Deutsches Verkehrsforum

Steering Committee 'Freight Transport'
at German Transport Forum

# Ten Criteria for Supply Chain Security

Adapt existing procedures – Keep EU market open

June 2007

# German Transport Forum

## Our mission

"Mobility for Germany" – in a functional, customer-driven, environment-friendly and integrated transport system

## What we do

We represent the common interests of the transport industry in Germany in the political domain, the media and society.

We support measures to further mobility and improve underlying conditions as essential prerequisites for growth and employment.

We create a "shop window" to promote exports of the transport industry's products and services and thereby help entrench its world lead.

## Our aims

- Universal recognition of the crucial importance of mobility and the transport industry.
- Efficient and developable transport infrastructure
- Intelligent networked transport systems allowing full utilisation of synergy potential and of the specific strengths of individual transport providers
- Fair competitive conditions for all modes of transport – national and international
- Customer-oriented, integrated mobility solutions

## Our activities

We provide the right platform for purposeful debate on core transport issues between customers, transport providers, business, science and government.

We further opinion-forming on current transport issues through critical and constructive comment, at round-table and other events, through press and PR activities

We cooperate with political decision-makers as well as with national and international federations of the road, rail, air transport, maritime and inland shipping industries – national and international.

Deutsches Verkehrsforum

Klingelhöferstr. 7
10785 Berlin

Tel. +49 30 / 26 39 54-0
Fax. +49 30 / 26 39 54-22

www.verkehrsforum.de
info@verkehrsforum.de

**Contents**

## Ten criteria for supply chain security

*Supply Chain Security is in industry's own interest*

German transport and logistics companies are naturally self-interested in secure trade flows and the protection of goods against unauthorised access. For that purpose, they have taken *in-house precautions* to make their business processes secure. Those company measures are augmented by a variety of *superposed security regulations* designed to safeguard goods traffic against terrorist attacks.

Extending legal security requirements by such measures as EU Regulation COM (2006) 79, which is intended to enhance security in the supply chain, does not however achieve *any security gain*. It gives rise instead to the risk of *new trade barriers* which have only recently been dismantled by the creation of the Single European Market. Additionally, they can impede bundled traffic which is both politically and economically desirable.

*Utilising existing structures*

In order to improve security in goods traffic, there is no need for new regulations but rather measures to *integrate* existing initiatives into a coordinated strategy. Prior to any ongoing development of the security regime, the efficacy of existing initiatives and investments should be scrutinised. The German Transport Forum advocates a *coherent, Europe-wide-harmonised and internationally recognised security strategy embracing all modes of transport*.

*Basic points for practice-driven security*

In its functions as a neutral platform for the entire German transport industry, the German Transport Forum has in cooperation with experts from its member-companies identified ten basic criteria which must be met by security regimes put forward in respect of supply chain security:

### 1. Protection against terrorism is an existential imperative

Industry has in its own interest already taken precautions against unauthorised access to the logistics chain. *Defence against the dangers of terrorism is, however, primarily the duty of the state.* Responsibility for supply chain security ought not be off-loaded to industry alone insofar as that is done purely to serve a public interest.

### 2. Analyse risks, act purposefully

Logistics chains consist of a variety of heterogeneous links which can in manifold ways be combined. After all, every transport chain is of its kind unique. Detailed risk analysis for the purpose of identifying and classifying risks, and differentiating between transport modes and the transport objective is, therefore, essential for establishing a successful security regime and systematically closing any security gaps.

**3. Secure external borders, safeguard EU internal market**

The s*tatus of "Authorized Economic Operator / AEO)" ,* available with EU customs reform from 2008, is a major measure *safeguarding the EU external borders*. An array of companies is expected to implement the required measures in order to acquire the status of an AEO. In that way, that status will become established as a quasi-minimum - standard for the security of the supply chain in EU external trade, and include not only the measures taken at seaports and airports but also the pre- and post-feeder traffic, especially surface traffic. Any further measures over and beyond that must be carefully thought through, since every intervention in EU internal traffic institutes *new trade barriers that impede efficiency. Liberalised internal traffic* ought not be jeopardised by unsuitable security structures.

**4. Focus on standardisation, recognise existing solutions**

Existing security regimes (See Annex) have been coordinated and established at considerable expense of industry and government at European and international level. These measures must be integrated in the standardising activities of CEN and ISO (e.g. ISO 28 000). The primary object is to ensure that existing and future security regimes can be compared for *benchmarking or classification* so as to allow unbureaucratic recognition of company security measures within the framework of superposed security regimes. The onus is on industry to drive this standardisation forward.

**5. Support global standards, provide interfaces**

European solutions must be based on *global standards* or at least furnish practicable interfaces which support global logistics chains. To that end, Europe must continue working on global standards in the international organisations while, simultaneously, strongly backing existing European solutions there and pressing for their international application.

**6. Create freedoms and incentives**

Implementation of security measures needs to be *genuinely incentivised* and, in return, create freedoms that reduce operating costs. The *benefits held out in that respect to security-conscious companies* must be concretised, if security regimes are to be successful.

**7. Clarify liability, eliminate weak- points**

The transport chain is only as strong as its weakest link. Within a security chain, therefore, it is essential to define the *liability* assigned to operators in the chain and *how shipments from non-certificated partners* can be integrated in the logistics chain without prejudicing the status of authorised partners. Inspection and onward transportation at a company's own risk is impracticable and non-insurable.

**8. Shun bureaucracy, encourage self-initiative**

In an efficient transport system, it is important that *logistics costs are not increased by additional bureaucracy.* Prior to implementation of a new security regime, the potential and expandability of existing systems should be scrutinized first. *Self-declaration/self-certification* by companies offers an efficient alternative to excessively bureaucratic certification procedures.

**9. Customise solutions, prevent competitive disadvantages**

The *heterogeneous structure of the transport business* should be taken into account when defining security measures*. Scalable measures* must ensure that customised solutions are available at affordable cost for small to medium-sized companies. Care must also be taken that *no competitive disadvantages* arise between individual transport providers and that security regimes do not counteract the desired bundling effects.

**10. Increase efficiency and service focus in administration**

Security regimes must be efficiently and competently supported in the administrative area so that the logistics industry can continue to meet its transport and delivery commitments without restraint. New and increasingly detailed security regulations add to the time and expense of inspection procedures which are primarily handled by state authorities. Every *inspection regulation* must, therefore, be accompanied by an increase in correspondingly *qualified staff.*

*Standardised "security culture" supports companies*

The German transport industry already lays on secure and efficient services suited to market requirements from end-to-end of the supply chain. The transport companies will continue to optimise their security processes in the future with their expertise and considerable resources in order to make their contribution towards preventing and averting risks. The aforementioned *framework for a standardised "security culture"* can support their endeavours more effectively than additional certification procedures and burdensome bureaucratic routine.

The object of a *practicable security strategy* must be to *safeguard the European external borders and standardise security regimes*. This paper spelling out the position of the "Freight Transport" steering committee at the German Transport Forum shows in what way existing security regimes can be utilised to secure the supply chain by observing the aforementioned ten criteria.

## I. Status Quo: Challenges from the global security situation

In the era of globalisation, logistics chains into and out of Europe have become indispensable lifelines for our economies. They underpin the international division of labour and generate a goodly proportion of added value in Europe. Germany in particular profits in this instance from its central position in the EU and maintains with its logistics services a quality lead.

*New challenges for supply chain security*

In the aftermath of 9/11, new factors came into play in the logistics chain alongside the "conventional" threats to freight transport from theft, vandalism and accidents:

- The danger posed to traffic flows by terrorist attacks or other intervention by third parties.
- The risk of direct or indirect misuse of the means of transport as weapons.

*Industry helps establish security regimes*

*Security of the Supply Chain* has consequently become a key quality attribute, which is increasingly becoming a competitive factor especially in a global environment. Logistics companies, trade and industry have already invested substantial effort in combating these threats. Operators in the logistics chain have, for example, set up at considerable expense their own *in-house security regimes,* like TAPA, which deny third parties any access to goods and their logistics chain:

- German airports spent a total of *45 million euros* in 2005 alone on security measures required by §8 of the Aviation Security Act (LuftSiG);
- Lufthansa Cargo AG is spending more than *80 million euros* yearly in complying with security regulations. These funds are expended, among others, on technical equipment. The Company is currently operating with more than 100 x-ray devices/explosive detection systems and around 2,000 cameras. Additionally, more than 100 of the staff are employed daily on security work;
- German seaports have spent more than 50 million euros on implementation of directives governing security at ports and in shipping;
- The company Schenker has invested 3.9 million euros on acquiring TAPA-FRS status at 35 European locations, plus 70,000 euros per year for certification;
- Alongside one-off (implementation) expenditure, ongoing costs are incurred by all security measures, e.g. for maintenance and staff training.

*Costs are particularly harsh burden for small to medium-sized companies*

The cost of security is disproportionately high, especially for small and medium-sized companies. According to EU Commission estimates, the average expense for structural adaptation and human resources in the implementation of EU regulation on supply chain security ([COM (2006)79] would cost mid-sized companies employing up to 250 staff up to *135,000 euros.* Yearly ongoing costs would amount to up to *131,000 euros.* Small to medium-sized firms would in total incur the greatest burden of around 90% of the necessary capital expenditure arising from implementation of this regulation.

A similar cost disparity would also occur between different modes of transport. Implementation of the supply chain security regulation would cost *road transport companies* up to 49,000 euros, it would cost railway companies up to 67,000 euros – 36% more. Into the bargain, they would incur proportional costs for other facilities, e.g. maintenance facilities, marshalling yards etc. (See DNV Consulting 2005[1]).

*Excess regulation leads to inefficiency*

Existing security regimes effectively secure the EU external borders at critical hub points – especially at inland shipping and seaports as well as airports. The diversity of existing but uncoordinated security regimes in the transport sector leads, however, to some *irrational developments* which, in turn, lead to *inefficiencies*:

- *Air cargo pallets* in transatlantic traffic with the USA, which weigh more than 68 kilos, must be inspected *manually* for any persons therein in accordance with TSA[2] regulations. That applies even if the pallet dimensions are so small that no human being would fit inside. To all intents and purposes, the ban on the use of technical equipment does not enhance security but counteracts all bundling effects and leads to substantial additional costs.
- Unlike Germany, France and the UK are exempted by bilateral treaties from manual inspection of these so-called built-up units and thereby gain *significant competitive benefits*.
- National interpretation of EU regulations gives rise to *differences in their implementation* within Europe's different national states, which distort competition. For example: The measures and equipment authorised Europe-wide for security controls are not recognised in Germany despite the pledge to harmonise security regulations Europe-wide.
- Aircraft crews are analogously to air passengers subject to comprehensive security checks, although they occupy a special position of trust and undergo regular checks by security authorities.

*Diversity requires harmonisation*

These inconsistencies highlight the fact that a review of the entire security scenario is long overdue. In the past few years, a variety of occasionally overlapping security regimes have been implemented, at times ad hoc and under pressure of time. The upshot is the present variety of competitive or counter-productive solutions which *urgently need to be harmonised*.

---

1 On behalf of EU Commission: DNV Consulting (2005): Study on the impacts of possible legislation to improve transport security.

2 Transportation Security Administration (TSA), U.S. Department of Homeland Security

## II. AEO programme: Practicable but with weakpoints

*Customs Code offers basis for practicable standard*

The EU *regulation* 1875/2006 *implementing amendments to the Customs Code* spells out the principles for improving security at the EU external borders. It requires traders and customs authorities to exchange advance information on all goods entering or leaving the EU. That way, it integrates security with customs requirements in trade with third countries. This coupling of the two makes sense, if multiple inspections are thereby avoided.

*AEO security: Benefits …*

From 1 January 2008, companies can apply to their national customs authorities for the status of Authorised Economic Operator (AEO). Certification is accompanied by the following *potential benefits in customs procedures*:

- *Recognition* of already applied security (superior) standards, such as that of "Regulated Agent[3]", on approval of AEO security status to avoid duplicate inspection,
- Application of *risk-related* controls instead of transaction-related controls,
- Paperless mailing of *advance information,* also as incentive for electronic processing of further processes.

*… critical points …*

But the following *critical points* need to be considered:

- Too great a scope is allowed in the formulation of national regulations, which results in different requirements being defined in the EU member-states for approval of AEO status, which in turn distorts competition;
- The financial and administrative expense involved in applying for and acquiring AEO status must be justifiable and acceptable for companies;
- Aside from the need for uniform requirements within the EU, mutual recognition of certificates between international customs authorities must be ensured. As the world's leading exporter, German economy depends on fast customs controls. Mutual recognition alone would save German operators unnecessary duplicate inspection in international trade;
- Administrative authorities must be prepared for recognition of AEO security status as well as institution of other security regimes so as to avoid long delays in granting approval or certification.

*… and open questions.*

Although it is already possible to apply for AEO status, some *questions* of elementary importance in the application process are *still open*.

- What benefits do authorised operators obtain?
- Must all participants in the international supply chain (manufacturers and forwarders) be accordingly accredited to ensure that shipments are safe?
- How can shipments from a non-certified economic operator be integrated in the logistics chain subject to the security regime? Can an

---

[3] The amendments to the German Aviation Security Act (LuftSiG) implementing the EU Regulation on Security in Civil Aviation came into force on 1 February 2006. This enables operators in the aviation industry to apply for the status of authorised economic operator. Applicant companies are required to comply with a range of security measures and requirements.

authorised economic operator make shipments from a non-AEO secure and thus "heal" the missing status? How should liability in this case be decided? (Compare "regulated agent" EU Regulation 2320/2003)

- Can customs process the additional data volume, which is required, and analyse it in a risk assessment (Datamining)?
- Will the procedure practised by national customs authorities be coordinated and standardised, Europe-wide?
- Is the extra expense practicable and affordable for small and medium-sized companies?

If the open questions are resolved and system faults rectified in accordance with the aforementioned criteria, the AEO security program would constitute an *effective standard* for securing the supply chain in the EU in trade beyond its external borders.

*Prevention of hindrances in internal trading*

Expansion of customs security requirements to *trading within the European internal market,* as envisaged by the draft regulation on supply chain security COM (2006)79 should, *however, be rejected*. That would be tantamount to re-introducing customs restrictions in the internal market and cannot be the aim of European trade policy.

## III. Standardisation: Making existing diversity practicable

A diverse array of security regimes, different in scope and application, are currently in existence. They embody different industry standards as well as provisions specific to individual transport providers. Existing solutions can be subdivided into *official regulations and company in-house* systems (See Annex).

*Pragmatic approach to integration of security regimes:*

The co-existence of security regimes, which leads to significant overlapping in actual application, must be replaced by the integration of those regimes in a coordinated concept in order to make significant gains in security. A pragmatic approach, as spelt out in the following, should be adopted:

- A security regime must in general satisfy the aforementioned *ten criteria* for practicable supply chain security.
- The *degree,* to which the framework set out by the criteria is *implemented*, should serve as a *benchmark* for rating a security regime and would facilitate comparison between different systems.
- The security regimes could be *classified* according to the degree of comparability they attain.
- A risk-oriented system based on *industry standards s*hould constitute the general framework in which the individual security regimes are grouped.

*ISO 28 000 as framework*

Making security regimes comparable and subordinating them to existing industry standards is the responsibility of industry. This is already effectively practised with other industry norms. On the international level, the *ISO 28 000* standard is a generally recognised and flexible tool for driving forward such *classification and standardisation.* Moreover, it augments the widely established quality norms of the ISO 9000 family. The initial steps to be taken towards that end are:

- institute suitable mechanisms and classes within the ISO 28 000 standard for *grading the diverse security regimes* and, thereby,

– create a basis for the simplest possible recognition of existing regimes.

## IV. Conclusions

1. Defence against terrorist attacks is first and foremost the *responsibility of the state*. The state must support the industries efforts to secure the supply chain, as part of its duty to *provide services of general economic interest.*

2. A practicable solution that can be implemented quickly must be based on *existing and generally recognised systems*; it must close any security gaps that eventually come to light in a *risk analysis* and create *clear structures.* The guidelines to follow are spelt out in the aforelisted ten criteria.

3. The status of *Authorised Economic Operator (AEO)* that becomes available with the amendments to the Customs Code in 2008 can serve as a suitable base for *securing the EU external borders* and sensibly augment existing solutions, if the highlighted weak-points are redressed during implementation.

4. Supply chain security in purely inland shipping must, however, continue to be shaped *in accordance with demand and industry-specific risks* on their *own initiative and voluntarily* by operators. Care must be taken that security regimes in this instance do *not create new trade barriers* in European internal market.

5. *Standardisation* of existing security regimes is in the long term indispensable. The heterogenety of present solutions must be resolved by *classification* in order to enable mutual recognition of security standards. The ISO norm 28 000 is a possible tool for driving forward the establishment of this grading system and bringing the security regimes under the umbrella of ISO into a *uniform international system*. Again here, the onus is primarily on industry but state security regimes must also provide interfaces to the standard so that company initiatives can be recognised expeditiously.

6. Pending conclusion of the standardisation process, the authorities and industry must work together to ensure that *recognition and inclusion of company in-house standard* is facilitated in the framework of state security regimes.

7. The *initiative of the European Parliament* stipulating that security regimes and the resultant measures introduced by the state should be scrutinised for their *suitability and efficacy* at regular intervals and eventually not be prolonged, is to be welcomed for the sake of system efficiency.

ANNEX

## Security regimes for the transport sector (Extract)

*Current official security regimes* in the transport sector are:

- *Customs-Trade Partnership against Terrorism (C-TPAT),* introduced in the USA in 2001. It involves voluntary acceptance by participating companies of security requirements defined by the US authorities in return for priority processing of shipments by US customs.
- *Container Security Initiative (CSI),* introduced for containerised cargo in the USA in 2002. The CSI specifies special rules for pre-screening of containers and submission of customs data, among them, controls on containers prior their loading on vessels at the port of origin. Under the *Advanced Manifest Rule (AMR)* in the CSI, all vessels heading for the USA are required to provide an electronic manifest, 24 hours before a container is loaded, to the US customs authorities (Customs and Border Protection – CBP).
- *EU Regulation 2320/2002* on civil aviation security. The regulation specifies security norms for civil aviation in the EU. Besides airports and airlines, the regulation applies to consignors ("known consignor" status) and forwarders in the airfreight business.
- *EU Regulation 725/2004* on enhancing security on ships and at port facilities. It came into force in 2004 and spells out stringent security norms on access controls and cargo loading. It complements the International Ship and Port Facility Security Code (ISPS Code), a set of measures to step up the security of ships and port facilities developed in response to perceived threats in the aftermath of 9/11. The EU regulation was further optimised by *Directive 2005/65/EC*.
- *Framework of Standards to Secure and Facilitate Global Trade,* adopted by the World Customs Organisation (WCO) in 2005. A set of standard rules for customs and industry on uniform advance electronic cargo information to prevent attacks.
- *Green Paper for critical infrastructure protection* put forward by the European Commission (COM (2005) 576) in November 2005. Its strategic goal is to protect endangered networks (energy, telecommunications and transport) against terrorist attacks.
- Comprehensive European regulations on the *protection of dangerous goods transports are in place* for all modes of transport at national and international level (e.g. ADR/RID/ADNR regulations)
- In order to bring EU requirements into line with US security initiatives and WCO proposals, the European Commission is amending the *EU Customs Code* (Regulation 648/2205) and the EU Customs Code amendment implementation regulation (Regulation 1875/2006). These provisions initiate the status of "authorised economic operators" (AEO), to whom customs authorities can grant permission to simplify trade by using simplified procedures with regard to safety and security-related customs controls.
- *EU Regulation 2580/2001 and 881/2002 Compliance:* These regulations are designed to "dry up" the funds of persons or entities associated with terrorist organisations. They forbid the provision of

financial assets of any kind to persons or organisations on US/EU terrorist lists.

- *Export controls / embargoes:* Diverse and mandatory export controls are in force for goods and technologies.

C*ompany in-house standards or industry norms* applied in the transport sector include:

- Framework for supply chain security of the *International Organisation for Standardization (ISO)*. Norms for supply chain security are under discussion in ISO PAS 28000 resp. 28001) Similar drafts are underway at the CEN European Committee for Standardisation.
- *TAPA-Freight Security Requirements (TAPA-FSR):* The freight security standards introduced in 2001 by TAPA (Technology Asset Protection Association) encompass instructions on the implementation of building, equipment and process security measures to ensure that goods from TAPA member companies are securely warehoused by logistics services providers during in-transit storage as they move through the supply chain. TAPA-FSR specifies minimum acceptable security standards at three levels in the supply chain.
- *Company in-house security standards* defined by logistics services providers specify minimum security norms for a location or other elements in the supply chain – e.g. the minimum acceptable security standard specified by the Schenker forwarding company for the German general cargo network or the Schenker minimum security standard for safeguards at locations in the Company's Europe-wide surface network.