FIATA

Schaffhauserstrasse 104, POB 364, CH-8152 Glattbrugg, Switzerland
Tel. +41 43) 211 65 00, Fax +41 (43) 211 6 65
E-Mail sangaletti@fiata.com, Internet http://www.fiata.com

DIRECTOR GENERAL

Doc. 30/255
2005-01-24

E only

To	:	all National Association Members of FIATA
Copy	:	Presidency of FIATA Extended Board of FIATA
From	:	Marco A Sangaletti, Director General FIATA Secretariat
Re	:	Summary of security requirements

Our National Association member from Germany (Deutsche Speditions- und Logistikverband e.V. DSLV) has published an excellent document “New security requirements for freight forwarders and logistics operators”. The original has been written in German, and was destined and distributed to the local members of the DSLV.

In view of the fact that this document might of interest to most of our members, we have arranged for a translation into English with DSLV’s permission. We think that the contents of this document would be of some value when a freight forwarder or logistic provider is trying to explain to clients who may be otherwise unaware of the real scope of security policies and systems in place.

We however have to point out that some sentences in the document are purely referring to the situation in Germany, and might not have validity of alien law.

Security

New security requirements for freight forwarders and logistics operators

Published by:
Deutscher Speditions- und Logistikverband e.V. (DSLV)
Weberstraße 77
53113 Bonn
www.spediteure.de

Telephon: (0228) 9 14 40-0
Fax: (0228) 9 14 40-99
Email: info@dslv.spediteure.de

Translation: FIATA Zürich, Schaffhauser Straße 104, CH-8152 Glattbrugg

Version: November 2004

C O N T E N T S

1. Introduction

Following the attacks of September 11th, 2001 in the USA and further attacks in Bali, Tunisia and in Madrid, numerous states and interest groups considered it necessary to establish measures against terrorist attacks not only on passenger services but also on cargo transports. The reason for this is that it is envisaged that means of transport constitute targets as well as potential weapons through attacks and manipulation of loads.

Primarily, of course, internal security is a matter for government agencies but it is unquestionably also a duty for private enterprise to make a contribution towards protection against threats. The freight forwarding industry is aware of this and acts accordingly. Although the subject of security is given top priority, there will never be absolute security. Therefore, one should not expect too much.

The English language term *"security"* in this context covers all measures taken to protect against premeditated interference of Third parties with drivers, means of transport and loads with the intention of misuse, abduction or theft. This should be distinguished from the "classical" transport *"safety"*. Its aim is primarily the protection from risks inherent in the act of transportation.

Numerous security measures and –standards are currently being developed partly for world-wide use, partly regionally limited without any co-ordination, by various initiators, with varying interests in mind and different protection aims, and incorporated into international or national legislation or established as industry standards or become quasi-binding through customer requirements. Whilst in the past the airfreight and sea freight sectors had been the subject of increased security measures, the focus is increasingly shifting to the entire logistics chain. Also the surface-based transport means: road rail and inland waterways and the infrastructures used by them (routes, transhipment points, terminals and ports) will be subjects of risks assessments with regard to protection against terrorist activities. Especially at international level there is a lack of co-ordination. Synergies are usually not taken into consideration during the development, resulting in the companies concerned being subjected to differing requirements and synergies can only be achieved to a limited extent.

Industries like Freight forwarding and Logistics that organise and help to design the Supply Chain and the interfaces between Production, Trade, Warehousing, Transport and Consumer, very often have to consider the security requirements of several security systems simultaneously. Here it is important to ascertain first whether and to which extent one's own company is affected by the various measures. Wherever possible interfaces with other regulations and industry standards (Dangerous goods regulations, security of installations, SQAS) should be used. Security measures ought to be an integral part of existing safety and quality management systems in every company.

This paper provides an overview of individual security requirements relevant to freight forwarders as well as a preview of initiatives that may be expected. Detailed information regarding the individual initiatives may be obtained from the cited sources or from the relevant specialists of the DSLV.

Bonn, November 2004

2. Existing or already passed legislative and other requirements regarding logistics security

2.1 Container Security Initiative (CSI)

The USA want to minimise the specific danger potential inherent in container transport / to which container shipments are subjected with the *Container Security Initiative (CSI)*. For this reason US Customs officials are deployed in the world's most important shipping ports to carry out risk analyses and spot checks on containers before they are loaded onto US-bound vessels. Since these checks take place on the territory of autonomous states, individual agreements with the countries concerned were reached. Germany signed such agreement already in August 2002. If a container is identified as bearing a high risk, German Customs officials check it, possibly together with US Customs officials in order to coordinate the next steps and to decide how the container should be handled upon arrival in the USA.

The Container Security Initiative consists of four core elements:

1. Security criteria to identify containers with a high risk potential;
2. Pre-Screening of containers, before they reach US ports;
3. Use of technology for the screening of containers with a high risk potential;
4. Development and use of "smart" containers.

Although CSI is primarily intended for Customs authorities it has repercussions for the activities of freight forwarders shipping containers. In order to make CSI really efficient the *24-hours Manifest regulation* has been developed.

Sources: ***www.customs.gov*** *(Quicklinks)*

2.2 24-hours Manifest regulation for sea freight

The freight forwarder's workload for the handling of US-bound consignments – and increasingly also for other destinations – has grown considerably due to the increased security measures. Most of it is caused by the so-called *24-hours Manifest regulation.*

December 2002 the USA put into force legislation that provides the basis for the electronic pre-advice of cargo data. This makes it obligatory for shipping companies to transmit electronically to the US Customs authorities the shipping manifest 24 hours before loading a vessel with US-bound sea containers *(Automated Manifest System – AMS).* Using their automated control system, the US Customs authority is able to filter out consignments with a high risk potential. This concerns not only consignments destined for the USA, but also transit shipments on board a seagoing vessel that will call on US ports at a later time. Apart from a precise goods description and the first six characters of the HS-Code of the goods, full load containers must also be secured with the so-called "High Security Seals". Consignments not in compliance with these regulations will not be approved for loading by the US Customs.

If the freight forwarder, as Non Vessel Operating Common Carrier (NVOCC) issues his own B/Ls for full containers or for LCL-consignments in a consolidation container, these data of such B/Ls must also be reported to the AMS. If the NVOCC does not report directly to the AMS he may ask the shipping company to do this for him.

The shipping companies generally charge for this service for each NVOCCB/L.

In addition, the freight forwarder needs to coordinate with the various participants in the transport chain in advance precise pickup and delivery times. If a consignment is subjected by the Customs authorities to a detailed examination the freight forwarder must provide additional information and possibly present further documents and participate in a possible x-raying of the container in a container checking station. This extra work far exceeds that for a normal export Customs clearance.

Sources: ***www.customs.gov*** *(Quicklinks)*

2.3 Customs-Trade-Partnership (C-TPAT)

Apart from CSI the USA have initiated the *Customs-Trade Partnership Against Terrorism (C-TPAT)*. This measure, too, is intended by the US Customs to make the transport chain more transparent and more secure and to speed up and intensify the information exchange between shippers, carriers and the relevant government agencies.

C-TPAT is based on bilateral agreements between the US Customs authorities and the individual participants in the economic processes. For the US Customs potential participants are: importers, carriers for deep sea and inland waterways as well as for rail and road transports. Also ship brokers, shipping agents, freight forwarders, companies handling and warehousing goods as well as manufacturers would be involved. These businesses should, on a voluntary basis, compile a comprehensive self-analysis regarding security, based on the guidelines of the US Customs authorities, complete a comprehensive questionnaire, introduce programs for the increase of transport security and to pass the US Customs guidelines on to other participants in the transport chain.

The C-TPAT-guidelines describe procedures for the physical security and personnel security and cover education and training, access controls, manifest procedures and transport security.

C-TPAT-participants may expect privileged clearance in the ports of departure and in the US ports of destination since their consignments will be considered less critical by the security analysis of the US Customs. In an initial run the US Customs particularly asked the large shipping companies to participate in C-TPAT. The shipping companies, in turn, have confronted the container terminals – also in German seaports – with the requirements. It may be assumed that after the shipping companies also all other participants in the transport chain, from the shipper to the port terminal, are to be gradually included in the C-TPAT-System. Thus, all service providers involved in a transport would be concerned, including all sub-contractors right down to the carrier who actually does the physical transportation.

Sources: ***www.customs.gov*** *(Quicklinks)*

2.4 International Ship and Port Facility Security (ISPS)-Code

The International Maritime Organization (IMO) on December 12th, 2002 supplemented the *International Agreement for the protection of human life at sea (SOLAS)* with Safety measures for sea transports. Based on this supplement the International Ship and Port Facility (ISPS)-Code – signed by the IMO signatory states – contains measures to prevent seagoing vessels and port facilities from becoming terrorist targets or seagoing vessels and their cargoes from being misused as carriers of materials or persons for terrorist attacks.

These measures had to be implemented by the signatory states by July 1st, 2004. Non-compliance with this deadline would have been meant a virtual exclusion from international shipping. The USA had declared that ships originating from so-called unsafe ports would be subjected to stricter controls or not be admitted at all. Only recently the US-Coast Guard published a list of 17 countries classified as unsafe. The area of application covers vessels from 500 tons gross tonnage upwards employed in international voyages and such port facilities catering for vessels with a gross tonnage of 500 tons upwards involved in international voyages. Thus, also inland port facilities may be concerned.

The legal implementation was accomplished in Germany with the *Law for amending the international Agreement of 1974 for the protection of human life at sea and the International Code for protection on board ships and in port facilities, supplemented by an implementation regulation for sea transportation*. Since German inland and coastal ports are matters of the relevant federal states, special legislation is required in each of these states. Such legislation, so far, has only been passed by some coastal states. North-Rhine-Westphalia is currently preparing legislation. Ports in federal states without appropriate legislation are observing the ISPS-Code directly with the support of their local ministries and authorities.

The Designated Authority will conduct a port facility security assessment for all port facilities concerned. Central coordinator for the Designated Authorities of the individual federal states is the Bundesamt für Seeschifffahrt und Hydrographie in Hamburg and Rostock (www.bsh.de). Every port facility has to appoint a Port Facility Security Officer. The risk assessment of the port facilities by the authorities should help with identifying objects at risk, to evaluate the risk of a potential threat and to identify existing protective measures. Based on this the port facilities operator establishes a Port Facility Security Plan which is to be certified by the Designated Authority. If necessary, physical or organisational measures have to be taken to reduce the risk of a terrorist attack. The plan must contain measures against bringing aboard dangerous goods or weapons, measures against unauthorised access, evacuation procedures in cases of threats, procedures for the cooperation between port facilities and ship as well as measures for the protection of the cargo against acts of violence.

For seagoing ships the ISPS-Code categorises measures into three different levels of threat. For this it is necessary to identify in which way threats may arise for the ship (route, cargo, crew, nationality, political situation). This is done with a Ship Security Assessment. The information gained through the Assessment and the measures arising from it are described in the Ship-Security-Plan (SSP). Whether these are sufficient will be decided by the relevant ship's registration authority.

The ISPS-Code has no direct impact of the freight forwarder's activities, unless the freight forwarder himself is the operator of a port facility or runs a shipping company. Indirectly, however, the ISPS-Code has a marked, especially financial, impact on all participants within the transport chain. After almost all port facilities and all renowned shipping companies have implemented the ISPS-Code the resulting costs will be increasingly passed on to their customers.

The EU-Commission wants to ensure the uniform implementation of the SOLAS-rules and the ISPS-Code in Europe. The *EU-Directive No. 725 for the protection of ships and port facilities* is directly or indirectly in force in all EU member states with effect of May 19th, 2004. In contrast to SOLAS also all national sea transports within the European Union are to be covered by this regulation with effect from not later than July 1st, 2007.

Sources: ***www.customs.gov*** *; www.bsh.de ; Gesetz zur Änderung des internationalen Übereinkommens von 1974 zum Schutz des menschlichen Lebens auf See und zum internationalen Code für die Gefahrenabwehr auf Schiffen und in Hafenanlagen (BGBl. Teil II Nr. 38 vom 31. Dezember 2003, S. 2018); Gesetz zur Ausführung des Gesetzes zur Änderung des internationalen Übereinkommens von 1974 zum Schutz des menschlichen Lebens auf See und zum internationalen Code für die Gefahrenabwehr auf Schiffen und in Hafenanlagen vom 25. Juni 2004 (BGBl. Teil I Nr. 31, vom 30. Juni 2004, S. 1389); EU-Verordnung Nr. 725 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen (EU-Amtsblatt L129 vom 29. April 2004;*

2.5 Electronic pre-advice of airfreight data to the Air AMS of the US-Customs (Air AMS = Air Automated Manifest System)

The final rule of the US-Bureau of Customs and Border Protection (CBP) regarding advanced information of consignment data was published on December 5th, 2003 in the *Code of Federal Register (CFR)*. The aim is – as with the 24 hours manifest regulation – to identify goods with a potential security risk.

For airfreight imports into the US the required consignment information must be transmitted to the Automated Manifest System (AMS) of the US Customs authorities at least four hours before arrival of the aircraft. This is an obligation for all incoming airlines.

Hence follows the obligation for the freight forwarder to provide the air carrier on time with the House AWB-data. This may be done – preferably electronically – directly to the carrier or via a communications platform like TRAXON.

Air AMS was implemented for the airports on the US East coast on August 13th, 2004. Central USA and the West coast follow on October 13th, 2004 and December 13th, 2004 respectively.

Sources: *Any transport operator import and export: CFR / Vol. 68, No. 234, S. 68140*
Airfreight: *Modifications to Part 122 - Air Commerce Regulations of the US-Trade Act 2002 and here especially the new § 122.48a Electronic information for air cargo required in advance of arrival (CFR S. 68170 to 68173).*

2.6 Implementation of the EU-Directive on air security

For some time the German Legislation have been working on the implementation of the *EU-Directive No. 2320/2002 with common rules for security in civil aviation.* It was planned to implement the new regulations in 2004. However, the Air Security Law, with the required legal stipulations, was only passed in October 2004, but has not yet been published in the statutes. As soon as it is in force the implementation of the new security measures may be expected.

The new freight rules concerning air security will still be based on the "*known shipper" concept.* This means basically: if the cargo originates from a known shipper, has been secure throughout the whole pre-carriage and no unauthorised interference has been detected, it will be considered as "known cargo" (random checks possible).

Otherwise it is considered as "unknown cargo", and must be delivered separately with subsequent security measures to be taken by the authorities/airline.

In order to be accepted as an *regulated agent* by the German Federal Aviation Authority (Luftfahrt-Bundesamt - LBA), the cargo agent must probably meet the following requirements (Details not yet specified):

- Status as IATA agent or cooperation of IATA agents/forwarders or proposed by an airline
- Implementation of an LBA approved air security program
- Appointment of a security official (security checked according to the new German Air Security Law) to be responsible for the air security program
- Acceptance, processing and handling of the airfreight consignment exclusively by reliable personnel with appropriate training to understand and accept responsibility for air security.
- Acceptance of audits (agreed visits) and tests (unannounced) regarding the compliance with the security measures by the LBA
- Availability of facilities providing sufficient protection of the cargo against unauthorised interference during their storage (access control to the warehouse, no access for unauthorised persons)
- Commitment to provide information at any time about transport subcontractors used. Only transport subcontractors are used who have signed a valid declaration of compliance with the security measures for cargo to be carried on board of an aircraft.

Sources: *Verordnung (EG) Nr. 2320/2002 vom 16. Dezember 2002 zur Feststellung gemeinsamer Vorschriften für die Sicherheit in der Zivilluftfahrt (Amtsblatt L355 vom 30.12.2002, S. 1); Entwurf eines Gesetzes zur Neuregelung von Luftsicherheitsaufgaben, Bundesrats-Drucksache 509/04 vom 18. Juni 2004*

2.7 Security provisions for the carriage of dangerous goods (road, rail, inland waterways)

With effect of January 1st, 2005 – with a transition period until June 30th, 2005 – security provisions come into force as part of the worldwide UN-recommendations and the international rules for the carriage of goods on roads *(ADR), on rail (RID) and by inland waterways vessels (ADN(R)), Chapter* 1.10. It is assumed that the potential dangers inherent in the substance characteristics and the transport risks could be increased by specific misuse for terrorist purposes. Everyone participating in the carriage of dangerous goods (i.e. principal, consignor, shipper, loader, carrier, vehicle holder, container operator, tank wagon operator, inland waterway vessels operator and consignee) must implement far-reaching organisational and technical measures. The measures themselves are dependent upon the degree of danger and the volume of the transported substances.

No measures need to be taken if the dangerous goods are carried in quantities for which the existing dangerous goods regulations offer exceptions (e.g. small quantities -LQ and Table 1.1.3.6.3 – no need for labelling road vehicles). If the processed, loaded or carried quantities exceed these limits, the company must introduce management- and control procedures to ensure that the identity of the carrier was established before the contract of carriage was agreed, that dangerous goods are only handed over to authorised persons and that the terminals and handling sections cannot be accessed by unauthorised persons.

In addition, the training measures regularly undertaken for staff in the dangerous goods section must be supplemented by instructions regarding security aspects.

If high consequence dangerous goods (approx. 1,000 substances, the misuse of which would threaten considerable loss of life and massive destruction) are dispatched, loaded, carried or received in certain quantities the parties concerned must introduce and implement additional security plans. The elements of these plans comprise a security policy, specific assignment of responsibilities to members of staff, the evaluation of intra-company processes (risk evaluation) and contingency plans in case of incidents and suspicious events (reporting), procedure for the monitoring of the effectiveness of plans, etc. Altogether the measures and procedures described here are comparable to the requirements of a functional quality management. In addition, the security of the vehicles and their loads during transit must be guaranteed by technical equipment and driver instructions.

The German Chambers of Commerce and Trade, acting for the Federal Ministry of Transport, will compile a central register of all ADR certificates for dangerous goods drivers and make this accessible to the authorities.

Beyond those measures specified by legislation on the transport of dangerous goods, companies in Germany that store, load or carry certain dangerous goods must accept official security checks on selected members of staff. If a secret service check of a member of staff is positive, that person will not be permitted to work in key-areas where a potential threat from insiders exists (e.g. sabotage). This applies to newly employed personnel as well as for personnel already employed. The *Sicherheitsüberprüfungsgesetz (SÜG) (Law on Security checks)* and the *Sicherheitsüberprüfungs-feststellungsverordnung (SÜFV) (Ordinance on the determination of the scope for security checks)* based on the former, effective since August 2003, concerns companies participating in the carriage of high consequence dangerous goods. Here those members of staff are to be registered for security checks who decide on security measures within the company (members of staff with managerial authorisation – this is not necessarily the dangerous goods safety adviser!). Companies subject to the extended obligations of the German Störfallverordnung (German Ordinance on the implementation of the EC Seveso II-Directive) for dangerous substances storage, may allow access to security sensitive sections of the warehouse only for authorised members of staff.

Sources: *17. ADR-Änderungsverordnung (BGBl. Teil II Nr. 28 vom 14. September 2004, S. 1274); 12. RID-Änderungsverordnung (BGBl. Teil II Nr. 33 vom 12. Oktober 2004, S. 1434); Sicherheitsüberprüfungs-feststellungsverordnung-SÜFV (BGBl. Teil I Nr. 39 vom 8. August 2003, S. 1553); www.spediteure.de: DSLV: Hinweise zur Umsetzung neuer gesetzlicher Sicherungsbestimmungen für Beförderung und Lagerung gefährlicher Güter und Stoffe (Leitfaden),Oktober 2004.*

3. Requirements in preparation

3.1 Customs-Security initiative of the EU

The EU-Commission will, in the near future, integrate a security initiative for the protection of the EU-external borders into the *Community Customs Code*. Core of the initiative, also known as the 24-hours regulation – is the electronic pre-arrival declaration of goods in the form of a summary declaration before arrival in the European Union or before exit from the European Union. The initially envisaged deadline of 24 hours applies only to carriage by sea, otherwise deadlines between 2 and 4 hours are envisaged. The so-called *„authorized economic operator"* will be allowed further time concessions.

The regulations should come into force not later than Spring 2005. Since, however, the implementation provisions of the Customs Code, containing the requirements from an authorized economic operator, the individual deadlines and also extensive exceptions, are not available even as a draft version, the implementation of the regulation regarding the security initiative will be delayed for some time. Also, the necessary electronic networking of all European Customs offices has only just started. Therefore, it is envisaged that all stipulations or the electronic exchange of data will be implemented three years after the effective date of the implementation order.

3.2 Freight Transport Security (EU-Supply Chain Directive)

The European Commission is currently preparing a Directive containing not only comprehensive EU-internal measures for the protection against terrorism but also against criminal phenomena making use of the transportation of cargo (e.g. trafficking of humans, drugs and arms). The so-called “Supply Chain Directive“ concerns the transport means road, rail and inland waterways. It is assumed that the means of transport of the surface carriers might both be a potential target and a weapon. Although consultations of the Commission have not been finished yet, it may already be feared that participants in European land mode cargo transport will be subjected to high extra costs. The EU-Commission intends to shift responsibility for security from seafreight and airfreight to surface transport. At present measures regarding security-standards, pre-advice for goods transports through conurbations, electronic sealing of containers and transport units, the introduction of the “Known Shipper“- and the “Regulated Agent“-concept are being discussed. A first proposed Directive may be expected from Brussels by the beginning of 2005.

Sources: *Freight Transport Security – Consultation Paper of the European Commission dated December 2003*

ATTACHMENT

Tabular overview

I. Initiative / Regulation	2.1 CSI	2.2 24-hours manifest rule for seafreight
II. Responsible / Initiator	USA	USA
III. Legislation / mandatory	No	Yes
IV. Effective date (transition period)	01.Aug.2002	02.Dec.2002
V. Protection intended / Aim	Program for the protection of the USA against terrorist attacks with sea containers	Regulation for the electronic transmission of manifest data for the identification of "Risk Containers"
VI. Contents		
VI.1 Organisation	Risk analysis Pre-checks of "Risk Containers" already at the port of departure Electronic pre-advice of cargo data Checks carried out by Customs officials Physical examinations	Electronic notification not later than 24 hours before loading onto the sea-going vessel Exact description of goods Specification of the HS-Code Manifest checks carried out by US-Customs officials 14 mandatory data elements must be transmitted to the Automated Manifest System (AMS) electronically
VI.2 Technology	Use of secure "intelligent Containers" ("Smart-Container") Use of IT-systems for the identification of "Risk Containers" X-raying of containers Use of state-of-the-art X-ray technologies for faster pre-checks	
VI.3 Qualification	./.	./.
VI.4 Authorisation / License / Registration	Bilateral national agreement	Transmission to the AMS only by authorised service providers

	2.1 CSI	2.2 24- hours manifest rule for seafreight
VII. Responsible / concerned parties		
VII.1 Freight forwarder		**X**
VII.2 Shipper		
VII.3 Carrier		
VII.3.1 Road		
VII.3.2 Rail		
VII.3.3 Inland waterways		
VII.3.4 Sea	**X**	**X**
VII.3.5 Air		
VII.4 Consignee		
VII.5 Infrastructure operator (terminal/port)		
VII.5.1 Road		
VII.5.2 Rail		
VII.5.3 Inland waterways		
VII.5.4 Sea	**X**	**X**
VII.5.5 Air		

I. Initiative / Regulation	2.3 C-TPAT	2.4 ISPS
II. Responsible / Initiator	USA	UN / IMO
III. Legislation / mandatory	No	Yes, through Federal legislation regarding seafreight and state laws for the ports
IV. Effective date (transition period)		01.July.2004 (none)
V. Purpose / Aim	Voluntary program for the creation of a constantly high level of security throughout the complete transport chain	Protection of ships in international sea transport against terrorist threats at sea and in their ports of call
VI. Contents		
VI.1 Organisation	Secure procedures, physical security, personal security, education and training, access controls, Transport security	Risk evaluations of ports and vessels Contingency plans Appointment of security officials Security measures Training and exercises for the security personnel
VI.2 Technology	Terminal protection Theft protection vehicles, containers	Securing of port installations and vessels Fences Guards Electronic access systems (ID-cards) Cameras
VI.3 Qualification	Personnel selection Certification of suppliers / subcontractors	Training Security personnel Instructions
VI.4 Authorisation / Licence / Registration	Certification/Agreement with US-Customs (“private-public-partnership“)	Approval of the contingency plans by the Designated Authority

	2.3 C-TPAT	2.4 ISPS
VII. Responsible / Parties concerned		
VII.1 Freight forwarder	**X**	
VII.2 Shipper	**X**	
VII.3 Carrier		
VII.3.1 Road		
VII.3.2 Rail		
VII.3.3 Inland waterways		**X** (in parts)
VII.3.4 Sea	**X**	**X**
VII.3.5 Air	**X**	
VII.4 Consignee	**X**	
VII.5 Infrastructure operator (Terminal/Port)		
VII.5.1 Road		
VII.5.2 Rail		
VII.5.3 Inland waterways		**X** (in parts)
VII.5.4 Sea	**X**	**X**
VII.5.5 Air	**X**	

I. Initiative / Regulation	2.5 Air AMS	2.6 Air security plan
II. Responsible / Initiator	USA	EU / Federal government (Implementation of EU Directive)
III. Legislation / mandatory	Yes	Yes
IV. Effective date (transition period)	Aug 13 / Oct 13 / Dec 13, 2004	December 2004?
V. Purpose / Aim	Identification of goods with security risks	Civil aviation safety
VI. Contents		
VI.1 Organisation		Security official Air security program Security along the transport chain Personnel selection Selection of transport sub-contractors
VI.2 Technology	Electronic pre-advice of consignment data	Terminal security
VI.3 Qualification		Security training of personnel
VI.4 Authorisation / Licence / Registration		LBA registered as “Reglemented agent“ (as a rule: IATA-Intermediary)

	2.5 Air AMS	2.6 Implementation EU-Directive on Air Security
VII. Responsible / concerned party		
VII.1 Freight forwarder	**X**	**X**
VII.2 Shipper		**X**
VII.3 Carrier		
VII.3.1 Road		**X**
VII.3.2 Rail		
VII.3.3 Inland waterways		
VII.3.4 Sea		
VII.3.5 Air	**X**	**X**
VII.4 Consignee		
VII.5 Infrastrukture operator (Terminal/Port)		
VII.5.1 Road		
VII.5.2 Rail		
VII.5.3 Inland waterways		
VII.5.4 Sea		
VII.5.5 Air		**X**

I. Initiative / Regulation	**2.7 Security provisions for the carriage of dangerous goods (road, rail, inland waterways)**
II. Responsible / Initiator	UN / OTIF / ZKR
III. Legislation / mandatory	ADR / RID / ADN(R) Chapter 1.10
IV. Effective date (transition period)	01. Jan. 2005 (01. July 2005)
V. Purpose / Aim	Protection against the misuse of dangerous goods
VI. Contents	Security measures – a) general, b) high consequence dangerous goods
VI.1 Organisation	Procedure for the identification of vehicle crews (a and b) Selection of carrier/transport contractor (a and b) Intra-company vehicle- and loading controls / checks (a and b) Personnel selection based on security aspects (b) Specific allocation of responsibilities (b) Theft protection for vehicles and loads (b) Security plan (b) - Risk assessment, register of high consequence dangerous goods - Description and evaluation of internal procedures (e.g., QM) - Security philosophy - communications (internal / external) / reporting - extended personnel training including documentation
VI.2 Technology	Terminal security (not specified) (a and b) Theft protection vehicles and load (b) Telemetry vehicles (preferred utilisation, if available) (b) Use of security technology to minimise risks (not specified) (b)
VI.3 Qualification	Internal personnel awareness training (a), extended (b), incl. documentation (a+b, both not specified) Personnel selection based on security aspects (b) (possibly specified by measures according to §11 SÜFV)
VI.4 Authorisation / Licence / Registration	Official controls (monitoring) (a and b) State register of ADR-certificates (drivers) (a and b)

	2.7 Security provisions for the carriage of dangerous goods (road, rail, inland waterways)
VII. Responsible / concerned parties	
VII.1 Freight forwarder	**X**
VII.2 Shipper	**X**
VII.3 Carrier	
VII.3.1 Road	**X**
VII.3.2 Rail	**X**
VII.3.3 Inland waterways	**X**
VII.3.4 Sea	
VII.3.5 Air	
VII.4 Consignee	**X**
VII.5 Infrastructure operator (Terminal/Port)	
VII.5.1 Road	**X**
VII.5.2 Rail	**X**
VII.5.3 Inland waterways	**X**
VII.5.4 Sea	
VII.5.5 Air	

I. Initiative / Regulation	3.1 Customs-Security initiative (Draft)	3.2 FTS (Consultation Paper)
II. Responsible / Initiator	EU-Com	EU-Com
III. Legislation / mandatory	Yes	Open
IV. Effective date (transition period)	Still open	Open
V. Purpose / Aim	Monitoring of goods import/export through pre-advice	Anti-terrorist protection Protection against goods theft Drugs trafficking Arms smuggle
VI. Contents		
VI.1 Organisation	IT, integrated into ATLAS	Security-standards Advance information
VI.2 Technology	IT, integrated into ATLAS	Theft protection load (seal)
VI.3 Qualification	No, covered by ATLAS-training	
VI.4 Authorisation / Licence / Registration	For “authorised participants“ Simplified pre-advice	Known Shipper Regulated Agent

	3.1 Customs-Security initiative (draft)
VII. Responsible / concerned parties	
VII.1 Freight forwarder	**X**
VII.2 Shipper	**X**
VII.3 Carrier	
VII.3.1 Road	**X**
VII.3.2 Rail	**X**
VII.3.3 Inland waterways	
VII.3.4 Sea	**X**
VII.3.5 Air	**X**
VII.4 Consignee	**X**
VII.5 Infrastructure operator (Terminal/Port)	
VII.5.1 Road	
VII.5.2 Rail	
VII.5.3 Inland waterways	
VII.5.4 Sea	**X**
VII.5.5 Air	**X**