

SECURE HARDWARE AND SOFTWARE: SECURITY-BY-DESIGN

WORKING GROUP 6 – Final Report:

Voluntary Security-by-Design Attestation Framework for Hardware and Software Critical to the Security of the Core Communications Network

September 2016

Table of Contents

1 Results in Brief 2

1.1 Executive Summary 2

2 Introduction 3

3 Objective, Scope, and Methodology 5

3.1 Objective & Scope 5

3.2 Methodology 5

4 Findings and Recommendations 6

4.1 Findings 6

4.2 Recommendations 10

5 Conclusions 11

Appendix A

Deliverable 2 – Voluntary Security-by-Design Attestation Framework

# Results in Brief

## Executive Summary

In addition to recommending voluntary best practices for successfully incorporating security-by-design principles in the core communications network, CSRIC was tasked with examining and reviewing the best ways to provide assurances to the FCC and the public that recommended security capabilities are being implemented by network equipment vendors, and to recommend voluntary mechanisms that provide assurances to the FCC and the public that the security practices are being applied. CSRIC recognizes that while communications network organizations’ efforts associated with security-by-design are foundational to secure communications, so too are means of demonstrating this security.

To develop these recommended approaches to assurances, CSRIC undertook a methodical surveying of the landscape as well as a detailed consultation with industry experts. CSRIC wishes to express its appreciation to the contributors to this report. The collaborative and open sharing of views and approaches was integral to the development of this report, and also reflects the continued success of the FCC CSRIC spirit.

As a result of this process, CSRIC formulated the following recommendation:

* CSRIC recommends that security by design/supply chain risk management programs may be appropriately considered, among other topics, at yearly in-person meetings that were contemplated as part of CSRIC IV, Working Group 4’s recommendations issued in March, 2015.[[1]](#footnote-1) CSRIC recommends against implementing any new or additional regulations to address conformity to a particular supply chain risk assessment mechanism, or any type of written attestation to the same. In person meetings will continue to foster the public-private sector collaboration encouraged in past CSRIC reports.

# Introduction

*CSRIC V Working Group 6: Secure Hardware and Software – Security-by-Design* has been formed by CSRIC and was tasked with developing voluntary recommendations and best practices to enhance the security of hardware and software used in communications critical infrastructure. The working group submitted to the CSRIC Council in March 2016 its report outlining recommendations and best practices. The working group was also tasked with a second deliverable, to develop a voluntary attestation framework that could be used by companies to demonstrate the success of the recommendations/best practices.

This appendix is an addendum to the working group’s report and outlines the voluntary attestation framework developed by the working group.

* 1. **CSRIC Structure**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Co-Chairs: Working Group 1 | Co-Chairs: Working Group 2 | Co-Chairs: Working Group 3 | Co-Chairs: Working Group 4 | Co-Chairs: Working Group 5 | Co-Chairs: Working Group 6 | Co-Chairs: Working Group 7 | Co-Chairs: Working Group 8 |
| Working Group 1: Evolving 911 Services | Working Group 2: Emergency Alerting Platforms | Working Group 3: Emergency Alert System | Working Group 4: Communications Infrastructure Resiliency  Sub-Group A: Submarine Cable Resiliency  Sub-Group B: Network Timing Single Source Risk Reduction | Working Group 5: Cybersecurity Information Sharing | Working Group 6: Secure Hardware and Software – Security-by-Design | Working Group 7: Cybersecurity Workforce | Working Group 8: Priority Services |

**Table 1 - Working Group Structure**

* 1. **Working Group 6 Team Members**

Working Group 6 consists of the members listed below:

| **First Name** | **Last Name** | **Organization** | |
| --- | --- | --- | --- |
| Joel | Molinoff | **CBS (Working Group 6 Co-Chair)** | |
| Brian | Scarpelli | **ACT | The App Association (Working Group 6 Co-Chair)** | |
| Rao | Vasireddy | **Alcatel-Lucent (TIA)** | |
| Chris | Boyer | **AT&T** | |
| Brian | Daly | **ATIS** | **(Cisco) (AT&T)** |
| Mike | Geller |
| Jamie | Brown | **CA Technologies** | |
| Steve | Goeringer | **Cable Labs** | |
| Rob | Covolo | **CenturyLink** | |
| Stacy | Hartman |
| Kevin | Beaudry | **Charter\*** | |
| Eric | Wenger | **Cisco** | |
| Glen | Pirrotta | **Comcast Cable** | |
| Kallol | Ray |
| Jon | Amis | **Dell** | |
| Gabriel | Martinez | **DHS** | |
| Alex | Gerdenitsch | **EchoStar** | |
| Jennifer | Manner |
| Peter | Allor | **IBM** | |
| Ethan | Lucarelli | **Iridium (Wiley Rein)** | |
| James | Bean | **Juniper Networks** | |
| Eli | Dourado | **Mercatus Center (GMU)** | |
| Angela | McKay | **Microsoft** | |
| Dorothy | Spears-Dean | **NASNA** | |
| Matt | Tooley | **NCTA** | |
| Jon | Boyens | **NIST** | |
| Kazu | Gomi | **NTT America** | |
| Masato | Kimura |
| Shinichi | Yokohama |
| Franck | Journoud | **Oracle** | |
| Richard | Perlotto | **Shadow Server** | |
| Patrick | Koethe | **Sprint** | |
| Jeff | Greene | **Symantec** | |
| Darren | Kress | **T-Mobile** | |
| Michelle | Rosenthal |
| Chris | Roosenraad | **TWC** | |
| Joe | Viens |
| Robert | Mayer | **US Telecom Association** | |
| Al | Bolivar | **Verisign** | |
| Tomofumi | Okubo |
| Heath | McGinnis | **Verizon** | |
| Peter | Ruffo | **ZTE USA** | |

**Table 2 - List of Working Group Members**

# Objective, Scope, and Methodology

## Objective & Scope

CSRIC V’s Working Group 6 was tasked with providing recommendations to help promote the use of security by design practices within the critical communications infrastructure. The Working Group determined the most efficient way to address these concerns is in the form of voluntary recommendations and best practices designed to enhance the security of the hardware and software in the core public communications network. The Working Group’s second deliverable is to develop a means to indicate to the FCC and the public that the security capabilities identified in the March 2016 CSRIC report are being implemented. As a means to provide this assertion the Working Group was tasked to identify voluntary mechanisms in the form of a voluntary attestation framework that could be used to demonstrate the success of the Working Group’s earlier recommendations and best practices as outlined in this final report.

## Methodology

In order to develop a voluntary attestation framework to demonstrate the success of the recommendations and best practices, a three-phased approach similar to the approach used for the initial report was used to complete the Working Group’s second deliverable:

* **Phase 1: Define Objectives, Scope, and Methodology**
* **Phase 2: Analysis and Determination of Findings**
* **Phase 3: Recommendations and Conclusions**

The Working Group used a combination of bi-weekly conference calls and in-person meetings to produce the above deliverables. The Working Group 6 members agreed that the attestation framework should apply the same concepts that were used in developing the recommendations and best practices.

With those principles in mind, Working Group 6 first did a survey of existing security frameworks and any associated methods for attestations to identify applicability to the recommendations and best practices made earlier by the Working Group. Members of Working Group 6 then evaluated those attestation methods in the context of vendor security management programs and practices.

# Findings and Recommendations

## Findings

CSRIC Working Group 6 examined a number of frameworks that might be useful for self-assessment against the 11 recommended best practices for communications sector members to use to assess and manage supply chain cybersecurity risk.

This analysis was done to complement and expand upon the Working Group’s initial findings. Several security frameworks exist, with varying levels of specificity and different, though sometimes overlapping sets of controls. Further, there is no common standard for assessing a company’s compliance with the reviewed security frameworks.

The Working Group noted predominant use of three general security frameworks within the communications sector: National Institute of Standards and Technology (NIST) Cybersecurity Framework, NIST Special Publications (SP), and International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 family of standards. Companies also use their own, organization-specific frameworks, which are frequently hybrid frameworks that use features of some of the three mentioned frameworks. It should be noted that NIST Cybersecurity Framework Core drew extensively from NIST SP 800-53, ISO/IEC 27001, COBIT 5, SANS’ CCS CSC, and International Society for Automation (ISA) standards.

Figure 1 provides a summary of these three frameworks and provides examples of self-assessment methodologies. Additional examples of self-assessment methodologies that originated in other sectors are also provided as examples of third-party assessment frameworks.

***General Security***

***Framework***

***Cyber***

***Supply Chain***

***Third Party***

***Assessment***

**SP**

**800**

**-**

**53**

**ISO/IEC 27001**

**ISO/IEC 27002**

**Organization**

**-**

**specific**

**NIST CSF**

**NIST SP 800**

**-**

**161**

**ISO/IEC 27036**

***Sector***

***-***

***Specific***

**CSRIC**

**WG4**

**ISO/IEC 20243**

**Cybersecurity**

**Capability**

**Maturity Model (C2M2**

**)**

**ISO/IEC 27011**

**Common Criteria;**

**Open Group Trusted Technology Provider Standard (O**

**-**

**TTPS) Accreditation**

**Program; ISO/IEC 27001**

**Certification; UL CAP Certification**

**ISO/IEC**

**27000**

**Family**

**NIST**

**Special**

**Publications**

**Frameworks**

**Custom Framework**

***Self***

***Assessment***

**NIST CSF; NIST SP 800**

**-**

**53; NIST SP 800**

**-**

**161; ISO/IEC 27001/27002/27011; ISO/IEC 20243; C2M2**

**Custom Framework**

**Custom Framework**

***Design***

***Security in***

***Controls***

***or processes***

**SP**

**800**

**-**

**53**

**SP 800**

**-**

**161**

**ISO/IEC 27001**

**ISO/IEC 27002**

**ISO/IEC**

**27011**

**ISO/IEC 27036**

**Custom Framework**

**CSRIC WG4**

**ISO/IEC 20243**

**Cybersecurity Capability**

**Maturity Model (C2M2)**

Figure 1: Common Security Frameworks

Although some of the frameworks reviewed have associated existing, third-party assessments, the Working Group found that there is no single, pre-defined attestation methodology that suitably meets the needs of companies applying the Working Group’s best practices recommendations. Table 1 provides more detail for each document listed in Figure 1and whether those documents can be used for a self-assessment, third party certification, or both.

Table : Document Summaries and Use for Self- and Third Party Assessment

| Title | Summary | Assessment |
| --- | --- | --- |
| NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems  and Organizations | Provides guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government. Is used by many private industry organizations globally to inform security programs. | Self and third party |
| NIST Cybersecurity Framework | The NIST Cybersecurity Framework consists of standards, guidelines, and practices to promote the cybersecurity resiliency of critical infrastructure. | Self |
| ISO/IEC 27001– Information Technology – Security Techniques – Information Security Management System | Provides information security management system (ISMS) requirements. ISMS is a risk-based information security program that involves assessing and evaluating risks, identifying risk treatment and selecting controls, implementing and maintaining these controls, and continually improving ISMS processes and controls. Provides a listing of ISO/IEC 27002 controls in Annex A. | Self and third party |
| ISO/IEC 27002 – Information technology – Security techniques – Code of practice for information security controls | ISO/IEC controls catalog to use in conjunction with ISO/IEC 27001 or as guidance for implementing information security controls. | Self and third party (with 27001 only) |
| Communications Security, Reliability and Interoperability Council IV, Cybersecurity Risk Management and Best Practices Working Group 4: Final Report | NIST Cybersecurity Framework implementation guidance for communications organizations. | Self |
| ISO/IEC 20243, Information Technology – Open Trusted Technology Provider TM Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products | Process-based standard that focuses on reducing the risk of counterfeit and taint in commercial-off-the-shelf (COTS) products and their supply chains. The standard contains processes and practices for information and communication technology (ICT) providers. | Self and third Party |
| Cybersecurity Capability Maturity Model (C2M2) | While initially developed for the Energy Sector, C2M2 now exists in a generic form and can be used for self-assessment by an organization from any sector. Focuses on the implementation and management of cybersecurity practices associated with the information technology (IT) and operations technology (OT) assets and the environments in which they operate. C2M2 lists NIST SP 800-53, ISO/IEC 27001, and ISO/IEC 27002 as references that apply to most of the model domains. | Self |
| ISO/IEC 27011 – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 | ISO/IEC security controls focused on telecommunications organizations. Security controls contained in this document are an extension of ISO/IEC 27002 controls specifically tailored to telecommunications industry. | Self and third party (with 27001 only) |
| NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, | NIST SP focused on integrating supply chain risk management into NIST risk management process. Provides supply chain risk management controls most of which extend NIST SP 800-53 controls. The document also contains three new controls in addition to NIST SP 800-53 controls. | Self and third party |
| ISO/IEC 27036, Information Technology – Security Techniques – Information Security for Supplier Relationships | Multipart standard that provides requirements and guidelines for information security in supplier relationships. Contains general requirements, ICT supply chain security, and cloud services. The standard is structured along ISO/IEC 15288 – System and Software Engineering – Lifecycle Processes. The standard is also mapped to ISO/IEC 27002 (in Parts 2, 3, 4, Annex B). | Self |
| Common Criteria for Information Technology Security Evaluation (CC) | CC and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Arrangement (CCRA), which ensures that: products can be evaluated by competent and independent licensed laboratories so as to determine the fulfillment of particular security properties, to a certain extent or assurance; supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies; the certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation; these certificates are recognized by all the signatories of the CCRA. | Third party |
| Open Group Trusted Technology Provider Standard (O-TTPS) Accreditation Program | The standard and the program recognize Open Trusted Technology Providers who conform to the standard and adhere to best practices across their entire enterprise, within a specific product line or business unit, or within an individual product. Accreditation is applicable to all ICT providers in the chain: OEMS, integrators, hardware and software component suppliers, value-add distributors, and resellers. | Third party |
| UL CAP Certification | The UL 2900 series of standard addresses the following criteria: fuzz testing of products to identify zero day vulnerabilities; evaluation of known vulnerabilities; identification of known malware; static source code analysis; static binary analysis; specific security controls identified for use in products that reduce the security risk; structured penetration testing; and risk assessment of product security mitigation designed into products. ISO/IEC 27001, ISO/IEC 27002, and NIST SP 800-53 (as well as many other documents) were used as sources of practice in the development of UL CAP certification. Currently UL CAP Certification is only available for industrial control systems and medical devices, and is therefore not available for communication sector systems. | Third party |

## Recommendations

In this second milestone, CSRIC was tasked with examining and reviewing the best ways of providing assurances to the FCC and the public that recommended security capabilities are being implemented by network equipment vendors, and to recommend voluntary mechanisms that provide assurances to the FCC and the public that the security practices are being applied. CSRIC designed these recommendations to promote cooperation between the FCC, other agencies, and the private sector to enhance security by design.

CSRIC recommends the following:

* CSRIC recommends that security by design/supply chain risk management programs may be appropriately considered, among other topics, at yearly in-person meetings that were contemplated as part of CSRIC IV, Working Group 4’s recommendations issued in March, 2015.[[2]](#footnote-2) CSRIC recommends against implementing any new or additional regulations to address conformity to a particular supply chain risk assessment mechanism, or any type of written attestation to the same. In person meetings will continue to foster the public-private sector collaboration encouraged in past CSRIC reports.

In March 2015, CSRIC IV recommended, among other voluntary mechanisms, that the FCC initiate confidential, company-specific meetings for companies to convey risk management practices. CSRIC IV explained:

The sector supports the development of a voluntary program for periodic meetings, or an alternative means of communications among the FCC, DHS, and individual companies that agree to participate. The purpose of these meetings would be to discuss efforts by the organizations to develop risk management practices consistent with the NIST Cybersecurity Framework or equivalent constructs. During the meetings, the participating companies would share information regarding cyber threats or attacks. Companies that choose to participate in this program would be afforded the protections that are given by the federal government to critical infrastructure operators under the PCII program or a legally sustainable equivalent.[[3]](#footnote-3)

CSRIC IV’s recommendation was intended to represent a “new level of industry commitment intended to promote additional transparency, visibility, and dialogue with appropriate government partners and our regulator in cybersecurity and risk management.”[[4]](#footnote-4) A key component of the recommendation was that companies were afforded PCII or similar protections – namely that the information shared is exempt from FOIA, State, tribal, and local disclosure laws, use in regulatory actions and use in civil litigation. These protections, combined with the voluntary nature of the in-person meetings provide an environment that facilitates a candid, in-depth discussion about risk management practices consistent with the NIST framework.

# Conclusions

Security-by-design and supply chain risk management practices naturally fall under the cybersecurity risk management theme, and it is logical to discuss the issues together. Thus the in-person meetings contemplated by CSRIC IV would also serve as the best venues for companies to explain their supply chain risk-management programs in a secure, candid environment in a way that protects the company, and benefits the federal government by providing visibility into supply chain security programs. CSRIC does not recommend addressing supply chain risk-management issues as a separate stand-alone in-person meeting.

CSRIC is pleased to have convened a diversity of stakeholders from across the public and private spheres to address both best practice recommendations and assurances related to securing the core communications network.

1. CSRIC IV, Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report, March 2015 (CSRIC IV report). [↑](#footnote-ref-1)
2. CSRIC IV, Cybersecurity Risk Management and Best Practices, Working Group 4: Final Report, March 2015. [↑](#footnote-ref-2)
3. CSRIC IV, CSRIC IV report at 7. [↑](#footnote-ref-3)
4. CSRIC IV, CSRIC IV report at 7. [↑](#footnote-ref-4)