Männistö, Toni; Hintsa, Juha

Conference Paper

A Decade of GAO's Supply Chain Security Oversight

Suggested Citation: Männistö, Toni; Hintsa, Juha (2015) : A Decade of GAO's Supply Chain Security Oversight, In: Blecker, Thorsten Kersten, Wolfgang Ringle, Christian M. (Ed.): Operational Excellence in Logistics and Supply Chains: Optimization Methods, Data-driven Approaches and Security Insights. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 22, ISBN 978-3-7375-4058-2, epubli GmbH, Berlin, pp. 443-472

A Decade of GAO's Supply Chain Security Oversight

Toni Männistö and Juha Hintsa

This study characterizes and synthetizes reports that the US Government Accountability Office (GAO), an independent government watchdog organization, has published on supply chain security (SCS) since 2005. The study follows a systematic and transparent protocol for examining the 25 identified GAO documents. The document review reveals benefits and drawbacks of US SCS policies, initiatives and regulations. The findings allow contrasting of the US government's approach to SCS to the one of the European Commission. This comparison reveals differences and similarities in supply chain security policies both sides of the Atlantic and allows the policy makers to benchmark their approaches to supply chain security. The comparative analysis also paves the road for further EU-US harmonization and mutual recognition of the SCS programs. The study is part of European FP7-Project CORE.

Keywords: Supply Chain Security, Government Accountability Office, Customs and Border Protection, FP7-CORE

1 Introduction

1.1 Background

The terrorist attacks of September 11 in 2001 started a new era in the security management and control of international trade and logistics networks. The tragic events raised concerns, particularly among the policy and law enforcement circles, about the possibility that terrorist organizations could exploit global supply chains to move tools, materials and operatives across borders. In the most alarming scenario, the terrorists would hide a weapon of mass destruction in a shipping container and detonate it at its destination. Soon after the September 11 tragedy, the focus on supply chain security shifted from theft prevention towards counter-terrorism (Lee and Whang, 2005, pp. 289), and this change in the general mindset eventually lead to introduction of a large number of new supply chain security (SCS) programs, laws and regulations (Hintsa et al., 2009, pp. 346). However, the problem with the new SCS initiatives was that they tended to disrupt free trade and international flow of goods. In other words, due to the new security regimes, it took now more time for shipments to travel through the global supply chain. What is more, the delivery times did not only get longer but also less reliable. And perhaps most importantly, the extra security increased shipping costs.

Governments and the trading community soon recognized that securing the supply chain without disrupting the cross-border flow of goods is to a large extent a matter of regulatory harmonization and mutual recognition. Back in early 2000's and still today, incompatible security regimes force

traders and logistics actors to comply with a broad disarray of security requirements (Grainger, 2011, pp. 39-40). In some cases, security controls are redundant: even if security checks are done in one country, the same controls must be redone in one or more countries along the international supply chain. The regulatory harmonization and recognition of one another's security controls would help to rationalize security processes throughout the international supply chains.

1.2 Post-2001 Supply Chain Security in the US

Ever since 2001, the US government has taken strong efforts to strengthen the security of the US-bound supply chain. The US Customs and Border Protection (CBP) launched a voluntary Customs-Trade Partnership Against Terrorism (C-TPAT) to engage the business community in the fight against terrorism. Not long after this precursor program, a stream of other SCS initiatives followed, most notably the Container Security Initiative (CSI) and the Known Shipper Program. At the same time, the US government modernized its regulatory framework in areas of air cargo security, maritime security and customs security.

The US government has naturally been very interested in monitoring effectiveness and efficiency of its SCS initiatives, and the impact of the security initiatives on the cross-border flow of goods. The US Government Accountability Office (GAO) has taken a major role in overseeing the US SCS initiatives. On its website, the US Government Accountability Office (GAO) characterizes itself as "an independent, nonpartisan agency that works for Congress." Colloquially speaking, GAO is a government watchdog organization with a mission of ensuring efficient use of US taxpayers' dollars. In fiscal

year 2014, GAO had a budget of $543,6 million, and it employed around 3000 people. The organization proclaims that at every dollar invested in GAO saves 100 dollars of the US taxpayers' money. Indeed, over the past ten years, GAO has produced a rather impressive library of independent, objective and open reports and testimonies on various US SCS initiatives. The quality of the GAO documents appears high: each report draws on the best possible information set available, whether it is a set of interviews, statistics or survey data.

The GAO reports comprise a unique body of SCS knowledge and experience that helps us to understand many benefits, drawbacks and development opportunities of most of the SCS initiatives that the US government has introduced. This information also allows foreign governments to better understand innovations and mistakes of the US programs and apply the lessons' learned when they launch or update their own SCS programs. The GAO information is especially useful for the European Union (EU) that runs many similar SCS programs than the US government. Besides, the GAO reports' detailed descriptions of the US SCS initiatives help policy-makers in other countries to see what it takes to align and harmonize requirements of their own and the US initiatives. Understanding the similarities and differences between the programs set the basis for mutual recognition of SCS initiatives.

Given the uniqueness and relevance of the GAO information for the policy-making in the EU, this study reviews reports that the US Government Accountability Office has published on supply chain security since 2005. This review seeks to identify drawbacks and benefits of the US SCS programs,

and contrast them against their counterparts in the EU. Formally stated, this study addresses following research question.

RQ: What can the EU supply chain security learn from the GAO's publications?

2 Research Methods

To carry out this review study, our research team respected the two main principles of the so-called systematic literature review (SLR) methodology: transparency and accountability (Tranfield et al. 2003). Our analysis, however, differed from the purist approach to the systematic literature review by focusing only on one body of literature, the GAO reports and testimonies, instead of exploring the full range of academic, governmental and business studies on the topic. Before engaging in the document reviews, our team devised an eight-step analysis procedure to extract relevant information from to-be-reviewed GAO documents. The team also agreed on system for documenting and archiving the review findings.

Next, after defining the common rules for doing the review, the team searched for suitable GAO documents to be reviewed by executing online inquiries with major academic and non-academic search engines and by visiting the GAO's official website. The team applied two inclusion criteria for the candidate GAO publications, which number totaled around 300 testimonies and reports. The documents had to discuss supply chain security or closely associated themes such as trade facilitation, and they had to been published in 2005 or later. The reason why we did not consider documents, that were older than ten years, was our intention to avoid reviewing

obsoleted documents and outdated information. After the team had identified the initial pool of documents, individual members of the team had an opportunity to suggest some additional GAO documents for the review that had escaped the initial search. The final sample of GAO documents ended up being 24 reports and testimonies.

The research team also agreed on an eight-step protocol for describing and analyzing the review documents (table 1 below). Besides basic citation information, the protocol instructed document reviewers to summary the document, examine the document using the common SWOT – strengths, weaknesses, opportunities, threats – framework, and to link review findings with the FP7-Project CORE work packages and demonstrations. In essence, the protocol guided the document reviewers to pay attention to the same issues, and facilitated the team to produce consistent and comparable document reviews that later enabled writing of quality cross-analyses and summaries.

Table 1 The 8-steps of the review protocol

Step	Importance
1. Basic citation of the document; and document availability	Mandatory
2. Summary of the document, including overall relevance for CORE	Mandatory

Step	Importance
3. Classification / keywords / navigation / tags for the document	Mandatory
4. Brief analysis, e.g. in "SWOT-style" (strengths, weaknesses, opportunities, threats) – if available either in literature or in your own work	If available
5. More detailed analysis of relevance for CORE, on WP / Task / Deliverable level	Nice to have
6. Cross-referencing between two or more documents	Nice to have
7. Anticipation whether CORE could have an impact on the future versions of this document	Nice to have
8. Full citation of the document, following Emerald guidelines	Nice to have

The document reviews produced 24 written document summaries, each of which follows the structure of the 8-step review protocol. As most of the reviews are too long to be included in this paper, the table 2 below presents a three-step excerpt of one GAO document review. The headline of the table shows the full citation details of the reviewed document. The main body of text summarizes the document (step 2) and elaborates its relevance to the CORE project (step 3). In particular, the analysis highlights that CORE's

work on risk management and awareness building benefit from the insights the reviewed GAO document describes. The full, eight-step analyses are five pages long on average, so due to the space constraints, we illustrate only the protocol's three most consequential steps in the table below.

Table 2 Example of two first steps of a GAO document review

SUPPLY CHAIN SECURITY - DHS Could Improve Cargo Security by Periodically Assessing Risks from Foreign Ports, GAO
This GAO report reviews maritime supply chain security programs that the Department of Homeland Security and its component agencies – mainly the Customs and Border Protection (CBP) and the Coast Guard – have implemented since 2001. The report examines (1) the extent to which DHS has assessed risk levels of foreign ports and allocated security resources accordingly and (2) activities DHS has taken to monitor and improve efficiency and effectiveness of its security initiatives. Drawing on numerous interviews of key stakeholders and examination of key documents, the report recommends CBP to consider expansion of its Container Security Initiative (CSI) into new ports based on a periodic risk assessment of foreign ports. The report also highlights opportunities for further harmonization of the US maritime security initiatives with their foreign counterparts through mutual recognition agreements. Since this report contains fundamental information about the US maritime security programs, many CORE work packages are likely to benefit from the insights this report provides. Especially, the demonstrations, which involve ocean shipping, as well as the risk cluster, can use this information to support and guide their work.
Detailed analysis of relevance for CORE: The report provides a comprehensive outlook on the US maritime supply chain security initiatives that

the DHS and its component agencies – mainly CBP and Coast Guard – have implemented since 2001. The report features some interesting figures that map the security initiatives on the global supply chain and that illustrate current solutions the US government employs to screen and examine US-bound shipping containers. The CORE's demonstrations that involve maritime shipping are likely to benefit from the information this report provides. Also the risk cluster can use the information, and especially the mapping of the US maritime security initiatives over the global supply chain, to design risk-based, layered approaches to maritime supply chain security. The education cluster can also reuse the contents of this report to produce relevant and informative training material for various supply chain stakeholders that are involved in the seaborne trade and logistics.

3 Analysis

3.1 Descriptive overview of GAO reports

The final review sample comprises 24 GAO documents. Of these documents, nine are testimonies (37,5%), and the remaining fifteen are reports (62,5%). The testimonies are formal statements addressed to one or more Congressional policy-making bodies, and which contents and recommendations are based primarily on earlier, more technical GAO reports.

Each of the GAO documents has a headline theme that is announced in the document's name with capital letters. The headline themes, as illustrated in the Figure 1 below, give a general summary of the topics that the GAO documents address, and they also indirectly hint about priorities of the US

government's SCS priorities. The most significant themes are supply chain security (38%), maritime security (33%) and aviation security (13%). More narrow topics – transportation security administration, transportation security, and transportation security information sharing and port security grant program – were the headline themes in one reviewed GAO document only. It is surprising, however, that none of the GAO documents discuss security in the context of road or rail transport. It would be reasonable if future GAO research or studies by other organizations addressed also these currently neglected modes of transport. Also, the existing GAO reports largely overlook important supply chain security themes such as cyber security and supply chain resilience. This statistics is visualized in figure 1 below.

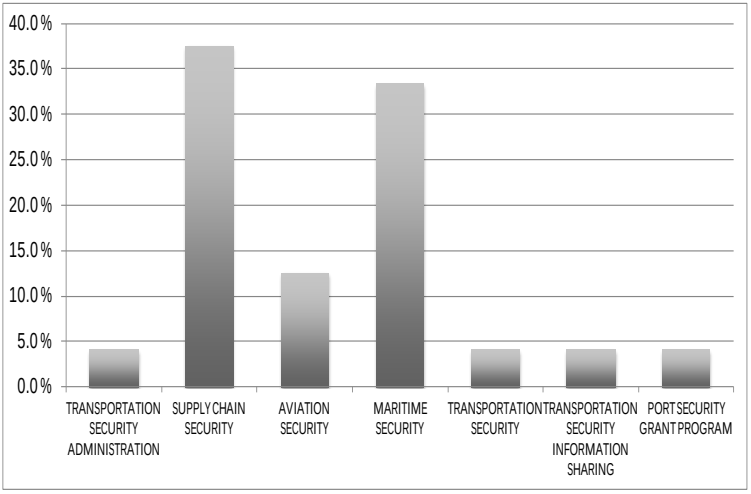

Figure 1 Statistics on the GAO document headline themes

The GAO documents are often addressed to a particular policy-making audience. Most of the reviewed GAO reports were addressed for "Congressional Requesters" in general. Testimonies, in turn, were often addressed for specific working groups and committees of the U.S Senate and the House of Representatives, for example the Committee on Homeland Security, the Subcommittee on Transportation and Infrastructure and the Committee on Commerce, Science and Transportation.

Table 3 Recommendation type

Theme	Number	Percentage
Information management	7	20,6%
Risk assessment	7	20,6%
Performance monitoring	5	14,7%
Cost-benefit analysis	3	8,8%
Resource planning	3	8,8%
Feasibility assessment	2	5,9%
Compliance monitoring	2	5,9%
Updating of plans	2	5,9%
Improved scanning	2	5,9%

The GAO reports and testimonies give many recommendations for various US government agencies. These recommendations are the key instruments for GAO to promote its mission that is to "the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people." The table 3 lists main types of recommendations that the GAO provide. Most often, the reports urge the US agencies to improve their processes for collecting, recording, analyzing and making use of information. The recommendations on information management also urge the agencies to collaborate more actively with one another and with their foreign fellow organizations. The second most common theme of the GAO recommendations is the risk assessment that includes identification of risk, evaluation of their likelihoods and impacts and assessment of overall vulnerabilities in the supply chain. Many of the reviewed reports also highlight the need to establish and improve indicators, measurements and procedures for monitoring performance of security initiatives. Related to the overall performance monitoring, many of the reports urge the US agencies to carry out cost-benefit and feasibility analyzes of governmental security investments. Resource planning and periodic revision of plans was also considered important area of improvement by the GAO documents. Important yet less commonly proposed recommendations consider calls for improved scanning technologies and more stringent and common compliance monitoring.

When the research team selected the GAO reports for this review, they decided to include all supply chain security reports that the organization has published in 2005 or later. Despite this scoping decision, in the final sample

of 24 articles, all reports and testimonies have been published after 2006. The oldest article dates back to 2007, and the newest one has been published in January 2015. Otherwise, the rest of the articles have been published relatively evenly over the years. The figure 2 below illustrates the distribution of the 24 reviewed articles over the past ten years. We see that many of the GAO documents are relatively old. Therefore, the SCS community would benefit from a more recent, up-to-date analyses of the initiatives. Therefore, EU funded supply chain security projects, such as the FP7 CORE, might choose to update the obsoleted documentation and this way increase the project's impact on SCS policy making and practice.

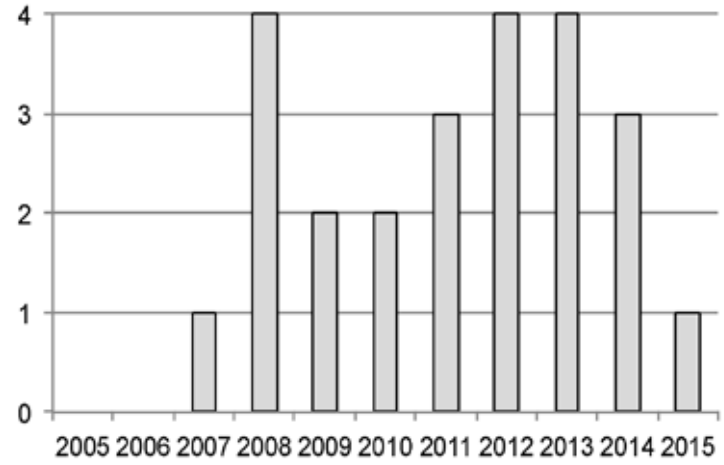

Figure 2 Publishing years of the 24 reviewed articles

3.2 Analytical Findings

The 24 reviewed GAO documents discuss a broad variety of US SCS initiatives. Many of these initiatives share similarities with the equivalent EU initiatives, and thus the EU policy-makers and authorities should at least consider whether the GAO recommendations could be applied in the EU context as well. This section shows connections between equivalent SCS programs in the US and in the EU and summarizes main recommendations that might be reasonable to put into effect on the both sides of the Atlantic. Readers who are interested in learning more about technicalities of the discussed SCS programs are advised to visit online sites of the US homeland security and European Commision. These online sources provide a large array of documentation on past and ongoing SCS initiatives.

Ocean-going vessels carry around 80% of the world's cargo by volume and 70% by value (UNCTAD, 2014), so it is not a surprise that the importance of the sea transport for the global cargo flows has attracted wide interest in maritime supply chain security both in the US and in the EU. Today, the US maritime security scheme comprises a set of security layers that are designed to mitigate the risk of maritime-related terrorist attacks. One key component in the US maritime security is the Advanced Targeting System (ATS), a risk assessment tool that calculates risk scores for US-bound maritime shipping containers and selects those containers that should be inspected for contraband at foreign ports or at the US destination upon arrival. The ATS uses an advance cargo information data (ACI), that carriers and importers submit to the CBP according to the 24-hour rule and 10 + 2 Importer Security Filing requirement, to calculate the risk levels. The equiva-

lent risk assessment scheme is in place in the EU as well, though the targeting is carried out by member states and the ACI dataset is submitted as part of the entry (or exit) summary declarations, before the goods enter (or leave) the EU customs security area (EU-28, Switzerland and Norway). The GAO reports suggest that the US CBP should update the weight set that the organization uses to calculate the risk scores, periodically, based on results of the most recent risk assessment. The reports also proposes that the CBP would create performance metrics to check effectiveness of the risk targeting efforts and to clarify rules that lead to waiving of container inspections at foreign ports. The table 4 below illustrates the US and EU programs on advance cargo information and targeting and related GAO recommendations.

Table 4 Advance cargo information and targeting

US program	Equivalent EU program	Main GAO recommendations
Advance Targeting System (ATS) based on 24-hour rule and 10 + 2 Importer Security Filing	National risk assessment systems based on Entry summary declaration	Ensure that future updates to the weight set are based on assessments of its performance Establish targets for performance measures and use those measures to regularly assess effectiveness of the weight set Clarify, harmonize and enforce the rules and the procedures for waiving the high-risk containers from examination

The advanced cargo information and the targeting highlights those shipping containers that require scanning with non-intrusive imagining technologies (colloquially referred as "X-rays"), radiation detection measures, or both. This scanning targets primarily radioactive and radiological weapons or material that could be used for terrorism on the US soil. The US has been rather active in setting up new counter-terrorism maritime security programs that involve scanning of shipping containers. The CBP did launch its first counter-terrorism container screening program, the Container Security Initiative, in January 2002. The vision of this program was to screen high-risk US-bound shipping containers for terrorist threats already at foreign ports. The US Department of Homeland Security also rolled out the Secure Freight Initiative (SFI) to screen a higher percentage of US-bound containers with the non-intrusive imagining technologies and the radiation detectors at foreign ports. SFI has been operational in six foreign ports since early 2007. At the ultimate program, as part of the "Implementing recommendations of the 9/11 Commission act of 2007," the US Congress required scanning every US-bound maritime container at the last foreign port. This 100% scanning legislation has been considered unfeasible by the trading community and by many foreign governments, and the Congress has already postponed its implementation two times. It is important to note that while the US has been active in promoting their maritime security scheme internationally, the EU has not established any major programs for screening EU-bound containers in foreign ports. To sum up, the table 5 below summarizes the US container screening programs and recommendations that the GAO reports propose to improve them.

Table 5 Maritime container screening

US program	Equivalent EU program	Main GAO recommendations
Secure Freight Initiative	N/A	Conduct periodic risk assessment in foreign ports
Container Security Initiative (CSI)	N/A	Revise staffing model Improve collection of process information (e.g., performance of scanning teams) Develop performance criteria Conduct periodic risk assessment of foreign ports
100% scanning legislation	N/A	Conduct feasibility study

Another important theme in the GAO documentation is air cargo security. The reviewed documents highlight the importance of establishing voluntary secure supply chain programs, which would allow air cargo operators to move security screening away from congested airports towards the upstream of the air cargo supply chain. The US Known Shipper and Certified Cargo Screening Programs (CCSP) are fundamentally similar to the European Known Consignor (KC), Account Consignor (AC) and Regulated Agent (RA) air cargo security programs. The both concepts aim to ensure that air

cargo originates from a trusted source and it travels to the airport through trusted logistics middlemen and that the cargo gets screened by certified screening operators. The GAO documents recommend (GAO, 2007; GAO, 2008b) US air cargo operators to improve security screening through better technology and procedures and to step up compliance monitoring of certified air cargo operators.

Another topical theme in the air cargo sector is the security of inbound cargo that comes from foreign countries. The problem in ensuring adequate security for the inbound cargo is that authorities cannot easily verify and enforce that security procedures are being carried out up to a satisfactory standard in foreign jurisdictions. To remedy this problem, both the US and EU legislators have been introducing new legal frameworks that force airlines, that operate from abroad into their jurisdictions, to comply with their security rules. Regulating the airlines avoids the problem of imposing rules directly on sovereign governments and meddling with their national legislations. In the EU, the law for ensuring adequate security of inbound air cargo is called ACC3 (Air Cargo or Mail Carrier operating into the Union from a Third Country Airport), and this piece of legislation was introduced as part of the amendment Regulation 1082/2012 of the EU Regulation 185/2010. The legal basis of the equivalent US legislation for screening inbound air cargo is the "Implementing Recommendations of the 9/11 Commission Act." The GAO reports recommend the US authorities to establish a risk-based air cargo screening strategy that would facilitate screening operators to identify high-risk shipments and assign them to more thorough screening. The reports also propose that the US authorities would increase both frequency and stringency of compliance monitoring activities that

seek to ensure that the air cargo industry complies with the legal requirements. The table 6 below lists the main air cargo security programs and presents recommendations that the GAO documents propose to improve them.

Supply chain security is fundamentally about collaboration between government agencies and the trading community. Put it simple, companies generally ship and move cargo, and the governmental actors enforce that the companies comply with necessary security and other regulations.

Table 6 Secure supply chain programs

US program	Equivalent EU program	Main GAO recommendations
Known Shipper / Certified Cargo Screening Program (CCSP)	Known Consignor (KC) / Account Consignor (AC) / Regulated agents (RAs)	Improve screening Step up compliance monitoring
100% screening of inbound air cargo	ACC3	Establish a risk-based air cargo security strategy Improve interagency communication nationally Step up compliance monitoring of foreign air cargo industry's stakeholders

Especially the US government has been very active in encouraging the business sector to strengthen voluntarily the security of their supply chains. The US Customs and Border Protection (CBP) has been running its security-centric AEO program, Customs-Trade Partnership Against Terrorism (C-TPAT), since November 2001. As part of the program, the CBP promises faster and simpler customs formalities for companies that agree to implement a set of voluntary security controls. Being the first operational AEO program, the C-TPAT has been an example for many subsequent AEO programs: for example, the EU AEO, the Canadian Partners In Protection (PIP), Secure Exports Scheme in New Zealand, and the Jordanian Golden List Programme. The GAO reports essentially recommend that the US CBP would improve its processes for validating and revalidating C-TPAT applicants and current members of the program. The reports also highlight the importance of setting up formal performance measures for assessing the degree of compliance with the C-TPAT requirements. The Table 7 below shows recommendations that GAO documents (GAO, 2008a; GAO, 2008d) propose for improving the C-TPAT government-business supply chain security program.

Table 7 Authorized Economic Operator programs

US program	Equivalent EU program	Main GAO recommendations
C-TPAT	EU AEO	Improve the process of validating security practices of C-TPAT members Develop performance measures

4 Discussion

The GAO reports raise many concerns regarding performance monitoring and auditing of the US SCS initiatives, and this emphasis could be seen as an incentive for the EU officials to check their approaches in these critical areas. Moreover, the information of the GAO documents set a solid basis for transatlantic harmonization of SCS regulations and programs. There are many SCS initiatives both sides of the Atlantic that seek to achieve the same security objectives. For example, both the European Commission and the US government run their own security-centric authorized economic programs, EU AEO-S and C-TPAT respectively. There are also quite similar security programs on air cargo security, and the US and EU authorities could look for ways to align these programs in terms of security requirements, renewal periods and training to align their Known Shipper, Known Consignor and Certified Cargo Screening programs.

The GAO reports highlight the importance of avoiding certain mistakes that the US SCS initiatives have made in the past. Most important lesson to learn is that it is often critical to involve relevant industries when designing new regulations and to get their buy-in, at least at some level, before forcing companies to comply with new security requirements. The US 100 percent scanning requirement is an archetypal example of a security regulation to which the US government has been spending a great deal of money and effort only to achieve mediocre impact: the legislation is still pending, and most likely, it will never become operational due to the fierce criticism from the trading industry, port operators and foreign governments.

The thoroughness of the GAO analyzes imply that the recommendations that the reports suggest are reliable and justified. These recommendations highlight issues that the US SCS programs have encountered, and thus the recommendations might prove useful also for EU authorities that run similar SCS programs than their US colleagues.

Having said all this, the EU policy-makers should still remain skeptical about the applicability of the GAO recommendations in the EU context. Sometimes differences between seemingly equivalent security programs exist, and these differences justify if not require different approaches to managing the programs. For example, the EU member states do not always share the US views on security risks and threats. From the European perspective, some of the US counter-terrorism initiatives, most notably the 100 percent scanning legislation, seem excessive and disproportionate to the risks they seek to address. Besides the perceptual differences, also the review methodology sets some limits to the validity and the generalizability of the findings. First of all, many of the GAO documents are relatively old,

and they thus may contain obsolete information about the US SCS initiatives.

Bottom line, the review team found that the GAO documents are not only highly relevant for SCS management and governance but also of high quality. In the EU, there are no similar independent watchdog organizations that would review SCS practices across the member states and suggest improvements for more efficient and effective use of government spending on SCS. Given the high relevance of the GAO reports, we therefore recommend the EU to consider establishing a quality assurance body equivalent to the GAO and to mandate this body to undertake periodic reviews on the EU's SCS programs. If this new auditing body had qualified experts onboard, it could also take care of evaluation of scientific quality of the many SCS research projects that the European Commission is funding. The table 8 summarizes the key findings and arguments of this discussion section.

Table 8 Summary of discussion

What GAO reports and testimonies offer	How EU policy making can benefit from the GAO reports and testimonies	Possible benefits
Detailed analysis of US SCS initiatives and programs	Understand similarities and differences of SCS programs both sides of the Atlantic	Alignment of C-TPAT and EU AEO-S programs Further harmonization of air cargo security regimes
Recommendations for improving SCS	Consider relevancy of the recommendations in the EU context	Learn from US mistakes and successes
Evidence of high quality government oversight	Consider establishing equivalent quality assurance body in the EU	Periodic, independent assessments EU's security programs Better oversight of EU's research projects

5 Conclusions and recommendations

The review of the GAO documents leads to some interesting findings. We found that the reviewed documents focus primarily on maritime and air cargo security, and that they largely overlook rail and road modes of transport. The air and maritime domains no doubt merit a great deal of attention, but we nevertheless recommend future GAO studies to investigate security challenges in road and road transportation, as well. The reviewed sample of GAO documents also neglects cyber security and supply chain resiliency, two increasingly relevant themes in the practice and theory of the modern-day SCS. We therefore recommend that GAO researchers and political entities, that assign studies to GAO, would address these themes in more detail in near future. Many GAO documents have also been published years ago, so there is an apparent need to update the contents of many GAO reports, especially in the area of air cargo security, a domain that has been subject to a relatively recent regulatory reforms (e.g., the regulation 185/2010 of the European Commission).

Moreover, given the high quality and relevancy of the GAO documentation to the SCS practice and theory, the EU might consider establishing a similar watchdog organization to assess effectiveness and efficiency of the SCS programs and SCS projects in the EU. The GAO documents provide, at least for the most part, first class analysis and propose warranted recommendations for improving US SCS programs. Because many of the US programs have their counterparts in the EU (e.g., the EU AOE is the equivalent of the US C-TPAT), and because similar programs most likely encounter similar problems at the both sides of the Atlantic, it would be useful for EU officials to study recommendations that the GAO reports propose and consider

whether it makes sense to put some of the recommendations in practice in the EU. The recommendations urge authorities, for example, to improve their information management practices, compliance monitoring, performance monitoring and risk-based decision-making. For instance, stepping up the compliance monitoring of the EU Authorized Economic Operator (AEO) program would allow border control agencies to put more trust on certified AEO companies and facilitate their cross-border trade. The risk-based decision-making holds a great promise for improving air cargo security screening without slowing down the speed of this time-critical mode of transport: if we were able to identify high-risk cargo, based for example analysis of rudimentary shipping information (e.g., sender, receiver and declared contents), we could subject high-risk shipments to stringent security controls and facilitate screening of low-risk cargo. Most importantly, understanding the GAO description of the US programs and the associated recommendations is crucial for a variety of EU regulators and policy-makers so that they can pursue further US-EU regulatory harmonization and mutual recognition of SCS programs. In particular, further harmonization could be achieved in air cargo security domain between the US certified screening program and the EU's security supply chain concept (covering Known Consignors, Account Consignors and Regulated Agents), at least in the areas of compliance monitoring and training. Also further harmonization of trusted trader programs, the US C-TPAT and the EU AEO, would lower security-related red tape and barriers for trade and logistics.

The review findings have some implications to the FP7-CORE. By addressing the overlooked themes and updating the obsolete GAO documentation, the CORE consortium could increase the project's impact on the SCS

policy making and practice. Those reviewed documents that deal with cybercrime and cyber security, clearly indicate that supply chain actors should pay more and more attention on the security of their ICT-based systems and communications. For this apparent reason, the CORE demonstrations might choose to include more elements of cyber security.

Acknowledgements

This paper results from the CORE Project, which has received funding from the Seventh Framework Programme of the European Commission, under Grant Agreement No. 603993. Ideas and opinions expressed by the authors do not necessarily represent those of all partners.

References

Government Accountability Office, 2007. Federal Efforts to Secure U.S.-Bound Air Cargo Are in the Early Stages and Could Be Strengthened, Aviation Security. Washington: GAO.

Government Accountability Office, 2008a. CBP Works with International Entities to Promote Global Customs Security Standards and Initiatives, but Challenges Remain, Supply Chain Security. Washington: GAO.

Government Accountability Office, 2008b. Transportation Security Administration Has Strengthened Planning to Guide Investments in Key Aviation Security Programs, but More Work Remains, Aviation Security. Washington: GAO.

Government Accountability Office, 2008c. Examinations of High- Risk Cargo at Foreign Seaports Have Increased, but Improved Data Collection and Performance Measures Are Needed, Supply Chain Security. Washington: GAO.

Government Accountability Office, 2008d. U.S. Customs and Border Protection Has Enhanced Its Partnership with Import Trade Sectors, but Challenges Remain in Verifying Security Practices, Supply Chain Security. Washington: GAO.

Government Accountability Office, 2009a. Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed, Maritime Security. Washington: GAO.

Government Accountability Office, 2009b. Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers, Supply Chain Security. Washington: GAO.

Government Accountability Office, 2010a. DHS Progress and Challenges in Key Areas of Port Security, Maritime Security. Washington: GAO.

Government Accountability Office, 2010b. DHS Should Test and Evaluate Container Security Technologies Consistent with All Identified

Government Accountability Office, 2011a. Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened, Port Security Grant Program. Washington: GAO.

Government Accountability Office, 2011b. Progress Made, but Further Actions Needed to Secure the Maritime Energy Supply, Maritime Security. Washington: GAO.

Government Accountability Office, 2011c. Progress Made, but Challenges Persist in Meeting the Screening Mandate for Air Cargo, Aviation Security. Washington: GAO.

Government Accountability Office, 2012a. Progress and Challenges Faced in Strengthening Three Key Security Programs Transportation Security Administration. Washington: GAO.

Government Accountability Office, 2012b. Container Security Programs Have Matured, but Uncertainty Persists over the Future of 100 Percent Scanning", Supply Chain Security. Washington: GAO

Government Accountability Office, 2012c. DHS Could Improve Cargo Security by Periodically Assessing Risks from Foreign Ports, Supply Chain Security. Washington: GAO.

Government Accountability Office, 2012d. Progress and Challenges 10 Years after the Maritime Transportation Security Act, Maritime Security. Washington: GAO.

Government Accountability Office, 2012e. CBP Needs to Conduct Regular Assessments of Its Cargo Targeting System, Supply Chain Security. Washington: GAO.

Government Accountability Office, 2013a. Action Needed to Strengthen TSA's Security Threat Assessment Process, Transportation Security. Washington: GAO.

Government Accountability Office, 2013b. DHS Could Benefit from Tracking Progress in Implementing the Small Vessel Security Strategy Maritime Security. Washington: GAO.

Government Accountability Office, 2013c. Progress and Challenges in Key DHS Programs to Secure the Maritime Borders, Maritime Security. Washington: GAO.

Government Accountability Office, 2014d. Ongoing U.S. Counterpiracy Efforts Would Benefit From Agency Assessments, Maritime Security. Washington: GAO.

Government Accountability Office, 2014e. Progress and Challenges with Selected Port Security Programs, Maritime Security. Washington: GAO.

Government Accountability Office, 2014f. Stakeholder Satisfaction Varies; TSA Could Take Additional Actions to Strengthen Efforts, Transportation Security Information Sharing. Washington: GAO.

Government Accountability Office, 2014g. CBP Needs to Enhance Its Guidance and Oversight of High-Risk Maritime Cargo Shipments, Supply Chain Security. Washington: GAO.

Government Accountability Office, 2015. Operational Scenarios to Ensure the Technologies Will Function as Intended, Supply Chain Security. Washington: GAO.

Grainger, A. 2011. Trade facilitation: a conceptual review. Journal of World Trade, 45(1), 39-62.

Hintsa, J., Gutierrez, X., Wieser, P., & Hameri, A. P. 2009. Supply chain security management: an overview. International Journal of Logistics Systems and Management, 5(3), 344-355.

Lee, H. L., & Whang, S. 2005. Higher supply chain security with lower cost: Lessons from total quality management. International Journal of production economics, 96(3), 289-300.

United Nations Conference on Trade and Development, 2014. Review of Maritime Transport. Geneva: UNCTAD.