Supply Chain Integrity

An overview of the ICT supply chain risks and challenges, and vision for the way forward

VERSION 1.1

AUGUST 2015

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

The first version of this paper has been published in October 2012. It was written by:

- Scott Cadzow, Cadzow Communications Consulting
- Georgios Giannopoulos, European Commission – Joint Research Centre
- Alain Merle, LETI France
- Tyson Storch, Microsoft
- Claire Vishik, Intel

- Slawomir Gorniak, European Union Agency for Network and Information Security
- Demosthenes Ikonomou, European Union Agency for Network and Information Security

This is a refreshed version that takes into account current evolvements in the subject of supply chain integrity. The update was performed in August 2015 by Slawomir Gorniak (ENISA).

Contact

For contacting the authors please use sta@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

For the elaboration of this study, ENISA and members of the expert group referred to above, engaged with Member States' relevant competent bodies in a dialogue to analyse the challenges with regard to the security of the supply chain and to identify feasible solutions, and to carry out a corresponding consultation with the private sector. The input was collected during interviews led by the members of the group from the competent bodies (mainly national security agencies) and from the relevant industry experts. The study has been presented to the experts from the Working Group 2 on "Baseline requirements for security and resilience of electronic communications" of the European Public-Private Partnership for Resilience (EP3R).

We would also like to acknowledge the representatives of European national competent bodies and experts from the industry for their useful input to this work and comments.

Table of Contents

Executive Summary

Supply chain integrity (SCI) in the ICT industry is a topic that is receiving attention from both the public and private sectors (i.e. vendors, infrastructure owners, operators, etc.) as part of a wider review of supply chain control. Understanding supply chains is a critical factor in business success and thus to the economy of nation states, and integrity is the element of managing the supply chain that this report focusses on with a view to providing guidance to EU member states. One of the many aims of this paper is to identify what SCI means in the ICT context and to propose means of giving assurance of SCI. The ICT sector is all encompassing and it would be difficult in a single report to cover all parts of it thus the main body of this report primarily considers the telecommunications sub-sector as a model of ICT in general.

Supply chains have become increasingly global in recent years with supply chains becoming longer both geographically and in the number of supply elements. This is consistent with the wider globalisation of markets and the move away from a major industry and its suppliers being geographically local to each other. Telecommunications operators and equipment manufacturers increasingly rely on globally sourced components. For niche markets a single supplier may support the entire industry (e.g. Microsoft supplying Operating Systems to 83% of the PC market) with distribution channels serving the dependent markets. A characteristic of large parts of the ICT market is the ability to distribute software, firmware and chip designs in "soft formats" that gives a different perspective to supply chain analysis than consideration of other forms of raw material, logistic distribution networks, and staff.

The root of this report is the assertion that Governments, corporations, organizations, and consumers are increasingly reliant on ICT products and services, and thus on the supply chains that deliver them. As a result of this reliance threats to supply chains have attracted more attention, including the threat of intentional tampering during development, distribution or operations, or the threat of substitution with counterfeit (including cloned or overproduced) components before or during delivery, and attacks against the economy through the supply chain. The present report identifies the nature of these threats and examines the strategies that may be used to counter them. The report recommends that participants in the supply chain follow a core set of good practices that can provide a common basis to assess and manage ICT supply chain risk – and to recognize that governments must work in collaboration with private industry to build international assessment frameworks. Such frameworks should be:

- Risk-based and grounded in good threat modelling;
- Transparent;
- Consistent;
- Flexible
- Standards-based; and,
- Based on recognition of the reciprocity that characterizes international trade relations.

1. Purpose of the document

The main objective of this document is to report on a study identifying the threats, risks and possible solutions related to the integrity of the supply chain. Through desk research and interviews with competent national bodies and industry representatives the study identifies good practices and pursues this topic with a broad view on various industry segments, taking into consideration existing limitations. The survey on the state-of-the-art has included reviewing the experience from all the key players in the supply chain, starting from the chip manufacturers, passing vendors, integrators, and operators and leading up to review of the end user organizations from several sectors. It identifies the commonalities across sectors, taking into account views from all the parties, and the feasibility of bridging the gaps in developing common guidelines.

To summarize, the study provides:

- An overview of threats and risks to the integrity of the supply chain of ICT equipment and services – in particular possible technical manipulations which could be performed by untrustworthy suppliers
- Recommendations on possible solutions – in particular on measures which allow prevention and detection of adverse manipulations in the supply chain of ICT equipment and services and so mitigating the risks
- Advice on a general strategy regarding handling of products and services coming from untrusted sources, containing as many global factors as possible

The targets of this study are the decision makers in the Member States and at the EU level. It does not provide information directly applicable in the European procurement processes.

Due to the high sensitivity of this topic, ENISA has carried out all activities in this context only in consultation and on a consensual basis with the competent bodies of Member States with the results of the consultations anonymised for the purposes of the report. A high level of confidentiality was also necessary to maintain trust between ENISA and its industry partners.

2. Definitions

Supply chain – a system of organizations, people, technology, activities, information and resources involved in moving a product or service from supplier (producer) to customer

Integrity – a concept that is related to perceived consistency of actions, values, methods, measures, principles, expectations and outcome

Supply chain integrity – indication of the conformance of the supply chain to good practices and specifications associated with its operations

Supply chain execution – the operation of the supply chain

System integrity – requirement that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system (NIST-95)

Supply chain governance – this topic refers to the management and organizational processes associated with supply chains

Supply chain evaluation / certification – approaches to obtaining information about the conformance of supply chain to good practices or international standards.

Supply chain security – security of the processes, techniques, and technologies associated with supply chains

Supply chain integrity controls – methodologies to ensure that supply chains are operating in conformance with the expectations and controls which allow them to maintain integrity

Supply chain anti-counterfeiting techniques – mechanisms to improve assurance for the authenticity of the ICT products in a supply chain.

Supply chain resilience – a key element for its integrity, consisting of putting in place the elements of the supply chain in order to reassure the business continuity

3. Overview of Supply Chain Integrity

A supply chain is a system of organizations, people, technology, activities, information and resources involved in developing or producing a product or service from supplier or producer to customer. Supply chain activities transform natural resources, raw materials and components into a finished product that is delivered to the end customer. In sophisticated supply chain systems, used products may re-enter the supply chain at any point where residual value is recyclable.

A supply chain includes a channel of distribution beginning with the supplier of materials or components, extending through a manufacturing process to the distributor and retailer, and ultimately to the consumer. Integrity is a concept that is related to perceived consistency of actions, values, methods, measures, principles, expectations and outcome. Supply chain Integrity is therefore not an all or nothing binary attribute, so it is useful to compare the impact on Supply Chain Integrity before and after modifications to elements in the chain. For example, adding links to a chain by inserting un-vetted brokers lowers integrity, whereas procuring items directly from the original trusted manufacturer typically increases integrity. Manufacturers of original components frequently establish authorized distribution networks where the links in the supply chain are accountable and have certificates of conformance for proper product protection protocols. Links in a supply chain that do not have credible proof of conformance mean lower integrity.

The meaning of integrity can change considerably depending on the context of its use:

- In the context of information security, integrity means that the data has not been altered in an unauthorized manner, degraded or compromised;
- Within the software context integrity is often defined as ensuring that the process for sourcing, creating and delivering software contains controls to enhance confidence that the software functions as the supplier and the customer intended[1]; and,
- In ICT in general, integrity is a complex notion linked to the concepts of security assurance and trust (we trust systems when they behave and perform in the expected manner).

In the context of the supply chain, integrity is a composite of the above definitions and can be used to indicate conformance of the supply chain to good practices and specifications associated with its operations. There are standards that apply to supply chain integrity together with other issues of the supply chain, and there are many standards and guidelines for good business management that have been studied and which when implemented give more likelihood of understanding of the supply chain and its influence on the underlying business or industry. The goal of supply chain integrity in the ICT domain, is to ensure that ICT products meet the intended specifications and nothing more.

Supply chains are relevant for both products (in terms of a bounded collection of hardware and software) and services (in terms of an organized system of apparatus, appliances, employees, etc. supplying some user requirement).

- Product oriented supply chains may consist of software and hardware design, testing, production, delivery, repair, support, and maintenance as well as organizations, people, and processes, engaged in its operations.

[1] e.g., SAFECode

- Supply chains related to telecommunications services include network design, testing, installation, network management, and other processes related to IT service production as defined e.g. by ITIL.

In the studies of supply chain integrity, the focus is frequently on the product oriented supply chains. A body of knowledge and viable approaches and practices have been developed in industry sectors such as automotive, aerospace, semiconductors, and telecommunications. The progress that has been made has permitted the technologists to move forward with the formalization of the knowledge acquired to create standards covering specific elements of the supply chain and to advise on best practices.

The field of supply chain integrity is now ready to look for commonalities in these standards, practices, and requirements, to move the field to a new level. A more coordinated framework is only beginning to emerge. We hope that this paper will permit the community of research and practice to move forward in combining productive approaches that have worked well in the past for a better vision of the practices that can improve supply chain integrity.

The definition of such a higher level framework needs to rely, in part, on common threat models, but creating such a threat model for supply chain remains a challenge. This is because threat analysis is easier to perform when it is product and service specific, and it remains context-dependent. In a hardware example, an integrated circuit that can be re-programmed after it ships from the original component manufacturer is easier to modify (attack) that an integrated circuit that can only be programmed with a ROM mask during wafer manufacturing. This threat is specific and doesn't apply to software or pharmaceutical products. In general, hardware threat profiles differ from software threat profiles. Consequently, approaches to supply chain integrity for different areas are context dependent, but have enough commonality to support the creation of a higher level coordinated framework.

We can generalize threats to the supply chain along simple principles. For example, it is clear that we need to mitigate attacks that are harmful and likely to occur first before working on mitigating attacks that are rare or unlikely to cause harm. This view is general and can help us work on a more general threat typology or a canonical set of high order threats that can help analyse a large proportion of the situations. In order to generalize the threats, we need to move from the context-based to general examples, and previous work in the area of supply chain integrity has created the premise for such a generalization.

Finally in an ICT context, an appropriate definition of integrity for supply chains includes the requirement that the delivered system performs its intended function in an unimpaired manner, free from deliberate or inadvertent manipulation[2].

[2] EU FP7 project BRIDGE (Building Radio frequency IDentification for the Global Environment), Deliverable D4.6.1: Supply Chain Integrity, December 2007 http://www.bridge-project.eu/data/File/BRIDGE_WP04_Supply_Chain_Integrity.pdf

4. Landscape of supply chain efforts

Current efforts in, and outside, the European Union have attempted to address various parts of the Supply Chain Integrity problem without initially stating what the problem is. Without a common problem statement it is difficult to state if the efforts being made are consistent, supportive or co-operative, or at worst divisive. However the very fact that many organisations in standardisation and in industry and in government have indicated a concern suggests that there is a common problem to be addressed. The work reviewed in the present report has made an attempt to catalogue the areas that these efforts cover, their participants, and the amount of overlap between efforts. The results presented herein indicate that although many countries, industries and agencies have similar concerns they are not working together to coordinate their efforts. The immediate conclusion is that there is an unfulfilled requirement for coordination of the efforts in the field. The present report is therefore in part the recommendation from ENISA of actions required to drive such a coordination programme.

While today's ICT and other supply chains are very complex, progress has been made in identifying current practices for some of the fields of study. The present report identifies some of the standards and definitional efforts as well as official reports connected with Supply Chain Integrity across the spectrum of problems. It aims at providing a more coordinated picture of SCI and to raise awareness of the gaps that remain and that need to be filled, in order to allow for a common approach to the Supply Chain Integrity and thus to harmonisation of SCI across the EU and it Supply Chain partners.

The importance of Supply Chain Integrity topic has been recognised in Europe for the first time by the ARECI study on the availability and robustness of electronic communication networks (http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm).

A number of means of classifying SCI standardisation efforts may be defined. For the purposes of this report the following broad lifecycle classifications are considered:

1. Origins (sources) of supply chains
2. Delivery and governance of the Supply Chain
3. Processing and configuration
4. Integrity techniques
5. Verification and checks

The listing of standards in Table 1 does not claim to be complete but is rather intended to indicate to the reader some of the confusion and diversity of standardisation efforts in the SC and SCI domains. The standards cited in Table 1 have created a strong impact to date and have sparked interest in SCI as a topic in its own right. However, it is evident that approaches to SCI continue to be fragmented. The activities highlighted should have a follow-up in order to create a consistent view, consistent practices and, eventually, consistent metrics that cover supply chain activities.

Table 1: Classification and identification of SCI standardisation efforts

Classification	Standard Development Organisation	Standard	Comments
1 Origins (sources) of supply chains	ISO SC27	ISO/IEC 27036: Guidelines for Security of Outsourcing	These are generic documents and not specific to SCI
2 Delivery and governance of the Supply Chain	NASPO (North American Security Products Organization) NIST		Nothing specific to SCI
3 Processing and configuration	ISO SC31 iNEMI Supply Chain study group HDPUG Supply Chain study group:	RFID supply chain applications Risk Modelling pilot Data Exchange pilot	Nothing specific to SCI
4 Integrity techniques	JTC1-SC27 Safecode Open Group	N10656: Update to ISO 27002: Security Techniques Open Trusted Technology Framework	Nothing specific to SCI
5 Verification and checks	ISO TC247	Fraud Controls and Countermeasures SEMI T20: Traceability (semiconductor industry)	Nothing specific to SCI

5. Supply Chain Integrity conceptual framework

5.1 Introduction

In order to evaluate SCI and to give assurance of SCI it is necessary to model it in sufficient detail to allow all the actors and stakeholders to visualise and analyse their role in SCI. There are multiple viewpoints of SCI, including those of policy makers and regulators, those of the manufacturers, of the operators, and of procurement. The model framework has to be readily understood and be useful at all levels and be extensible to cover their specialised views within SCI.

First, it should be noted that a supply chain is not really a chain with each link joining 2 suppliers together and there being a single path from start of the chain to the end of the chain. In such a chain the loss of a single link is visible and straightforward in its impact – the chain breaks (see Figure 1).

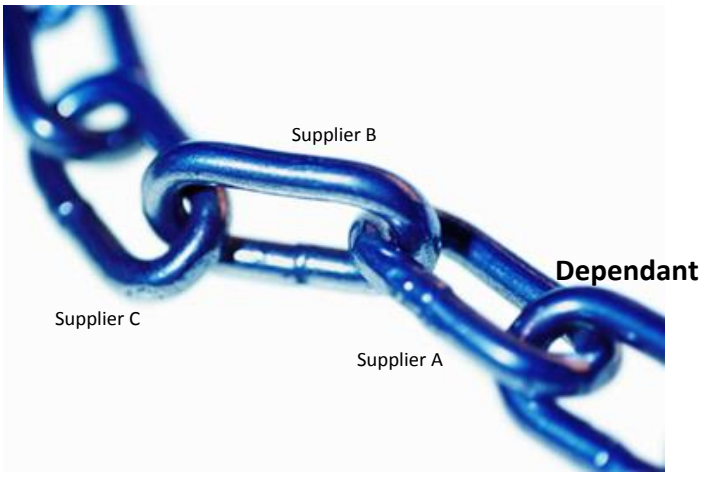

Figure 1: Simplistic view of a supply chain

In practice supply chains are more like the fishbone structure of Figure 2 in which each supplier has their own supply chain and in which a single supplier may exist in many chains.

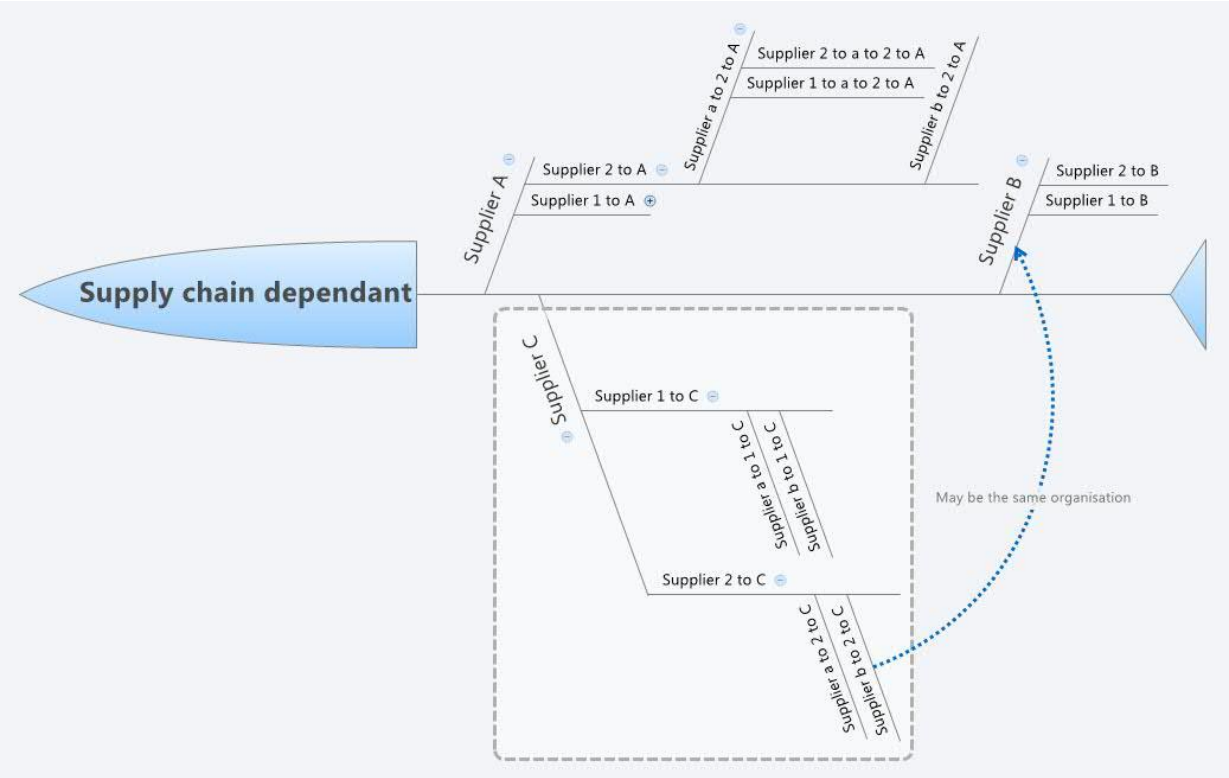

Figure 2: Supply Chain generic view

Thus when considering the topic of SCI it is critical to fully specify the point of view being assessed and the goals of such an assessment.

In order to achieve consistency, constraints are placed on the supply chain to ensure integrity. These may take the form of technical measures (often referred to in the security domain as controls) to prove the authenticity and integrity of components, and procedural controls to validate the means by which suppliers are selected and managed. In addition techniques, technologies, and operations need to be defined to support integrity. Secure environment, secure development and authenticity are some generic attributes that can be used in order to establish a conceptual framework of supply chain integrity.

At a more technical level, these terms are specialized to certain measures and instruments that are used in supply chain operations in various sectors. This approach is applicable to process, technologies and human resources-related procedures that complete the image of the supply chain.

Delivery of products and services, including ICT products, has to comply with export, import, and customs (border control or border crossing) regulation as well as rules regarding some aspects of delivery of certain products (these are not harmonised but may include areas such as timing (e.g. for degradable goods), methods, safeguards (e.g. handling of dangerous goods)).

Not all parts of the supply chain exist in the same legal jurisdiction, and the framework for supply chain integrity needs to analyse the effects of geographic differences. Examples of issues that display some levels

of diversity include: liability (although it is mostly an ex-post legal instrument); and export control[3]. Although supply chains rarely include personal information, data movement in the supply chains needs to be designed in a privacy friendly manner and if privacy legislation is assumed to apply to legal entities then the legal entities involved in the supply chain have to be protected in line with such legislation. When discussing integrity-related standards, practices, and approaches, privacy needs to be taken into consideration early in the process. The EU guidelines on Privacy Impact Assessment may act as a suitable starting point for such considerations.

It is important to ensure that dynamic supply chains are fault tolerant and can recover from failures in a predictable manner. We need to determine how a supply chain can be maintained if its links are damaged – hence we need to link supply chain integrity and supply chain resilience when designing standards, best practices, and approaches to integrity,. In most industries, good practices have been developed to support recovery in case of serious problems. These practices are by necessity context based and define a wide range of situations such as limited availability for spare parts for older products, catastrophic or weather events, testing, introduction of new products, etc. Most of these practices do not apply directly to integrity as defined in this paper, but these activities are necessary to improve integrity as a general feature of supply chains.

5.2 Risk management areas

5.2.1 Secure environment

Robust risk analysis cuts across all the elements previously mentioned in order to quantify and qualify risks to the integrity of the supply chain. In doing so, the analysis identifies the cost of disruption of the SC and may be used to evaluate alternative scenarios related to measures applied to the SC, which improves the integrity and resilience and their associated costs.

In 2005, the American Defense Science Board focused on the technical solutions for issues associated with the introduction of multiple suppliers of hardware and software[4]. The program "Trust in IC"[5] was started by DARPA in 2007 to develop efficient methods for Hardware Trojan detection as well as hardware "fingerprinting" based on intrinsic properties of integrated circuits. For SCI such programmes should be seen as components within the overall risk management strategy.

In the European Commission, Project UNIQUE funded under Future and Emerging Technologies program focused on similar issues, developing early stage technologies that could counterbalance more advanced forms of counterfeiting.

The approach to systems analysis and evaluation given in the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), and specifically the means to identify the boundary between environment and system (for this document the system is the Supply Chain), and the means by which the system under evaluation interacts with the environment, is recommended as a starting point to analysis of the supply chain. Notwithstanding that the Common Criteria (CC) is a norm dedicated to the evaluation of security products and has been used to assess the security performance for a wide range of products, from integrated circuits to software components it is also suitable to analysis of large and dynamic systems. The rigour of complying to CC identifies and places requirements on the product or service (security functions)

[3] For example devices containing cryptographic material are classified as dual-use goods and subject to certain constraints are not freely exportable across international borders.
[4] American Defense Science Board. "Task Force on High Performance Microchip Supply". 2005
[5] DARPA. "Trust in Integrated Circuits (TIC)". 2007. Available at: http://www.darpa.mil/MTO/solicitations/baa07-24/

and gives proof to 3rd parties that the requirements are fulfilled and sufficient to address the security problems, this extends through the life cycle of the product or service and stresses Integrity Assurance (IA) as a key concept for the development environment and configuration control. This requirement mainly relies on the idea of an "acceptance procedure" when integrating Commercial Off The Shelf (COTS) components, bespoke components, commercially available development tools into the design or the production of a device. However, in practice, controls are limited to what is technically realistic (i.e. limited ability to apply custom controls to commercial tools or devices) and most often applied in the design phases. Currently, efforts are under way to develop supply chain guidance in the CC to further address integrity issues in evaluations. This work is in its initial stages and requires collaboration of multiple stakeholders to determine feasibility and develop new ideas in this area.

Resilience of supply chain is a key element for its integrity. It is in the core business of supply chain integrity since it is the only instrument that can reassure the continuity of the supply chain in case of disruptive/malicious events. It consists of all these elements that should be put in place in the supply chain in order to reassure the business continuity (e.g. recovery plans, increase the buffering capacity of the supply chain).

5.2.2 Secure development

A number of standards including IEEE/EIA 12207.0[6], ISO/IEC 12207[7], ISO/IEC 15504[8], and ISO/IEC 15288[9] identify a number of stages in the lifecycle of a system against which it is necessary to identify the set of SCI functions, if any, to be implemented in the system and all include essentially the same set of processes:

- Primary life cycle processes
    - Acquisition process
    - Supply process
    - Development process
    - Operation process
    - Maintenance process
- Supporting life cycle processes
    - Audit process
    - Configuration Management
    - Joint review process
    - Documentation process
    - Quality assurance process
    - Problem solving process
    - Verification process
    - Validation process
- Organizational processes
    - Management process
    - Infrastructure process
    - Improvement process

[6] IEEE/EIA 12207.0, "Standard for Information Technology – Software Life Cycle Processes"
[7] ISO/IEC 12207:2008 "Systems and software engineering -- Software life cycle processes"
[8] ISO/IEC 15504 "Information technology — Process assessment", also known as SPICE (Software Process Improvement and Capability Determination)
[9] ISO/IEC 15288:2008 "Systems and software engineering -- System life cycle processes"

- Training process

SCI can only be successfully applied when the steps or processes are satisfactorily completed across the lifecycle, otherwise it would be difficult to give assurance of the authenticity or integrity of any component. Thus a key element in both development and SCI management across the lifecycle is the identification of points of measurement, and points of intervention or control. It should be stressed that not all of the processes identified above need modification to address SCI but it is stressed that the SCI analysis has to consider all of the processes.

- SCI Point of Measurement (PoM)
  - A point in the overall SC where the integrity can be measured and compared to the control value[10].
- SCI Point of Control (PoC)
  - A point in the overall SC where intervention can correct the overall SCI.

Having addressed the lifecycle processes the secure development of a Supply Chain has to assess risk through analysing the impact and likelihood of attacks, covering malicious, "accidental" and planned (e.g. degradation, maintenance), on the system and from this analysis identify the set of controls (SCI PoM and SCI PoC) necessary to manage the risk to an acceptable level of residual risk.

5.3 Authenticity

Within the supply chain, authenticity applies to both the supplier and the supplied product.

One of the goals of ICT Supply Chain Risk Management is to manage supply chain risks in a way that provides reasonable assurance that products haven't been tampered with during development or their subsequent production and that the customer gets the product that he expected. When working with trusted suppliers along well defined guidelines and standards, the risks of counterfeit products or concerns about the authenticity of suppliers can be minimized.

5.3.1 Component authenticity

In complex ICT systems, components may be software, hardware, documentation, or a mix of these. The measuring of authenticity, and subsequent asserting a level of assurance to, a component is intrinsically complex. The recommendation is that acceptance of a component (service or product) is subject to acceptance criteria that are explicit and achievable and asserted at delivery. This has been the norm in many component supply industries and has been addressed in many very detailed procurement specifications prepared that suppliers have to comply with. This is a contrast between detail procurement specifications and the standards produced by many SDOs. Whilst SDO specifications may be cited in procurement they may not be sufficient to prove authenticity (in practice most standards are "minimum" to allow interoperability of many implementations complying with the standard).

Methods to verify claims made about a component are necessary to establish and maintain supply chain integrity; this may include a signed component compliance report.

Active adversaries can attempt to insert tainted or counterfeit components into supply chains, and component verification and authentication methods are needed that can quickly detect when penetration attacks have succeeded. These verification methods can be used in conjunction with a sampling plan to monitor the integrity of components in supply chain to a statistically confidence level. Defining the required confidence level is beyond the scope of this document, but is a worthy goal for the continuation

[10] The metric used to identify the level of integrity that the system has to achieve

of this work. The sampling rate and the selection of samples have to be sufficiently random to inhibit the opportunity of an attacker to avoid detection (on the understanding that not every item can be subjected to detail acceptance testing).

It is noted that the design for assurance paradigm promoted in ETSI and elsewhere may provide a framework for the steps to achieve component authenticity.

5.3.2 Supplier authenticity

Verifying the authenticity of a supplier is not always straightforward and properly identifying a supplier is unlikely to be sufficient. There are a number of supplier quality measures that may be used to gauge the viability of a supplier including Quality marking (e.g. ISO 9000 series certification), Security Management (e.g. ISO 27000 series certification) and Environmental process management marking (e.g. ISO 14000 series certification). As noted earlier, SCI can also be translated to trust to the various suppliers that compose the whole chain of the product to be delivered and in addition to the various ISO schemes may be added past and current financial performance; past and current SC performance. In the area of financial performance, the Just in Time schemes, such as the Balanced Scorecard, may be considered as a trust building element.

Aside from partner assessment (i.e. who to trust and allow to enter the SC) there are technical means to consider for trust validation, including, technical approaches to trust and integrity, such as integrity metrics, digital signatures, and Trusted Computing techniques including the Trusted Platform Module (ISO/IEC 11889).

Verifying the claims of each suppler in a chain is an important, but not necessarily sufficient process step in establishing integrity of a supply chain. Claims of certification to standards (such as ISO 9000, ISO 14000, ISO 27000, etc.) need to be authenticated and verified. Records that these claims have been authenticated need to be protected (e.g., with digital signatures or other IT security techniques). Other criteria to establish confidence in a supplier, such as financial or operational performance may be included in authentication reports.

5.3.3 Trust in the supply chain

There are a number of elements that may be used to build trust in SC partners that include: personnel identification and authentication; access management; past and current financial performance; past and current SC performance.

There are technical means to determine if the entity at the end of the SC is a genuine representation of the SC (noting that each SC link (or node) may modify one or more components). At the technical level, SCI can be reassured within a secure environment, through secure development and through authenticity proofing of the end product:

- Secure environment in this instance is an environment in which intentional insertion of malware or other intentional tampering with a product or service during product development or production operations has been mitigated.
- Secure development and production is that set of processes and procedures deployed in order to give assurance that the quality of the final product (as well as any intermediate products) is within the contractual boundaries.
- Authenticity gives assurance of the genuineness of the final product as coming from a managed supply chain.

It is one of the recommendations of this report that a (physical) supply chain establishes a “Chain of Custody” of elements in the supply chain. Conceptually this is similar to a “Root of Trust” for digital certificates and digital signatures in Public Key Infrastructures (PKI). The process should include a method

to detect false chain-of-custody claims. If the chain of custody documents and the shipment manifest documents are digitally signed, a basis to believe supplier claims about the handling of components is established. However in making such a recommendation it is recognised that the scope of “Chain of Custody” assertions may be limited as many supplier arrangements are subject to non-disclosure agreements, in other words if Party A receives goods from Party B there may be no means of Party A knowing details of the chain of custody of any party further back in the chain than Party B without violating commercial privacy or non-disclosure agreements.

One aspect of SCI integrity is trust between the system integrator (hardware or software) to the various suppliers that compose the whole chain of the product to be delivered, and also trust between the intermediate suppliers of the chain. From the smaller subcontractor that develops components or software code to the final system integrator, to delivery to the end user, trust is identified as the key element that assures the operation of the supply chain. However, trust is not easily measurable, and more concrete assessments need to be developed to evaluate supply chain integrity. This aspect of the supply chain integrity highlights the complexity of the issue as although the final creator bears the responsibility for a product, it is important to remember that most ICT products today are built from multiple and diverse components (e.g., a smart phone contains more than a hundred parts from different suppliers, and a modern car contains hundreds of such parts). The reality of this is often evident if a claim against a product is made to the final creator, who in turn will seek damages from across the supply chain. Software and applications present the same level of diversity, especially in mobile devices where distributed application development is enabled and encouraged.

6. Challenges

6.1 General observations

Electronic communications networks comprise numerous network elements, many of them consisting of outsourced components supplied by both new and established equipment vendors. Over the last few years, network operators have been deploying multiple network technologies in support of multiple services in order to increase their market share by capitalizing on the trend towards convergence in the services offered to end-users of ICT products. This trend has led to a situation where single network operators have to manage and co-ordinate different network technologies whose interfaces are not always standardised and may instead be based on incompatible software and hardware architectures, supplied by multiple equipment vendors.

Today's supply chains are global. The global nature of the ICT markets complicates the structure of the supply chains and underlines the importance of maintaining their integrity. The role of standardisation as a means of reaching consensus amongst an affected community on how to interface between two technologies cannot be understated: Standardisation may reduce the risk of an operator having to bridge the gap between vendors and suppliers thus mitigating some of the vulnerabilities. At the same time where the standards are open and well defined, the market is open to entrants from a wider geographic span and this may exacerbate the difficulties of SC management.

One common business model followed by network operators when outsourcing the deployment, operations and management of network(s) is the use of equipment from different vendors (multiple vendor strategy). This allows network operators to benefit from the competition between equipment suppliers while at the same time reducing the risk of having all network operations controlled by a single vendor. However, such market decisions lead to increased complexity in verifying the integrity of the supply chain. It also may increase the risk of unknown vulnerabilities being introduced into the supply chain if best practices are not observed and controls are weak, but this is true for every type and areas of a supply chain. In the case of the failure of the controls, the responsibility ('overhead') for fault detection, isolation and resolution could be placed on the network operator. However, modern network operators have processes, practices, and standards in place to protect their operations.

To summarize the challenges posed by a study of integrity of the ICT supply chain include:

1. Complex nature of globally distributed supply chains (people, processes, and technologies)

   Components used in ICT are manufactured in various countries around the world and, in many cases, are assembled in other countries and eventually sold in still more countries. They may be contracted by resellers and integrators with a global scope of activities and subsequently installed and operated by a variety of organizations.

2. Lack of common guidelines for achieving and measuring ICT supply chain integrity

   Good practices and guidelines have been formulated by different industries, but they are not always consistently used in purchasing and protecting the supply chain. Not implementing standardized practices in purchasing, appropriate for each industry segment, makes it harder to ensure that products are not altered, counterfeited, or misconfigured.

3. Absence of tools, processes and controls to help measure statistical confidence levels and verify integrity across the IT ecosystem

Existing approaches and tools are, in many cases, not compatible with today's dynamic environment. The evaluation focuses on blueprints rather than actual instances of systems and is slower than the requirements of the typical product cycle of today.

4. Ineffective methodologies and technologies for end-user verification of products

   Systems delivered to the end-users cannot always be evaluated because of a lack of appropriate evaluation approaches, methodologies, and tools.

5. Lack of broadly applicable tools, techniques, and processes to detect or defeat counterfeiting and tampering in systems to assist in the definition of a coordinated framework.

   New tools and approaches are necessary to help defeat counterfeiting for all ICT products at all levels of the supply chains.

6. Lack of coordinated approaches to preserving integrity for different types of products from production to deployment

   Product manufacturers and software developers own product integrity through delivery to the first owner of record. Purchasing organizations need better purchasing methodologies to keep counterfeits and subverted products out of their inventories and systems. The absence of common, well-defined framework(s) addressing the problems shared by all entities involved in the ICT supply chain presents an opportunity for technologists. All points of the supply chain can be evaluated and the best known methods can be shared, while looking for gaps in coverage. This is especially important in light of the growing sophistication of attacks on various elements of ICT infrastructures.

7. Absence of compatible integrity requirements across various ICT segments

   The ICT supply chain is not homogeneous. Many organizations claim to have developed and articulated, from varying points of view, their own good practices, approaches and technology tools to assure the integrity of their supply chains. However these are often organisation or sector specific and have rarely been made open for review or for use by other organisations or sectors. Consolidation of this knowledge and these approaches is necessary for progress.

6.2 Concerns expressed by the public and private sectors

Concerns expressed by both public and private sectors are converging to similar conclusions, only the target of potential threats is different. On the side of governments the stress is on the continuity of functioning of the critical public services, on the side of the industry the continuity of their normal operations.

In 2011 ENISA performed a study entitled 'Technologies with potential to improve the resilience of the Internet infrastructure'[11] where supply chain integrity was also considered. The participants in the study represented seven countries and 16 organizations, including telecommunications and Internet operators, network vendors, research institutes and universities and others.

In this study a questionnaire was sent to several telecom equipment suppliers, telecom operators, regulators and government authorities. Added to this, about ten people of the same type of stakeholders and several European national security agencies were especially interviewed in relation to supply chain integrity issues. Generally the summary of the questions and interviews was.

[11] 'Technologies with potential to improve the resilience of the Internet infrastructure', December 2011,

Awareness of supply chain integrity: Supply chain integrity is known as a basic concept to most of the respondents, but at a deeper level it was fairly unknown.

Standards or good practices related to the supply chain integrity: Standards or practices related specifically to supply chain integrity are usually rarely implemented. When they existed, they were based on traditional security or procurement frameworks rather than focusing on the supply chain itself. Some of the respondents try to control the supply chain by agreeing with the supplier directly. The telecom equipment suppliers are willing to implement supply chain integrity auditing methods to their processes, e.g. vendor audits are in use. In the other groups assessing supply chains was minimal. There are some methods and practices used to audit and test the telecom equipment (like in CSEC) but they are complex and time consuming.

Internal/external regulation (liability, export control, privacy) of HW/SW: Most respondents commented that procurement of new HW/SW is subject to internal or external regulations, such as procurement laws (public sector) and ISO 27001/2 security standards, and internal security testing procedures were also mentioned. Only one operator organization had tests of security features of the hardware and software before acceptance. One governmental organization performed risk analysis to parts of the system (i.e. did not carry out a comprehensive risk analysis).

Metrics related to the supply chain: No supply chain integrity specific metrics are used in supply chains among respondents. Otherwise supply chains are measured in traditional metrics, e.g. service level agreements (SLA) in service oriented supply chains. In fact the SLA levels were the only metrics mentioned relating to supply chains.

Risks on telecom network implementation: The people who were interviewed pointed out that besides the product supply chain integrity it is even more important to assure the integrity of the service chain. From the network resilience point of view the priorities of supply chain integrity are:

1. Network management and maintenance
2. Network implementation
3. Network design
4. Network products

In general the service providers interviewed for the purpose of this study agreed that problems in supply chain integrity may have a big impact on the resilience of telecommunications networks. It was a common understanding in the interviews that service oriented supply chains (network management and maintenance, implementation) were more critical factors to resilience than product oriented (hardware/software) supply chains.

Sharing of supply chains: The suppliers, in their products or services, often have components which are also in use in their customer's products and services. The same components are used in network devices. Especially in low end devices the core chip sets are produced only by a handful of vendors. The software may be also shared: in many embedded devices there is Linux or FreeBSD running in the core. Protocol stacks are also often shared by several vendors. A zero day vulnerability in these core hardware or software components affects a large number of products from different vendors. The similar situation is on the service supply chain. The same service company may be supplier to several operators. A security problem in the processes or personnel of this supplier affects a large group of operators, in the worst case all the major player in a certain country.

General observation from this stock taking is that the assessment of supply chain integrity is uncommon with exception of certain vendors. The concept is fairly new, its importance is not fully recognized, there are different views of its focus (product vs. service) and generic, standardised good practices have not been developed for it.

6.3 SCI future outlook in the context of the Transatlantic Trade and Investment Partnership (TTIP)

The ultimate goal of the Transatlantic Trade and Investment Partnership (TTIP) is to increase trade and investment between the EU and the US by unleashing the untapped potential of a truly transatlantic market place. It is aimed at removing some of the barriers limiting free trade between EU Member States and the US. The following areas are in the focus of TTIP:

- Greater regulatory compatibility between the EU and the US
- Paving the way for setting global standards
- Eliminate duties and other restrictions for trade in goods
- Freeing up commercial services, providing the highest possible protection,
- Increasing access to American public procurement markets
- Removing unnecessary regulatory constraints on trade
- Obtaining stronger protection of European Geographical Indications
- Facilitating customs formalities
- Addressing competition rules.

TTIP was officially launched on the 17 June 2013, after a series of negotiations that began in 2011. The Commission has foreseen that the talks will last 'a couple of years'.[12] The TTIP is negotiated between the European Commission from the EU side (DG TRADE) and the Office of the US Trade Representative on the US side. The current scope of TTIP consists of many areas including **ICT (e-health, encryption, e-accessibility, enforcement and e-labelling)**. The European Commission maintains a list of areas and their status, available at the EC web site[13].

Support for ICT supply chain and the introduction of relevant integrity measures are not explicitly mentioned in TTIP. However, supply chains have become global, which is consistent with the globalisation of markets. ICT operators and equipment manufacturers increasingly rely on globally sourced components. In this respect, specific good practices should govern the ICT supply chain.

One of the important goals of the TTIP is to facilitate an easier access to public procurements in the EU and US. Harmonizing these approaches from the point of view of ICT (compatibility, security) and supporting harmonized public procurement rules is also of interest.

[12] FAQ on the EU-US Transatlantic Trade and Investment Partnership
http://trade.ec.europa.eu/doclib/html/151351.htm
[13] Source: State of Play of TTIP negotiations after the 6th round 29 July 2014,
http://trade.ec.europa.eu/doclib/docs/2014/july/tradoc_152699.pdf

7. Gaps analysis

Identification of gaps in the efforts so far, in methodologies and approaches that have been applied at global level for assessing integrity in supply chains for the ICT sector is a key element of the present report. This should be the basis for the drafting recommendations for the policy makers. This gap analysis is structured in three groups:

1. Gaps at technical level and the associated tools to assess the integrity of components of supply chains are presented.
2. Gaps in state of the art for a harmonized risk analysis methodology that identifies in a clear and consistent way risks for the whole supply chain and prioritizes them in order to evaluate alternatives are presented.
3. Standardisation gaps allowing for a harmonized standardization scheme that can empower policy makers to reduce SCI risks.

7.1 Technical level gaps

As mentioned before, ISO/IEC 15288 identifies a number of stages in the lifecycle of a system against which it is necessary to identify the set of Supply Chain Integrity /Resilience functions to be implemented in the system. In addition, DARPA, in the "Trust in IC" program, highlight the fact that "Even analysed, validated, certified organization can be corrupted, integrity checking has to be an intrinsic feature of the products".

A methodology called Trusted Computing (http://www.trustedcomputinggroup.org/) implements this recommendation for software components. Based on a secure hardware "root of trust" (Trusted platform Module, TPM) integrity checking of software components is checked on their loading. Even if seldom used, TPM are implemented in PCs and in some mobile devices (smartphones).

However, even if secured hardware components can be considered as offering a good security level (as those Common Criteria certified), potential existence of hardware Trojans or the existence of counterfeited components must be taken into account. . ICs are subject to both reverse engineering and side channel attacks (commercial reverse engineering services are available). There are also documented cases of IC mislabelling and IC counterfeiting that has occurred. As pointed out by Dr. Dean Collins, Deputy Director, MTO, DARPA: "Trustworthy computing (with software) cannot exist until we have trustworthy hardware to build it on".

There are also promising methods to control the integrity and the authenticity of hardware components. Although not all of them apply across the board, at an industry segment level good progress has been made, Current standards, practices, and safeguards provide a safety net for hardware products produced by technology vendors. Key purchasing processes can protect organizations from inadvertently acquiring products originating from a grey market.

Alternatives to intrinsic integrity checking could be set up with organizational measures derived from the "acceptance procedure" of Common Criteria such as digital signature of software, authentication and tracking of hardware and subcomponents. However, this requires that all the actors of the supply chain agree to implement such a service and also agree in establishing a trust chain. This is far from being the case.

7.2 Risk analysis framework gaps

Current forms of risk analysis, such as those supporting the Common Criteria, are product driven, or in the financial world are based only on financial risk. The complexity of Supply Chain Integrity requires that such methods be extended to address highly dynamic real-time systems. However, efforts are under way to use Common Criteria framework for supply chain analysis.

7.3 Standardization scheme

Third party evaluations, audits and certification are key elements for the confidence and trust in products and actors. As seen in previous chapters, the existing norms and certification schemes do not give an efficient answer.

Common Criteria is certainly the most effective scheme for security products, however it is product oriented (even if some attempts have been made to evaluate and certify production sites, this has to be seen as mutualizing the effort required by various products instead of a real site or actor certification). In addition, the lack of technical solutions for integrity checking in some areas does not allow for really implementing controls for commercial subcomponents or COTS. In some areas, however, controls have been developed, based on technology and supply chain processes, and these successes indicate that additional efforts will be instrumental in reducing uncertainty where it still remains. Potential adaptation of Common Criteria to the supply chain remains promising, although still in the future.

8. Recommendations

8.1 Key R&D areas to address

Based on the study of issues in ICT supply chains and related problems and technologies, several key areas for actions can be identified, which can lead to the emergence of the common framework that will strengthen insights into the integrity of the supply chain,. In these recommendations the target bodies/instruments for their implementation are also mentioned.

1. Improved and innovative trust models

   Currently, most commercial systems operate with implicit trust from their operators only. Moreover, hierarchical trust models in systems lead to numerous dependencies (e.g., software packages need to trust each other and the operating system, from the bottom to the top of the stack). These trust models need to be augmented to enable end-to-end verifiable trustworthiness of ICT systems. Innovative approaches need to be defined to create a new generation of trust models. Trust (defined as the expected behaviour of a product) and integrity need to be verifiable in solutions that cut across the development and production process covering all the components of ICT systems (hardware, software, COTS, specific developments …). Integrity checking has to be an intrinsic feature of the new architectures enabling on on-line permanent checking by the system itself.

   Another interesting area is recovery of trust and integrity, a set of approaches and techniques to use if an ICT product has been compromised in order to recover some integrity.

   Recommendation towards: European Union (EU) funded research programs (FP7).

2. Improvement in evaluation and integrity checking techniques

   Evaluation approaches as currently used, while very useful in many contexts, provide no assurance under operational conditions (at run time) and rely on the evaluation of the general design rather than an instance of a product. New dynamic evaluation mechanisms for integrity or an extension of the existing approaches are required to enhance the role of evaluation. Cost and time effective solutions have to be developed for all the components of ICT systems including hardware (commercially available ICs, ASICs, FPGA, …).

   Recommendation towards: European Union (EU) funded research programs (FP7).

3. Deeper study of good practices currently used in various industry segments and in government procurement

   Good practices in supply chain management, which are already deployed by the industry without public disclosure, can provide important insights into technology and process developments that will increase the integrity of ICT supply chains. Government procurement practices are of interest, as can their comparison with other best practices.

   Recommendation towards: European institutions, supported by the Member States

4. Improved technology solutions to detect and prevent counterfeiting or overproduction

   Non-authentic components (eg, networks or endpoints) are more likely to fail or be breached. New technologies to determine the provenance of ICT systems are needed to protect the ICT systems. All components must be taken into account, from hardware to software, from specific developments to COTS or subsystems.

Intrinsic integrity assurance primitives, as well as organisational measures (product identification and tracking over the whole supply chain) should be addressed.

Recommendation towards: European Union (EU) funded research programs (FP7).

5. New approaches to security assurance

   Auditable, transparent and uniform supply chain integrity practices and tools are needed to achieve higher levels of assurance in critical systems without significantly increasing their cost. New technologies to define inherently trustable complex systems are necessary, too. There are two aspects of improving security assurance: greater assurance in supply chains for existing products and designing new architectures that can provide better assurance in new ICT products. Finally, currently available evaluation and assurance frameworks, such as Common Criteria, need to be improved to cope with the risks.

   Recommendation towards: European institutions.

6. Better approaches to inventory and configuration control and maintenance

   The resilience of a system is dependent on the ability of the operator to verify the integrity of the hardware, software and configuration after any updates, repairs, or patching. Introducing compromised elements into the solution can severely impair a system's resilience. New technologies are needed to manage deployed complex systems in order to ensure integrity after modifications. Furthermore, tools and techniques to define, track and measure the integrity of ICT systems will allow real-time verification of their integrity.

   Recommendation towards: European Union (EU) funded research programs (FP7).

7. Study of approaches for assessing policy needs on a global scale

   There is an opportunity for industry and academia to study balanced approaches for addressing policy needs in the area of ICT supply chains on a global scale, based on the examples of good practices available from a range of use cases, such as highly global ICT supply chains, supply chains in regulated industries or examples of organizational good practices. Relevant study ideas can be gleaned in technology and process innovations in ICT supply chains, as well as in the deployment of environments with high levels of assurance.
   Recommendation towards: European Union (EU) funded research programs (FP7), European institutions, National Policy Makers.

8.2 Certification

Independent evaluation and certification is a key element for the confidence and trust in security systems. It should be implemented and promoted through requirements for certified products (tenders, regulations, etc).

8. Development of a transnational recognition of certificates based on common specifications (and their local interpretations) and on confidence in the technical evaluation process. Common Criteria offer an international recognition of certificates (through the so called **Common Criteria Recognition Arrangement**, **CCRA**), a mechanism for security specifications (through Protection Profiles or Security Targets) and an organization for ensuring that the technical level of evaluations is comparable in the signing countries (through cross audits). It is a good candidate to become the reference in certification even if some works has to be initiated towards a better adaptation to the whole range of products and complex systems. Another example is the **SOGIS MRA (Senior Officers Group for Information Systems, Mutual Recognition Agreement)**, developed and signed in Europe. While the CCRA limits mutual recognition to intermediate levels of evaluation (up to EAL4), SOGIS MRA looks for the recognition of

highest security levels (up to EAL7 level). However, the lack of efficient technical solutions for integrity checking does not allow for thoroughly implementing controls for commercial subcomponents or COTS. Appropriate methods should address highly dynamic real-time system. This recommendation is also valid within the context of discussions on the Transatlantic Trade and Investment Partnership (TTIP).
Recommendation towards: European institutions, National Policy Makers.

8.3 Supply Chain Integrity framework

There is no existing framework to measure and evaluate SCI and this needs to be corrected in order to allow measurement of SCI performance.

9. Development of a SCI framework formalizing the terms and definitions of SCI, including the terms used in this report, as well as better identifying where the R&D activities listed above impact the SCI elements. A consequence of defining the SCI framework will be to identify the SCI PoM and PoC and thus to give a structure for the certification and, if necessary, the regulation of supply chains.

Recommendation towards: International Standardisation Organisations (ISO).

8.4 Legislative level

To date, integrity of the supply chain was not an object of interest for legislation (including the proposed NIS Directive) – also due to the lack of standardized frameworks, tools and methods. With the evolvement of technical means such initiatives can be undertaken, moreover, can become a catalyser for their further development.

10. Development of proposal of legislation allowing for further investigation of supply chain integrity issues.

Recommendation towards: European institutions.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu