The Global Cyber Security Challenge

It is time for real progress in addressing supply chain risks

Andy Purdy
USA Cyber Security Officer
Huawei Technologies

June 2016

HUAWEI

Authors

I would like to express my gratitude to those who have given me valuable suggestions and made a significant contribution to this document: John Suffolk, Jeff Nan (Jianfeng), Jupiter Wang (Weijian), Andie Zhang (Jingfei), Xue Yongbo, Mu Dejun, Water Zhang (Zhiliang), Wout Van Wijk, David Pollington, Tero Tammisalo, Jackie Wang (Rui), Jessie Luo (Ming), Peter Rossi, Hosoi Yoichi, Ulf Feger, Jorg Alexander Albrecht, David Francis and others who contributed to this paper directly or indirectly. Please accept my apologies if I have neglected to name you, and thank you for your contribution.

Andy Purdy

TABLE OF CONTENTS

June 2016

1 Foreword

Cyber security continues to be an issue of intense interest governments and our customers; and with the passage of time, it has only become more so. The imperative that we emphasized in our three security white papers beginning in 2012 remains important, but insufficiently realized across the whole of industry; it is only by working together internationally, as vendors, customers and policy and law makers, will we make a substantial difference in addressing the global cyber security challenge.

While there is still no simple answer or solution to the cyber security challenge, it is increasingly apparent that there are steps the global community can take – as well as individual organizations – to drive demonstrable progress in reducing cyber security risk, including that of collaborating so as to reach an agreement on principles, laws, standards, best practices, norms of conduct, and protocols – with recognition that trust has to be earned and continuously validated. Huawei commits itself to supporting such an endeavor.

This white paper builds on the three prior security white papers issued by Huawei and discusses our approach to addressing one of the biggest cyber security challenges, the global supply chain risk.

As the Deputy Chairman of the Board of Huawei and the Chairman of the Global Cyber Security and User Privacy Committee of Huawei, I would like to re-confirm our company's commitment to continue to work with all stakeholders to enhance our capability and effectiveness in designing, developing, and deploying secure technology, and reducing information and communications technology (ICT) risk. We reiterate this commitment:

> **We will support and adopt any internationally agreed standard or best practice for cyber security in its broadest sense; we will support any research effort to improve cyber defences; we will continue to improve and adopt an open and transparent approach enabling governments and our customers to review Huawei's security capabilities, and finally, as we have done to date, we warmly welcome the assistance from governments and our customers in enhancing our processes, our technology, and our approach to cyber security so that we can provide even greater benefits to them and their customers.**

As I have said before, we firmly believe that the world is a better place when the innovations and capabilities made possible through the use of technology are maximized and made available to more of the world's population; in short, when they improve people's lives and improve economies. Huawei will continue to uphold our open and transparent approach and responsible attitude in our operations and in everything we do.

Ken Hu

2 Introduction

This fourth white paper in Huawei's cyber security series on the vexing challenges facing the global information infrastructure and the organizations that support and depend on it focuses on supply chain risk. Organizations and consumers need to be able to take advantage of the full benefits of information and communications technologies that flow from a truly global supply chain. Supply chain risk management is not just about ensuring that products and services will be there when needed, but it is also about a product lifecycle approach that minimizes the risk that products will be tainted by the behavior of malicious actors, or that the products may be counterfeited or contain counterfeit components that can be exploited for illicit purposes.

Supply chain risk is one part of the over-arching cyber security risks that an organization must understand and manage in order to be successful. It is important to recognize that an organization cannot address supply chain risk appropriately without implementing the measures necessary to handle risk across the board. Accordingly, we will first look at the major factors organizations should consider, including their approach toward more effectively managing their risk. Next, before focusing on supply chain risk, it is imperative that an organization has an understanding of its overall cyber security risk and preparedness posture – which includes cyber security risk as one important component -- and develop and implement a plan to address it. This is where the NIST *Cyber Security Framework* (thereafter, the *Framework*) comes in.[1]

The NIST *Framework* is a tool that can help an organization to understand their risk level and chart a path toward a more appropriate and sustainable risk environment and state of preparedness. Against this backdrop, we will discuss the fact that for an organization to move to a more appropriate, sustainable, and transparent supply chain risk posture requires three things: (1) the organization needs to understand what supply chain risk entails; (2) the organization needs to know how to address the risk; and (3) the organization needs to be motivated to act by internal and/or external drivers, and to be held accountable if they fall short.

We have made the most progress on what stakeholders need to worry most about, namely, risk awareness. Although the specific recognition of supply chain and third-party risk is a more recent phenomenon, it is one that is still incomplete. In this paper, we will include a discussion of cyber security supply chain risk – what it is, what the threats are, and the scope of the task of identifying and managing risks from suppliers and third parties. For those organizations that have at least a rough understanding of the importance of the risk, many struggle with what they need to do about it, particularly in the face of numerous standards and best practices. We will then discuss some of the activities taking place around the world to contribute to the effort to better understand and address supply chain risk.

Next, we go into some detail about Huawei's approach to supply chain risk, not to suggest that we have the perfect approach, but to share and invite commentary on what we are doing to meet customers' needs and to encourage sharing of lessons learned and increased collaboration among stakeholders to drive real progress in reducing risk.

We will also discuss another very important tool available to help organizations address cyber security risks, namely, the Open Trusted Technology Provider Standard (O-TTPS), which focuses on supply chain and third-party risk.[2] The O-TTPS

[1] NIST has not yet fully included supply chain and third-party risk into the *Framework*, but it is an issue that they have said they will address in some fashion, either as an overlay on the *Framework* or as a roadmap that organizations can use to manage risk from suppliers and third parties.

[2] *The Open Trusted Technology Provider Standard – Mitigating Maliciously Tainted and Counterfeit Products (O-TTPS) V1.0*, https://www2.opengroup.org/ogsys/catalog/C139

was developed by the Open Trusted Technology Forum, of which Huawei is a member, and was recently recognized by the International Standards Organization (ISO) during the second half of 2015.

Regarding what needs to be done about supply chain risk, we will discuss efforts by the EastWest Institute (EWI) Global Cooperation in Cyberspace Initiative to drive collaboration among key cyber stakeholders to address some major, difficult cyber issues, with a particular focus on their Breakthrough Group – co-led by Huawei, Microsoft, and the Open Group -- that is working to promote the global availability and use of more secure ICT products and services, by developing what is in essence a type of framework for a risk-informed, fact-based, global level playing field for ICT products.

Finally, we will also discuss a critically important issue: how to motivate stakeholders who have appreciation of the importance of supply chain risk and what they need to do about it, to take the necessary actions and be held accountable if they fail in this regard. The bottom line is that governments and major private organizations need to step up and drive more significant, better coordinated progress to address supply chain risk if we are to be able to take full advantage of the benefits of ICT technology to make the world a better place for its citizens.

3 Executive Summary

This fourth white paper in Huawei's cyber security series focuses on cyber security supply chain risk. Organizations and consumers need to be able to take advantage of the full benefits of information and communications technologies that flow from a truly global supply chain. Supply chain risk management is not just about ensuring that products and services will be there when needed, but it is also about a product lifecycle approach that minimizes the risk that products will be tainted by malicious actors, or that they will be counterfeit or contain counterfeit components that can be exploited for illicit purposes.

Supply chain risk is one part of the risk that an organization must understand and manage in order to be successful. An organization cannot address supply chain risk appropriately without implementing the measures necessary to handle risk across the board. It is a very important part of the journey to a more secure risk posture for individual organizations to recognize and appropriately put into place key mechanisms that can help an organization successfully manage risk.

Of particular importance for an organization in building an effective risk management capability is for it to commit to addressing security and privacy risks; establish an internal governance mechanism led by the organization's top leadership; identify requirements and baselines across all parts of the organization; implement robust verification and compliance; and incorporate priority requirements into departmental or business group goals and metrics, as well as individual performance metrics, to provide incentives and facilitate accountability.

Next, it is imperative that an organization has an understanding of its overall cyber security risk and preparedness posture – which includes cyber security risk as one important component -- and develop and implement a plan to address it. This is where the NIST *Cybersecurity Framework* comes in.[3]

[3] NIST has not yet fully included supply chain and third-party risk into the *Framework*, but it is an issue that they have said they will address in some fashion, either as an overlay on the *Framework* or as a roadmap that organizations can use to manage risk from suppliers and third parties.

The *Framework* is an important tool that can help organizations understand their risk and chart a path toward a more appropriate and sustainable cyber risk environment and state of preparedness. The NIST *Framework* provides organizations with one piece of the puzzle with regard to addressing the risk they face. It is a standard-neutral tool to assess their own cyber security risk and preparedness that gives them the ability to set a course toward a more appropriate security posture given their risk environment, with readily accessible references to standards and best practices, which they can choose from based on their unique circumstances.

For an organization to move to a more appropriate, sustainable, and transparent supply chain risk posture requires three things: (1) an understanding of supply chain risk; (2) they need to know how to address the risk; and (3) internal and/or external drivers to take action, and accountability if they fall short.

Although we as an industry have already come a long way as regards what stakeholders need to worry about -- awareness of the risk -- the recognition of supply chain and third-party risk is a more recent phenomenon, one that is still incomplete. In this paper, we will include a discussion of supply chain risk – what it is, what the threats are, and the scope of the task of identifying and managing risks from suppliers and third parties. The ICT supply chain for a product can involve scores or even hundreds of components from a comparable number of global companies. Addressing supply chain risk can represent a daunting challenge for an organization that may be struggling with addressing the risk solely affecting its own operations.

Those who rely on ICT are slowly coming to realize that supply chain risk can no longer be ignored or its significance minimized. With this growing recognition comes a growing awareness among key cyber stakeholders of their responsibility to move beyond sometimes impassioned discourse to actually making real progress toward addressing supply chain risk in a collaborative, cooperative manner.

For those with at least some understanding of the risk, many struggle with what to do about it, particularly in the face of numerous standards and best practices. There are some activities taking place around the world that can contribute to the effort to address supply chain risk: SAFECode; Underwriters Laboratory; the ENISA report in European supply chain integrity; the EastWest Institute's cyber initiative; in the UK, the efforts of CPNI and the Trustworthy Software Initiative; in China, cyber security and anti-terrorism legislation; in Japan, the governmental efforts to implement a strategy on supply chain risk; and in the United States, initiatives in the energy, defense, and financial sectors to address this issue.

We next provide details about Huawei's approach to supply chain risk, which is part of a larger end-to-end, global assurance program to share details of what we are doing to invite feedback and encourage and facilitate a broader dialogue among stakeholders about how to better address supply chain risk and build greater trust in the global ICT supply chain.

Regarding the need to move forward, this paper builds on an underlying theme and message of Huawei's previous security white papers: that there is a compelling need for global collaboration among government, industry, and end-users to achieve consensus on how all need to work together to define and reach an agreement on specific norms of behavior, standards, good practices, and laws and regulations, and how we can promote and drive progress to reduce privacy and security risk in global and nationally significant networks and communications systems.

It is important to facilitate collaboration in driving toward collective agreement on laws, norms of conduct, standards and best practices for suppliers/vendors, and independent verification mechanisms, with an effort to educate and organize ICT buyers to leverage their purchasing power to drive the availability of more secure products. But to do this, buyers need to be more informed about appropriate, risk-informed security requirements, more consistent in incorporating those requirements into their purchasing decisions, and more organized by bringing together like-minded buyers to communicate common requirements.

This need makes even more significant the fact that there is now an internationally recognized tool available to help organizations address their supply chain and third-party risk, the Open Trusted Technology Provider Standard (O-TTPS),[4] recently recognized by the International Standards Organization (ISO). The standard identifies and categorizes applicable technology industry-secure engineering and supply chain integrity best practices whose systematic use can make a vendor's products worthy of being considered more secure and trustworthy by commercial or governmental enterprise customers. Importantly, accreditation is only granted after an independent third-party evaluator confirms it is warranted.[5] The O-TTPS can help to meet the need of suppliers and buyers of ICT for greater clarity than they get from multiple standards to affect what they develop and how, and what they purchase and why.

We will also discuss another critically important issue: that of how to motivate stakeholders who, although they may understand cyber risk and what they should do about it, nonetheless, need to be motivated to do it, and to be held accountable if they fall short. It is apparent that too few organizations will do what is risk-appropriate without having meaningful motivators or incentives to do so and rigorous mechanisms to hold them accountable should they fail to act. Governments and private organizations have a responsibility to contribute to developing and putting in place these motivators and incentives.

[4] *The Open Trusted Technology Provider Standard – Mitigating Maliciously Tainted and Counterfeit Products (O-TTPS) V1.0*, https://www2.opengroup.org/ogsys/catalog/C139. *See also*, ISO/IEC 20243:2015, *Information Technology -- Open Trusted Technology Provider™ Standard (O-TTPS) -- Mitigating maliciously tainted and counterfeit products* (2015). http://www.iso.org/iso/catalogue_detail.htm?csnumber=67394

[5] http://reports.opengroup.org/membership_report_all.pdf

4 Previous White Papers

In our first white paper, *Cyber Security Perspectives: 21st century technology and security – a difficult marriage* (September 2012),[6] we provided a forthright picture of Huawei's approach to cyber security and the implications and impact it has on technology, society and our lives. We presented a high-level view of the state of cyber security, outlining its historical context, the key players involved, and the challenges that the global ICT supply chain poses for everyone.

We also provided a summary of the Huawei approach to the cyber security and global supply chain challenge and made some suggestions as to how to act preemptively and pragmatically across the industry in which we operate. We emphasized that to proactively manage cyber security in general and global supply chain risk in particular requires transparency and an even-handed, collaborative approach across our industry between and among the public and private sectors.

We emphasized then, as we have since, that Huawei is dedicated to collaborating with other global organizations in the innovation and establishment of international standards to ensure that the integrity and security of our networked solutions and services meet or exceed the needs of our customers and provides the assurances that are in turn required by their own customers. The first white paper was intended as a concrete step in improving industry awareness of Huawei's efforts to help ensure a secure and better cyber future for everyone and to articulate our view on the actions companies and governments need to take to help manage the global cyber security challenge.

In our second White Paper, *Making cyber security a part of a company's DNA - A set of integrated processes, policies and standards*, published in October 2013,[7] we explained in some detail our approach to end-to-end cyber security processes, an approach which we believe is fairly comprehensive. We noted that cyber security is an issue of great interest to our governments, vendors, and our customers alike –and that this is reflected in the fact that cyber security assurance is one of Huawei's core strategies.

As we said at that time, and continue to believe, it is essential that we work together on a global basis –as vendors, customers and policy and law makers – if we are to have any chance of making a substantial difference in addressing the global cyber security challenge. We also said that it is very important that we share our experience about what works and what does not to reduce the risk that people will use technology for unintended and malicious purposes.

In our 2014 white paper, *Cyber Security Perspectives: 100 requirements when considering end-to-end cyber security with your technology vendors*(December 2014) (hereafter, *Top 100 Requirements*),[8] we detailed our *Top 100 Requirements* list, which focuses on what security-related requirements buyers of technology should consider asking of, or requiring from, technology vendors. We generated the list based on questions posed to Huawei and our assessment of a range of standards and best practice in order to try to help buyers systematically analyze the cyber security capabilities of vendors when dealing with tenders.

In the paper, we noted that in many countries the number of legal and industry requirements relating to cyber security was on the increase and that some governments and regulators were beginning to impose accountability and liability

[6] http://pr.huawei.com/en/news/hw-187387-securitywhitepaper.htm#.Vw92Gfl97RY

[7] http://www.huawei.com/en/cyber-security/hw_310548

[8] http://pr.huawei.com/en/connecting-the-dots/cyber-security/hw-401493.htm

for failure related to cyber security issues national critical infrastructure providers and computer or IT service providers. We anticipated optimistically that more companies will be required to detail both their approach to cyber security and the analysis and assessment they undertake to evaluate the risk from their technology vendors and service providers.

We offered the *Top 100 Requirements* as a starting point for organizations to begin to mitigate their own risk when evaluating a supplier's cyber security capabilities. We reasoned that the more informed and demanding the buyer and the more consistent those buyers are in asking for high quality security assurance, the more likely ICT vendors are to invest and to raise their security standards. We stand by that view and build on it in this white paper.

We are pleased that the EastWest Institute has included the *Top 100 Requirements* in the work of their Breakthrough Group on Promoting the Availability and Use of More Secure ICT Products and Services. It is anticipated that the group's outreach effort and online survey will generate input to the *Top 100 Requirements* and help it evolve. The *Top 100 Requirements* could prove to be a useful tool for organizations and industry sectors in creating and customizing their own sets of requirements for vendors and suppliers.

5 Success Factors for an Organization to Address Cyber Security Risks

In this section, we discuss some of the key actions and activities that organizations should seriously consider in areas such as their approach to more effective risk management. In our view, these "success factors" are an important part of the journey to a more secure state for individual organizations. It is essential for every organization to recognize and put into place key mechanisms informed by their experience and that of other organizations – customized for their particular industry, organizational structure and culture, and risk environment -- that can help successfully manage risk, including issues touched upon in our second and third security white papers.

In our view, the key success factors for addressing organizational security risk are commitment; governance; clear security requirements; consistent processes; performance metrics for individuals; internal compliance; and transparency.

To be successful in managing cyber security and privacy risk, an organization should make commitment at all levels to address cyber security and privacy risks, among others, and systematically incorporate these risks into their risk management program as part of an over-arching strategy to inform, prioritize, and address current and future risk challenges.[9]

Every organization needs clear internal governance roles and responsibilities related to cyber security and privacy risk, including the active involvement of the leadership and senior management from across the organization, with top leadership continually monitoring the effectiveness of the management of the risk and the program implementation.

[9] *See*, for example, *FFIEC Cybersecurity Assessment Tool: Overview for Chief Executive Officers and Boards of Directors*, Federal Financial Institutions Examination Council (June 2015), http://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf and *Third Party Relationships: Risk Management Guidance*, Office of the Comptroller of the Currency, OCC BULLETIN 2013-29, http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

Senior leadership needs not and should not micromanage risk, but needs to "own" the risk management process and its results. This should not be merely an abstract commitment.

In the global environment and diverse supply chains it is extremely difficult to control, or even identify, the wide variety of different occurrences and conditions that may raise the probability of a cyber security vulnerability, or lead to an incident or violation. It is well understood that it is impossible to mitigate all risks, at least with reasonable costs. Therefore, the incorporation of cyber security risks into organizational risk management is vital, which will include the establishment of processes and mechanisms to create and implement mitigation plans, even for very unlikely occurrences.

Each organization and its key departments and components should have clear and specific security-related requirements appropriate to their respective roles -- cyber security baselines relevant to risk-related functions. For example, in the case of a company that produces certain products, the baselines should protect product integrity, traceability, and authenticity. Similarly, individuals with cyber-security–related responsibilities should have performance metrics that align with the baseline requirements, performance metrics and milestones of the department or business unit in which they work. In addition, the organization should strive to have consistent and replicable processes imbedded into the regular business operations of the organization, and those should be continuously improved based on changing circumstances.

Another essential factor in effective risk management is an internal compliance and verification program based on the separation-of-duties principle. This ensures that there is always independent assessment of whether, and to what extent, organizational and individual requirements are successfully met, and where and in what ways improvement is necessary.

Finally, it is important for every organization to be open and transparent with their customers and stakeholders regarding their risk management progress, successes, and failures. This transparency, coupled with individual and organizational accountability, is essential if an organization is to dynamically address risk in the fluid risk environment we face today and will face in the future.

6 The NIST Framework: a Tool for Assessing Organizational Cyber Security Risks

Of those organizations that have at least a rough understanding of cyber security risk, many struggle with how to assess the risk their organization faces, and how to chart a path toward a more informed stance on risk tailored to their individual situation - particularly in the face of numerous sets of standards and best practices. Accordingly, we are heartened to discuss the NIST *Cybersecurity Framework*,[10] envisioned as a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" using "a voluntary risk-based [...] set of industry standards and best practices to help organizations manage cybersecurity risks." The *Framework* "focuses on using business drivers to guide cyber security activities and considering cybersecurity risks as part of the organization's risk management processes."

The *Framework* could serve as a valuable risk assessment tool for any organization, regardless of what standards or best practices that organization may abide by. The *Framework* gives organizations one piece of the puzzle concerning the risk they face – a standard- and vendor-neutral tool to assess their own level of risk and preparedness that guides them toward a more appropriate stance on security posture given their risk circumstances. It could also help organizations to compare their risk management with that of suppliers and business partners.[11] The *Framework* can be a good starting point for any organization that wants to better understand, and improve, their risk posture.

In our third security white paper, *Cyber Security Perspectives: 100 requirements when considering end-to-end cyber security with your technology vendors* (December 2014), we developed a list of requirements focusing on what demands technology consumers should make of their technology vendors. The purpose of the paper was to help buyers analyze the security capabilities of their vendor cyber security capability when dealing with tenders. In the paper, we noted that in the face of the existence of a great number of sets of standards:

> **We will never get to "One standard" given the breadth of technology but what we can do is to focus on the key requirements that are often documented (maybe using different words) in many of the standard, codes, and best practice, but position them to focus on what vendors should be collectively doing to improve the security of their products.**[12]

The NIST *Framework*[13] performs just such a valuable function, and could complement the use by purchasing organizations of lists of security queries and requirements, such as Huawei's *Top 100 Requirements*.

Significantly, and appropriately, the NIST *Framework* has been characterized informally as a "risk analytic tool" and "translation engine." The *Framework* is a "risk analytic tool" in that it is entirely neutral as to what standard(s) may be applicable in risk determination for a particular organization, but it lays out a method of risk analysis informed by standards and best practices, so any organization can use it. It also provides guidance to inform an organization and help them to

[10] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, National Institute of Standards and Technology" (February 12, 2014), http://www.nist.gov/cyberframework. *See also*, "CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES WORKING GROUP 4: FINAL REPORT," (Mar. 2015) [hereinafter WG4 Final Report] *available at* http://transition.fcc.gov/pshs/advisory/csric4/CSRIC_WG4_Report_Final_March_18_2015.pdf, *and* https://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC_WG4_PresentationFinal_31715.pdf (Working Group presentation of the Report).

[11] As this is being written, NIST has not yet fully included supply chain and third-party risk in the Framework, but it is an issue that they have said they will address in some fashion, perhaps as an overlay to the Framework or, more likely, as a roadmap that organizations can follow to manage supply chain and third-party risk.

[12] http://pr.huawei.com/en/connecting-the-dots/cyber-security/hw-401493.htm , p. 3.

[13] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, National Institute of Standards and Technology" (February 12, 2014), http://www.nist.gov/cyberframework.

determine and implement their best path forward to a better state of risk management consistent with their own risk environment and the nature of their sector or industry. Quite significantly, the *Framework* does not adopt any one standard or a combination of standards, but instead provides what is essentially a risk-analysis tool that provides insight into what an organization needs to consider from a risk and preparedness perspective, and it provides reference to existing standards which organizations can use to inform risk evaluation and the path forward to meaningful risk mitigation and management.

In addition, the *Framework* can be seen as a risk "translation engine" in that the user does not need to have knowledge or experience any existent sets of standards to use it to assess and compare the risk posture of their organization with that of another organization, or the risk posture of two or more organizations, even if the organizations follow entirely different standards. Much like the challenge of translating from one language to another, without such a risk-analysis tool, it would be difficult and time consuming, at best, to compare the risk posture of two or more organizations. Significantly, the *Framework* also maps the risk elements to whatever standards are applicable or relevant to the requirement to help organizations who may be unfamiliar or inexperienced with applicable standards.

One very important concept to keep in mind in using the *Framework* is that it is envisioned that its use by an organization will be motivated by business drivers and it is critical that cyber security risks be included in an organization's overall risk management processes. The *Framework* is not a "one size fits all" tool. It provides organization and structure to the myriad of approaches employed in cyber security by pulling together standards, practices, and other norms of conduct in current use, from which an organization can select from and use depending on their place in the global marketplace, industry sector or subsector, and in the context of their unique risk environment.

By providing these benefits, the NIST *Framework* provides a starting point for organizations which are motivated to better understand and manage their risk, or those seeking a way to evaluate the risk posture of other organizations, a place to start. As we will discuss later in this paper, although a vital topic, this is only the beginning of the story.

7 Supply Chain Risk – Organizations Need to Understand It and Address It

7.1 What Is Supply Chain Risk?

Supply chain risk has been defined as "the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system."[14] Threats to supply chains can include: sabotage, tampering, counterfeiting, piracy, theft, destruction, disruption, exfiltration, infiltration, subversion, diversion, export control violations, corruption, social engineering, insider threat, pseudo-insider threat, and foreign ownership.[15]

[14] Section 806 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011, available at http://www.gpo.gov/fdsys/pkg/BILLS-111hr6523enr/pdf/BILLS-111hr6523enr.pdf. Axelrod, C. Warren, "Mitigating Software Supply Chain Risk," ISACA JOnline, August, 2013. Available at http://www.isaca.org/Journal/archives/2013/Volume-4/Pages/JOnline-Mitigating-Software-Supply-Chain-Risk.aspx

[15] Goertzel, Karen M., *et al. State of the Art Report on Supply Chain Risk Management for the Off-the-Shelf (OTS) Information and Communications Technology (ICT) Supply Chain*, U.S. Department of Defense, Information Assurance Technology Analysis Center (IATAC), (2010), p. 40. https://www.csiac.org/content/state-art-report-soar-security-risk-management-shelf-ots-information-and-communications-tech

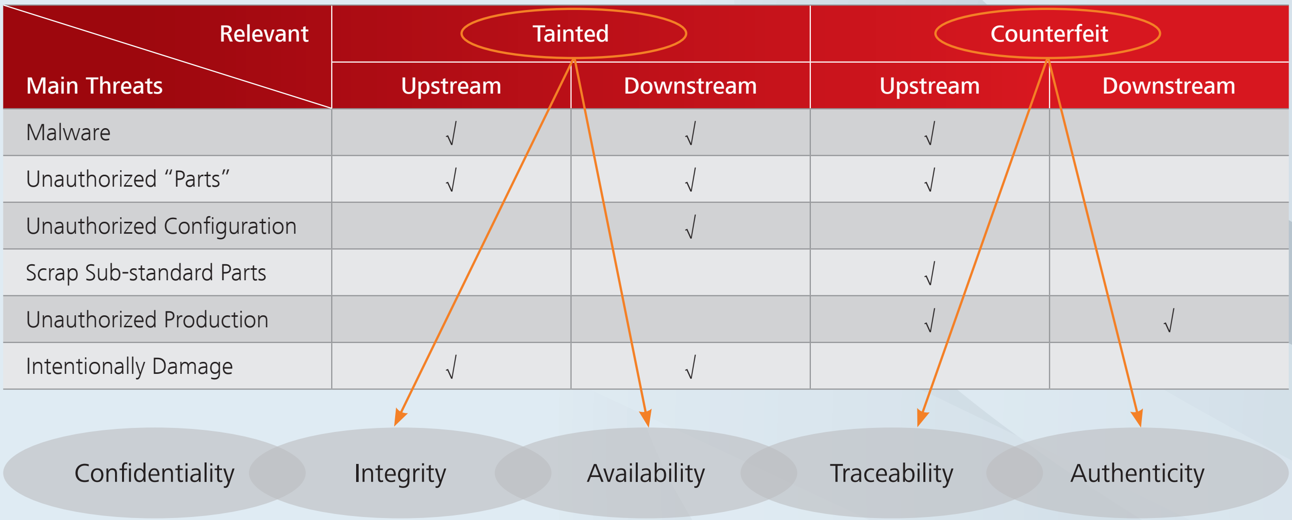
Naturally, foreign ownership itself is not a threat as such, but it can cause several cyber security related threats, such as: less control and visibility to an entity and its processes and resources in a different country; the operations may be subject to third country jurisdiction and regulation concerning security and privacy; and there may be difficulties or extra costs when security and privacy requirements are enforced into subcontractor products.

More specific examples of such threats are the following: (1) installation of malicious logic on hardware or software; (2) installation of counterfeit hardware or software; (3) failure or disruption in the production or distribution of a critical product or service; (4) reliance upon a malicious or unqualified service-provider for the performance of technical services; (5) installation of unintentional vulnerabilities on hardware or software.[16]

To date, all too often, supply chain risks are not addressed at all or they prove inadequate, ineffective, or inefficient in managing emergent information technology supply chain risks.[17] Two categories of threats are maliciously tainted products and counterfeit products.[18]

The risks may affect the supply chain can flow upstream (*e.g.* suppliers of components – software or hardware, like chop manufacturers or driver developers) and downstream (*e.g.* integrators and distribution channels, from which products are sourced by acquirers).[19]

Supply Chain Threats and Relevant Parties—The Open Group



Relevant	Tainted		Counterfeit	
Main Threats	Upstream	Downstream	Upstream	Downstream
Malware	√	√	√	
Unauthorized “Parts”	√	√	√	
Unauthorized Configuration		√		
Scrap Sub-standard Parts			√	
Unauthorized Production			√	√
Intentionally Damage	√	√		

Tainted products is a main threat in the supply chain. Thus, how to prevent products from being tainted is a critical task. Establishing and maintaining an effective traceability system for components and products, generally, is another important task, because it must minimize the risk of tainted and counterfeit products entering the supply chain.

[16] http://www.gao.gov/assets/590/589568.pdf

[17] http://www.gao.gov/assets/590/589568.pdf

[18] *The Open Trusted Technology Provider Standard – Mitigating Maliciously Tainted and Counterfeit Products (O-TTPS) V1.0 (April 9, 2013)*, pp. 1-2, https://www2.opengroup.org/ogsys/catalog/C139. (1) Maliciously tainted product – the product is produced by the provider and is acquired through a provider’s authorized channel, but has been tampered with maliciously; and (2) Counterfeit product – the product is produced other than by, or for, the provider, or is supplied to the provider by other than a provider’s authorized channel and is presented as being legitimate even though it is not.

[19] *Ibid*., p. 14. *See also*, ISO/IEC 20243:2015, "Information Technology -- Open Trusted Technology ProviderTM Standard (O-TTPS) -- Mitigating maliciously tainted and counterfeit products" (2015). http://www.iso.org/iso/catalogue_detail.htm?csnumber=67394

7.2 Organizations Are Beginning to Understand the Importance of Supply Chain Risk

We are slowly making progress on supply chain risk awareness, but it is by no means universally recognized. In this section, we discuss why organizations need to take supply chain risk seriously. It can be a particularly daunting undertaking for organizations struggling with the challenge of addressing more traditional cyber security risks focusing on their own operations. The supply chain for an ICT product typically consists of hundreds or even thousands of components from a similar number of companies, involving multiple processes and geographic locations.

As discussed above, the NIST *Cybersecurity Framework* is a valuable tool for organizations to better understand cyber security risks and to shape a path forward to an organization-appropriate risk posture. The NIST *Framework*, however, does not as of now address supply chain risk in a similar manner, although it is anticipated that in 2016, the NIST will provide guidance about supply chain risk, possibly in the form of a roadmap for organizations to follow.

At present, organizations are less likely to think about risk from suppliers and third-party providers and more likely to think of risk from the perspective of a user or operator of a network or ICT system. For example, they may ask how likely is it that someone will attack a system to steal something, say, intellectual property or information that can be used for identity theft, or to simply steal things of financial value, and what the import of that harm or loss is. They may also ask if it would be possible for someone to intrude into a system to disrupt or damage it, or surreptitiously intrude in the system to have the ability to do harm at some time in the future.

Like Huawei, Microsoft also has long recognized the potential for hostile actors to insert malicious, unwanted and unauthorized functions or counterfeit elements or components into the global ICT supply chain, which could later be used to disrupt or degrade technology systems or to facilitate surveillance. This presents a challenge for governments and businesses which, at a minimum, require recognition that supply chain risk is a shared problem that necessitates cooperation among stakeholders to find solutions founded on standards and best practices and work to implement them.[20]

For some years now, governments of countries around the world – including the United States – have been moving away from heavy reliance on internally developing their own systems and products around ICT, such as, hardware and government off-the-shelf (GOTS) software, and moving toward commercial products such as hardware and commercial off-the-shelf software (COTS). There was a gradual shift evident over ten years or so ago when government purchasers began to look more to industry for their information and communications technology systems and components. Governments came to realize that doing everything in-house with solutions customized to their own mission needs took too long, cost too much, and that they could simply not move as fast as technology was changing. The bottom line was they could not keep up with the innovation and increased functionality in the private sector.

As a result, governments moved away from internal customized development to external providers for COTS ICT, who they found could produce more reliable and more innovative products, and evolve those products more quickly and at a significantly lower cost. It was not very far into that process before governments realized that they were opening themselves up to supply chain and product integrity risk in shifting to commercial vendors, which had not been of great concern when they made everything themselves in-house. As they started to look more seriously at purchasing COTS ICT, they realized that, on balance, although this was the right way to go, by doing so, they exposed themselves to additional risk because they did not know, and could not always easily determine, the provenance of the products,

[20] *Security: Building Global Trust Online, 4th Edition, Microsoft Perspectives for Policymakers*, p. 18. http://www.microsoft.com/en-us/twc/policymakers.aspx

where parts and components came from, and who had access to them along the supply chain, which was becoming increasingly global for all ICT products at the time. In short, they did not have confidence that the products or their components had product integrity and were trustworthy, or if they might have been maliciously altered along the supply chain to add unwanted functionality or vulnerabilities for later exploitation, or if they might include counterfeit parts that, similarly, could not be trusted.

Accordingly, governments concluded that if they bought COTS ICT, they needed to be sure they were buying from trusted technology providers who followed best practices across the whole life cycle of their products, including the supply chain. At the same time, a threat environment involving a range of malicious actors came to the forefront of government concerns, with the onset and proliferation of malware, identity theft, and exploitable vulnerabilities that received inadequate attention, thus leaving product users open to attacks on government and private networks and systems, including critical infrastructure.

It is generally understood that malware can be introduced into systems through a variety of mechanisms, including through employees downloading attachments in phishing or spear-phishing emails, connecting external devices (e.g. USB drives), or visiting compromised web sites, or through unauthorized parties using stolen employee or third-party credentials to install malware directly on systems, or by insertion into the global supply chain.[21]

One of the more recent developments that has magnified the concerns of governments and other key cyber stakeholders regarding potential cyber attacks against government and critical infrastructure services, and a heightened concern about supply chain risk, is the use of destructive malware (DM).[22] While this is relatively infrequent at present, it is potentially catastrophic, because it can represent a significant threat to an organization's operations and business continuity (and those who depend on them). This is a threat which could impact the confidentiality, integrity and availability of data, and one which could negatively impact an organization's ability to recover from an attack. Two recent cyber attacks against the Las Vegas Sands and SONY Entertainment illustrate how DM can compromise an organization's data integrity, disrupt business operations, and harm brand reputation.

There appears to be a pattern in supply chain risk just as in cyber security risk, generally: often there is a long, slow path from awareness of the risk, to a growing understanding of what you need to do to address the risk, to the challenge of how you drive action to actually reduce risk and increase trust and assurance. This is even true of some government agencies concerned about national security risks and threats to government systems and critical infrastructure. To date, all too often, emergent information technology supply chain risks are not effectively addressed.[23] Two important categories of such risks are maliciously tainted products and counterfeit products.[24]

These are factors that contributed to the formation of the Open Group Trusted Technology Forum (OTTF) and the development of the Open Trusted Technology Provider Standard (O-TTPS), discussed later in this paper.

[21] *Joint Statement on Destructive Malware*, FFIEC.https://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf

[22] *Joint Statement on Destructive Malware*, FFIEC.https://www.ffiec.gov/press/PDF/2121759_FINAL_FFIEC%20Malware.pdf

[23] http://www.gao.gov/assets/590/589568.pdf

[24] *The Open Trusted Technology Provider Standard – Mitigating Maliciously Tainted and Counterfeit Products (O-TTPS) V1.0 (April 9, 2013)*, pp. 1-2, https://www2.opengroup.org/ogsys/catalog/C139. (1) Maliciously tainted product – the product is produced by the provider and is acquired through a provider's authorized channel, but has been tampered with maliciously; and (2) Counterfeit product – the product is produced other than by, or for, the provider, or is supplied to the provider by other than a provider's authorized channel and is presented as being legitimate even though it is not.

8 Initiatives to Address Supply Chain Risks

This paper builds on one of the underlying themes and messages of Huawei's three previous security white papers: that there is a compelling case for governments, the industry, and end-users worldwide work together to collectively come to a common understanding, define, and reach agreement on specific norms of behavior, standards, good practices, and laws and regulations, as well as how we can drive progress to reduce privacy risks and security risks in global and national networks and communications systems.

In the next section we discuss examples of encouraging initiatives around the world that aim to help address supply chain risk, and can serve as inspirational models for others.

8.1 SAFECode

The Software Assurance Forum for Excellence in Code (SAFECode) is a global, industry-led non-profit organization working to increase trust in information and communications technology (ICT) products and services by promoting availability, awareness, and use of more secure and reliable software, hardware, and services.[25] SAFECode brings together subject matter experts with experience in managing complex global processes regarding software development, integrity controls, and supply chain security.

SAFECode has created a framework[26] to help an organization select the most appropriate process-based assessment method for evaluating the development process of commercial technology providers when there is no applicable international standard.

8.2 Underwriters Laboratory

Underwriters Laboratory (UL)[27] is an independent global safety science company working to help safeguard people, products, and places by providing what they call "comprehensive functional safety services." UL has a testing and certification schema for numerous products that allows a product to carry the "UL" seal, indicating conformance with a specific set of requirements unique to that product. For example, UL helps identify software weaknesses in industrial control systems relative to published specifications and helps to provide technical criteria to facilitate managing risks associated with these software weaknesses. UL has launched a new business line, its Cybersecurity Assurance Program (CAP), which is working on a program for testing, rating, and certifying connected devices, with an initial focus on industrial control systems and medical devices.[28] In the future they hope to expand the program to cover ICT products.

[25] http://www.safecode.org/

[26] Shaun Gilmore (Microsoft), Reeny Sondhi (EMC), Stacy Simpson (SAFECode), *Principles of Software Assurance Assessment -- A Framework for Examining the Secure Development Processes of Commercial Technology Providers*, SAFECode, http://safecode.org.

[27] http://industries.ul.com/functional-safety/cybersecurity

[28] https://sid4gov.cabinetoffice.gov.uk

8.3 ENISA

The recently updated report of the European Union Agency for Network and Information Security (ENISA),[29] "Supply Chain Integrity - An overview of the ICT supply chain risks and challenges, and vision for the way forward," recommended that supply chain participants follow good practices that provide a basis to understand and address ICT supply chain risk. Significantly, the report also recommends that governments work with the private sector to develop international frameworks to facilitate comparison assessment of ICT supply chain risk management efforts. The report recommends that the 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.[30]

The ENISA report pointed out that although many countries, industries, and agencies have concerns about supply chain risk, their efforts to address these have been fragmented and lacking in coordination, and that greater cooperation is necessary. The report includes a number of actions that it characterizes as necessary, including the need for a consistent view, practices, and metrics that would result in an appropriately coordinated program, including in the areas of research and development; the need for independent evaluation and certification; a supply chain integrity framework, referenced above; and the need to consider legislative action.[31]

The report gives recommendations to a variety of European institutions, and in some cases, national governments. Regarding the need for a supply chain integrity framework, ENISA recommends that ISO develop a framework to measure and evaluate supply chain integrity so that performance can be measured. ISO recognized and released the O-TTPS as a new standard shortly after the ENISA report, which indicated that supply chain integrity frameworks are a common need.

8.4 Chinese Government Initiatives

This section discusses the following government initiatives in China: the counter-terrorism law and cyber security draft legislation.

The first Chinese Counter-terrorism Law (CTL), which took effect on January 1, 2016, outlines obligations for telecom and Internet enterprises to cooperate with government authorities in investigating terrorism activities, and these obligations may have a significant impact on the operation of Internet and tech firms in China. Telecom and Internet service providers are required to support and assist efforts by government and national security authorities engaged in the lawful conduct of terrorism prevention and investigation,[32] but the CTL does not specify the procedure and documentation required for such requests. The CTL also requires Internet service providers to implement network security and information and content monitoring systems, and adopt technical security measures to prevent the dissemination of information containing terrorist or extremist content.

In July 2015, China issued the draft cyber security law, which covered a range of issues, including cyber security certification and inspection for critical network equipment, requirements for specialized network security products[33]

[29] "Supply Chain Integrity -- An overview of the ICT supply chain risks and challenges, and vision for the way forward," European Union Agency For Network And Information Security (VERSION 1.1, August 2015), p. 10, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/sci-2015. In a table referencing various supply chain-related efforts, the ENISA report said that the Open Group work had "nothing specific to SCI [supply chain integrity]." Ibid., at p. 11. See also, Croll, Paul, "Supply Chain Risk Management -- Understanding Vulnerabilities in Code You Buy, Build, or Integrate," CrossTalk (March/April 2012). http://static1.1.sqspcdn.com/static/f/702523/17039817/1331310005287/201203-Croll.pdf?token=NawZKwikQkEjI7VEFo86BdQjAKo%3D

[30] *Ibid*., p. 5.

[31] *Ibid*., pp. 25-27.

[32] Counter-Terrorism Law, article 18.

[33] Cyber security Law (draft 6th July, 2015), article 19.

and the security inspection of procurement of network products and service of critical information infrastructure operators.[34] The draft also required the localization of personal data for critical information infrastructure operators.[35]

8.5 UK Government Approach to Supply Chain Risk

In the UK, the Centre for the Protection of National Infrastructure (CPNI) has warned organizations of the national security threats that can come from the ICT global supply chain; principally, the potential exposure to terrorism, cyber-attacks by nation states, and large-scale cyber-crime.[36] CPNI awareness efforts include recommendations that organizations should incorporate supply chain risk as part of an existing risk management approach.

CPNI also advises organizations to implement a risk mitigation plan that includes the following: comprehensive mapping of all tiers of the upstream and downstream supply chains to the level of individual contracts; risk-scoring each contract to link in to the organization's existing security risk assessment; due diligence, accreditation, and assurance of suppliers (and potential suppliers); the adoption, through contracts, of proportionate and appropriate measures to mitigate risk; audit arrangements and compliance monitoring; and contract exit arrangements.[37]

One UK-based initiative is the UK Trustworthy Software Initiative (TSI),[38] which is supported and funded by the UK Government's National Cyber Security Programme (NCSP) with a mission to help promote trustworthy software (to "Make Software Better") among the supply, demand, and education communities in a risk-based, whole lifecycle process. To provide guidance, the TSI has created a compendium of relevant standards and best practices and incorporated it into its Trustworthy Software Framework (TSF).[39] The Framework has been formalized in a British Standards Institution Publicly Available Specification, PAS 754:2014, "Software trustworthiness – Governance and management – Specification," "which includes technical, physical, cultural and behavioral measures alongside effective leadership and governance techniques to address five key facets of trustworthiness: safety, reliability, availability, resilience and security."[40]

Under the auspices of the UK government Cabinet Office and Home Office, the online system, SID4GOV,[41] formerly a common supplier information database for the health sector, has been modified to be an online platform for UK public sector buyers giving them access to supplier information through a single online system, to help promote sustainability and information security reporting. The platform enables buyers to access aggregated information inputted directly by suppliers for a single view of up-to-date data about critical suppliers and vendors. The SID4GOV portal and database is coordinated by NQC, Ltd. which was founded in 2003 by public procurement experts.

NQC is providing supply chain services through their supplier engagement system. The system was designed to measure and report on suppliers, with the aim to provide supply chain assurance as part of overall risk management. NQC supports a database that buyers can use to look at available information about vendors and suppliers. At present,

[34] Cyber security Law (draft 6th July, 2015), article 30.

[35] Cyber security Law (draft 6th July, 2015), article 31.

[36] https://www.cpni.gov.uk/highlights/Security-in-the-Supply-Chain

[37] https://www.cpni.gov.uk/highlights/Security-in-the-Supply-Chain/#sthash.v6L3m2o3.dpuf. *See also*, Supply Chain Risk Scenarios, MITIGATING SECURITY RISK IN THE NATIONAL INFRASTRUCTURE SUPPLY CHAIN --A GOOD PRACTICE GUIDE FOR EMPLOYERS (April 2015). https://www.cpni.gov.uk/documents/publications/2015/13-april-2015-mitigating-security-risk-in-supply-chain.pdf?epslanguage=en-gb

[38] The TSI is a not-for-profit organization which "aims to collect, organise and share the wealth of knowledge, experience and capabilities that already exist in the UK public and private sectors and in academia about trustworthy software to give people a joined-up, curated view of the information that is available. It is supported by a number stakeholders and it is governed by a Management Board led by Government representatives from the Department of Business, Innovation and Skills (BIS) and the Centre for Protection of National Infrastructure (CPNI). http://www.uk-tsi.org

[39] http://www.uk-tsi.org/trustworthy-software-framework---tsf

[40] http://www.uk-tsi.org/pas754

[41] https://sid4gov.cabinetoffice.gov.uk/

there are over 225,000 individual company profiles in the system, and it is estimated that over 1700 public-sector buyers are using it. The system includes the use of supplier-completed questionnaires about a company's background, supplemented by Dunn and Bradstreet data, and data collection regarding sustainability, information assurances, and the like. Questionnaires are tailored based on the particular procurements, for example, for food supply contracts, it might involve questions on sourcing transparency that would then be assessed against the balanced scorecard.

8.6 Japan

Japan issued its latest Cyber Security Strategy in September 2015,[42] which included an emphasis on strengthening organizational capabilities by, among other things, seeking to raise awareness about the importance of the "Security by Design" approach and to enhance cyber security throughout the inter-organizational supply chain.[43] In the area of risk management, the Japanese government will provide support for organizations about cyber security-related management and mechanisms and will work to develop a framework for objective evaluation of enterprises' activities taken using methods such as third-party certification. They also pledged to work internationally to help create frameworks for "mutual recognition" of security standards and will promote effective supply chain risk management through necessary R&D and through bilateral and regional cooperation with ASEAN and other countries.

In the updated Japanese critical infrastructure protection policy,[44] "Basic Policy of Critical Information Infrastructure Protection,"[45] the Japanese government said that they will "promote the use of internationally-approved third-party certification schemes that enable objective evaluations on the level of satisfactory security performance, taking into account the fact that specialized knowledge and skills are necessary for the procurement and operation of ICS [industrial control systems] and other associated equipment."[46]

8.7 The United States

There are a number of initiatives in the U.S. relevant to cyber risk management and supply chain risk management, in addition to the work of NIST,[47] several of which are discussed below.

In one of the initiatives coming out of President Obama's Executive Order on Cybersecurity, the U.S. General Services Administration and the Department of Defense developed and put into motion six reforms to improve the U.S. Federal Acquisition System from the perspectives of resilience and cyber security risk, including the development of a repeatable process for all federal procurements for cyber security risk mitigation across the product lifecycle – development, acquisition, sustainment, and disposal.

[42] http://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

[43] *Ibid*., p. 20.

[44] *The Basic Policy of Critical Information Infrastructure Protection* (3rd Edition) (May 19, 2014), Information Security Policy Council (May 25, 2015 (Revised)), Cybersecurity Strategic Headquarters, Government of JAPAN.

[45] [footnote in original text] Information and communications services, financial services, aviation services, railway services, electric power supply services, gas supply services, government and administrative services (including local governments), medical services, water services, logistics services, chemical industries, credit card services, and petroleum industries.

[46] *Ibid*., p. 25.

[47] Building on the work of the Cybersecurity Framework, NIST is expected to provide guidance to organizations regarding supply chain risk during 2016, in addition to their Special Publication released in 2015,*Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. SP 800-161, National Institute of Standards of Technology, U.S. Department of Commerce (April 2015).

http://dx.doi.org/10.6028/NIST.SP.800-161. More recently, NIST released a Request for Information about the Framework, potential updates, and its future management. http://www.nist.gov/itl/acd/20151210rfi.cfm

The Department of Defense has incorporated consideration of supply chain risk into their federal acquisition requirements.[48] In early 2015 the Federal Chief Information Officers (CIO) Council and the Chief Acquisition Officers (CAO) Council created a working group to review current contract clauses and information technology (IT) acquisition policies and practices around contractor and subcontractor information system security. This interagency group was comprised of senior experts in acquisition, security, and contract management and their recommendations are included in draft guidance to Federal agencies on implementing strengthened cyber security protections in Federal acquisitions.[49] The draft guidance contained a requirement for GSA to establish a "Business Due Diligence" capability to reduce cyber-related threats and vulnerabilities in the Federal supply chain. The finalized version has yet to be released.[50]

The Office of Management and Budget (OMB) published the "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government" (OMB Memo M-16-04) on October 30, 2015.M-16-04 requires the U.S. General Services Administration (GSA) to "…develop a Business Due Diligence Information Service that will provide agencies with a common government-wide capability for identifying, assessing, and managing cyber and supply chain risk throughout the acquisition process".[51]

In January 2016 the Federal Energy Regulatory Commission (FERC) announced a Final Rule to revise seven reliability standards for critical infrastructure protection. The purpose is to address supply chain cyber risks to communication networks and the bulk electric systems, as well as develop standards for supply chain management security controls with the aim of protecting the bulk electric system from malware threats and security vulnerabilities.[52] The revisions are designed to protect communication links and sensitive data among bulk electric stakeholders. The Commission did not itself address supply chain risk management issues, but did direct the convening of a staff-led technical conference to facilitate a structured dialogue on supply chain risk management issues to help it determine the appropriate action to take on this issue.

The U.S. financial sector regulatory oversight body, the Federal Financial Institutions Examination Council (FFIEC),[53] which coordinates risk guidance to the six U.S. financial regulatory organizations, including risk related to cyber security,[54] has issued a Cybersecurity Assessment Tool[55] (Assessment) for institutions to use to evaluate their cyber security risks and preparedness. The Office of the Comptroller of the Currency (OCC) examiners will gradually incorporate the Assessment into examinations of national banks, federal savings associations, and federal branches and agencies (collectively, banks) of all sizes.

Similar to the British buying program mentioned above, although in this case organized and run by the private sector, a coalition of major companies in the U.S. defense/aerospace industry -- Lockheed, Boeing, Raytheon, BAE, Rolls JV -- has developed a trusted online acquisition platform that has morphed into an independent company called Exostar.

[48] DoD 5200.44 *Trusted Systems and Networks*: This document establishes policy and responsibilities for the identification and protection of critical functions through Program Protection. CNSS 505.Defense Federal Acquisition Requirements (DFAR), SUBPART 239.73--REQUIREMENTS FOR INFORMATION RELATING TO SUPPLY CHAIN RISK, http://www.acq.osd.mil/dpap/dars/dfars/html/current/239_73.htm

[49] https://policy.cio.gov/

[50] https://www.fbo.gov/notices/230732591f542b7da9b9fc3e6c167eec/; *see also*, https://www.gpo.gov/fdsys/pkg/FR-2015-05-29/html/2015-13016.htm. On April 6 and 7, NIST is hosting the Cybersecurity Framework Workshop 2016 at NIST in Gaithersburg, Maryland. http://www.nist.gov/itl/acd/upload/Agenda_Cybersec-2.pdf

[51] https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf (Section II.d.)

[52] The revisions will go into effect 65 days after the Final Rule. 18 CFR Part 40 [Docket No. RM15-14-000], Revised Critical Infrastructure Protection Reliability Standards (Issued January 21, 2016), http://www.ferc.gov/whats-new/comm-meet/2016/012116/E-2.pdf

[53] The FFIEC comprises the principals of the following U.S. financial regulatory bodies: The Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee.

[54] www.ffiec.gov/cybersecurity.htm

[55] *FFIEC Cybersecurity Assessment Tool: Overview for Chief Executive Officers and Boards of Directors*, Federal Financial Institutions Examination Council (June 2015), http://www.ffiec.gov/cyberassessmenttool.htm, and *Third Party Relationships: Risk Management Guidance*, Office of the Comptroller of the Currency, OCC BULLETIN 2013-29 http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

Exostar has created a platform they call a Trusted Workspace for Secure Information Sharing, Collaboration and Process Integration Across Global Networks."[56] This program facilitates collection and sharing of information related to risk of suppliers, with a primary data collection instrument being a 22-question survey, in addition to input from their members.

8.8 The EastWest Institute

The EastWest Institute (EWI) Global Cooperation in Cyberspace Initiative is working to leverage and drive collaboration among key cyber stakeholders to address major, difficult cyber issues, including an important one to promote the global availability and use of more secure ICT products and services. This group is working to develop a type of framework for a risk-informed, fact-based, global level playing field for ICT products.

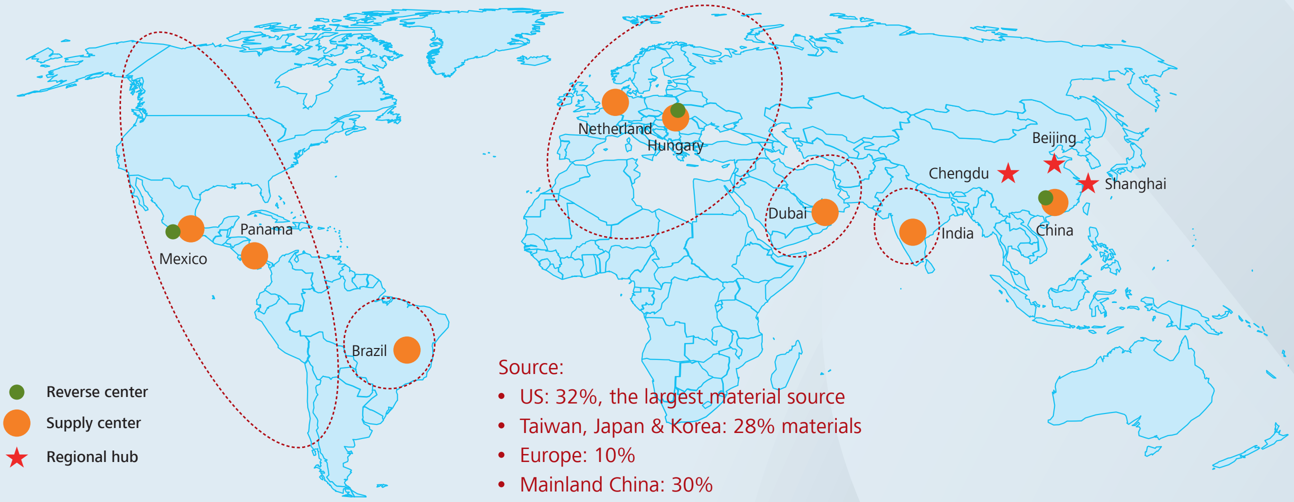
During 2016 EWI will work globally to finalize, refine, and mobilize support for the framework among key government and private stakeholders. It is anticipated that the deliverables will include three key elements: (1) a set of principles, (2) a compendium of standards and best practices that suppliers should consider referencing in their internal requirements (and for their suppliers), and (3) mechanisms that buyers of ICT products can use to leverage their purchasing power to incentivize suppliers/providers to raise the bar on their security and product integrity processes and requirements.

9 Huawei's Approach to Supply Chain Risks

Addressing supply chain risk at Huawei is part of the overall, company-wide assurance program that was discussed in some detail in Huawei's second security white paper, *Cyber Security Perspectives: Making cyber security a part of a company's DNA – A set of integrated processes, policies and standards*. This task falls under the purview of the Global Cyber Security and User Privacy Protection Committee (GSPC), which is the top-level cyber security and privacy management body of Huawei, responsible for ratifying the strategy of cyber security and privacy assurance, and providing oversight of its implementation. Members of the GSPC are both the decision-makers behind and the owners of cyber security strategy. They are responsible for implementing cyber security strategies in relevant fields and are subject to the monitoring of the audit committee.

[56] http://exostar.com

Huawei Global Supply Network



Source:

- US: 32%, the largest material source
- Taiwan, Japan & Korea: 28% materials
- Europe: 10%
- Mainland China: 30%

Supply Center	Reverse Center	Local EMS
• China (Delivery for the globe) • Europe (Delivery for West Europe & North Africa) • Latin America (Delivery for America, except Brazil) • Brazil (Delivery for Brazil) • India (Delivery for India) • Dubai (Delivery for Middle East)	• China • Mexico • Europe	• Brazil, Mexico, India and Hungary supply centers work with local partners to do manufacturing and make delivery

Comprehensive supply chain management program

Supply chain is one of the business processes incorporated into security assurance, along with R&D, sales and marketing, delivery, and technical services. This integration is a fundamental requirement of the quality management system. Huawei reinforces the implementation of the cyber security assurance system by conducting internal auditing and receiving external certification and auditing from security authorities and independent third-party agencies. Huawei has been BS7799-2/ISO27001 certified since 2004. It complies with applicable cyber security standards and receives third-party certification when appropriate, such as ISO9001, ISO14001, OHSAS18001, ISO26000, ISO27001, C-TPAT, and ISO15408.

Huawei's over-arching information security management system is based on ISO 27000 standards and includes ISO 27001 certification. Huawei has established a supply chain security management system based on Huawei's requirements and processes for quality assurance, information security, environmental protection, and IT assurance, as well as the requirements of ISO28000 (supply chain security management) and C-TPAT10 (Customs-Trade Partnership Against Terrorism). The supply chain security management system has passed third-party certification requirements for ISO28000.

The Huawei supply chain management (SCM) program regards product quality as part of its strategic priority and continuously improves product quality and process efficiency through activities, such as Six Sigma, optimization projects, quality control circles (QCCs), the traditional suggestion box, and the Huawei Production System (HPS). For example, since the launch of Six Sigma in 2002, Huawei has extended its quality efforts from internal product quality to external customer satisfaction and from production to end-to-end supply chain process, such as planning and order management. Huawei has also optimized its development and supply chain management practices by referring to the Open Trusted Technology Provider Standard (O-TTPS), discussed later in this paper.

Huawei believes that malicious damage can occur at any point in the supply chain, so it is important to focus not only on individual activities, but also the supply chain as a whole. Supply chain threats fall into two major categories: tainted products and counterfeit products. Threats that can result in tainted or counterfeit products include malware, unauthorized parts, unauthorized configuration, scrap and sub-part parts, unauthorized production, and intentional damage.

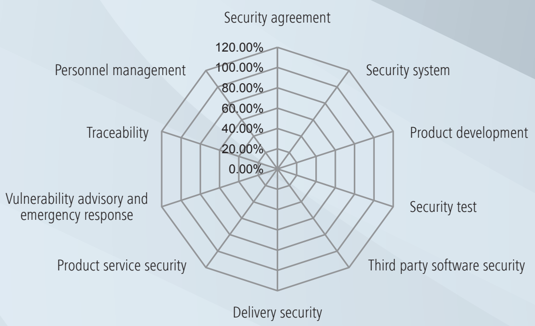
As part of the effort to address supply chain risk, Huawei has established a comprehensive, ISO 28000-compliant supplier management system that can identify and control security risks during the end-to-end process from incoming materials to custom delivery. Huawei selects and qualifies suppliers based on their systems, processes and products, choosing those that contribute to the quality and security of the products and services procured by Huawei. Huawei continuously monitors and regularly evaluates the delivery performance of qualified suppliers and checks the integrity of the third-party components during each of the incoming material, production and delivery processes. Huawei records the performance and establishes a visualized traceability system throughout the process.

Supplier Cyber Security System Qualification Standard

Supplier Name		Audit Date	
Audited Location		Contact Person & Title	
Lead Auditor		Auditor	

No.	Item	Weight	Percentage	Weighted Score	Remarks
1	Security agreement	7%			
2	Security system	12%			
3	Product development	18%			
4	Security test	20%			
5	Third party software security	6%			
6	Delivery security	5%			
7	Product service security	5%			
8	Vulnerability advisory and emergency response	16%			
9	Traceability	5%			
10	Personnel management	6%			
Total					
Grade					

This audit checklist includes 10 items and 49 questions, each of which weights 5% to 15% of the total score. There are 1 to 10 questions in each item to evaluate the supplier's cyber security.

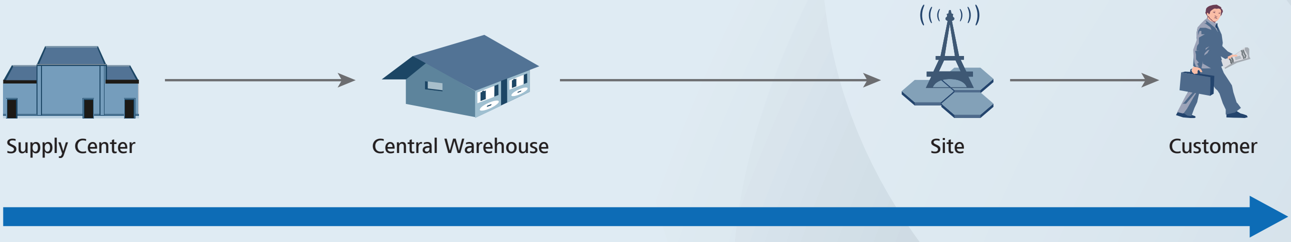


Weighted Score	Grade	Risk Level
< 70%	D Failed	High risk
≥ 70%	C Normal	Medium risk
≥ 80%	B Good	Low risk
≥ 90%	A Excellent	Benchmark

Rigorous evaluation of suppliers

Through its global logistics management process and regional and country logistics processes, Huawei manages its global logistics in a hierarchical (global-regional-country) manner that supports the supply chain security management system. Huawei has deployed an IT system, Huawei Transportation Management (HTM), which enables visualization and monitoring of the transportation process. Huawei is committed to applying the newest industry security practices in the logistics process.

logistics process transparent management



Accurate information: ship to correct address
Exact time: exact time delivery
Accurate configuration: ship the correct goods

Right place: GPS electronic fence control
Exact time: delivery / receipt time interlock, upload on-site photo of completion of receipt and inspection
Correct goods: barcode collection

Authenticity & integrity inspection: customer can inspect device’s authenticity & integrity by NMS and electronic label

Huawei has established processes for supply chain return performance

Huawei sets requirements for the applicable return, or reverse-goods handling methods. We identify the modules that may contain personal data and mark them in our Product Data Management (PDM) system, optimize our logistics management system so that the personnel of each Huawei branch can automatically identify and manage these materials in the process of inbound and outbound handling based on local laws and regulations so as to meet all local requirements for obsolete and returned goods. To ensure the customer's data security, such as the risk that sensitive data might exist in the returned equipment, Huawei requires the customer to properly erase any data before the equipment is returned.

Huawei has developed supply chain cyber security baselines to ensure the integrity, traceability, and authenticity of the products in the supply chain. These baselines include requirements on physical security (entity delivery security), software delivery security, and organizational, processes, and personnel security awareness. Physical security baselines are designed to prevent physical access that might permit tampering or implementation of unauthorized code.

Supply Chain Cyber Security Baseline

There are 46 procurement cyber security red lines, covering five categories of material security, software outsourcing security, EMS security, Logistics security and Engineering services security.

Security Attribute
Protecting personal data and privacy
No attacking or destroying the customer's network
No authorized operation
No backdoor or virus
Background data security
Consistency
No use of unauthorized account
No authorized access
Security test
Emergency response
No installation or running of unauthorized software
Agreement signing
Traceability
Training and education
Key personnel security management
Open source software security
Software outsourcing delivery security
Security qualification
Configuration management
Software burning security
The security of reverse material maintenance
Shipment security
Warehousing security
Logistics system security
Security defense management

Structure of Procurement Cyber Security Baseline					
Management Category	Material Security	Software Outsourcing Security	EMS Security	Logistics Security	Engineering Services Security
Delivery Security	No backdoor or virus	Security test	Consistency	Consistency	Protecting personal data and privacy
	Background data security	Software outsourcing delivery security	Software burning security	Shipment security	No attacking or destroying the customer's network
	Consistency		Security test	Warehousing security	No authorized operation
	Security test		Virus detection and removal		No use of unauthorized account
	Open source software security		Configuration security		No authorized access
			Reverse material maintenance security		No installation or running of unauthorized software
			Delivery security		
Assurance Management	Emergency response		Emergency response		Emergency response
	Agreement signing	Agreement signing	Agreement signing	Agreement signing	Agreement signing
		Security qualification	Security qualification	Security qualification	
	Traceability	Traceability	Traceability	Traceability	Traceability
		Configuration management		Training and education	Training and education
				Key personnel security management	Key personnel security management
				Logistics system security	Security defense management

Huawei sets clear baseline standards to ensure supply chain security

Software delivery security ensures the end-to-end integrity of software by preventing unauthorized physical access to software and enabling technical verification. To manage risks related to incoming materials, Huawei inspects incoming materials based on the technical specifications for the materials and on relevant quality standards and materials guidelines, and then follows unique processes in each of the following phases of the product lifecycle: procurement, development, and supply chain.

Software management is a significant part of security management. Huawei uses key software security management methods for the supply chain, including strict access control and physical security. Huawei applies a unique Part Number for each software version (VRC), which will be delivered to customers, and this Part Number is used all the way through the software delivery process. In the software delivery process the system generates the related authorization and license automatically according to contract information; meanwhile, the system sends a software pre-loading request to the manufacturing (ATE) server automatically and deletes the software when the ATE test is finished. All of these data transfers between systems are conducted automatically, without manual intervention, to avoid the risk of tampering. We keep detailed records for software loading and testing, and when we need to track something, such as a software version in the equipment of a certain site, it can be quickly located.

Huawei continuously improves its support systems and software distribution platform to support service engineers, provide upgrading services to customers, and support customer self-upgrading programs. Huawei adopts a hierarchical authorization management approach where only authorized employees can apply and download software (including digital signature files or digital certificate) or the software license from the support system and the software distribution platform according to the contract or the equipment requirements, otherwise, the system will deny the login or download. All requests and the individuals who accept the requests are fully logged for auditing purposes.

As a key part of the supply chain security management system, Huawei has established a traceability system covering the whole supply chain from material acceptance, material distribution, PCBA and testing, whole equipment assembly and testing, packaging, transportation to regional delivery. From this traceability chain, Huawei can quickly determine from which supplier what materials were purchased; in which products these materials were used; what specific software was uploaded to these products; to which country and customer these products were shipped (via which logistics service provider); and who the handlers were in all these processes and in production. At the present time Huawei can trace 258 categories of materials, including IC, memory devices, resistors, capacitors, PCBs, tin cream for soldering, etc., which account for 98% of the total production materials (the only materials that cannot be traced are fixtures, labels, packing materials, documents, package and specification). In order to realize the above-mentioned level of traceability, Huawei collects more than 0.2 billion pieces of barcode information, involving more than 30 billion fields.

Huawei established a traceability chain in the software delivery system (SDP), which keeps records of information about applicant, approver, customer name, contract number, product name, software part number, software version and license version to enable query and traceability. By integrating with contract and barcode application at regional warehouses, the traceability system accurately records information related to product delivery, contract, software version, time, and site.

Huawei started to build the barcode traceability system in 2000, and has worked to continuously optimize the system. At present, Huawei can successfully trace the following within one hour:

- information about purchased materials (hardware, software)
- purchased materials (hardware, software) used in various components
- component used in each product
- what software was loaded, which version of the software, and which license
- component and product production process and who worked on them
- component and product shipped to which country, which customer, for which contract
- the transportation process
- inbound and outbound records at destination country
- Trace faulty component repairing records for both production process and reverse process.

10 Open Trusted Technology Provider Standard (O-TTPS)

It is encouraging, and potentially quite significant, that there is now an internationally recognized tool available to help organizations address risks related to supply chain security, third-party providers, and product integrity -- the Open Trusted Technology Provider™ Standard (O-TTPS)[57] -- recently recognized by the International Standards Organization (ISO) International Electrotechnical Commission (IEC) as ISO/IEC 20243:2015.[58] The standard provides a set of prescriptive requirements and recommendations for organizational best practices that apply across the product lifecycle, many of which are highly correlated to threats of malicious tainted and counterfeit products and others that are more foundational.[59]

The newly recognized standard goes beyond existing ISO standards in the breadth and depth with which it addresses supply chain risk,[60] – primarily because it deals specifically with COTS ICT, and is applicable to all IT provider constituents in the chain. It also has an existing certification program for assuring conformance and identifying, on a

The Open Group Trusted Technology Forum

A global industry-led initiative defining best practices for secure engineering and supply chain integrity so that you can *"Build with Integrity and Buy with Confidence™"*

[57] *The Open Trusted Technology Provider Standard – Mitigating Maliciously Tainted and Counterfeit Products (O-TTPS) V1.1 (July 2015) https://www2.opengroup.org/ogsys/catalog/C147; see also*, ISO/IEC 20243:2015, "Information Technology -- Open Trusted Technology Provider™ Standard (O-TTPS) -- Mitigating maliciously tainted and counterfeit products" (2015) http://www.iso.org/iso/catalogue_detail.htm?csnumber=67394

[58] http://www.opengroup.org/news/press/OTTPS-approved-as-ISO-IEC-international-standard. *See* ISO/IEC International Standard (ISO/IEC 20243:2015). *See also*, ISO/IEC 15408: Information Technology – Security Techniques – Evaluation Criteria for IT Security (Common Criteria); ISO/IEC 27000:2009: Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary. *See also, Information Security in Supplier Relationships*, ISO/IEC 27086-1-204, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=59648

[59] *See, Supply Chain Risk Management Practices for Federal Information Systems and Organizations,* NIST Special Publication 800-161 (April 2015), http://dx.doi.org/10.6028/NIST.SP.800-161

[60] *See, for example*, ISO/IEC 15026 (*Systems and Software Assurance*: A four-part, international standard provides an "assurance case" linked to life-cycle processes) and ISO/IEC 27036 (*Information security for supplier relationships*: This international standard addresses the issue of how data is protected in a supplier/acquirer relationship).

public registry, any Open Trusted Technology Provider™ that conforms. The O-TTPS was developed by The Open Group Trusted Technology Forum (OTTF), a cross-industry forum of providers and other stakeholders, which includes Huawei as a member. The OTTF set about to identify and memorialize a collection of applicable secure engineering and supply chain security best practices whose systematic use can make a vendor's products worthy to be considered more secure and trusted by commercial or governmental enterprise customers. The member organizations contributing to the work included a broad range of global suppliers, buyers of products and third-party test labs.

The O-TTPS is intended to mitigate the risks associated with tainted and counterfeit products, which can result in: product failure, degraded performance, and weakened security mechanisms, allowing rogue functionality, critical damage and theft of intellectual property. Counterfeit products can have several consequences. For customers, if the product fails at a critical point, it can affect productivity, revenue, and reputation. For providers, it can impact the revenue stream and damage brand and reputation.

Significantly, accreditation is only granted after an independent third-party evaluator confirms that the applicant company has produced sufficient evidence to demonstrate conformance with the O-TTPS requirements. The scope of the accreditation can be based on an entire company, a business unit, or one or more product lines.

The O-TTPS can help to meet the need of suppliers and buyers of ICT for greater clarity than they get from multiple standards to affect what they develop and how, and what they purchase and why. The O-TTPS helps organizations move past multiple standards to zero in on key requirements that have been previously referenced by multiple sources and help stakeholders focus in on what vendors/producers should be doing collectively to improve the security of products.

ISO recognition of the O-TTPS -- with its genesis, breadth of applicability, and requirements for independent verification -- is precisely the kind of development that we have been calling for in our security white papers: the need for governments and private organizations to work collaboratively to reach agreement on principles, laws, standards, best practices, norms of conduct, and protocols – accepting that trust has to be earned and continuously validated.

Prior to the O-TTPS, most accreditation offerings dealt with the products themselves, with the government focusing on product evaluation as the only available way to address risk concerns. However, those product-based evaluations did not address concerns related to functions and processes such as what happens during creation of the code itself, or during the outsourcing of code creation, or in purchasing open source software, or what happens in the manufacturing facilities and throughout the supply chain. Additionally, the standard, by addressing process requirements, complements existing standards covering product security functionality and product information assurance, such as ISO/IEC 15408 (Common Criteria).[61]

The O-TTPS industry best practices for trusted technology providers are applicable to each of the various constituents in the IT supply chain: original equipment manufacturers (OEMs), hardware and software component suppliers, integrators, value-add resellers and distributors.

The best practices within the O-TTPS have been organized and defined by category, with best practice requirements for each category in turn contained within the subsections of the particular category. The idea is that an organization consistently conforming to the requirements within the best practice categories will be most effective in managing the product security risk.

[61] The Open Group Trusted Technology Forum OTTF™), "Open Trusted Technology Provider Framework (O-TTPF™) -- Industry Best Practices for Manufacturing Technology Products that Facilitate Customer Technology Acquisition Risk Management Practices and Options for Promoting Industry Adoption," (February 2011), p. 5. https://www2.opengroup.org/ogsys/ServePublicationGraphic?publicationid=12341

The categories chosen represent the most critical areas within the processes related to development and manufacturing "where risk management and assurance have the greatest impact on the quality and integrity of a commercial off-the-shelf (COTS) technology product."[62] It is anticipated that the categories and associated practices will change over time as methods and techniques identified and adopted by technology providers (suppliers of technology components or product or solution vendors) change.

The critical categories of the O-TTPS are grouped under two groups, relating to the product life cycle: Technology Development and Supply Chain Security. The activities of a provider of a COTS ICT product, under Technology Development, are primarily within the purview of the provider's in-house supervision as to whether and how they are executed.

The Technology Development category of the product lifecycle includes the Product Development/Engineering Method and the Secure Development/Engineering Method. As seen in current practice and as envisioned by the OTTF, trusted technology providers are those who "use a very well defined, documented, and repeatable product development or engineering method and/or process,"[63] the effectiveness which is generally managed using metrics and managerial oversight.

Similarly, when designing and developing their products, trusted technology providers are those who employ a secure engineering method. The providers and suppliers of software often employ methods or processes to uncover and fix or remediate exploitable vulnerabilities and to assure the security and resiliency of the products. So the providers and suppliers of hardware use processes to protect against counterfeit software or hardware and mitigate the risk from software that is unverified or demonstrably counterfeit.

The Supply Chain category in the O-TTPS addresses the way Open Trusted Technology Providers manage their supply chains through the application of defined, monitored, and validated supply chain processes. The O-TTPS Supply Chain Security activities focus on best practices where the provider must interact with third parties who produce their agreed contribution with respect to the product's life cycle. Here, the provider's best practices often control the point of intersection with the outside supplier through control points that may include inspection, verification, and contracts. These processes, embodied in best practice requirements and recommendations, seek to ensure the security of the supply chain throughout the life cycle.[64]

The Accreditation Program for the O-TTPS guarantees that the provider is using the specified practices in accordance with the O-TTPS requirements. When an Open Trusted Technology Provider™ is successfully accredited, there is formal recognition of conformance to the specifications of the standard.

By describing how companies and organizations can securely develop and manufacture products, the O-TTPS Accreditation Program will facilitate the awareness and use of the best practices across the industry. The global technology supply chain is comprised of consumers, integrators, vendors, and manufacturers. While it may not be possible, much less practical, to procure exclusively from trusted local suppliers, the O-TTPS can make it easier for the buyers of ICT to act responsibly in their procurement strategies and decision making relative to the integrity of technology products, and easier for ICT stakeholders to foster accountability.

[62] *Ibid*., p. 8.

[63] *The Open Trusted Technology Provider Standard – Mitigating Maliciously Tainted and Counterfeit Products (O-TTPS) V1.1* (July 2015), p. 16, https://www2.opengroup.org/ogsys/catalog/C147, https://www2.opengroup.org/ogsys/catalog/C139. *See also*, ISO/IEC 20243:2015, "Information Technology -- Open Trusted Technology Provider™ Standard (O-TTPS) -- Mitigating maliciously tainted and counterfeit products" (2015) http://www.iso.org/iso/catalogue_detail.htm?csnumber=67394

[64] *The Open Trusted Technology Provider Standard – Mitigating Maliciously Tainted and Counterfeit Products (O-TTPS) V1.1 (July 2015)*, p. 15.

11 Driving Change: How to Motivate Organizations to Act

There is no magic formula for how to help move organizations along the path from relative ignorance to awareness that supply chain risk is something they should worry about, to an understanding of what they can and should do to address the risk, to driving concrete action– but it is clear that talk alone is not going to do it. With the passage of time in the face of a growing threat and insufficient action, supply chain risk continues largely unabated. That is among the reasons we are so supportive of the NIST *Framework*, the O-TTPS, and the various steps we see being taken in the form of positive initiatives and efforts around the world. And why we are proud of our three security white papers.

There a number of internal and external drivers that can motivate an organization – public or private – to better understand and reduce risk. These include statutory and regulatory requirements,[65] customer requirements and customer contractual provisions, due diligence requirements of members of organizational Boards of Directors and C-level executives, insurance incentives and requirements, a desire to maintain performance compared to competitors, and the desire to sell products and services.

Although formal government statutes and regulations are only one way to motivate organizations to action, government, major organizations, industry groups, think tanks and academia can play very important roles as conveners and facilitators to help bring about action leading to demonstrable progress using any number of the motivators listed above. Governments, critical infrastructure owners and operators, and major private organizations–including both buyers and providers of ICT products–have critical roles to play in reducing cyber risk to networks, systems, and services of government, critical infrastructure and private organizations.

The role of governments is not limited to situations where the government has specific regulatory authority over a particular sector of the economy, and whether or not government chooses to use the authority it has. A crawl-walk-run approach to risk can have advantages over the inertia of inaction, or waiting for some day in the future when some perfectly formed model or mechanism may appear that provides greater clarity on a detailed set of actions that will be required or even recommended. The risk is too great to idly sit by and wait.

Internationally, on the supply side of the ICT market, governments, private organizations, and industry groups can help to bring together the major suppliers of ICT and promote collaboration among them to identify the standards and best practices and guidelines that they think make the most sense for suppliers to follow to be considered as trusted providers. The O-TTPS and the NIST Framework could be good reference documents to include in those conversations.

On the demand side, governments or private groups would do well to initiate conversations among major buyers of ICT about what security requirements they should consider asking of, or requiring from, their suppliers. Convening meetings of representatives of key sectors of critical infrastructure could identify sector-specific security requirements that cut across the sector. Using a crawl-walk-run approach might encourage sector representatives to come up with at least some initial requirements, which could be supplemented by the more specific risk-informed requirements of particular organizations, and then modified over time by sector representatives and individual organizations based on

[65] The U.S. National Defense Authorization Act of 2016 requires the Secretary of Defense to complete an evaluation of the vulnerabilities of all major U.S. weapons systems and propose mitigation strategies by December 31, 2109, with periodic reporting to Congress and others.
https://www.congress.gov/bill/114th-congress/house-bill/1735/text#toc-H6234F5DE9FA74324AF387AF9B14DBC16

experience and changes in the risk environment of the sector or organization.

Where possible, requirements should be built into contractual provisions so that there are clear, quantifiable consequences for a failure to meet them. Any commonality between requirements of different sectors and government could create substantial business drivers to incentivize suppliers to raise the bar to meet the requirements. This is the thinking behind our third security white paper, "Cyber Security Perspectives 100 requirements when considering end-to-end cyber security with your technology vendors" (December 2014).[66] One of the greatest incentives for any organization to raise the bar on their cyber security practices – including how they address supply chain risk – is the desire to sell products and services. The conduct of buyers is critical to driving real progress.

Governments, private organizations, industry groups, and others can learn from the experience of the collaborations discussed above and decisions can be made about whether and how to amend statutory or regulatory requirements and government and private organizations can collaborate to use non-regulatory motivators to impact possible voluntary collective actions.

For example, the process described above could influence insurance companies to consider cyber risk in the threshold requirements they might set for organizations to get coverage at all, as well as the traditional view that cyber risk mitigation efforts can result in insurance coverage that may be more affordable and/or more comprehensive. In addition, government and major buyers of cyber insurance could perform a convening function to bring together insurance companies to share information about more targeted, risk-informed security requirements for their coverage and underwriting.

Governments and private industry can collaborate to communicate with industry associations, sector groups, and individual organizations about the importance of the risk and what organizations can and should do to better understand their risk and relative risk posture compared to competitors and others in their respective sectors. This kind of executive communication – preferably done in concert with respected industry groups and corporate leaders – can directly impact the due diligence requirements of the leaders of organizations, particularly publicly traded ones. It can also motivate organizational leaders to take action to keep them at least roughly consistent with their competitors, if not for competitive reasons then at least in part because of the impact on their reputation if they are not.

[66] http://pr.huawei.com/en/connecting-the-dots/cyber-security/hw-401493.htm

12 Conclusion – Going Forward Together

We conclude where we began. We must build on the work that has been done to create awareness of supply chain risk and what needs to be done about it, and work harder – collaboratively – to drive real progress to better understand and address that risk. Governments and the private sector have to work together and neither can afford to wait for the other to step up and act. To help protect national security, public safety and law enforcement, the availability of government services, critical infrastructure, and private organizations, and the privacy of information of organizations and individuals, a government should use its capability as a convener and facilitator – and as a regulator when absolutely necessary -- to raise awareness and drive progress regarding supply chain risk, hopefully in each instance informed by experts in private organizations, academia, and government.

Organizations should employ proven success factors and activities to better understand and seriously address, and effectively manage, cyber security and privacy risk. Organizations should consider the NIST Framework, or its equivalent, to understand the unique risks to their organization and where they should want to work toward going forward. In addition, organizations should take seriously the importance of understanding and addressing the risk they face from suppliers and third-party providers across the entire lifecycle of products.

Let's use available tools at our disposal, such as the Open Trusted Technology Provider Standard (O-TTPS) – or at least the proven methods and processes it references – preferably with independent verification that we are doing so, for the sake of our reputations and the trust of our customers, and to live up to the commitment that our respective organizations have or should make, to address cyber security and privacy risk in an effective manner for the good of the global community.

Let's support the objectives and work of the EastWest Institute initiative to promote the global availability and use of more secure ICT products and services through a principle-based, risk-informed, fact-based level playing field for ICT so that all the world can share in the benefits of the innovation, competitiveness, and connectivity of the most modern information and communications technology.

Finally, the greatest incentive to drive faster and more substantial progress in the availability and use of more secure ICT products and services is perhaps the key message in our *Top 100 Requirements* white paper: we need to work collaboratively to make the buyers of ICT more informed about what they should consider using as security requirements for their purchasing, make them more consistent in the use of such requirements, and make them more organized in working with like-minded buyers to strengthen and leverage their purchasing power to drive the availability and use of more secure ICT products and services, as well as to facilitate accountability for those who fall short.

In conclusion, it is our hope this paper contributes to greater collaboration, discussion, understanding, commitment, and concrete action to reduce global ICT supply chain risk.

13 About Huawei

Huawei is a leading global information and communications technology (ICT) solutions provider. Driven by responsible operations, ongoing innovation, and open collaboration, we have established a competitive ICT portfolio of end-to-end solutions in telecom and enterprise networks, devices, and cloud computing. Our ICT solutions, products, and services are used in more than 170 countries and regions, serving over one-third of the world's population. Huawei is committed to enabling the future information society, and building a Better Connected World. We have over 170,000 employees, and the average age of our employees is 32.5. On average, 72% of our people are locally-employed in countries where we operate. More than 140 capital cities have adopted Huawei LTE solutions, and we have commercially deployed over 400 LTE networks and over 180 EPC networks.

Huawei has a leading role in the industry through continuous innovation and has one of the most significant IPR portfolios in the telecommunications industry. Huawei respects and protects the IPR of others. Huawei invests more than 10% of its sales income into R&D, and 45% of our employees are engaged in R&D. In 2015, Huawei invested ¥ 59.6 billion ($ 9.18 billion) in R&D, increasing by 46.1% and accounting for 15.1% of the total annual income of 2015. The total investment in R&D in the last decade is over ¥ 240 billion ($ 36.97 billion).

By December 31, 2015, Huawei has been granted 50,377 patents, and has applied for 52,550 patents in China and 30,613 patents outside China in total. Compared to the quantity, Huawei attaches more importance to the commercial values and quality of IPR. Since 2010, our 849 core proposals on 3GPP LTE have been granted, ranking No. 1 in industry. Huawei holds a leading position globally in terms of patents in fiber to the premises (FTTP), Optical Transport Network (OTN), G.711.1 (fixed broadband audio) and so on. The protection of IPR is therefore critical to the ongoing success of Huawei, and because of this, Huawei is an advocate of IPR protection.

We have 16 research centers around the world, 36 joint innovation centers, and 45 training centers. About 60% of our revenue is generated outside of Mainland China. 70% of our materials come from non-Chinese providers, and the United States is the largest provider which accounts for 32%.

Huawei has acquired an accumulated total of over 450 contracts for managed IT and CT services, supported 23 of top 30 operators worldwide, and served over 150 networks in more than 85 countries to help customers achieve operational excellence. For cloud computing, Huawei has over 500 partners, 1000 customers, and deployed 255 cloud data centers.

In 2015, Huawei shipped over 100 million smartphones with an increase of more than 40% year-over-year.

Huawei is passionate about supporting mainstream international standards and actively contributes to the formulation of such standards. As of December 31, 2015, Huawei had become a member of over 300 standards organizations, industry alliances, and open source communities, holding more than 280 important positions. Huawei is a board member of IEEE-SA, ETSI, WFA, TMF, OpenStack, Linaro, OASIS, and CCSA. We submitted more than 5,400 proposals in 2015, with the total number exceeding 43,000.

The Employee Shareholding Scheme (the "Scheme") involves 79,563 employees as of December 31, 2015. The Scheme effectively aligns employee contributions with the company's long-term development, fostering Huawei's continued success. This gives us the ability to take a long-term view; it also ensures balance among risks, rewards, and strategies. Employees know if we do not excel at serving our customers or if we undertake inappropriate activities, their equity and pensions may be affected.

This document is provided "as-is" without warranty of any kind, express or implied. All warranties are expressly disclaimed. Without limitation, there is no warranty of non-infringement, no warranty of merchantability, and no warranty of fitness for a particular purpose. Huawei assumes no responsibility for the accuracy of the information presented. Any information provided in this document is subject to correction, revision and change without notice. Your use of, or reliance on, the information provided in this document is at your sole risk. All information provided in this document on third parties is provided from public sources or through their published reports and accounts.