modifications, etc.) should be increased through this subcommittee to help ensure consistencies among the various modalities and that C-TPAT remains effective, efficient and reflects requirements appropriate with the ever-changing supply chain environment.

To encourage consistency between and in conjunction with the USG Inter-Agency Cooperation Workgroup, collaboration with the trade should be increased through this subcommittee to facilitate recognition of "trusted trader" status, use of related supply chain security elements from one agency to satisfy supply chain security elements of other

agencies, and use of the C-TPAT Security Link Web Portal to allow companies to communicate with other agencies.

What additional information sharing opportunities should be considered to enhance global supply chain security?

Timely sharing of accurate, actionable intelligence, both classified and unclassified, among governmental agencies and with private sector stakeholders should be a strategic security priority. The strategy should tackle the problem of over-classification of information; excessive use of the designation “Law Enforcement Sensitive” or internal strictures on information sharing imposed by senior officials in the Federal government. Sustainable means must then be implemented through targeted programs and operating procedures to ensure the consistent dissemination of relevant security information during normal operations, periods of heightened threat and during and following security incidents.

From a maritime (liner shipping and marine terminal) perspective, local information sharing is fairly effective. The Federal Bureau of Investigation (FBI), US Coast Guard (USCG) and Office of Naval Intelligence (ONI) do a good job of sharing local information. Unfortunately, the sharing of internationally-centric information that could impact the global supply chain is challenging and needs more attention. Examples of information a liner shipping company could use include notification that: (a) risks of stowaways have increased dramatically at a location that, in the past, did not represent a high risk; (b) drug trafficking has shifted to locations not normally thought of as high risk areas; and (c) notification that suspicious packages were found on multiple vessels operated by different companies at the same port. In all three examples, liner shipping could shift resources, take additional counter-measures and/or mitigate risks given the information provided.

The USG should better utilize the private sector as a “force multiplier” in protecting the supply chain. For example, the USG should encourage the reporting of suspicious activity to the intelligence community. Unfortunately, the conduit for reporting security information by the private sector is unclear, fragmented and typically uni-directional. Enhanced feedback to the reporting entities would benefit industry in understanding the threat posture and what impact our efforts are having in mitigating that threat. By way of example, we would like to receive direct feedback on suspicious activity reported (e.g., reported incident was followed up and resulted in a person of interest being contacted). This would confirm that efforts were worthwhile.

Some form of analysis indicating the value of Closed Circuit Televisions (CCTVs), perimeter detection and other technologies could influence/support future spending decision. For example, knowing the number of documented incidents in which an illicit act was detected via CCTV could help justify the initial investment and on-going maintenance cost.

DHS/CBP should look at the OSAC program run by the State Department which provides invaluable information-sharing opportunities. The trade is able to get critical information about different areas of the world and existing risk factors that apply. DHS/CBP should consider partnering with OSAC in extending its scope to supply chain security. This would

allow DHS/CBP to benefit from OSAC's experience and reduce implementation costs of standing up a separate stand alone system.

The USG should develop a long term strategy that would allow multiple parties to enter shipment information currently required into a common government database. This will speed up and enhance the delivery of important data to be used for targeting analysis, tracking changes (in providers) and identifying anomalies (is the common denominator to all the high-risk cargo a single trucker?). Alternatively, continuing the practice of limiting the input of shipment information to carriers, importers and third party providers demands multiple data handoffs increasing the probability of errors and transmission delays.

What is the state of technology solutions and what role should they play in global supply chain security?

Technology is a critical component of supply chain security, but it should not be perceived as a panacea. Rushing unproven technology into the supply chain will undermine progress made to date, provide a false sense of security and will make the supply chain less secure. Too many people are interested in the "silver bullet" solution to supply chain security through the use of technology. Unfortunately, available and emerging supply chain technology often requires a high degree of human intervention, potentially causing bottlenecks, false positives and delays in the supply chain without a commensurate improvement in security. Successful security will require a continuation of the multi-layered approach that DHS has been following to date.

Most container-centric technology solutions that companies are encouraged to use present many practical problems and little hope of reducing the risk of terrorists using containers as Weapons of Mass Destruction (WMD) delivery tools. The amount of money spent, for example, on developing the Conveyance Security Devices (CSDs) is significant given the security benefits expected (even assuming the most optimistic results). The amount of money spent on the Advanced Conveyance Security Devices (ACSD) is also something to reconsider. Increased engagement with private sector stakeholders would help ensure money is spent more effectively in developing technology solutions.

Bottom-line, the fact that cargo tends to be high volume, non-homogenous, and in many cases environmentally sensitive, reduces the opportunity for an efficient and cost effective over-arching solution. Technology along with people, process and training must be incorporated into the global supply chain from origin to delivery.

Part 4  
**Commercial Operations Advisory Committee**

**Additional Questions Posed by COAC**

When the DHS *Strategy to Enhance International Supply Chain Security* was initially published, the focus of the document was the prevention of a weapon of mass effect being introduced into the international maritime supply chain. Since that time, supply chain security has not only improved, but has expanded beyond just the prevention of the “bomb in a box.” In addition to looking at other modes of transportation (i.e., air, rail and truck), should the strategy also look at the issue of import health and safety? The Import Safety Working Group established under former President George W. Bush put together a “strategic framework for continual improvement in import safety.” Should that framework and accompanying action plan be considered as part of the larger DHS strategy?

How does the USG measure risk and how are these metrics used to allocate limited resources across the supply chain?

How quickly can risk be re-calibrated and counter measures identified?

What protocols can be put in place which may or may not require regulatory change to allow the USG to consult with the private sector early in the development of new legislation/regulations?

What protocols can be put in place which may or may not require regulatory change to allow the USG to consult with the private sector after public comments are received?

How will the multi-modal strategy incorporate cohesive USG leadership designed to minimize the sparring amongst agencies that feel they have the authority for a specific transportation mode? This will be critical after a major event that impacts the supply chain where certain conflicting priorities must be managed.

As part of any supply chain logistics system, any nodal pivot point may represent a key vulnerability/choke point that could significantly delay trade resumption. Should the White House directed, interagency effort to develop a National Strategy on Global Supply Chain Security include “critical infrastructures” in the US? Should it address critical infrastructure outside of the US? Should this issue be addressed by the COAC GSCS Subcommittee?

Should CBP create an Export C-TPAT program?

This topic is important for many in the trade, so we have provided some visibility into the COAC recent GSCS discussions on this topic.

Many believe achieving mutual recognition with various Authorized Economic Operator (AEO) programs provides a means by which to help facilitate secure trade. By leveraging the investments made by certified C-TPAT participants and their overseas factories and logistics service providers, the trade community should be able to mitigate the incremental costs of participating in additional AEO programs. Consequently, many in the trade have requested CBP to pursue mutual recognition with our key trading partners.

Because many AEO programs are bi-directional, some believe securing mutual recognition with C-TPAT has proven to be, and will continue to be a challenge for CBP. On the other hand, mutual recognition has already been achieved with five (5) countries (Canada, Japan, Jordan, Korea and New Zealand). While foreign Customs authorities should not use the existence of an export based supply chain security program as a hard and fast requirement to determine eligibility for mutual recognition, it is nonetheless worth further consideration and analysis by CBP and the COAC.

Participation in an export oriented supply chain security program may be a challenge for a large segment of US exporters. Approximately 80% of US maritime exports to Asia are low value goods (e.g., hides, waste paper, liner board, hay, cotton, clay, grain, etc.). International competition is stiff and margins are low for these industries. The additional costs associated with implementing a broad-based security program with required minimum security criteria, that does not take into consideration the specific threats/risks of these supply chains, would likely create a barrier to participation for this cross section of US exporters. Yet, CBP would have to dedicate a portion of their limited resources to the program, regardless of how well received.

However, not all US export cargo and associated supply chains fall in the above low value, low risk category. High technology, high value cargo that is exported via air, and to a lesser extent ocean, or that travels via truck or rail across the northern and/or southern borders may justify expansion of C-TPAT to include exports.

CBP, in collaboration with the trade, should review existing C-TPAT security criteria and ensure that any expanded program continues to allow for flexibility and customization of security plans based on a member's business model. DHS currently bases its efforts on a layered, risk management approach. The individual elements of DHS' policy are built upon risk analysis specific to the risk area covered in the supply chain. We feel this approach:

- is consistent with DHS and CBP's current risk based approach; and
- supports the desire of US importers and exporters to advance mutual recognition. and
- recognizes the special challenges of some US exporters