

SECURITY SPAGHETTI: IS IT RECONCILABLE WITH SUPPLY CHAIN MANAGEMENT PRINCIPLES?

Andrew Grainger, PhD(London) MA(Warwick) BSc(Cardiff) CILT
Director, Trade Facilitation Consulting Ltd; grainger@tradefacilitation.co.uk

Keywords: security, supply chain management, trade facilitation, controls and procedures

Abstract

The UK, like many other modern-day economies, has recently witnessed an avalanche of new, security-focused control regimes in international supply chain operations. SITPRO and Grainger (2008) count 37 different, often overlapping, security driven procedures and controls. The resulting regulatory burden on supply chain operations can be described as 'security spaghetti'. Within some policy circles rhetoric seeks to strike a balance between enforcing additional controls and promoting international trade. This paper asks whether both can be achieved. It holds that regulatory control objectives do not necessarily have to be an additional burden and can be reconciled with supply chain management principles.

Security Spaghetti

Over the last few years there has been an avalanche of new security-focused control regimes with an explicit focus on international supply chains. These add to what is already a complex operational and institutional environment. Instruments have been drafted at international, regional and national policy levels and have direct implications on international supply chain operations. Examples of recent supply chain focused programmes include the United States led Customs and Trade Partnership Against Terrorism (CTPAT), Container Security Initiative (CSI) and the Secure Freight Initiative (SFI). The European Union has introduced its Authorised Economic Concept along with a comprehensive overhaul of its customs legislation – the so-called Security Amendment to the Customs Code. Many other countries have followed suite with similar initiatives. At the international level, further programmes include the World Customs Organisation's SAFE framework of standards, the International Maritime Organisation's security amendment to the Safety of Life at Sea Convention (SOLAS) and the newly drafted Ship and Port Facilities Security Code (ISPS Code), numerous conventions and recommendations from the International Civil Aviation Organization and the International Air Transport Association, as well as the International Standards Organisations ISO 28000 series of security management standards. In addition, the UK has added its own layers of controls and procedures through the agency of Customs, the Department for Transport and the Home Office. Each of these procedures places obligations on traders, their contracting logistics and transport providers as well as on port operators (sea or air). If mapped in a diagram, the regulatory overlap quickly resembles a bowl of spaghetti (Table 1).

While all of the previously cited regimes have been introduced since 11th September 2001, security and safety concerns are nothing new. SITPRO and Grainger (2008) count 37 different, largely overlapping, security-driven procedures that apply to businesses operating in the UK (Annex 1). Their analysis does not include the even longer list of security controls and procedures that are enforced by governments prior to goods arriving in the UK or after leaving the UK. Security-focused procedures can be group into four categories: 1) umbrella: aimed at security risks in their broadest sense; 2) goods specific: aimed at risks specific to individual types of goods; 3) control type specific: aimed at meeting narrowly specified control objectives; and 4) safety: concerning themselves with the safety of staff and use of critical infrastructure (Table 1). In addition to the regulatory driven burden, businesses apply their own, commercially driven layers of protection against unforeseen risks. These include normal due-diligence practices (e.g. collecting references, credit checking, signing of contracts and specification of guarantees) and insurance instruments (SITPRO and Grainger 2008).

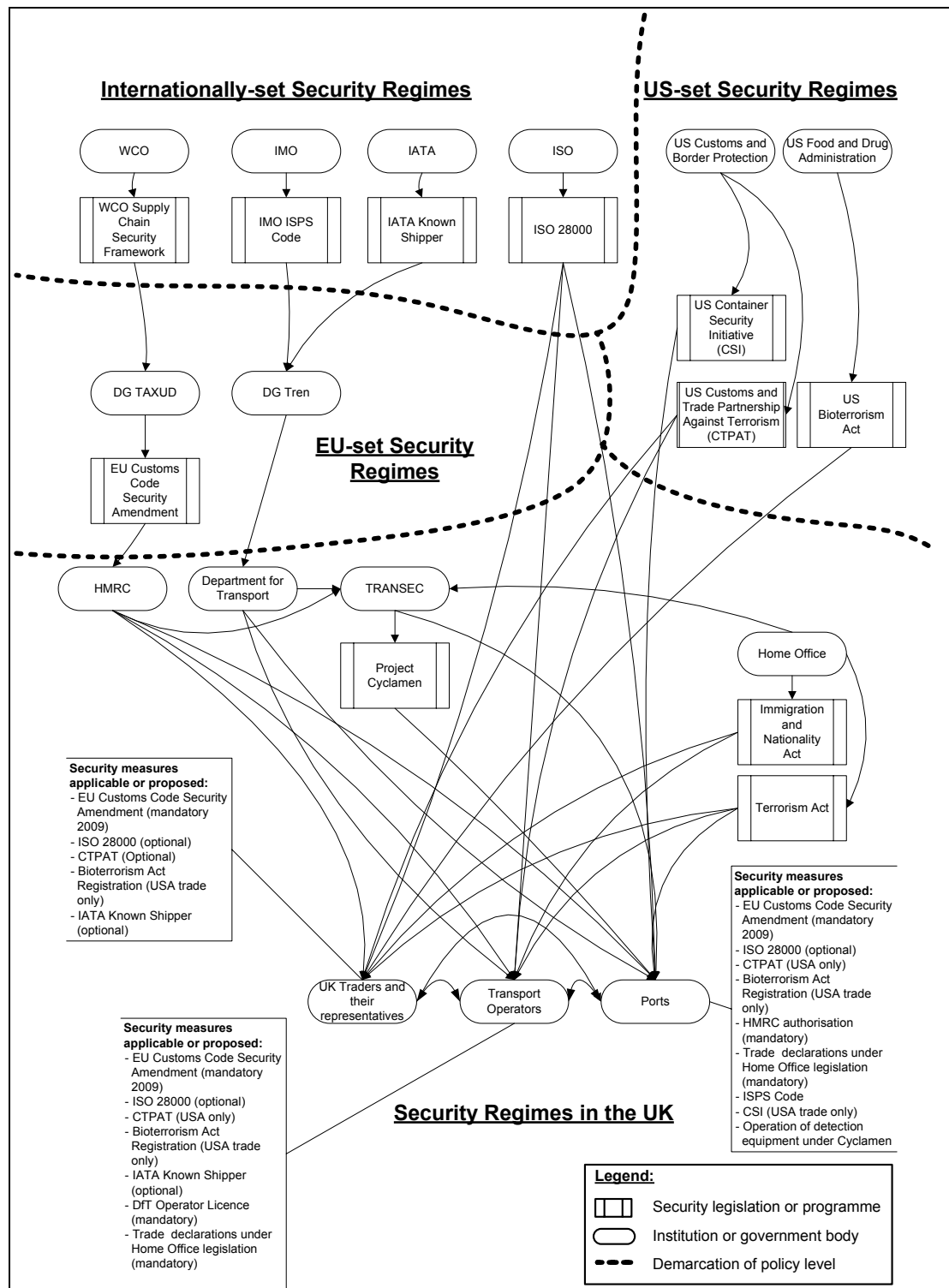


Table 1: Security Spaghetti (Grainger 2007b)

Security and Government Actors

Traditionally most controls in the international movement of goods take place at the border. The border (in the shape of a land-crossing, airport or seaport) is normally the first or last point over which a government is able to exercise sovereign authority. In contrast, the underlying objective for many of the newly added security regimes is to identify security risks before goods move. Underpinning these

new regimes is the desire by governments to enhance control without disrupting current trade flows whilst making best use of finite control resources (Grainger 2007b). To meet these objectives, enforcement agencies are now increasingly aiming at becoming an integral thread within supply chain operations – keeping a regulatory hold right through from supplier’s suppliers to customer’s customers (often referred to as ‘supply chain security’).

Regulators are now in the process of redefining their relationships with business operators across the supply chain. However, unlike the national border, the supply chain is a construct that governments do not directly own. They need to find means – such as through incentives and preferential treatment and coercion or sanctions – to encourage the desired degree of behaviour and cooperation from business actors. At the same time, governments are required to be sensitive to business needs. Heavy handedness, poorly designed operational practices and unnecessary disruption will drive businesses away and frustrate economic activity. For example, in a survey of UK importers 19% (N=131) of respondents admitted to actively diverting traffic cargo to an alternative port because of actual or perceived differences in the enforcement of rules and procedures (Grainger 2007a). Subsequently, many policy circles speak of the need to ‘balance’ security with facilitation measures (Grainger 2008b).

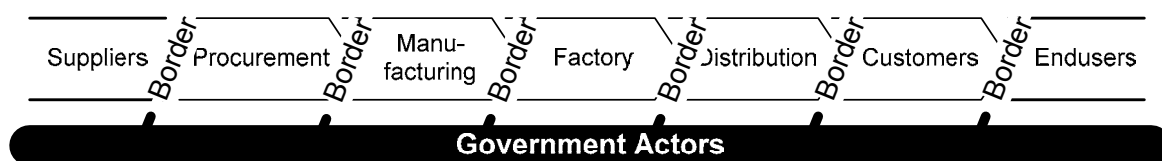


Figure 2: Government actors – a new thread running across the supply chain (Grainger 2007b)

Cost and Value: introducing a supply chain management perspective

In view of the considerable regulatory overlap and apparent duplication of activities between government agencies as well as amongst interacting businesses – across the supply chain – the question is whether there is a better way to meet regulatory control objectives. Businesses frequently complain about red-tape. Costs suffered can be direct and indirect. Examples of direct costs include: the payment of inspection fees, testing fees, security levies, the time and expense associated with submitting declarations, the costs associated with gaining accreditation, time spent making applications, fiscal securities, building security specific infrastructure (e.g. cameras, fences, computer systems), and more. Indirect costs can be described as those costs that are subsequent to direct costs. These include delays at the border, additional storage and demurrage charges, missed business opportunities and loss of competitiveness.

Good supply chain management practice, phrased in the simplest of terms, is about reducing costs and adding value (e.g. Christopher 1992). From the standpoint of security ‘value’ may be equated with ensuring that no security threats to business or society stem from within the supply chain. ‘Costs’ include all those inefficiencies that multiply the previously cited direct and indirect costs. Framed in terms of value and costs the question of tightening-up security is no longer one of striking a balance between control and facilitation. Rather, it is a question about how to add value (security) and reduce costs.

The Concept of Trade Facilitation

Fortunately, the question of meeting regulatory objectives – such as tightened security – and reducing costs is not new. Trade facilitation practitioners have been concerning themselves with this question for many decades. Surprisingly, there has been very little overlap into the related supply chain literature and published literature has only recently gained in substance. Trade facilitation recognises that transaction costs between business and government in international supply chain operations are undesirable. Its proponents have produced catalogues of prescriptive recommendations (e.g. UN/CEFACT and UNCTAD 2002). Trade facilitation themes specific to security now include: the use of risk management techniques; the development of partnership programmes between government agencies and businesses; the preferential treatment of authorised (trusted) firms and individuals; the standardisation of data requirements to reduce costs associated with lodging declarations and sharing information; cooperation and mutual recognition of controls between agencies and governments; and the replacement of paper documents with the use of electronic reporting systems (Grainger 2007c). However, current debate amongst trade facilitation practitioners includes many more concepts that

promise a reduction of costs whilst meeting regulatory objectives. Andrew Grainger lists 18 trade facilitation concepts (Grainger 2007c; 2008b) that concern themselves with the governing regulation and the use of information technology (Figure 3)

<p>Better regulation:</p> <ol style="list-style-type: none"> 1. Simple rules and procedures 2. Avoidance of duplication 3. Memoranda of Understanding (MoUs) 4. Alignment of procedures and adherence to international conventions 5. Trade consultation 6. Transparent and operable rules and procedures 7. Accommodation of business practices 8. Operational flexibility 9. Customer-service provisions for government administrations 10. Mechanisms for corrections and appeals 	<ol style="list-style-type: none"> 11. Fair and consistent enforcement 12. Proportionality of legislation and control to risk 13. Time-release measures 14. Risk management and trader authorisations <p>Information and communication technology:</p> <ol style="list-style-type: none"> 15. Standardisation of documents and electronic data requirements 16. Automation 17. International electronic exchange of trade data 18. Single Window
---	---

Figure 3: Trade Facilitation Concepts (Grainger 2007c; 2008b)

This would be a long paper, if it included a discussion on each of the listed concepts (for details see Grainger 2008b). However, their underlying desire is to improve the regulatory interface between business and government. At the heart of most of these concepts is the recognition that transaction costs between business and government are undesirable. Four guiding principles apply to reducing costs while meeting objectives. These are the simplification, harmonisation, standardisation and modernisation of trade procedures – including the 37 procedures identified by SITPRO and Grainger (2008) that concern themselves with security-type issues.

New Supply Chain Management Challenges

The growing interest of government actors in supply chain operations has many implications for supply chain management. Foremost, it introduces ‘Government’ as a new type of actor to the supply chain literature (Grainger 2007a). Government actors have a direct impact on supply chain operation by enforcing controls and physically interfering in the flow of goods. Moreover, they play an active role in shaping the environment within which supply chains operate. In view of the many procedures that concern themselves with security-type issues, businesses are right to question whether they add any value in terms of security. Subsequent pressure applied by lobbyist and business interest associations to overhaul trade and security procedures is legitimate. This gives rise to what Andrew Grainger (2007b) calls the ‘Trade Procedures Reform Cycle’ (Figure 3).

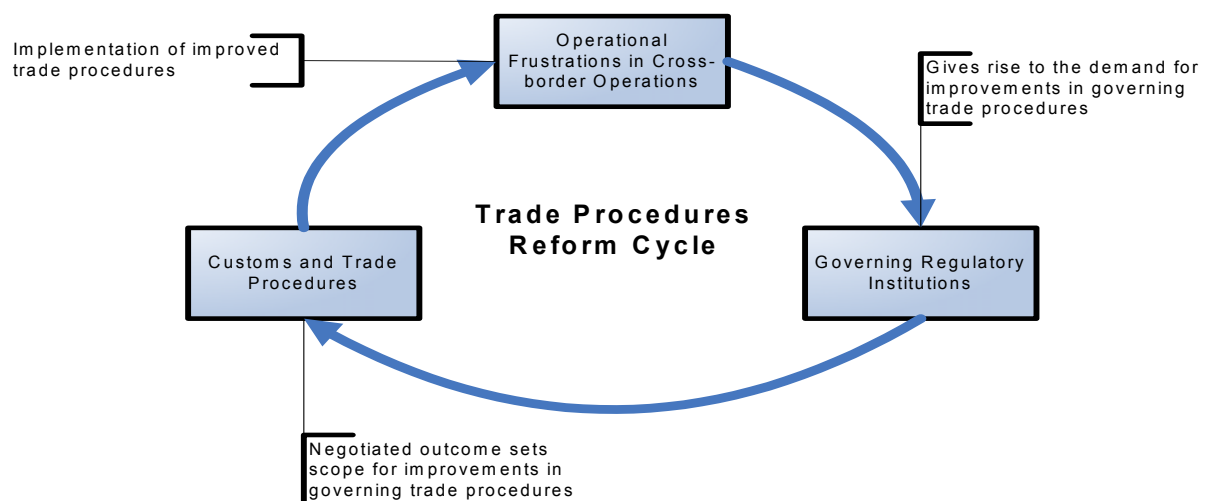


Figure 3: Trade Procedures Reform Cycle’ (Grainger 2007b)

As new procedures are being implemented a range of different business behaviours can be observed. For example, those with little experience in working with policy makers might reluctantly bow to the demands (and costs) imposed upon them through security regulations. Others might see new procedures as an opportunity to distinguish themselves from their competitors. Business strategies include the development of superior capabilities (e.g. by being innovators or first movers) and strategic positioning (e.g. by seeking a regulatory outcome that plays to their market strengths). Subsequently, a range of relationship building strategies between business and government are employed. These include: the shared use of IT systems; employment of 'boundary spanners'; use of shared office space and ensure physical proximity; use memoranda of understanding; participation in pilot programmes; active contributions to the work of business interest and trade associations; participation in government consultations and consultation groups; informal influencing of key policy makers; soliciting support from 'higher' institutions (e.g. international and regional bodies); taking private ownership of regulatory space (e.g. through self-regulation or use of industry standards); and mobilising or threatening to mobilise political power to achieve preferred regulatory results.

Unfortunately, any improvement to the regulatory environment is likely to suffer a range of obstacles that are not easily overcome. These include conflicting interests, institutional limitations and lack of knowledge (Grainger 2008b; 2008a). Conflicting interest in the shape of the regulatory environment may be found: between businesses with different types of operational requirements and capabilities; between business interests and the interests of individual executive agencies; between competing government departments (e.g. Department for Transport vs. Customs vs. Home Office); between competing policy priorities when bidding for implementation budgets; and between protectionists and liberal trade policy tendencies. Institutional limitations can be found: within the path-dependencies or 'stickiness' of existing regulatory regimes and sluggishness in accommodating regulatory improvements; between the distance that lies between policy executives and those with operational experience; and between local, national, regional and international regulatory dependencies that take time to negotiate.

Lack of knowledge is a further obstacle to finding regulatory improvements. International supply chains tend to be complex arrangements and vary from one company to the next. Few individuals are able to take an umbrella view. The operational detail has barely been explored and trade facilitation recommendations are largely prescriptive in nature. In contrast, a bottom-up approach to understanding the trade environment and cross-border operations is likely to yield many new insights that help find cost reductions and value (security) improvements. Research cuts across disciplines, bringing together the management disciplines (such as strategy, supply chain management, information technology, transport, operations and logistics), the legal fields (the laws of trade, customs, contract and agency amongst others) and the political and economic sciences (for example, economics, public administration, international relations and political economy). Few organisation or institutes have yet attempted to take on the challenge and develop a body of knowledge that can help find and implement improvements to the interface between business and government in cross-border operations.

Conclusion

This short paper has described a regulatory environment that includes many overlapping procedures that concern themselves with security-type issues. The paper asked whether security-type controls can be reconciled with good supply chain management practices where the objective is to increase value (security) and reduce costs. Trade facilitation is identified as a field which concerns itself with the challenge of meeting regulatory objectives and reducing transaction cost type burdens. In this light, one conclusion is that supply chain management as a discipline has much to gain by embracing trade facilitation as a topic. It introduces 'government' as an actor in the supply chain. It also widens research to include institutional and regulatory variables that stretch from examining the operational practices that are employed by government executives to the mechanisms that form and shape the environment within which supply chains operate. The paper also makes reference to how business actors seek to influence regulatory outcome. However, the obstacles that frustrate efforts – as evidenced by the many overlapping security procedures – remain all too evident.

Supply chain management as a research discipline is familiar with examining business systems and the dynamics found within the relationships between its actors. For example, the conflict between arms-length and cooperative behaviour is a common theme when examining supply chain relationships. The literature also recognises that in today's business environment competition

increasingly takes place between supply chains and not so much between individual firms. For example, Nigel Pain (2005) finds that nearly one-half of all merchandise exports to the USA (the UK's single largest export market) are by UK-based, US-owned affiliate companies and by UK parent companies to their US affiliates. Thus, when examining the current security spaghetti (or any other procedure with impact on cross-border operations) the guiding objectives of SCM – ensuring cost and value advantages – still apply. While obstacles to finding system wide improvements to security whilst reducing costs are formidable, it is a challenge that the supply chain literature should not shy away from.

References

- Christopher, M. (1992). *Logistics and Supply Chain Management : Strategies for Reducing Costs and Improving Services*, Pitman.
- Grainger, A. (2007a). 'Government Actors in International Supply Chain Management Operations: assessing requirements for skills and capabilities' *Logistics Research Network Annual Conference 5-7 September*, Hull, CILT.
- Grainger, A. (2007b). 'Supply chain security: adding to a complex operational and institutional environment' *World Customs Journal*, Vol. 1(2): pp.17-29.
- Grainger, A. (2007c). *Trade Facilitation: a review (Working Paper)*, Trade Facilitation Consulting Ltd: www.tradefacilitation.co.uk
- Grainger, A. (2008a). 'Customs and trade facilitation: from concepts to implementation' *World Customs Journal* Vol.2(1): 17-30.
- Grainger, A. (2008b). *Trade Facilitation and Import-Export Procedures in the EU*. Brussels, European Parliament
- Pain, N. (2005). *Networks, Multinational Firms and UK Export Performance*. National Institute of Economic and Social Research, <http://www.esrcsocietytoday.ac.uk>. [R000223590: 1-11]
- SITPRO and A. Grainger (2008) *A UK Review of Security Initiatives in International Trade*, London, SITPRO.
- UN/CEFACT and UNCTAD (2002). *Compendium of Trade Facilitation Recommendations UN/CEFACT*, UN: ECE/TRADE/279.

Annex I: Security Procedures and Controls Found in UK Trade Operations

1. Authorised Economic Operator	22. Customs Pre-notifications (Security)
2. Container Security Initiative (CSI)	23. Use of additional scanning equipment (e.g. x-ray scanners, scanning for radioactive materials, scanning for explosives, etc.)
3. Secure Operator - proposal	24. Immigration Controls (passengers)
4. Aviation: "Known Shipper"	25. Immigration Controls (vehicle operators)
5. Maritime: ISPS Code and SOLAS Convention	26. Financial crime and terrorist financing, restrictions and controls
6. ISO 28000	27. Prior Ship-notification
7. Customs and Trade Partnership Against Terrorism (USA)	28. Road Operator Licensing
8. TAPA-Freight Security Requirements	29. Immigration (outward) - as proposed under eBorders
9. Multi Agency Threat and risk Assessment	30. Dangerous Goods Declarations (Air)
10. Export Controls (Precursor Drugs)	31. Dangerous Goods Declarations (Rail)
11. Carcinogenic substances - Import Licences	32. Dangerous Goods Declarations (Sea)
12. Rough Diamond Certificate	33. Dangerous Goods Declarations (Road)
13. Export Controls (End-use and Destination)	34. Compliance with specified Health and Safety procedures for the handling of goods
14. Export Controls (Technology, Dual-use & Military)	35. Formal Cooperation Agreements between Businesses and Executive Agencies (including MoUs)
15. Medical Equipment Licensing	36. Due-diligence activities (e.g. contracts, guarantees, letters of credit, request for references, credit checking etc.)
16. Medicines and Drugs Licensing	37. Commercial Insurances
17. Animal Health Controls and Licensing	
18. Plant Health Controls and Certificates	
19. Food and Hygiene Controls	
20. Bio Terrorism Controls for export to the USA	
21. Secure Freight Initiative (100% freight screening)	