CSTA

Cargo Shipping Transportation Analysts
8 Floral Lane
St. James, NY 11780
Phone 631-862-1259
Fax 631-862-1443
E-mail RFCaton@csta-intl.com

Response to Air Cargo Security Requirements NPRM

Docket No. TSA-2004 -19515

My Background:

I am a lead air-cargo industry process and procedures analyst with a growing background in security applications. I am also a Transportation Technology Application Integration Engineer. (T.A.I.E.) As a T.A.I.E I review technology developments that have the potential to be used in the transportation industry. There is a tremendous amount of technology available that can be used to enhance the security effort yet is not being considered because government's effort is based on legislative mandates from those unfamiliar with how cargo moves through the supply chain. Toward the end of this response I will briefly outline the Aviation Security Technology Evaluation Center (ASTEC) initiative which represents an aviation industry alternative approach to the security effort against acts of terrorism.

Preface:
Although many within the industry agree that more is needed to address vulnerabilities in air-cargo security, there is a tremendous concern that government is not knowledgeable enough in air cargo industry handling characteristics, hence regulations being put forth represent derivatives of those being applied in passenger security. Reflected in this NPRM is an identified and acknowledged need for better communication between government, airport operators, carriers and IAC's however nowhere within this document is any mention of the problems that have arisen since 9/11 where information dissemination and regulatory interpretation have caused severe problems in applying the existing regulations.

Ex: "Emergency Amendments" (EA's) are prepared in Washington and then given to the Principle Security Inspectors (PSI) or International Principle Security Inspectors (IPSI) for dissemination to carrier headquarters. In the international carrier arena English is a second language and in most cases there has been a difficult time understanding the regulations and implementation required.

Cargo Shipping Transportation Analysts
8 Floral Lane
St. James, NY 11780
Phone 631-862-1259
Fax 631-862-1443
E-mail RFCaton@csta-intl.com

Add to the issue that a carrier that operates into several US cities, each having its own TSA Security Director, stands to interpret the regulations differently at each airport. Therefore inconsistencies cause confusion making the rule interpretation difficult for carriers and other stake holders to implement a standard practice at all its cities.

Another example of regulatory interpretation inconsistencies can be seen here in this NPRM when compared to those EA's published earlier this year.

Ex:
Clarification of comments made in Page 65259 where the description of CBP role "regulates cargo into the United States" doe not provide an accurate description of the CBP role since CBP is also involved with oversight of movement of cargo leaving the United States. And although within the same paragraph reference is made to the "TSA solely responsible security of shipments" does not take into account that the TSA presently does not have the jurisdiction to "Hold" freight while awaiting verification of specific information. As a result they must rely on CBP authorization to Hold cargo that may pose a security risk.

Another questionable reference in the subsequent paragraph where claim is made that there is no CFR for freighter carriers where (Take-off Weight) exceed 45,500 kgs when in fact CFR 1550 was amended to include all cargo carriers not previously identified in parts 1544-1548.

Air-cargo Industry Security:

Although I applaud the ASAC group for their role in regulatory input to mitigate the impact of severe rule changes, we must remember that the majority of stake-holders involved in air-cargo transportation are limited in their understanding of security and therefore may not be aware of alternative technology options. In many instances its Government dictating what they perceive as being necessary for air-cargo security yet government has limited knowledge of the intricacies involved with cargo as it moves within the supply chain. The government agenda is strictly based on security and are not considering if the security methods can be integrated into existing air cargo handling methods, to minimize extra work needed to meet security requirements.

Cargo Shipping Transportation Analysts
8 Floral Lane
St. James, NY 11780
Phone 631-862-1259
Fax 631-862-1443
E-mail RFCaton@csta-intl.com

Throughout the NPRM mention is made for a “Layered Approach” however because of the disparity between DHS understanding of cargo handling and the ASAC limited understanding of security technology, (outside what is being offered by government) the air-cargo security is getting deprived of viable technology that both enhances security with minimal impact on actual flow.

TSA’s “Security Threat Assessment” overlaps CBP C-TPAT Requirements:
CBP and TSA must look at their collective responsibilities to determine what information over-laps and insure that there is no redundancy. It’s quite possible that mandatory C-TPAT is further away that this Final Rule adaptation however since C-TPAT requires the same requirements as the STA, the DHS must now begin to identify then link those areas common in both TSA and CBP.

When considering STA for carriers the majorities of carriers are operating on airports and therefore have their employee background checks as a result of Section 1542 being required by Airport Operators when employees operate in SIDA areas. The TSA must also keep in mind that CBP also requires background check for those carrier employees that work in bonded areas. In most cases carrier all cargo personnel have already been screened by Airport Operator and CBP. Therefore the STA for air-carriers should indicate that carriers not requiring SIDA access under 1542 would require an STA of their staff

In connection with STA the TSA must also establish its Transportation Worker Identification Credential (TWIC) so that others working in a secured environment can easily identify those without authorization to be is a secured area. The STA and TWIC program must work hand in hand in-order to achieve maximum utilization of both.
(See example of TWIC Program identified by the ASTEC initiative)

Note: CBP must modify C-TPAT to allow Air-cargo Warehouses, Ground Handlers and Pick-up and Delivery truckers to participate in the program.

Cargo Shipping Transportation Analysts
8 Floral Lane
St. James, NY 11780
Phone 631-862-1259
Fax 631-862-1443
E-mail RFCaton@csta-intl.com

Air Cargo Security Technology:

The expansion of the “Known Shipper” program must take into consideration the following;
1) Validation of “Known Shippers” should be done by professionals. Many of the “Known Shipper” validations are done by members of IAC’s with little to no security background. Since others using the TSA database must rely on information supplied by an IAC the integrity can be compromised based on the entity validating the “Known Shipper”.

2) Consideration must be given to avoid redundancy between the “Known Shipper” program along with CBP’s Automated Export System (AES). Some of the components of AES allow for more comprehensive information than that of the “Known Shipper” program. Both the “Known Shipper” and AES database (for international shipments) should be integrated to avoid information redundancy.

Alternative technology options to be explored:

One of the things the air-cargo industry faces is that many in politics and who work outside the supply chain, do not understand how cargo moves through the supply chain. Politicians compare passenger and baggage screening to cargo handling however very rarely does anyone without security clearance even get close to an aircraft, when cargo is being loaded. Although the inference of this NPRM reflects that there are carrier employees that require criminal history checks, however under Part 1542 of the TSA regulations requires that those operating in SIDA areas must have an employment background check as well as receiving a criminal history check. The majority of carriers operating at the major airports are already required to have criminal background checks for their employees with warehouse and ramp access.

The big difference between passenger and the cargo concern is;

Passenger Handling;

1) Passengers have direct access to an aircraft
2) Passengers are not required to have a background or criminal history check
3) The have access to carry-on luggage during flight
This makes the passenger handling more susceptible to acts of terrorism.

CSTA
Cargo Shipping Transportation Analysts
8 Floral Lane
St. James, NY 11780
Phone 631-862-1259
Fax 631-862-1443
E-mail RFCaton@csta-intl.com

Cargo Handling:

1) Cargo is handled a minimum of 3 times when delivered directly to the carrier's cargo warehouse. (each time by someone with a criminal history check)
2) As a result of the "Known Shipper" requirement cargo is normally tendered to an IAC before it is even transported to the airport.
3) The average shipment is handled a minimum of 10 times before it gets onto an aircraft, therefore an explosive introduced anywhere in the supply chain would require a detonating device (including a stow-away) in order to complete a terrorist act.

There is technology available that can enhance the detection of detonating device which will not significantly impact cargo flow and represent a low cost solution.

Ex: There have been at least 3 cases since 9/11where stow-aways were believed to make their way onboard to an aircraft. There is simple technology available that can be used to detect movement in a box or crate.
Radarvison for example is used by both Police and Military to detect movement through walls.
Rubblevison is able to detect a heartbeat in 10 feet of rubble. Since both of these products utilize Ultra Wide Band (UWB) Radio frequency technology it is believed that with some medication that they would also detect Cell Phone and Power Source if used as a detonating device. (Many recall that the terrorist bombing in Madrid used cell-phones as detonators)

This is one of the reasons why I recommend support for the ASTEC Initiative so that technologies like UWB can be explored for applicability

Terrorism Training Handled like D/G Training:

Throughout the various parts of this NPRM is reference to terrorism training and especially the need to have those seeking Security Threat Assessments for their employees to obtain this training. The rule calls for stake holders to provide their own security program indicating the terrorism security training employees will receive. However as we all know there are no air-cargo specific terrorism awareness programs that identify in detail what employees need to look for. Instead there are just general outlines of what a program should consist of. The TSA should look to adapt the same kind of Terrorism Training criteria as presently done for the Handling and Transportation of Dangerous Goods.

Cargo Shipping Transportation Analysts
8 Floral Lane
St. James, NY 11780
Phone 631-862-1259
Fax 631-862-1443
E-mail RFCaton@csta-intl.com

The TSA should designate and certify those security companies or educational institutions that offer approved Terrorism Awareness Classes.

Care in Implementation of Security Threat Assessment:

The NPRM is leaving the onus of responsibility to obtain STA criminal background checks (CBC) on those stakeholders requiring to submit an approved TSA security plan. There could be a severe civil liberty violation based on the way the STA-CBC is outlined in the NPRM.
Ex:
The 3 forms of employer notification may be deemed a civil liberties violation in the event employee termination or employment is blocked as a result of employer receiving denial information from the TSA. This would be especially detrimental if an employee has worked for an IAC better than 10 years, requires a criminal history check and then denied as a result of TSA intelligence profile. Care must be used to avoid backlash of litigation in the event an employee is denied STA authorization.

Note: The TWIC database proposal which is part of the ASTEC Initiative would allow flagging and monitoring of those STA-CBC workers where their criminal history check identified questionable activity. In any case it’s best that the STA-CBC and TWIC program be administered by either Federal or Local government to avoid employer litigation.

IAC Screening of Cargo:

This would require better communication between IAC and Carrier and a mechanism to identify that an IAC has the ability to screen cargo and then also a method for the carrier to identify that a shipment has been screened via the IAC. The exact details would need to be ironed out.

Cargo Shipping Transportation Analysts
8 Floral Lane
St. James, NY 11780
Phone 631-862-1259
Fax 631-862-1443
E-mail RFCaton@csta-intl.com

Other Recommendations:

1) Suggest that a higher emphasis is placed on screening of Unknown Shipper cargo.

2) Presently the TSA regulations and the dissemination of Sensitive Security Information (SSI) is entity specific.
Ex: Part 1542 Airport Operators get SD and EA specific to changes the TSA makes to these rules. Part 1544/1546/1550 carriers are handed requirements based on the airport operators' interpretation of the Part 1542 SD. Since carriers are not privy to the SSI provided to the Airport Operator, the SD interpretation is subject to the individual interpretation of the Airport Operator at a given airport.

The big concern is that information integrity is being jeopardized because the communication methods are outdated. One person, telling another person, telling another person, represents the worst method to disseminate sensitive security information. Like the children's "Telephone Game" by the time the information reaches the end of the line, the details are skewed and no longer represent the primary purpose. The TSA must look to adapt an information sharing method that allows stakeholders to get first hand information so that there is no confusion as to what the actual mandates will be.

3) The TSA must also be open to review and consider security alternatives posed by stakeholders.
Ex: Some all cargo carriers went ahead and decided to place Hardened Cockpit Doors in their all cargo aircraft. The principle of doing this for passenger aircraft was to avoid someone rushing into the cockpit and taking over the aircraft. Although even in this NPRM the taking over an all cargo aircraft is a concern, however no consideration is given to carriers who went above the minimal requirements and secured the cockpit doors.
The adage that "There is more than one way to skin a cat" can also be applied to air cargo security.

Summary: Although this NPRM reflects recommended changes, careful planning and review is required to insure that the regulations