

**České Vysoké Učení Technické v Praze**  
**Fakulta dopravní**



**Bc. Ondřej Stejskal**

**Vzájemné uznávání bezpečnostních iniciativ celního  
a obchodního partnerství**

**2014**



**K617 ..... Ústav logistiky a managementu dopravy**

**ZADÁNÍ DIPLOMOVÉ PRÁCE**  
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

**Bc. Ondřej Stejskal**

Kód studijního programu a studijní obor studenta:

**N 3710 – LO – Logistika, technologie a management dopravy**

Název tématu (česky): **Vzájemné uznávání bezpečnostních iniciativ  
celního a obchodního partnerství**

Název tématu (anglicky): Mutual Recognition of Customs - Trade Partnership  
Security Initiatives

**Zásady pro vypracování**

Při zpracování diplomové práce se řiďte osnovou uvedenou v následujících bodech:


- Uveďte prostředí mezinárodní přepravy zboží v souvislosti s problematikou bezpečnosti.
- Popište Gutiérrez a Hints model a jeho aplikaci na bezpečnostní iniciativy v dodavatelských řetězcích.
- Charakterizujte iniciativy spolupráce mezi celními správami a podniky a dohody jejich vzájemného uznávání.
- Proveďte analýzu bezpečnostních kritérií vybraných iniciativ, posuďte srovnatelnost jejich požadavků z hlediska vzájemného uznávání a případně navrhněte jednotný systém bezpečnostních kritérií pro získání statusu v těchto iniciativách.
- V závěru vyhodnoťte současnou bezpečnostní situaci v závislosti na globalizaci těchto iniciativ.


- Rozsah grafických prací: dle pokynů vedoucího diplomové práce
- Rozsah průvodní zprávy: minimálně 55 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)
- Seznam odborné literatury: Supply Chain Security Initiatives: A Trade Facilitation Perspective  
SAFE Framework of Standards to secure and facilitate global trade, 2012  
Authorised Economic Operators Guidelines, 2012  
C-TPAT Strategic Plan


Vedoucí diplomové práce: **Ing. Martina Vitteková, Ph.D.**

Datum zadání diplomové práce: **28. června 2013**  
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání diplomové práce: **30. listopadu 2014**  
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia  
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

  
prof. Ing. Petr Moos, CSc.  
vedoucí  
Ústavu logistiky a managementu dopravy

  
L. S.

  
prof. Dr. Ing. Miroslav Svítek  
děkan fakulty

Potvrzuji převzetí zadání diplomové práce.

  
Ondřej Stejskal  
jméno a podpis studenta

V Praze dne..... 6. května 2014



**CZECH TECHNICAL UNIVERSITY IN PRAGUE**

Faculty of Transportation Sciences

Dean's office

Korviktská 20, 110 00 Prague 1, Czech Republic

**K617 ..... Department of Logistics and Management of Transport**

## **MASTER'S THESIS ASSIGNMENT**

(PROJECT, WORK OF ART)

Student's name and surname (including degrees):

**Bc. Ondrej Stejskal**

Code of study programme code and study field of the student:

**N 3710 – LO – Logistics, Technology and Management in Transport.**

Theme title (in Czech): **Vzájemné uznávání bezpečnostních iniciativ  
celního a obchodního partnerství**

Theme title (in English): Mutual Recognition of Customs - Trade Partnership  
Security Initiatives

### **Guides for elaboration**

During the elaboration of the master's thesis follow the outline below:

- Specify an environment of international transport of goods in relation to the issue of security.
- Characterize programs of cooperation between customs administrations and enterprises and projects of their mutual recognition.
- Describe Gutiérrez and Hintsa model and its application to security initiatives in international supply chains.
- Perform analysis of security criteria of the selected initiatives, evaluate the comparability of their requirements in terms of mutual recognition, and alternatively design a unified system of criteria for obtaining a possession of status at these initiatives.
- In conclusion, evaluate the current security situation according to the globalization of these initiatives.

Graphical work range: According to the character of thesis topic

Accompanying report length: minimum 55 pages of text (including images, graphs and tables, as part of the accompanying report)

Bibliography: Supply Chain Security Initiatives: A Trade Facilitation Perspective  
SAFE Framework of Standards to secure and facilitate global trade, 2012  
Authorised Economic Operators Guidelines, 2012  
C-TPAT Strategic Plan

Master's thesis supervisor: **Ing. Martina Vitteková, Ph.D.**

Date of master's thesis assignment: **June 28, 2013**  
(date of the first assignment of this work, that has been minimum of 10 months before the deadline of the theses submission based on the standard duration of the study)

Date of master's thesis submission: **November 30, 2014**  
a) date of first anticipated submission of the thesis based on the standard study duration and the recommended study time schedule  
b) in case of postponing the submission of the thesis, next submission date results from the recommended time schedule

  
prof. Ing. Petr Moos, CSc.  
head of the Department  
of Logistics and Management of Transport



  
prof. Dr. Ing. Miroslav Svítek  
dean of the faculty

I confirm assumption of master's thesis assignment.

  
Ondrej Stejskal  
Student's name and signature

Prague ..... May 6, 2014

## Prohlášení

Nemám závažný důvod proti užívání tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

V Praze dne 30.11.2014

Bc. Ondřej Stejskal

podpis



## Poděkování

Velice rád bych poděkoval paní Ing. Martině Vittekové, Ph.D. za vstřícnou spolupráci, Ing. Peterovi Vittekovi za přínosné odborné konzultace a Kateřině Boháčové za korekturu. Dále bych rád poděkoval svým rodičům a prarodičům za podporu mého studia na vysoké škole a své nejmilejší za podporu při psaní této práce.

Ondřej Stejskal

## ABSTRACT:

Author's name and surname: Bc. Ondrej Stejskal

Title of the diploma thesis: Mutual Recognition of Customs-Trade Partnership Security Initiatives

Name of the university: Czech Technical University in Prague  
Faculty of Transportation Sciences

Thesis supervisor: Ing. Martina Vittekova, Ph.D.

Key words: transport of goods; supply chain; security; unlawful activity; standardization

Number of pages: 71

The purpose of this thesis is to address the issue of international supply chain security. In particular, the author looks into the initiatives of the partnership among customs administrations and businesses. The paper consists of three main parts. In the first part, the author introduces the background of developing illegal activities in the international transport and the principle of the Customs – Trade Partnership programs. In the second part the process of the mutual recognition of such programs is described. The third part contains an analysis of security criteria in particular programs, and the author herein designs a useful aid to help companies obtain the certified status. In the conclusion, the author summarizes the results reached, evaluates the outputs and compares them to the objectives of the thesis.



## ABSTRAKT:

Jméno a příjmení autora:	Bc. Ondřej Stejskal
Název diplomové práce:	Vzájemné uznávání bezpečnostních iniciativ celního a obchodního partnerství
Označení a místo vysoké školy:	České Vysoké Učení Technické v Praze Fakulta dopravní
Vedoucí bakalářské práce:	Ing. Martina Vitteková, Ph.D.
Klíčová slova:	přeprava zboží; dodavatelský řetězec; zabezpečení; protiprávní činnost; standardizace
Rozsah stran:	71

Smyslem této práce je zabývat se problematikou zabezpečení mezinárodního dodavatelského řetězce. Autor se zabývá zejména iniciativami partnerství mezi celními správami a podniky. Práce obsahuje tři hlavní části. V první části autor popisuje pozadí vývoje nezákonných aktivit v mezinárodní dopravě a principu programů celního a obchodního partnerství. V druhé části je popisován proces vzájemného uznávání těchto programů. A třetí část obsahuje analýzu bezpečnostních kritérií v jednotlivých programech, a návrh užitečné pomůcky pro firmy k získání certifikace. V závěru jsou shrnuty dosažené výsledky, hodnoceny výstupy a porovnány s cíli práce.

## Content

List of Abbreviations .....	12
Introduction .....	13
1. Security Environment in International Transport.....	14
1.1 Background .....	14
1.2 Security Initiatives in the International Supply Chain.....	15
2. Customs - Trade Partnership Security Initiatives.....	17
2.1 Background.....	17
2.2 Characterization and Principle of the C-T Partnership.....	18
2.2.1 Environment.....	18
2.2.2 Obligations and Benefits .....	18
2.2.3 Suitability for Companies.....	19
2.3 Admission Procedure .....	20
2.3.1 Eligibility.....	20
2.3.2 Minimum Security Criteria .....	21
2.4 Customs-Trade Partnership Against Terrorism (C-TPAT).....	23
2.4.1 Introduction .....	23
2.4.2 Objectives of the Program.....	24
2.4.3 Benefits .....	24
2.4.4 Participants.....	24
2.4.5 Enrolment Conditions .....	25
2.4.6 Implementation.....	26
2.4.7 Minimum Security Criteria .....	26
2.4.8 Risk Assessment.....	27
2.4.9 C-TPAT Manuals .....	27
2.4.10 Annual Security Profile Review.....	28
2.4.11 Validation .....	28
2.5 Mutual Recognition of the C-T Partnership Programs .....	30
2.5.1 Background .....	30
2.5.2 Definition of Mutual Recognition .....	31
2.5.3 Concerns of Mutual Recognitions Processes .....	31
2.5.4 Benefits of Mutual Recognition .....	32

3.	Gutiérrez and Hints Model .....	34
3.1	Background .....	34
3.2	Model Structure .....	34
3.3	Features of the Model .....	36
3.4	Application.....	37
4.	C-T Partnership Programs Criteria Analysis.....	38
4.1	The Issue .....	38
4.2	Compatibility of C-T Partnership Programs .....	39
4.2.1	Mutual Recognition of C-TPAT and AEO.....	39
4.2.2	C-TPAT Mutual Recognition Compatibility Matters.....	41
4.3	Actual Convenience for Businesses.....	43
4.3.1	Generally Speaking .....	43
4.3.2	Individual Point of View .....	43
4.4	Identification of a Unified Model for Self-Evaluation .....	45
4.4.1	Stimulus.....	45
4.5	Draft of the Unified Model .....	47
4.5.1	Data Acquisition.....	47
4.5.2	Analysis and Classification of Data .....	48
4.5.3	Outputs of the Analysis .....	49
4.5.4	Scoring and Weighting.....	63
4.5.5	Results.....	64
4.5.6	Further Observations .....	66
	Conclusion.....	67
	List of sources.....	69
	List of figures .....	71
	List of tables .....	71

## **List of Abbreviations**

AEO – Authorized Economic Operator

CBP – Customs Border Protection

CCTV – Closed - Circuit Television - video surveillance

CSI – Container Security Initiative

C-TPAT – Customs – Trade Partnership Against Terrorism

EMEA – Region of Europe, Middle East and Asia

EU – European Union

FAST – Fast and Secure Trade

IMO – International Maritime Organization

ISPS Code – International Ship and Port Facility Security Code

MT – Mutual Recognition

PAS – Publicly available specification

SCS – Supply Chain Security Management System

TAXUD – Directorate-General for Taxation and Customs Union (European Commission)

WCO – World Customs Organization

## **Introduction**

When my bachelor thesis began form in 2011, the topic of security was almost untouched in Czech literature. The paper was therefore predominantly focused on security issues, principles of security initiatives, research of existing projects, and estimation of economic benefits.

The Czech Republic, as an integral part of the European free trade zone, shares its external borders. Thus, it has to respect the security policy, and especially the businesses with third countries should follow a certain regime. In addition, just in 2012 the EU and the US signed an important document, strengthening international trade relations. It proved the globalization of security efforts and the dynamics of the security matter.

However, today's Czech research still does not pay greater attention to security, and, in comparison to safety, protection against illegal activities is still a minor subject to tackle.

Safety issues are naturally linked to the nature of transport, same as to any other satisfaction of human needs. The goal is to get passengers or goods transported safely from the point of origin to the destination, while avoiding damage of equipment, personnel, information, or any other resources necessary to carry out this transport.

This can be easily demonstrated on the example of a transport container. The focus will always be put on the load bearing capacity of the construction, prior to measures preventing concealing some undesirable material inside. This fact does not detract the relevance of security. Nevertheless, safety failure may occur simply due to the impact of physical laws or misconduct of the human factor. It is not caused by an intentionally performed act aiming at harm or loss.

Unfortunately, rapidly developing technologies do not serve only humans to facilitate and accelerate work. It is also misused by criminals as an effective instrument to commit crimes. Security initiatives are developing and expanding, and in recent years also interconnecting to joint systems of protection.

Due to the mentioned facts, a decision was made to focus the diploma thesis more deep on the security matters, in which I see the potential to support Czech companies and their international operation. The paper aims to provide a detailed exploration of the Customs – Trade Partnership programs.

# **1. Security Environment in International Transport**

## **1.1 Background**

At the turn of the century, the risk of loss, or detriment to the human life or property, during international transport of goods undoubtedly increased. Due to the historical development of ever-improving illegal activities, such threats generally rise over time. The 9/11 terrorist attacks in the US became a turning point, and investments into security were inevitable. The affected US became the main initiator of new security measures, responding to these events by restructuring government agencies, and began developing robust security defenses.

The outputs of my bachelor's thesis, containing a complex characterization, have clearly outlined that the security of shipping should not be perceived only as a protection to the physical movement of goods. An effective intervention should include the protection of all the elements within the supply chain. These elements are not limited only to carriers, freight forwarders and service providers, port facilities and airports, warehouses, interim storage facilities and container terminals. Security systems are also introduced to manufacturers, processing and distribution companies, in general to shippers, actively involved in trade and movement of goods along the international supply chains.

The basis of all the initiatives is the standardization of procedures, technology and behavior during regular operation, with regard to security. Naturally, the goal is to achieve a state when a potential security occurrence occurs very exceptionally, or does not occur at all. The focus is placed on the analysis of threats, discovering weaknesses in each element and the adoption of such measures to reduce the likelihood of adverse events.

If the security situation has already occurred, procedures should be in place to ensure timely, rapid and appropriate actions. The aim should be to eliminate danger, minimize the damage to health and property, and to restore the system to a standard operation within the shortest time possible.

Owing to modern terrorism and sophisticated practices of organized crime, additional investments into security are unavoidable. Security measures within the implementation of new programs undoubtedly have an impact on trading and transporting. They cause additional expenses, often reflected in increased prices, and may tend to slow down the trade. On the other hand, a membership can reduce insurance

costs or delays within customs procedures. And, last but not least, a membership can reduce product loss and protect the flows of goods from intruders.

In addition, program strategies also address the maintenance of trade continuity and free movement of goods and passengers, while running these measures.

## 1.2 Security Initiatives in the International Supply Chain

Following **Table 1** shows major security initiatives securing international trade and transport of goods.

**Table 1: Major Security Initiatives [Source: Lánská, Supply Chain Security]**

Abbreviation	Program Name	Description
ISPS Code	International Ship and Port Security Code	Comprehensive package of measures to enhance security of ships and port facilities in the supply chain. Intended to increase the flexibility of responding to the specific risk situations.
WCO SAFE	WCO Framework of Standards to Secure and Facilitate Trade	Unified global platform to assist customs administrations with implementation aiming both secure and facilitate world trade, in order to reap all the economic, financial, and social benefits.
ISO 28000	Standard ISO/PAS 28000	Global standard for management of supply chain security. Requirements include all aspects to ensure security of financing, production, information management, and equipment for packaging, storage and transfer of goods between vehicles and locations.
C-TPAT	Customs-Trade Partnership Against Terrorism	Joint effort of the U.S. government and businesses to secure importing goods into U.S., while facilitating trade and maintaining its continuity.
AEO	Authorized Economic Operator	WCO program of partnership between customs and trade, based on the platform of the WCO SAFE, aimed to protect goods importing or exporting to/from relevant country, while facilitating trade and maintaining its continuity.
TAPA	Technology Asset Protection Association	Association of security professionals and business partners cooperating to address threats to high-tech

		industries. The main vision is to reduce losses during production, transportation and distribution of products.
CSI	Container Security Initiative	Regime for prevention of illegal use of containers to transport undesirable freight. Containers intended for importation into the U.S, posing a potential risk, are identified and inspected, prior to loading, using advanced non-invasive technology.
Importer Security Filing – “10+2 Rule”	Importer Security Filing and Additional Carrier Requirements	Electronic submission of preliminary information about cargo transported to U.S. by vessel, improving the ability to identify high-risk shipments.
AMS	Automated Manifest System	Inventory and reporting system for freight transport, currently used only for manifests of air carriers. System reduces reliance on paper documents, and speeds up the processing of bills of lading and other declarations.
Pre-arrival/ Pre-departure information	EU Customs Security Program	Traders are required to provide the certain information about goods, prior to import or export to/from EU.
FAST	Free and Secure Trade	Contracts created to secure borders between U.S., Mexico, and Canada. Unification of processes for clearance of shipments, using principles of risk management, supply chain protection, industrial cooperation, and advanced technologies.
BTA	Bioterrorism Act	U.S. law, containing a number of provisions, designed to increase efforts on food security against possible bioterrorism attack.
APEC	Asia-Pacific Economic Cooperation	Forum of 21 pacific rim member economies, seeking to promote free trade, and economic cooperation throughout the Asia-Pacific region. Although it is not primarily security initiative, members adopted a risk-based approach with multiple layers of security, as a shared goal for secure the trade, and the travel system.



## **2. Customs - Trade Partnership Security Initiatives**

### **2.1 Background**

As outlined in the introduction, certain tragic events have revealed weaknesses and inadequacy of inspecting passengers and goods crossing state borders. It became clear that any disruption could cause significant losses reflected in various sectors from trade and tourism, through deferred or unrealized investments, to delays or rerouting flows, and many more in either direct or indirect way.

The response was a sharp tightening of security checks and required information. In particular, more frequent scrutiny and detailed documentation aiming to prevent potential adverse events caused a noticeable slowdown of cross border movement. This naturally slowed down the trade, implying loss of revenues, but also loss of customs duties, taxes, etc.

In such an undesirable situation, government agencies recognized the burden of measures should not be limited only to the phases of border crossing and loading/unloading of transportation means. It led to putting more effort in the protection of freight already at the point of origin, during the movement throughout the supply chain, up to the domestic borders.

Furthermore, during the first implementations of the newly created programs the government authorities found out that the only way to achieve a high security level is an involvement of all the elements along the supply chain, such as importers, carriers, manufacturers, warehouses and customs brokers.

On these facts, the first Customs - Trade Partnership Security Initiative was established in USA, followed by other countries.

## **2.2 Characterization and Principle of the C-T Partnership**

### **2.2.1 Environment**

The Initiatives based on the customs - trade partnership constitute one of separate groups of international security programs, and therefore show its specific features.

On one side, there are governmental authorities, aiming to prevent damage to health of civilians, or damage or loss of public or private property. Furthermore, the government also oversees the fulfillment of obligations, associated with international trade, such customs duties and taxes. Therefore, the government seeks to protect the transport and trade against any unlawful actions.

On the other side, there are companies, variously involved in the supply chain with a desire for the smoothest and cheapest transfer of their goods among the markets of different countries. Companies have a natural interest in protecting their property and employees. At the same time, they are reluctant to put money into investments with uncertain returns.

As tightened security measures, slowing down the trade and disrupting its continuity, are inevitable, a compromise comes as a cooperative partnership among businesses and customs administrations.

### **2.2.2 Obligations and Benefits**

Companies are required to comply with minimum security criteria in various fields within their operations. Moreover, certain information about the company has to be provided, such description of its activities, its business background, and its roles in the supply chain.

In addition to the demonstration of suitability, the company should also prove awareness about the security of their business partners. The company is expected to select its business partners also participating in the program or to require non-participants to follow appropriate security standards and exhibit behavior according to the program's security patterns.

In return for demonstrating credibility, predictable behavior and identification in the supply chain, the companies are rewarded by predetermined benefits. These include shortened waiting and accelerated customs clearance at the borders, reduced number of security checks, simplified documentation, information exchange with customs administrations and among other participants, etc.

### **2.2.3 Suitability for Companies**

Unlike some other security initiatives, C-T Partnerships are fully voluntary programs. For example, the ISPS Code provisions are binding for all governments within the member states of the International Maritime Organization.

So far, there is no security program requiring mandatory participation for all companies involved in international trade. However, there are companies requiring partners to participate. These are multinational corporations with a power to choose suppliers and thus enter into contracts with reliable and proven partners. Such cases can occur in the automotive industry or freight forwarding, when greater amount of service providers is taking part.

Therefore, it is up to each company whether to join the program. It may be an uncertain decision. Based on past experience, admission into the program requires a significant investment and subsequent operating costs. Companies need to compare the costs with potential benefits and profits arising with membership. [1]

Especially for voluntary programs the financial burden and economic returns should be considered. For individual companies, warehouses, terminals and other elements of the supply chain, it is desirable to evaluate the effectiveness of a particular program, taking into account the company's specifics.

## **2.3 Admission Procedure**

### **2.3.1 Eligibility**

The first step is usually to verify compliance with the eligibility conditions for membership. Not all businesses can become a participant. Taking part in the international supply chain might not be a guarantee of eligibility.

To demonstrate this, the eligibility requirements for the participation of a third party logistics provider (3PL) at the C-TPAT program, are [2]:

1. Be directly involved in the handling and management of the cargo throughout any point in the international supply chain, from point of stuffing, up to the first U.S. port of arrival. Entities which only provide domestic services and are not engaged in cross border activities are not eligible.
2. Manage and execute these particular logistics functions using its own transportation, consolidation and/or warehousing assets and resources, on behalf of the client company.
3. Does not allow subcontracting of service beyond a second party other than to other C-TPAT members (does not allow the practice of “double brokering”, that is, the 3PL may contract with a service provider, but may not allow that contractor to further subcontract the actual provision of this service).
4. Be licensed and/or bonded by the Federal Maritime Commission, Transportation Security Administration, U.S. Customs and Border Protection, or the Department of Transportation.
5. Maintain a staffed office in the United States.

From the foregoing, already the compliance with the eligibility conditions can indicate a considerable step for a potential applicant, such as changing business partners.

### **2.3.2 Minimum Security Criteria**

While the eligibility conditions often determine whether the enterprise itself is capable to participate, compliance with certain minimum security criteria is usually the most time-consuming and financially challenging part of the entry process.

A conducted research asking companies with experience in these programs showed that, at the initiation of the process of compliance, the companies had virtually none, or only few of the necessary security precautions. [1]

If the company does not have the required measures yet, it is unavoidable to invest in the physical provision of areas, facilities and internal enterprise infrastructure, physical measures maintaining the integrity of vehicles and cargo, training of employees and background screening for candidates, information systems and protection of sensitive data, and in other spheres associated with the activity to satisfy customer's needs.

Statistical outcomes of research also indicate an individual impact of a membership on each company regarding the amount of investment in contrast with perceived advantages and the overall perception of promised benefits for the company.

Most companies need considerable steps to comply with the minimum requirements. It may not occur to such an extent, where the company already meets standards of other certain security initiatives. For instance, C-TPAT minimum security criteria guidelines for MPTO (Marine or Port Terminal Operators) state the physical access control provisions are satisfied for vessels and port facilities by their compliance with the ISPS Code and MTSA (Maritime Transportation Security Act) regulations. [3] It may also be shown at the example of the AEO program, which also refers to internationally recognized standards in some areas. The following ISPS Code and ISO / PAS 28001:2006 standards are recommended to comply with the AEO requirements to prevent unauthorized access to goods during storage. [4]

Beside ISPS Code and WCO Safe Framework, the ISO standards are also globally accepted and widely utilized. They provide basic and proven practices to achieve a comprehensive supply chain security.

Mentioned ISO 28000 (Specifications for Security Management Systems in the Supply Chain) specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Supply Chain Security Management System (SCSMS), using a continual improvement approach. [5]

Unlike the ISPS Code and the WCO Safe Framework, ISO 28000 does not primarily represent a security program with typical features. However, the principle of demonstrating compliance with certain criteria in exchange for obtaining a certified status remains the same. Despite the fact the ISO security standards are voluntary, ISO member institutions also intervene in both government and private structures, where they create partnerships. The ISO standards can be considered a proven pattern for newly developing security programs.

The aim of new initiatives such as the C-T partnership programs is not to duplicate effective standards of other running initiatives and burden businesses by irrational and impractical requirements. The objective is to use them as a base to build on and to identify the best practices over time.

The topic of minimum security criteria is analyzed in detail in the last chapter of this paper.

## **2.4 Customs-Trade Partnership Against Terrorism (C-TPAT)**

In order to outline the fundamental structure of the C-T partnership programs valid for such programs, mostly general core principles have been described so far. It is from this perspective that the involved authorities, agencies and companies should perceive them, in terms of requirements, objectives and benefits that such programs entail.

As mentioned above, although the basic structure should remain the same, practical solutions for each program could be designed specifically. At this point it is appropriate to introduce a specific example.

### **2.4.1 Introduction**

In November 2001, the Customs Border Protection agency has established this voluntary government initiative to build cooperation for the strengthening of the international supply chain and support of the border security of the United States. C-TPAT is of the opinion the only way to achieve a high level of freight transport security is close cooperation with end-links in the international supply chain, including importers, carriers, customs brokers and manufacturers.

Through such cooperation with the international community, the initiative seeks to internationalize the fundamental rules and develop unified administration for relevant procedures.

C-TPAT also supports the CBP strategic plan in prevention of terrorist weapons entering to the United States, the DHS strategic plan in the effort to develop a national strategy for the protection of freight transport, and the strategy of the President for national security.

Initially, the project covered only trade routes into the United States. It has subsequently turned out that a disruption of the international supply nets at any point in the world could significantly affect and have a devastating impact. C-TPAT therefore supports the global economy and goes far beyond the borders of the United States, where it provides protection from production to distribution. Through C-TPAT, the CBP asks businesses to ensure the integrity of their security practices, communication and verification of procedures of business partners within their supply chains.

## **2.4.2 Objectives of the Program**

The CBP strategy within C-TPAT relies on a multi - level process that can be summarized into the following main objectives [10]:

### **Goal 1**

Ensure that C-TPAT partners improve the security of their supply chains pursuant to C-TPAT security criteria

### **Goal 2**

Provide incentives and benefits to include expedited processing of C-TPAT shipments to C-TPAT partners

### **Goal 3**

Internationalize the core principles of C-TPAT through cooperation and coordination with the international community.

### **Goal 4**

Support other CBP security and facilitation initiatives

### **Goal 5**

Improve administration of the C-TPAT program

## **2.4.3 Benefits**

C-TPAT offers businesses an opportunity to play an active role in the war with terrorism. By participating in a worldwide initiative, the companies gain greater security and speed for employees and customers. In addition to these general advantages, the certified member categories include [9]:

- ▲ Reduced number of inspections by the CBP (shorter delays at borders)
- ▲ Priority checking by the CBP (priority clearance at borders, if conditions allow)
- ▲ Assignment of SCSS - Supply Chain Security Specialist that will work with the company to validate and strengthen security throughout its international supply chain
- ▲ Potential eligibility for the CBP ISA program - Importer Self-Assessment program with an emphasis on self assessing
- ▲ Eligibility for participation at training sessions on supply chain security

## **2.4.4 Participants**



Participation is available for the following types of companies, involved in the international supply chain of the United States [9]:

- *Importers*
- *Air, Rail, Sea, and Truck Carriers*
- *Brokers*
- *Air Freight Consolidators*
- *Ocean Transportation Intermediaries*
- *Non-vessel Operating Common Carriers*
- *Port Authorities*
- *Terminal Operators*
- *Warehouse Operators and*
- *Selected Foreign Manufacturers.*

#### **2.4.5 Enrolment Conditions**

Participation requires the filing of a formal agreement that commits the applicant to undertake the following [9]:

- Conduct a comprehensive assessment of supply chain security using C-TPAT security guidelines developed by Customs and the trade community
- Complete and submit the supply chain security questionnaire to Customs
- Develop and implement a system to enhance security throughout the supply chain in accordance with C-TPAT guidelines
- Communicate C-TPAT guidelines to other companies in the supply chain, and work toward building the guidelines into relationships with these companies

#### **2.4.6 Implementation**

For greater security and facilitating the flow into the US, the CBP ensures that all partners fulfill their commitments by verifying the implementation of agreed security measures. [10]

CBP officers visit C-TPAT members around the world and verify that the security meets the C-TPAT minimum criteria and best practices, and procedures are reliable, accurate, effective, and comply with agreed standards.

The CBP encourages private sector to participate in the C-TPAT program, which is prerequisite for the program FAST and other CBP projects for expedited handling on borders.

#### **2.4.7 Minimum Security Criteria**

Companies willing to participate have an obligation to take certain precautions. Individually defined minimum security criteria to be found online for different types of participants [11]:

- Air Carriers
- Consolidators (Air Freight Consolidators, Ocean Transport Intermediaries, and Non-Vessel Operating Common Carriers (NVOCC))
- Customs Brokers
- Exporters
- Foreign Manufacturers
- Highway Carriers
- Importers
- Long Haul Carriers in Mexico
- Marine Port Authority and Terminal Operators
- Rail Carriers
- Sea Carriers
- Third Party Logistics Providers (3PL)

### **2.4.8 Risk Assessment**

5 Steps Risk Assessment Process is a recommended guide, in order to help participants carry out the risk assessment in compliance with the C-TPAT minimum security criteria. There is a guide available for these steps, elaborating some basic tips, resources and examples which should be considered and used during the risk assessment. The guide does not include all the information needed to ensure the requested security. Nevertheless, it contains helpful information.

The 5 Steps risk assessment process is as follows [12]:

1. Mapping cargo flow and identifying business partners (directly or indirectly contracted)
2. Conducting a threat assessment focusing on terrorism, contraband smuggling, human smuggling, organized crime, and conditions in a country/region which may foster such threats and rate threat – high, medium, low
3. Conducting a vulnerability assessment in accordance with C-TPAT minimum security criteria and rating vulnerability – high, medium, low
4. Preparing an action plan
5. Documenting how risk assessments are conducted

### **2.4.9 C-TPAT Manuals**

The Supply Chain Security C-TPAT Compliance Manuals are comprehensive guides, helping step by step to design and implement a security policy in correspondence with specific requirements of a particular company. The essence lies in the understanding of the company's procedures and exposure to security risks and threats. Manuals lead the implementation of a comprehensive system that meets all the CBP requirements for the program.

The manual contains 12 key topics from physical security, personnel security, access control, education and training up to documentation policy. Since the security requirements vary for different types of participants, manuals also differ depending on the specific operations of particular company.

#### **2.4.10 Annual Security Profile Review**

After signing the contract and approval of the partnership, the participant has to perform an annual self-assessment to provide the security profile of the company, later listed in the program secure web portal.

With the signature, these comes an obligation to provide an annual report of the security profile and update information about the company. Such review provides valuable information for the specialist (SCSS - Supply Chain Security Specialist) who prepares the company for the upcoming validation, and allows to re-evaluate the current security policies.

#### **2.4.11 Validation**

Validation is a process by which the CBP meets company representatives and visits domestic and foreign locations in order to verify the measures contained in the security profiles of the participants. These security measures are accurately determined and should be respected. Checks by the CBP are not considered audits.

The main objective is to ensure that the security profiles of the companies are reliable, accurate and effective.

Validation also provides a forum, where discussions about the problems of supply chains and sharing "best practices" can be carried out. The CBP and the participants can build a stronger partnership and jointly develop solutions for potential weaknesses.

The nature of such verification encourages the CBP and C-TPAT participant to better understand the roles of each other in protecting borders from international terrorism.

Validation is targeted precisely and concisely. The duration should not exceed 10 working days of the company. Nevertheless, in some cases, it can take up to two weeks due to planning and traveling.

The CBP verifies the profiles of C-TPAT participants in accordance with the requirements of the port security (SAFE Port Act). This law requires validation within one year from the certification of the company. [13]

The order in which the profiles are selected for verification is based on the principles of risk management. Validation can be initiated by the volume of imports, security anomalies, based on the strategic threat characterizing the geographic area, or on other

information related to risk. Some verification processes can also be done as a matter of routine supervision.

Satisfactory conclusions of validation increase the level of the benefits provided to the involved importers. However, if the conclusions reveal serious shortcomings in the fulfillment of the criteria, some or all benefits may be suspended or removed until corrective measures are taken and verified.

## 2.5 Mutual Recognition of the C-T Partnership Programs

### 2.5.1 Background

The C-T Partnership programs were primarily designed to reinforce the function of state borders, generally to prevent entry of undesirable goods or persons, or any illegal border crossing such as imports of contraband, illegal immigration, refugees, etc.

The first C-T partnership program was C-TPAT, originated in frightened and heavily damaged US by the terrorist attacks in 2001. In 2005, the global customs community also responded to the events by adoption of the WCO Framework of Standards to Secure and Facilitate Trade. This unified platform was designed to assist customs administrations with the implementation of measures to protect international supply chain and facilitate trade. Despite its being voluntary and non-binding instrument, many WCO members have committed to adopt the Safe Framework or promised implementation of appropriate measures. [6] Thus US C-TPAT was later followed by the introduction of the Authorized Economic Operator programs in other countries, as one of the pillars of the WCO Safe Framework. Some of these are Canada, New Zealand, Japan, Korea, Hong Kong and European Union.



**Figure 1: Logos of AEO EU, Korea, Japan, Hong Kong and Taiwan**  
[Source: cargoservicesgroup.com, ktcintl.co.kr, nikkeikinholdings.com, info.gov.hk, uctc.com.tw ]

After a certain period of implementation and a course of new programs, it became more and more evident that especially companies with extensive business relations in various countries will be burdened by similar requirements of different programs. Hence, the concept initially created to simplify and maintain the fluidity of the market, could become impractical.

Therefore, a trend of future agreements on mutual recognition of certified statuses was predestined to be born.

### **2.5.2 Definition of Mutual Recognition**

The CBP and TAXUD very aptly defines mutual recognition as an agreement by which each party recognizes the compatibility of the other party's trade partnership program, and agrees to treat the holders of a membership status under the other customs authority's program in manner comparable to the way it treats members in its own program to the extent practicable and possible. [7]

For the basic understanding, the TAXUD definition describes the essence of mutual recognition very well.

When every participant of the supply chain is a mutually recognized as secure (in relation to certain rules), it should reduce threats and likelihood of adverse events for the whole system. Nowadays, mutual recognition is part of the C-T Partnership program's strategies, aiming to increase efficiency and reach facilitation and acceleration of trade, while securing the entire supply chain. The MT process of some programs can be carried out on bilateral, regional or potentially global levels.

### **2.5.3 Concerns of Mutual Recognitions Processes**

Unfortunately for the current situation, when the C-T Partnership programs began to develop, regions and states that have decided to follow this concept approached the issue on a relatively individual basis. This obviously carries certain complications in the synchronization processes of the programs. The case of MT between the US and the European program raises the following difficulties:

- *Development of equivalent measures*  
Efforts of countries should lead to the development of equivalent measures and security levels, while encountering challenges arising from geographical, political, technological and legislative aspects and specific risks and threats in the country or the region. [6]

- *Import and export*

The AEO certification applies to both import and export operations, while C-TPAT was established focusing solely on imports. This evident deficiency from the US program forced the CBP committees to discuss and prepare a development.

- *Data processing*

Ensuring timely exchange of relevant data between customs administrations is very important. The AEO status has to be taken into account during risk analysis, where the holder can take advantages from the promised benefits. It carries a need to standardize unique identifiers for the holders of a status. These are MID (Manufacturer Identification Number) used by C-TPAT and EORI (Economic Operator Registration and Identification) used by AEO.

It is proper to note, the structures of some programs undergoing the MT process have more distinctions than others. Therefore, the course of mutual recognition may be individual, such as the case of C-TPAT and AEO, in comparison to MT of single AEO programs in individual regions.

#### **2.5.4 Benefits of Mutual Recognition**

Broadly speaking, benefits derived from a C-T partnership within a single program are extended by MR to an additional territory of the state or the region by complying also with its security requirements and policy.

Besides businesses, also customs administrations benefit from MR, as indicated in the following summary:

##### **MR Benefits for Businesses**

- *Common standard*

Participants in programs under MT only have to conform to one set of security requirements. As shipment occurs in different countries during movement through the international supply chain, MR is avoiding the burden by different sets of security requirements. [7]

- *Reduction of validations*

Companies are no longer validated twice. MR is avoiding unnecessary duplicate processes. C-TPAT and AEO could be illustrative example again. For companies operating transportation between the US and the EU, membership in both initiatives means double validation and revalidation.



- *Reduction of inspections*

A certification, recognized by both programs is used as a risk-assessment factor in automated targeting systems. A holder of a status authorized by other customs administration will be considered favorably in risk assessment by domestic customs administration. [7] Reduced risk score will be reflected in number and extent of conducted inspections, leading to a quicker release of goods and priority treatment.

- *Marketability*

The status holder will be recognized as secure and reliable by both countries under the MT. This badge of quality helps to increase the brand equity and the global reputation. Company can also obtain collaboration with relevant business partners seeking cooperation with certified suppliers, and gain new lucrative opportunities around the world. Many holders of AEO status have indicated they applied for the program only due to the vision that MR of the AEOs among major trading partners will soon be more widespread and lead to benefits. [6,7]

### **MR Benefits for Customs Administrations**

- ▲ *Simplification of validation process*

Before obtaining the status, authorized personnel have to make a validation visit to verify compliance with minimum security criteria. When the company is already certified by one program, such a visit during the certification of the second program no longer needs to be conducted. [7]

- ▲ *Saving resources*

Customs authorities do not have to expend limited resources by sending staff overseas to validate a facility that has already been certified by the second party. Sharing and exchange of information to target high risk shipments allows greater focus and more efficient use of scarce resources. [6,7]

- ▲ *Transparency in international commerce*

Closer collaboration, among customs administrations and between customs administrations and trade partners, should lead to higher transparency in operations of international commerce. Similar security platforms and exchange of information between partners expedite and facilitate commerce. [7]

### **3. Gutiérrez and Hintsa Model**

#### **3.1 Background**

Since 2001, security initiatives have been developed at different levels, in different regions, by varying degree of interdependence.

In 2008, Supply Chain Security Initiatives: A Trade Facilitation Perspective was published as one of the first studies providing a comprehensive picture of security initiatives and its development from the turning point in 2001. In the subchapter Supply Chain Security Management the authors refer to the scientific paper of researchers Ximena Gutierrez and Juha Hintsa.

In this paper, the authors describe the individual security initiatives, comparing the content. The key for comparison is a generic model designed above all major initiatives, serving as an analytical instrument to assess security criteria and requested minimum standards of the individual programs.

#### **3.2 Model Structure**

The model, so-called General Supply Chain Security Management Framework, divide security standards into 5 basic categories: which are Facility Management, Cargo Management, Human Resources Management, Information and Communication Management and Business Network and Company Management Systems. [11]

Subsequently revealed, in addition to preventive measures, the fundamental pillars of Supply Chain Security Management (SCS) should also include measures for most efficient and quick remedy of damages, caused by events which failed to be averted. Therefore, the model was supplemented by the sixth category called Crisis Management and Disaster Recovery. All six fundamental categories of the general SCS model are shown in **Table 2**.

**Table 2: Categories of Supply Chain Security Management System**  
 [Source: Gutiérrez; Hintsa, Voluntary supply chain security programs]

<b>Category</b>	<b>Subcategories</b>	<b>Description</b>
<b>Facility management</b>	<ul style="list-style-type: none"> <li>• Warehouse layout</li> <li>• Inventory management and control</li> <li>• Facility protection</li> <li>• Facility monitoring</li> <li>• Access control</li> </ul>	Guaranteeing the security of the facilities where cargo is stored and handled.
<b>Cargo management</b>	<ul style="list-style-type: none"> <li>• Prevention, detection and reporting of anomalies</li> <li>• Inspections</li> <li>• Exploitation of cargo inspection technical solutions</li> <li>• Exploitation of cargo tracking technical solutions</li> <li>• Exploitation of cargo and vehicle anti-tampering solutions</li> </ul>	Protecting cargo during all shipping and transport processes.
<b>Human resources management</b>	<ul style="list-style-type: none"> <li>• Employee hiring/exit process</li> <li>• Personnel training</li> <li>• Information dissemination</li> <li>• Organizational roles and responsibilities</li> <li>• Security culture development</li> </ul>	Guaranteeing trustworthiness and security awareness of all personnel in direct and indirect contact with cargo and other company assets.
<b>Information management</b>	<ul style="list-style-type: none"> <li>• Quality of information and data management</li> <li>• Protection of business information/data</li> <li>• Recordkeeping of shipping information</li> <li>• Data exchange with Customs Administrations</li> <li>• Use of international standards for data management</li> </ul>	Protecting critical business data and exploiting information as instrument for detecting illegal activities, and preventing security breaches.
<b>Business network &amp; Company management systems</b>	<ul style="list-style-type: none"> <li>• Company security Management system</li> <li>• Logistics system designed to reduce daily operational risks</li> <li>• Logistics system designed to guarantee quick disaster/failure recovery</li> <li>• Business partners evaluation system</li> <li>• Collaborative relationships with authorities</li> </ul>	Building security into internal and external organizational structure and company's management systems.
<b>Crisis Management and disaster recovery</b>	<ul style="list-style-type: none"> <li>• Business continuity plans</li> <li>• Formal security strategies</li> <li>• Emergency control centers</li> <li>• Incident management</li> </ul>	Managing complex environment of supply chain facilities.

### 3.3 Features of the Model

It may seem that the structure of the model selects basic elements contained in all the examined programs. The reality is slightly different. The authors have identified three important features [11]:

▲ *Extent of the Provided Information*

Requirements for security standards are presented with varying degrees of specificity. While some programs provide a complete list of activities, processes and technologies needed to be implemented, others provide only a small list, putting the onus on each company to enforce the security measures they consider necessary according to their constraints.

Nevertheless, most programs promote security measures targeting one or more goals, based on the mentioned fundamental elements.

▲ *Possibility Compliance with Standards in Different Ways*

For instance, Information Management is a combination of procuring high quality cargo information, stored adequately, shared with the pertinent partners and protected from unauthorized access. However, high quality cargo information can be also achieved by implementing error-proof documentation processes. Taking into account this fact, but still retaining the essence of a common supply chain security management framework, the authors have extended the fundamental elements of subcategories displayed also in **Table 2**. The model has gained an appropriate level of detail, but still remains general enough to serve for comparison.

▲ *Usefulness of the Framework*

The designed framework has covered most of the security measures suggested by major security programs. However, the authors emphasize there is no exact pattern to establish an adequate supply chain security management system. The implementing of all measures does not necessarily mean the security system becomes complete. At the same time the implementation of only some of them does not necessarily mean the security is inadequate. Thus, the framework provides a better understanding of the suggested measures and can be used to evaluate the similarity of these programs.

### **3.4 Application**

A united framework of required standards could be a useful instrument for projects of mutual recognition. It can help to organize the required minimum standards and divide them into basic categories and subcategories, clearly defined and easily comparable.

Here the question arises whether all programs are comparable. Among 9 surveyed programs, the average percentage value of conformity, within 5 basic categories and subcategories, ranges around 54%. [11]. It should be noted here that these results, with such a range of programs of different origin and character, are not surprising.

More interesting results could be achieved by comparing only two C-T Partnership programs undergoing projects of mutual recognition. Customs and government authorities could use the generic framework as a collection of current best practices. These could be then customized and adjusted to the particular project and situation. Conformity will be then assessed by a calculated coefficient, showing a degree of compatibility.

Such an instrument could also become a helpful guide for enterprises seeking to obtain a certified status. According to this guide, they would verify and demonstrate their compliance or non-compliance with the requested minimum criteria.

## **4. C-T Partnership Programs Criteria Analysis**

In this part, we analyze the structure of the programs in more detail, and tackle one of the main tasks of the thesis. The fourth chapter is specially focused on the processing and analysis of minimum security requirements, and all related matters and pitfalls.

To acquire objective answers, obtaining empirical data and experience became inevitable. For this reason, several visits were made to the Customs office in Ceske Budejovice, the center of the AEO certification for the entire country.

Thanks to thorough consultations, the missing information has been obtained. Discussions have been led especially on the subjects of security audit, program implementation, program operation and management, but also mutual recognition with the US program. The acquired data were subsequently processed and analyzed.

Without such experience from practical environment, the issues in this chapter could not be credibly addressed.

### **4.1 The Issue**

There are several uncertainties which were appearing already during the research for bachelor's thesis and which have accumulated with further examination of the security field. It has brought some questions this practical part should seek to answer. Some of the main issues are:

1. Compatibility of C-T Partnership Programs
2. Actual convenience for various types of businesses
3. Identification of an unified model for self - evaluation

## **4.2 Compatibility of C-T Partnership Programs**

For this consideration we should take into account two messages outlined in the introductory chapters.

First, although security programs, across the regions, represent the same concept, it has been designed and implemented with certain differences. Second, within mutual recognition, customs administration surrenders the possibility to perform its own assessment of a company, using the benefits according to the status given by other customs administration.

Thus, several questions have been raised, such as what are the eligibility criteria for a merger, does it bring any adjustments to the security criteria, does it need a single frame, what is the cooperation of both participating sides etc.

There is a question how to measure the degree of comparability, compatibility, and thus the feasibility of mutual recognition of C-T Partnership Programs.

The transatlantic cooperation of the US and the EU programs is one of the recent MR executed. Such an arrangement should be a good practical example and provide some explanations.

### **4.2.1 Mutual Recognition of C-TPAT and AEO**

The document (MR) was signed in Washington on May 4, 2012. By this moment, the US C-TPAT and the EU AEO have established their trade security partnership.

So far, the MR has been divided into several sequential phases. On July, 2012, the CBP started providing a reduction in the targeting score for AEO companies, exporting to the US. The CBP also accepted the AEO certificates of the EU based facilities as a replacement for a validation visit. In phase 2, on January, 2013, the EU started providing a targeting reduction for C-TPAT importers also exporting to the EU.

C-TPAT signed its first MR arrangement with New Zealand in June, 2007, followed by similar arrangements with South Korea, Japan, Jordan, Canada, the EU, Taiwan, Israel, and Mexico.

### ***Prerequisites***

To avoid wasting time and resources, the parties aspiring for MR should be adequately prepared. Before the CBP begins to discuss MR with the foreign Customs Administration, eligibility requirements must be met [14]:

1. *Operational Program in Place*

The foreign Customs Administration must have a full-fledged operational program in place – i.e. not a program in development or a pilot program;

2. *Methodology in Place*

The foreign partnership program must have a strong validation process, built into its program;

3. *Security Component*

The foreign partnership program must have a strong security component, built into its program;

4. *Customs Mutual Assistance Agreement*

The foreign Customs Administration must have a Customs Mutual Assistance Agreement (CMAA) with the US;

### ***Mutual Recognition Process***

The C-TPAT MR process involves [14]:

1. *Side by side comparison of the program requirements*

Designed to determine if the programs align on basic principles, and to determine if there is a security aspect in the program;

2. *Joint validations in both countries*

Pilot program of joint validation/observation visits; this is designed to determine if the programs align in basic practice;

3. *Formal signing of a Mutual Recognition Arrangement (MRA)*

4. *Implementation*

Development of MR operational procedures, primarily those associated with information sharing;



#### **4.2.2 C-TPAT Mutual Recognition Compatibility Matters**

Here, an example of differences in the approach when developing programs in different regions can be found.

##### ***Different Approach***

The CBP, responsible for the protection of borders and international trade, have created a program primarily focused on the flow of goods into the country. The American concept resembles an onion of which layers form a robust protection system that, via borders, isolates the country from anything undesirable. The 9/11 tragic events that indicated a failure of checks and protection of vehicles destined to the US were the major cause, for such an approach.

The CBP admitted that an effective protection can be reached only by efforts extending far beyond the borders, to the countries of the goods' origin. However, C-TPAT still kept its focus on import only. And since the AEO programs, based on the WCO Safe Framework, deal both with direction border crossing flows and with protection more globally, in the context of MR, certain synchronization had to be considered.

Furthermore, as C-TPAT has continued its evolution, the important role of exports in international supply chains has also become apparent. Developing a C-TPAT Export Component would further enhance both the program and its relationship with other mutually recognized foreign Customs Administrations. [15]

Thus, on July 9, 2014, the CBP released the eligibility requirements and security criteria for exporters, as part of an effort to approximate an AEO type program, similar to those maintained by customs authorities of some of the largest trading partners, including Europe and Japan.

### ***EORI to MID***

To allow AEO certified manufacturers and suppliers to benefit from a lower risk score in the CBP risk assessment system, identification instruments has had to be unified. In the American system, the risk assessment is transmitted through the manufacturer's identification number (MID). Therefore, MID has to be paired with the EU EORI numbers and then the benefit is provided within the CBP system.

These EORI registered numbers are used in communications with customs authorities in the EU, for example in customs declarations or when providing pre-arrival/pre-departure information where identifiers are required. The first problem occurred when European AEOs had to register in a database and associate their EORI with a MID. But while EORI was provided by operators involved in import, export, and transit procedure, C-TPAT provided MID only to foreign manufacturers.

Actually, the identification problem concerned both parties, because all available cargo reporting systems identified primarily importers, exporters, consignors and consignees, but not other players such as port operators, customs brokers, warehouse keepers and manufacturers. Therefore, systems introduced later were expected to be amended, in order to share data among other participants in the supply chain. [6,8]

## **4.3 Actual Convenience for Businesses**

### **4.3.1 Generally Speaking**

We have already spoken about the need for an profitability assessment before the company's decision whether to enter the program or not can be made.

It could be stated with confidence, that any inclusion in such a project is definitely the right decision. Clear information about the company and an identification of its supply chains always create good reputation for the company, improve relations with state authorities, and help gain significant trading partners and external suppliers.

Additionally, by mutual recognition, the governments give an indication of trying to cooperate, and unite security efforts across the world. The globalization of security initiatives results in secure international supply chains increasing the efficiency and accelerating international trade. Such an arranged business network of recognized entities may follow the principles of customs unions. These unions are isolated from external environment by robust measures, where entry into the area means scrutiny and evaluation, while free trade flows inside.

### **4.3.2 Individual Point of View**

However, idea of global benefits cannot naturally be considered as a sufficient argument for the decision to participate.

A company is an economic entity, led by its financial indicators. Therefore, programs are primarily taken as an investment with a certain return and corresponding benefits. Each business must realize its share in international trade and define or at least estimate what exactly are the benefits from the certification, hence what it all means for its business, in terms of time and money.

Empiric data from customs officers have identified some features. Participation is almost vital for contractors of large industrial enterprises and conglomerates. Especially, when the majority of the production goes to such a significant customer, and ensures sales for a long time in advance. The big players are in position to choose reliable and verified partners. They often require compliance with certain standards and in case of non-compliance, they may replace the supplier.

In the same manner, companies can evaluate the benefit of Mutual Recognition. One respondent company has reduced the time associated with issues, related to importing

goods from the US to the EU from 4 days to 4 hours. Even without detailed knowledge of the company's activity, one can consider what a difference 92 hours can make:

▲ *Personnel Costs*

- drivers, security
- dispatching

▲ *Storage and Operation Costs*

- rent / complementary services / deposits

▲ *Technological Supplies Costs (foodstuffs, substances and material)*

- maintaining temperature conditions (cooling, heating)
- expiration
- ripening (cheeses, beer)
- drying (wood)
- dangerous substances (special treatment, security)

▲ *Competitiveness*

- increased - revenue / profit / mark-up / response to demand
- decreased - costs / price / lead time / bound capital

## **4.4 Identification of a Unified Model for Self-Evaluation**

This subchapter is an important practical part of the thesis. The aim is to provide an experience-based comprehensive guidance for businesses seeking the certification.

### **4.4.1 Stimulus**

The programs provide potential applicants with aids for the successful preparation for the necessary required measures.

Certainly, the first and the most important ones are the official guidelines containing the precisely defined regulations. In addition to basic documents, there are some materials provided as a guide to proper understanding of terms and interpretation. These are usually explanatory notes, frequently asked questions, and other instructions. AEO has even published a special overview of risks that need to be taken into account in which all the frequent and recurrent deficiencies are emphasized.

On the market, there are also companies promoting and selling manuals especially designed for the successful implementation of the required measures. There are even private entities providing consulting services. For considerable charges, they work with companies with a promise of complete preparation to pass the audit, and gain a certified status.

However, several cases show that even a consultant was not a guarantee of success and compliance with all the points, and the certification was not reached. For the AEO certification, a failure to comply with any of the minimum criteria, at least to a certain extent, means the conditions for obtaining the status have not been met. Nevertheless, the company gets a deadline to correct the deficiencies. The consultations have pointed out that when a hired person performing the compliance is not experienced enough with implementations, the project can end up with incomplete execution, wasting time and money.

The AEOs that operated import or export with the US could be noted as another case. They all became the subject to the participation in C-TPAT to avoid the strict inspections and associated delays. The evaluation methodology of compliance with the criteria for C-TPAT differs from the AEO one:

- AEO considers the security system slightly more complex, each point of minimum criteria has to be satisfied at least to a certain extent, otherwise the status cannot be granted.

- C-TPAT evaluates various areas proportionately. This means that the shortcoming in one point may be compensated by a higher degree of compliance elsewhere.

The preceding description is simplified, but, again, we encounter the problem of varying approaches in designing programs, fortunately disappearing thanks to the projects of Mutual Recognition.

Based on these facts, it has been determined that it is appropriate to establish a simplified model. Based on empirical data, such an instrument is a consolidation of practical experience during the audits, arranged into a clear structure. It will help companies avoid the most common mistakes and weaknesses in the process of obtaining a status.

The reasons could be summarized as follows:

### **1. Mutual Recognition**

Expansion of MR projects (especially AEO), connecting regions and the international commerce, will ensure that by obtaining of AEO certification, the company will enter into a system of interconnected programs, sharing the relevant benefits.

### **2. Individual Approach of Auditors**

The whole AEO is based on the basic structure of the WCO Safe Framework, and controlled by one body, the European Commission, based in Brussels. However, auditors can accommodate assessment of compliance slightly subjectively. In principle, the strictness should be hopefully the same.

Dealing with the human factor, it cannot be guaranteed that what one auditor rejects, it is not considered sufficient by another. Likewise, a difference may appear in a different emphasis placed on some of the criteria, as well as in the focus on the individual points against the focus on the overall security of the system.

Therefore, it is important to identify a base, constituting the necessity for success, whatever the scale is.

### **3. Provision of a Useful Aid**

Through the instrument, the interviews, conducted with customs officials, should be indirectly mediated to future candidates. Actually, it should

summarize all the issues that would later be very likely the subject of corrections during the real visit of the customs auditors.

## **4.5 Draft of the Unified Model**

The model is created according to the analysis of an auditor's experience and based on the principles of Authorized Economic Operator, a pillar of the WCO Safe Framework. As a worldwide extended initiative, under the patronage of the World Customs Organization, AEO forms a comprehensive security scheme, and comprises the majority of the running programs.

### **4.5.1 Data Acquisition**

Customs officers were interviewed mostly by open-ended questions. The discussed topics followed the general Gutiérrez and Hintsa model, which had previously been slightly customized. 6 basic sections of the general model remained the same, but the appropriate AEO security requirements corresponding to certain AEO regulations had been assigned to the subsections.

All the interviews were held in connection with the audit process, i.e. from its preparation on the side of a company and self-assessment, as well the data analysis from the side of the Customs Administration, to the course of the audit during the visit and final evaluation resulting in granting a certification or not.

Finally, step by step, all the 6 main sections were talked about. The questions were asked in the following manner:

- Which security requirements do you consider for this particular section? (Facility Management, Cargo Management, etc.)
- Do you find the requirement more crucial/superior in comparison to others?
- Can you compare the severity of requirements?
- Can you identify areas that are so crucial, that applicants cannot be successful unless they meet them?
- Can you identify deficiencies that occur more frequently, or/and in most cases?

#### **4.5.2 Analysis and Classification of Data**

After collecting a sufficient sample, the data was analyzed, sorted, and assigned to the sections of the model. Within the sections, the edited subsections were linked with new identified appropriate security measures, and put into order.

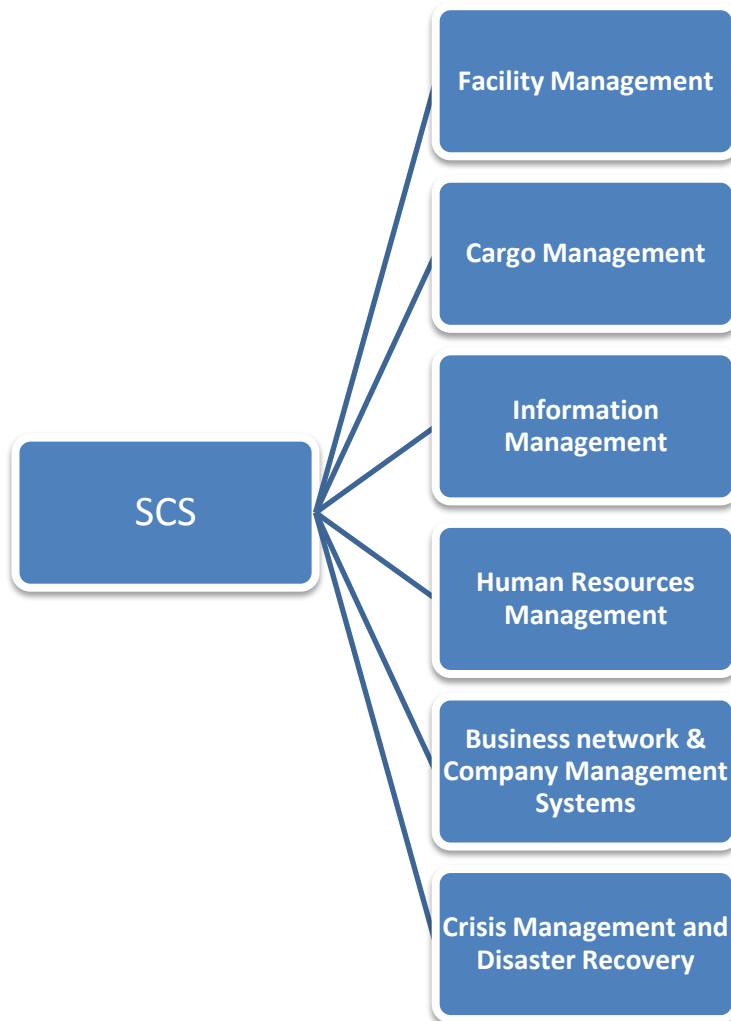
These new, sorted data clearly represent clearly recognizable measures for which the company should be able to determine whether it is in place or not. Therefore, these measures constitute the significant elements which customs officers will surely investigate during the audit.

Each section is assigned with an interpretation that highlights the important aspects which should be taken into account. This comment also points out the frequent shortcomings and offenses.



### 4.5.3 Outputs of the Analysis

The outputs are presented in the table form, where each section of the Gutiérrez and Hintsa model is assigned to the appropriate measures, supplemented by an interpretation. **Figure 1** shows the general Supply Chain Security Management System (SCS), dividing security criteria into six main sections.



**Figure 2: Diagram of SCS**

[Source: Gutiérrez; Hintsa, Voluntary supply chain security programs]

The following part contains an interpretation, supplemented with measures for all six individual sections. A sample of the classification into individual sections, demonstrated on facility management, is shown in **Figure 2**.

## ***1. Facility Management***

### *1.1. External borders*

- ▲ External border is one of the main subjects tested; The inspection verifies the compliance and compares the results with the self-assessment, a preliminary performed by the company;
- ▲ It is crucial that outer boundaries are coherent (nothing else than fences and entrances); it is desirable to minimize the number of entry points, better guarded;
- ▲ Importance of a CCTV system; CCTV is standard equipment, but not an obligation; The best solution is a video surveillance with online access monitored by a security agency; CCTV system could be alternatively replaced by a confluence of other measures, e.g. circuits of patrolmen; parts of audits can be carried out just from the records of CCTV by monitoring the operation at the gates, warehouses, etc.



**Figure 3: Warehouse surveillance [Source: [logistika.ihned.cz](http://logistika.ihned.cz)]**

- ▲ Maintenance of outer borders - forests, trees, tall grass should be maintained that an intruder can be seen and clearly identified; customizing the type of fencing to nature surroundings; sometimes the installation of infrared or radio locators fences;
- ▲ Buildings and building materials mostly match the requirements, although guarding of the entrances (doors, windows) should not be underestimated;

- ▲ A particular case when the building is part of the external border – need to put emphasis on the object isolation – grating, CCTV, taking out the door handles; example – when a company does not operate in its own area but within an industrial building where it rents spaces;
- ▲ Premises should be divided into zones and sections, with the degree of associated risk; within these zones the access and authorization should be clearly defined;
- ▲ **Desirable conditions** – online CCTV system, security agency in place, ideally patrolling the perimeter; circuits should have irregular periods and irregular routes, with chip reader spots; readers detect when and whether the guard was in place, and records should be made and kept; the outer borders should be constantly monitored;

Category	Sub-category	Measures
<b>1</b> Facility Management	<b>External borders</b>	Limited number of gates and entrances
		Guarding of gates and entrances
		External borders including buildings - sealing of windows, doors
		Outer perimeter
		Other exits and gates - locks, seals
		Other exits and gates - cameras
	<b>Lightening</b>	Maintenance of external borders - forest, grass, vegetation
		Outer perimeter
		Gates and gateways
	<b>Access of persons, vehicles and goods</b>	Ramps
		Permanent monitoring of frequent spots
		Gatehouse
		Video surveillance
		System of authorised persons
		Preliminary cargo information
	<b>Parking of private vehicles</b>	ID tools - badges, chips
		Separate parking outside the perimeter
		Separate parking within the area
		List of vehicles with permission
		Vehicle clearly marked - cards, labels
Distinguishing of temporary and permanent permits		
<b>Internal physical security</b>	Distinguishing manager and workers vehicles	
	Clear identification - badges, labels	
	Clear identification - uniforms	
	Clear identification - chips, chip cards	
	The system detecting unauthorized access	
	Records of personnel movement	
	System of keys	
Random checks of employees - opening bags, car trunks		
Zones and sections with restricted access		

**Figure 4: Facility management – classification of security measures**

## 1.2. Lighting

- ▲ During the audit, lighting is one of the most peripheral matters; any additional lighting projects are usually not a problem;
- ▲ Great importance when lighting is part of overlapping measures to secure location (night cameras versus appropriate light and cameras); gates and perimeter lighting; external border lighting in case of security circuits – need for proper visual inspection of a guard – without sufficient lighting, the security system loses efficiency;
- ▲ Specific lighting should take place on the ramp to check whether the reception/expedition of goods is performed correctly;



**Figure 5: Fenced and enlightened outer perimeter [Source: cast-lighting.com]**

- ▲ Evaluation should take into account the daytime of cargo flows to / from the area (can take place mainly during the day, night inactivity – thus no need to put as great emphasis);
- ▲ A problem to deal with, when the company is not the owner of the area, requirements for isolation should be satisfied at least to certain extent;
- ▲ Audit methodology: visual inspection at night; screening the records of the CCTV the night operation;
- ▲ **Desirable conditions** – appropriate lighting, supported by online CCTV, monitored by security agency; alternative to the CCTV system, are circuits on a well-lighted perimeter;

### 1.3. Access of Persons, Vehicles and Goods

- ▲ Permanent guarding and surveillance of frequented spots;
- ▲ It is crucial to have a system of authorized persons, responsibility for security (particular area, particular period, particular authorization); mostly gatehouses in place, where the security service is usually based;
- ▲ There should be a direct correlation between the frequency on spot and the level of security (frequent spot should be secured by an authorized employee, badges and/or chip card readers, CCTV, while a small side gate should be secured by a reliable lock, possibly a camera, and a security seal);
- ▲ Preliminary information about incoming shipments (especially when coming from the third countries) – security services at the entrance decide how the incoming goods should be treated, even after working hours – security workers should know exactly how to behave (accept, guard, forward to logistics department, park truck / trailer to a special spot inside the area); security workers should preliminarily know the customs status of the goods, and know the procedures;
- ▲ **Desirable conditions** – permanent securing of frequented spots, clear system of authorization and responsibilities; all security employees should know the procedures when various events occur;

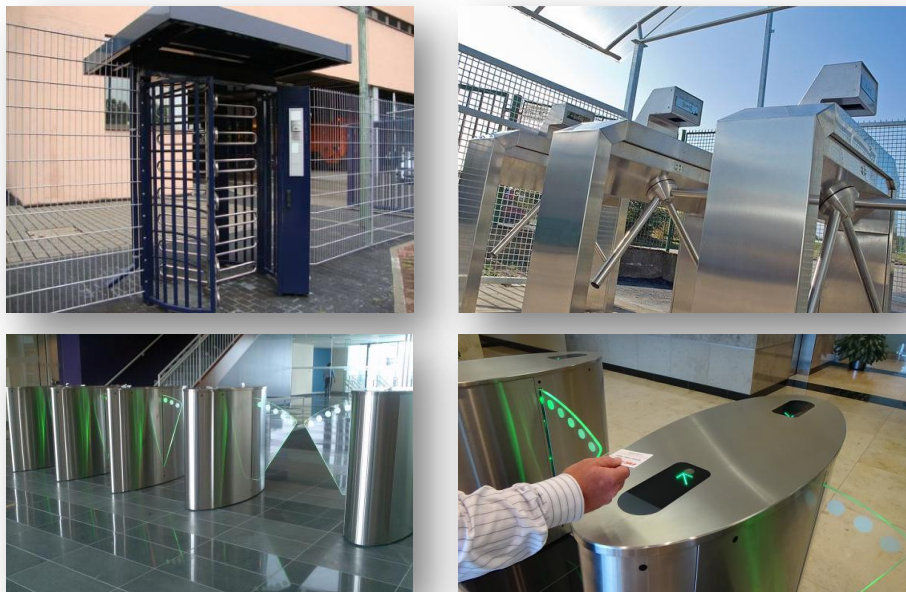


Figure 6: Solutions for restricted access [Source: airport-int.com, boonedam.us]

#### *1.4. Parking of Private Vehicles*

- ▲ Preventing loss or theft by private cars parked nearby or in the risk zones and sections; these parking areas preferably completely separated, or an introduction of a strict security regime;
- ▲ The importance of having a list of all vehicles, best to be complemented by IDs uniquely identifying the vehicle and its authorization, especially for cars with a foreign registration number;
- ▲ Clearly defined permissions, differentiated whether to permanent or temporary;
- ▲ Requirement for the separation of the management and others, and linking parking lots with registration numbers;
- ▲ **Desirable conditions** – regime in place to prevent adverse activities, using private vehicles; to have an awareness and knowledge of all vehicles and its owners entering into the area;

#### *1.5. Internal Physical Security*

- ▲ Access only to persons with a proven identity; for unambiguous identification the chip technology is the most desired option – the employee is able to reach only the sections for which they are authorized;
- ▲ Color distinguishing uniforms – e.g. warehousemen in a green; possibly supplemented with badges, cards, etc.;
- ▲ Audit methodology: random selection of employees, and examining the correctness of the card access settings for particular areas; testing unauthorized access attempts, and its identification in the system;
- ▲ Division into zones and sections with a clearly stated policy of access;
- ▲ System of keys – awareness how many keys are in circulation, measures against making of copies; keys are nowadays replaced by chips and chip cards, that should be protected as well;
- ▲ **Desirable conditions** – a system set in such a manner that when anybody located in or moving to an area without authorization should be immediately recognizable; zones, sections and secure access are the key factors;





**Figure 7: Color distinguishing uniforms [Source: indigo.co.uk]**

## ***2. Cargo Management***

### ***2.2. Reception***

- ▲ Visual inspection, comparing content of shipments with the documentation (e.g. 6 pallets, 80 pieces of carton); there should be procedures to resolve divergences and other non-standard situations; given responsibilities and appointed contact persons;
- ▲ Company (logistics department) should get a preliminary information about the incoming goods, before they reach the area, preferably a day in advance; it is crucial to have the shipment information in advance, especially for goods from third countries;
- ▲ Conducting 7 point inspection of transport units, including checking the integrity of seals, tarpaulin, registration marks etc.;

### 2.3. Expedition

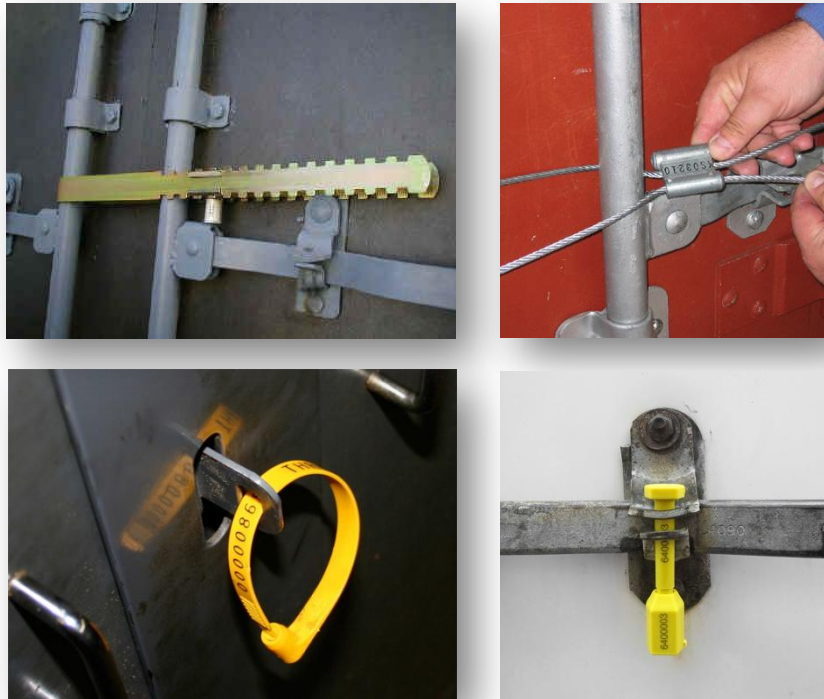
- ▲ The security of transport units is considered for cartons, pallets, boxes, and the security of transport and shipping concerns units such as containers, trailers, trucks etc.;
- ▲ In case the elementary transport units (pallets, boxes, etc.) are sufficiently secured and sealed (plastic packaging, where the breach is immediately obvious), emphasis on trucks or trailer security is not necessary, sometimes not even possible – transportation consolidating shipments destined to various locations;



**Figure 8: Transport units protection – sealing tape, stretch wrap, pull tight seal, wire seal**  
[Source: [interplas.com](http://interplas.com), [diebolddirect.com](http://diebolddirect.com), [fricknet.com](http://fricknet.com)]

- ▲ Inspection during packaging, to prevent insertion of objects; using stretch wraps for protection; administering documentation with signatures of the persons involved in expediting;
- ▲ Radiation detectors are mostly not required in the Czech Republic, with the exception of specific commodities, following requirements of other standards or legislation;





**Figure 9: Security seals – barrier seal, cable seal, plastic seal, bolt seal**  
 [Source: americanseals.com, lucenadeals.com, leghornseals.com, novavisioninc.com]

### 2.1. Reception / Expedition

- ▲ Trained personnel should be aware of all procedures on how to treat cargo, and know their competencies – what they can perform and what they cannot;
- ▲ Processes should be checked by an authorized person; additional cameras upon ramps and interface of the reception;
- ▲ Special treatment of goods from third countries before the release to free circulation – for such goods, a special place should be allocated in the warehouse, and they should either not be put in the system, or be temporarily blocked.
- ▲ Prevention of access of unauthorized persons;
- ▲ High value goods - special location in the warehouse - may have fenced area with restricted access; special arrangements and procedures;
- ▲ **Desirable conditions** – clearly defined procedures and behavior for situations that can occur; training of employees, determination of responsibilities and inspection of the process; strict adhering to the requirement of preliminary information of incoming cargo; simultaneously, employees should be aware of who they dispatch outgoing shipments to;



**Figure 10: Fenced area for high value goods**  
[Source: redirack.com ]

### ***3. Human Resources Management***

#### ***3.1. Recruitment / Termination***

- ▲ Selection of employees - conducting risk assessment, investigation of criminal records - assessing the severity of offences, with respect to the particular position;
- ▲ When cooperating with a personnel agency, recruiters should not mindlessly rely on the agency's choice, but still use their own screening procedures;
- ▲ Sensitive positions should be determined; when recruiting, the decision whether to prefer an employee already working in the company (trained, experienced), or an external candidate should be made; sensitive positions should be connected with more frequent and detailed screening;
- ▲ Proper employee termination procedures – completion of output documents, withdrawing all devices for access (cards, keys), deactivation of passwords; audit methodology: selection of a former employee, and test of access with the password, especially when the company uses remote access;

### *3.2. Training*

- ▲ Training and information system in place, so that all employees know how to act in all situations; including procedures for extraordinary situations;
- ▲ Employees should be aware of procedures, know what is forbidden behavior, and be able to prove the knowledge, e.g. knowledge how to conduct 7 point inspection;
- ▲ Training for employees should also inform about the placement of cameras, parking, system of zones, etc.;
- ▲ Training on security should be included in the initial training;
- ▲ Maintaining training records; documentation of attendance; training plans;
- ▲ **Desirable conditions** – to perceive personnel security as a whole – examination during the selection process, provable training for operation and proper checking; a system of documentation in place, and maintaining the records; to put the emphasis on the system of recruiting, as well as on the termination procedures;

## **4. Information Management**

### *4.1. Goods*

- ▲ High importance of preliminary information about incoming goods;
- ▲ Integrated system (logistic, accounting) - goods should be traceable and have available proper information – origin, amount, stage of processing, and other relevant parameters, including the position in the warehouse; these documents later constitute annexes to the audit protocol;
- ▲ Identification – commonly a bar code system or RFID; not required during an audit; it is important to have a proper documentation system, regardless of the method;

### *4.1. People*

- ▲ Recording – creating and maintaining a proper and well arranged records of staff trainings, periodic inventories; detection of breaches and shortcomings; checks of CCTV records, etc.;
- ▲ Method and speed of distributing information in the enterprise – changes of directives; awareness of all relevant employees, etc.;

- ▲ **Desirable conditions** – constant overview of goods, moving across the company; ability to trace information; to put great emphasis on the timely completion of the customs duties; to make and keep records of relevant activities; to manage that important information may be quickly reached by all the relevant persons;

## **5. Business Network & Company Management Systems**

### *5.1. Business Network*

- ▲ High importance of awareness and knowledge of carriers, suppliers, customers, service providers, etc.; knowledge of partners also applies for the customer; for instance, when a company sells weapons, they should definitely know the purchasers;
- ▲ It is desirable to use the minimum amount of carriers and service providers possible; sometimes, could appear more suitable to use a new partner, for instance when one that is experienced and has a good reputation in the region;
- ▲ Example – it is different to have five carefully selected carriers, audited by company, as opposed to having greater number of unidentified and unpredictable carriers, as well as although a small number of carriers, but with unpredictable behavior and an unidentified staff;
- ▲ Selection criteria of partners should be quality, security features, reputation, knowledge of the region etc., the prices should not be the primary selection criterion;
- ▲ External employees, such as service providers (cleaning, maintenance), should not move within the area and facilities unattended, especially when they work out of regular working hours;
- ▲ **Desirable conditions** – identification of the business network and supply chains; advanced knowledge of business partners; efforts to minimize and screen external partners, and create a reliable confidential links; to require business partners to comply with security standards, according to the principles of the AEO;

## **6. Crisis Management and Disaster Recovery**

### *6.1. Disaster Recovery*

- ▲ It is required to keep a record of any emergency events occurred, and to demonstrate corrective measures and steps, taken to prevent recurrence;
- ▲ All candidates are required, already during the self-assessment, to perform a risk analysis - what the risks are, what events can occur, statistics of emergencies, etc.;
- ▲ Conducting periodical reassessments; when an emergency occur, a response is always expected;
- ▲ **Desirable conditions** - It is necessary to perform a risk analysis, by which the security measures should be adapted; the company should be able to demonstrate risks and weaknesses, and in the event of an emergency, to demonstrate corrective measures and prevention;

## **7. Customs Duties**

Although the requirement for s proper performance of the customs duties does not belong in a chapter of security measures, the equal prominence brings the need to make readers familiar with the necessary knowledge.

- ▲ It is crucial to set a proper process for customs paperwork:
  - correct tariff classification
  - customs valuation
  - payment of customs debts
  - respecting current restrictions of commodities (anti-dumping import duties, prohibitions, etc.)
- ▲ Appointment of a person responsible for performing the duties, internally trained for the position;
- ▲ Interconnection with the accounting system - licenses for the movement of goods;
- ▲ Distinguishing whether the company uses a customs agent – direct / indirect; In case of using a company customs agent, all the responsibility lies on the company.
- ▲ It is essential to set the responsibilities for issuing customs declarations;

- ▲ Training for the performance of customs issues, and knowledge of customs regimes;
- ▲ Audit: Breaches of duties - auditors check the frequency of lawfully proven breaches – if charged a higher fine, examination of severity and nature, and share of breaches to the volume of transactions – if the breach is serious or repeated – further examination on the premises – there the applicant has a chance to present the whole process, and prove corrective actions – it may be solved by a new system for timely payments, or an external operator; company still can explain the cause, and show the actions taken, which may finally be acknowledged positive; the worst is ignorance or inaction;
- ▲ Sometimes a company may seem to have no problems, thus there is a subsequent evaluation of the documentation (random selection), where other breaches could be found; primary checking of the fundamental four points of customs paperwork, mentioned above; the process may be paused, waiting for the outcome of a thorough check - the results will bring the granting or withholding of the certificate;

#### 4.5.4 Scoring and Weighting

During the interviews, a different level of significance was discovered within security measures. Therefore, there is an option to design a rating scale assigning an adequate weight to the measure.

Since we have the knowledge about the varying relevancy of certain measures for the auditors, such measures should have varying importance. This rating difference will be then reflected in an output.

So finally, these rated measures will get together an overall security score, which will numerically or in percentage express the total security level of the entire system. An initial proposal for the scoring of the measures is shown in **Figure 3**. The weights are tentatively estimated, according to the statements of the customs officers. For an accurate calculation, we expect to use the Analytic Hierarchy Process (AHP), a decision-making method serving, among other uses, to rank alternative solutions.

W	Category	W	Sub-category	S	Measures			
2	1	Facility Management	2	External borders	2	Limited number of gates and entrances	✓	2
					3	Guarding of gates and entrances	✓	3
					2	External borders including buildings - sealing of windows, doors	✓	2
					3	Outer perimeter	✓	3
					1	Other exits and gates - locks, seals	✓	1
					2	Other exits and gates - cameras	✗	0
			1	Lightening	1	Maintenance of external borders - forest, grass, vegetation	✓	1
					2	Outer perimeter	✓	2
					3	Gates and gateways	✓	3
			2	Access of persons, vehicles and goods	3	Ramps	✓	3
					2	Permanent monitoring of frequent spots	✗	0
					1	Gatehouse	✓	1
					3	Video surveillance	✓	3
					2	System of authorised persons	✓	2
					3	Preliminary cargo information	✓	3
			1	Parking of private vehicles	2	ID tools - badges, chips	✓	2
					3	Separate parking outside the perimeter	✗	0
					2	Separate parking within the area	✓	2
					2	List of vehicles with permission	✓	2
					2	Vehicle clearly marked - cards, labels	✓	2
					1	Distinguishing of temporary and permanent permits	✓	1
			1	Internal physical security	1	Distinguishing manager and workers vehicles	✗	0
					1	Clear identification - badges, labels	✓	1
					2	Clear identification - uniforms	✗	0
					3	Clear identification - chips, chip cards	✓	3
					3	The system detecting unauthorized access	✓	3
					2	Records of personnel movement	✓	2
					3	System of keys	✓	3
2	Random checks of employees - opening bags, car trunks	✓			2			
3	Zones and sections with restricted access	✗	0					

Figure 11: Facility management – example of scoring of security measures

#### 4.5.5 Results

The analysis of the criteria has refuted or confirmed some assumptions, and also brought some new findings about the process of obtaining certification. These results are summarized in the following points:

- It is inaccurate to strictly assign the criteria into sections of the Gutiérrez and Hints model. Research has found the sections are interrelated and cannot be clearly evaluated separately.

The reception of cargo is a typical example. As it is apparent from the title, it should be covered in Cargo Management section. But in fact, we should also consider:

- ▲ Physical security in the form of CCTV, lighting, and restricted access for unauthorized persons (*facility management*)
- ▲ Properly trained staff, a system of authorized persons, responsibility for checking, performance of customs duties and customs regimes (*human resources management*)
- ▲ Timely reception of advance information on cargo, and its subsequent processing (*information management*)
- ▲ Knowledge and identification of suppliers, particularly from third countries (*business network*)
- ▲ Response procedures in the event of anomalies or breaches (*crisis management and disaster recovery*)

The division of measures into sections should be supplemented by identifying general principles, repeatedly stressed by customs officers during the interviews. Following elementary principles should be adopted by every business, seeking certification.

##### 1. Company Risks Identification

The first step is to be aware of the status of security in the company. The management should be able to identify risks and vulnerabilities that may occur not only as objections from auditors, but may already cause a loss. The applicant should consider that, by admission, the company will become part of the system. The necessity of integral boundaries of physical facilities and processes from the outside environment should be realized. Self-assessment is a crucial task, and should be performed by each applicant.



## **2. Process Risk Identification**

Each applicant should know the security obligations arising from the activities of the company. It is essential that processes, especially those associated with goods and production, are operated only by authorized and properly trained staff. A greater emphasis should be put on the processes by which the goods enter or leave, or could illegally leave the premises. One of the most important factors is the proper observance of customs duties. In case of breaches, corrective actions must be proven.

## **3. Staff Awareness**

The company should always know its employees, and who can be assigned to determined sensitive positions. All employees should always be properly trained to know, how to behave and react in all situations, and who to contact if appropriate. All relevant information should be, as soon as possible, delivered to all relevant employees.

## **4. Business Network**

The candidates should definitely know their business network. They are expected to be aware of their suppliers, but also of the purchasers they supply. They should be aware of all the partners, including HR agencies, cleaning and maintenance, security agency, and customs agents. Special caution is expected from companies doing business with weapons, explosives and hazardous substances (dangerous goods).

## **5. Reaction To Shortcomings**

Companies should have processes to react on abnormal situations, or even collapses. Such processes include directives on the manner in which such situations are handled, and processes ensuring that staff is trained in how to react and who to contact. The situation changes, if the company has noticeable experience with such adverse events. Then they have to clearly demonstrate the taken adequate measures to remedy the event and prevent further recurrence. This also applies to breaches of customs duties.

#### **4.5.6 Further Observations**

- For companies already holding some of the security certificates (ISO, ISPS Code, etc.), the audit could be greatly accelerated.

First, there is knowledge about what is expected, what documentation should be processed, kept and provided, and what main subjects are of the auditor's interest.

Second, within the implemented standards, there are supposed to be a security policy and measures already in compliance with the AEO security requirements.

- The solving of identified and experienced security occurrences appears essential. Auditors are naturally interested in the cause of which the event occurred. Principally, they inquire for the company's approach, and the measures taken to remedy, and prevent such events.
- The level of security measures should follow the AEO guidelines. Sometimes, the company could have self-made directives related to the particular circumstances and specifics of the company, which is not problem. However, the directives should comply with the principles of AEO.
- It is impossible to clearly define the manner and extent of compliance with the requirements necessary to obtain the status. As already mentioned, the security can be achieved by an accumulation of various measures, depending on specific conditions. However, the auditors always look at the system as a whole. It should be sufficiently secured, no matter the manner.

## Conclusion

Nowadays, security is undoubtedly incorporated into the matters of the international supply chain management.

Intense globalization is one of the reasons for this. Companies are expanding, conglomerates are rapidly growing by mergers and acquisitions, and companies are willing to expend considerable resources for internationalization. Such actions necessarily need to include organized flows of goods and materials among the strategic points, the so-called supply chains. Furthermore, when supply chains are operated internationally, they usually never sleep and never close. No matter the daytime or the season, the product must reach the customers in the required quality, and for minimal costs.

Unfortunately, there is also a growing crime rate, due to use of modern technologies to intentionally damage or steal. It is not only terrorists, threatening by bombings or assassinations. There are organized groups which, never stop constantly inventing techniques to steal valuable goods, or even just diesel from trucks.

Combating the intruders is demonstrated by cooperation among governments on efforts to share a common standard of protection. The WCO Safe Framework, and its pillar the Authorized Economic Operator could certainly be an appropriate schema for such a standard. In recent years, the AEO has become an instrument of conformity, to protect the supply chain.

An analysis of data obtained from interviews with customs officers has showed the functionality of the Gutiérrez and Hintsá model. It has confirmed the existence of a general model to achieve the proper security in various types of companies.

The measures can actually be distributed over the six basic groups, which, however, significantly overlap. Thus, when implementing them, it is always necessary not to only take an action of meeting the individual tasks, but to consider the integrity of securing the entire system. It is desirable to protect not the points, but create security throughout the processes.

The outputs of this research could be considered the key to obtaining the certified status, but also a way to make companies and their supply chains properly secured.

Despite all the physical measures and the directives, it remains essential to adjust the thinking of people, and spread the awareness about the need for comprehensive protection and the cooperation, within international supply chains.

## List of sources

- [1] DIOP, Abdoulaye, David HARTMAN a Deborah REXRODE. Customs-Trade Partnership Against Terrorism: Cost/Benefit Survey. *UNIVERSITY of VIRGINIA* [online]. August, 2007 [cit. 2012-04-18]. Available on: [http://www.virginia.edu/surveys/press/2007/ctpat/2007\\_CTPAT\\_Final%20Report%20Only.pdf](http://www.virginia.edu/surveys/press/2007/ctpat/2007_CTPAT_Final%20Report%20Only.pdf)
- [2] Third Party Logistics Providers 3PL. *Department of Homeland Security: U.S. Customs and Border Protection* [online]. [cit. 2014-11-22]. Available on: <http://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat/security-guidelines/third-party-logistics-providers>
- [3] Marine Port Authority and Terminal. *Department of Homeland Security: U.S. Customs and Border Protection* [online]. [cit. 2014-11-22]. Available on: <http://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat/security-guidelines/marine-port-authority-terminal-operators>
- [4] Authorised Economic Operator (AEO): AEO Guidelines. EUROPEAN COMMISSION. *Taxation and Customs Union* [online]. Brussels, April 9, 2012 [cit. 2014-11-22]. Available on: [http://ec.europa.eu/taxation\\_customs/resources/documents/customs/policy\\_issues/customs\\_security/aeo\\_guidelines2012\\_en.pdf](http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/customs_security/aeo_guidelines2012_en.pdf)
- [5] ISO 28000:2007: Specification for security management systems for the supply chain. *ISO* [online]. 2014 [cit. 2014-11-22]. Available on: <https://www.iso.org/obp/ui/#iso:std:iso:28000:ed-1:v1:en>
- [6] Mutual recognition of Authorised Economic Operators and security measures. AIGNER, Susanne. *World Customs Journal* [online]. 2010 [cit. 2014-11-22]. Available on: <http://www.worldcustomsjournal.org/media/wcj/-2010/1/Aigner.pdf>
- [7] Frequently Asked Questions EU – US Mutual Recognition Decision. *Taxation and Customs Union* [online]. January 13, 2013 [cit. 2014-11-22]. Available on: [http://ec.europa.eu/taxation\\_customs/resources/documents/common/whats\\_new/13\\_01\\_31\\_eu-us\\_questions-answers.pdf](http://ec.europa.eu/taxation_customs/resources/documents/common/whats_new/13_01_31_eu-us_questions-answers.pdf)
- [8] EU – US AEO Mutual Recognition: AEO – C-TPAT Mutual Recognition for all?. THOMPSON. CONEX [online]. Paris, August 16, 2012 [cit. 2014-11-22]. Available on: [http://www.conex.net/images/stories/pdf/EN/EN\\_AEO\\_CTPAT\\_Mutuel\\_Recognition\\_Sept12.pdf](http://www.conex.net/images/stories/pdf/EN/EN_AEO_CTPAT_Mutuel_Recognition_Sept12.pdf)
- [9] Trade Library: Customs - Trade Partnership Against Terrorism (C-TPAT). *Law Offices of George R. Tuttle* [online]. [cit. 2014-11-22]. Available on: <http://tuttlelaw.com/subjects/ctpat.html>
- [10] C-TPAT Strategic Plan. *U.S. Customs and Border Protection* [online]. WASHINGTON, DC 20229, November, 2004 [cit. 2014-11-22]. Available on: [http://www.cbp.gov/sites/default/files/documents/ctpat\\_strat\\_plan\\_3.pdf](http://www.cbp.gov/sites/default/files/documents/ctpat_strat_plan_3.pdf)
- [11] VOLUNTARY SUPPLY CHAIN SECURITY PROGRAMS: A SYSTEMATIC COMPARISON. GUTIERREZ, Ximena a Juha HINTSA. CROSS-BORDER RESEARCH ASSOCIATION. *Academia.edu* [online]. Lausanne, Switzerland, 2006 [cit. 2014-11-22]. Available on: [http://www.academia.edu/6945568/VOLUNTARY\\_SUPPLY\\_CHAIN\\_SECURITY\\_PROGRAMS\\_A\\_SYSTEMATIC\\_COMPARISON](http://www.academia.edu/6945568/VOLUNTARY_SUPPLY_CHAIN_SECURITY_PROGRAMS_A_SYSTEMATIC_COMPARISON)

[12] C-TPAT 5 Step Risk Assessment Process Guide. *U.S. Customs and Border Protection* [online]. March, 2010 [cit. 2014-11-22]. Available on: [http://www.cbp.gov/sites/default/files/documents/supply\\_chain\\_assess\\_guide\\_3.pdf](http://www.cbp.gov/sites/default/files/documents/supply_chain_assess_guide_3.pdf)

[13] C-TPAT Validation Process: Frequently Asked Questions. *U.S. Customs and Border Protection* [online]. [cit. 2014-11-22]. Available on: [http://www.cbp.gov/sites/default/files/documents/ctpat\\_validation\\_faqs\\_3.pdf](http://www.cbp.gov/sites/default/files/documents/ctpat_validation_faqs_3.pdf)

[14] Customs - Trade Partnership Against Terrorism: Mutual Recognition. *U.S. Customs and Border Protection* [online]. [cit. 2014-11-22]. Available on: <http://www.cbp.gov/border-security/ports-entry/cargo-security/c-tpat-customs-trade-partnership-against-terrorism/mutual-recognition>

[15] Exporter Eligibility Requirements: C-TPAT Exporter. *U.S. Customs and Border Protection* [online]. [cit. 2014-11-22]. Available on: <http://www.cbp.gov/sites/default/files/documents/Exporter%20Eligibility%20and%20Minimum%20Security%20Criteria.pdf>

## List of figures

FIGURE 1: LOGOS OF AEO EU, KOREA, JAPAN, HONG KONG AND TAIWAN [SOURCE: CARGOSERVICESGROUP.COM, KCTCINTL.CO.KR, NIKKEIKINHOLDINGS.COM, INFO.GOV.HK, UCTC.COM.TW ] ....	30
FIGURE 2: DIAGRAM OF SCS [SOURCE: GUTIÉRREZ; HINTSA, VOLUNTARY SUPPLY CHAIN SECURITY PROGRAMS].....	49
FIGURE 3: WAREHOUSE SURVEILLANCE [SOURCE: LOGISTIKA.IHNED.CZ].....	50
FIGURE 4: FACILITY MANAGEMENT – CLASSIFICATION OF SECURITY MEASURES.....	51
FIGURE 5: FENCED AND ENLIGHTENED OUTER PERIMETER [SOURCE: CAST-LIGHTING.COM] .....	52
FIGURE 6: SOLUTIONS FOR RESTRICTED ACCESS [SOURCE: AIRPORT-INT.COM, BOONEDAM.US].....	53
FIGURE 7: COLOR DISTINGUISHING UNIFORMS [SOURCE: INDIGO.CO.UK] .....	55
FIGURE 8: TRANSPORT UNITS PROTECTION – SEALING TAPE, STRETCH WRAP, PULL TIGHT SEAL, WIRE SEAL [SOURCE: INTERPLAS.COM, DIEBOLDDIRECT.COM, FRICKNET.COM].....	56
FIGURE 9: SECURITY SEALS – BARRIER SEAL, CABLE SEAL, PLASTIC SEAL, BOLT SEAL [SOURCE: AMERICANSEALS.COM, LUCENADEALS.COM, LEGHORNSEALS.COM, NOVAVISIONINC.COM].....	57
FIGURE 10: FENCED AREA FOR HIGH VALUE GOODS [SOURCE: REDIRACK.COM ] .....	58
FIGURE 11: FACILITY MANAGEMENT – EXAMPLE OF SCORING OF SECURITY MEASURES .....	63

## List of tables

TABLE 1: MAJOR SECURITY INITIATIVES [SOURCE: LÁNSKÁ, SUPPLY CHAIN SECURITY] .....	15
TABLE 2: CATEGORIES OF SUPPLY CHAIN SECURITY MANAGEMENT SYSTEM [SOURCE: GUTIÉRREZ; HINTSA, VOLUNTARY SUPPLY CHAIN SECURITY PROGRAMS].....	35