Communications Security, Reliability and
Interoperability Council

CSRIC

SECURE HARDWARE AND SOFTWARE: SECURITY-BY-DESIGN
WORKING GROUP 6 – Final Report:
Best Practices Recommendations for Hardware and Software Critical to the Security of the Core Communications Network
March 2016

Table of Contents

1 Results in Brief

1.1 Executive Summary

This CSRIC V Working Group 6: *Secure Hardware and Software – Security-by-Design* (Working Group 6) was formed and tasked with developing voluntary recommendations and best practices to enhance the security of hardware and software in the core public communications network. In a separate report due in September of 2016, the Working Group will provide voluntary mechanisms to demonstrate success of these best practices.

As the CSRIC has moved into its current iteration, this collaborative Federal Advisory Committee has proven itself a trustworthy public-private partnership forum able to evolve to address emerging public safety issues faced by the communications sector. As a recent example, in March 2015, CSRIC IV Working Group 4 completed the task of developing voluntary mechanisms that gave the Federal Communications Commission (FCC) and the public assurance that communications providers are taking the necessary measures to manage cybersecurity risks across the enterprise; as well as provided implementation guidance to help communications providers use and adapt the voluntary National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF).

Communications network organizations' efforts associated with security-by-design are foundational to secure communications and are also part of the larger ecosystem that faces increasing security threats. To accomplish its goal for this deliverable, Working Group 6 initiated an open, accessible and consensus-based forum to discuss security-by-design practices. Working Group 6's membership consisted of a broad array of stakeholders, both public and private, that own, operate, service, or are otherwise impacted by the core network.

After determining the objective, scope, and methodology for its work, Working Group 6 found that a diverse and vibrant ecosystem of consensus-driven voluntary standards bodies and consortia exist that are already engaged in efforts to address security-by-design (many of which are referenced in the NIST CSF). Working Group 6 believes that public-private coordination and collaboration, particularly through such standards bodies and consortia, is critical to advancing security-by-design.

The NIST CSF is a flexible, scalable framework that provides tools the communications sector can use to assess security-by-design, utilizing a risk management approach. Hence, Working Group 6 leveraged the NIST CSF to provide recommendations that can be adopted by communications sector stakeholders to improve security-by-design practices. This report is intended to address best practices for service providers seeking to manage cybersecurity risks associated with technology obtained from third party vendors, suppliers, and/or integrators for use in their core networks.

As a result of this process, Working Group 6 formulated the following recommendations:

- Communications sector members should use the best practices detailed in this report as a reference for working with vendors and suppliers to reduce cybersecurity risk within the core network. Communications sector stakeholders that provide hardware and software products and services for the core network should reference the best practices to help ensure that security-by-design principles are collaboratively addressed.

- The voluntary approach embodied by the NIST CSF and available technical approaches to securing the core network should be leveraged to drive future development of security-by-design standards and best practices. This approach will enable network stakeholders to keep pace with the dynamic nature of threats to the core network.
- Public-private coordination and collaboration in advancing security-by-design should be encouraged and enabled in order to avoid inconsistencies in approaches to security-by-design and to ensure increased intelligence sharing. Information sharing about supplier risk between government and industry is recommended as well.

Working Group 6's completion of this report and recommendations is an important step forward in securing the core network. However, organizations must continue to advance their security-by-design efforts to ensure that they are able to respond to the ever-changing threat landscape. Working Group 6 will continue its work on a future report identifying voluntary mechanisms that demonstrate the success of the recommendations and best practices in this report.

2 Introduction

Today's communications services and products face increasing security threats, which means service providers and their hardware and software suppliers must evolve risk management practices in order to better protect the communications critical infrastructure. To accomplish this, network owners and operators, working collaboratively with equipment providers, have worked to develop a common set of guiding security principles to foster 'security-by-design' – the concept of building security concepts into hardware and software from the developmental stages to the "end of life."

In recent years, both public and private stakeholders have worked together to design practical reference models that would be useful for increasing resiliency during attacks on the core network. The 2013 Presidential Executive Order (EO) 13636, "Improving Cybersecurity Critical Infrastructure,"[1] and the subsequent 2014 release of the NIST CSF Version 1.0,[2] have provided global leadership in emphasizing cybersecurity risk management as the foundation for a voluntary, risk-based model for protecting our nation's critical infrastructure and enabling organizations to prioritize and implement solutions based on informed, enterprise-tailored, business-driven considerations. Such an approach has widely been promoted by the U.S. government and industry alike as a pragmatic way to improve network security. The Communications, Security, Reliability & Interoperability Council (CSRIC) IV's Working Group

[1] Executive Order No. 13636, *Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[2] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0 (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

4: *Cybersecurity Risk Management and Best Practices*[3]Report, released in March of 2015, provided implementation guidance to help communications providers adapt the voluntary NIST CSF for their specific use, demonstrating not only the flexibility and scalability of the Framework, but the commitment of the communications industry at large to proactively enhance the sector's security posture.

This CSRIC V Working Group 6: *Secure Hardware and Software – Security-by-Design* has been formed and tasked with developing voluntary recommendations and best practices to enhance the security of hardware and software used in communications critical infrastructure. In addition, in a separate report due in September of 2016, the Working Group will provide voluntary mechanisms to demonstrate success of these best practices. Building on the strong foundation laid by EO 13636, the NIST CSF, and CSRIC IV Working Group 4, this report demonstrates the value of a voluntary and standards-based risk management approach in constantly improving the security of the communications network.

Using the NIST CSF as a baseline, this report contains recommendations and best practices for communications providers that allow for the evaluation and validation of existing security-by-design processes. The recommendations are intended for use by any organization – regardless of size – that must address the integrity of the core network. In developing this report, the stakeholders provided the perspective of owners and operators of the core network; as well as that of suppliers and vendors who prioritize the incorporation of security principles into the life cycle of their products and services.

2.1 CSRIC Structure

CSRIC V: Working Group Structure								
Susan Sherwood Jeff Cohen (Co-Chairs)	Francisco Sanchez Farrokh Khatibi (Co-Chairs)	Steven Johnson Kelly Williams (Co-Chairs)	Kent Bressie Catherine Creese (Co-Chairs)	Jennifer Manner (Chair)	Rod Rasmussen Chris Boyer Brian Allen (Co-Chairs)	Brian Scarpelli Joel Molinoff (Co-Chairs)	Bill Boni Drew Morin (Co-Chairs)	William Reidway Jr. Thomas Anderson (Co-Chairs)
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	**Working Group 4**: Communications Infrastructure 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

[3] The Communications Security, Reliability and Interoperability Council IV, *Final Report, Working Group 4: Cybersecurity Risk Management and Best Practices*, March 2015 (available at: https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf) (visited February 24, 2016) (CSRIC IV Working Group 4 Report).

Table 1 - Working Group Structure

2.2 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)**
Steven	McKinnon	**Federal Communications Commission (Working Group 6 Liaisons)**
Emily	Talaga	
Andy	Ellis	**Akamai**
Michael	Stone	
Chris	Boyer	**AT&T**
Brian	Daly	**ATIS (AT&T)**
Mike	Geller	**(Cisco)**
Jamie	Brown	**CA Technologies**
Steve	Goeringer	**Cable Labs**
Rob	Covolo	**CenturyLink**
Stacy	Hartman	
Kevin	Beaudry	**Charter**
Mike	Geller	**Cisco**
Lisa	Meyers-McDonald	
Eric	Wenger	
Leslie	Krigstein	**College of Healthcare Information Management Executives**
Michael	O'Reirdan	**Comcast Cable**
Glen	Pirrotta	
Kallol	Ray	
Jon	Amis	**Dell**
Gabriel	Martinez	**Department of Homeland Security National Protection and Programs Directorate**
Alex	Gerdenitsch	**EchoStar**
Jennifer	Manner	
Bill	Olson	**General Services Administration**
Peter	Allor	**IBM**
James	Bean	**Juniper Networks**
Eli	Dourado	**Mercatus Center at George Mason University**
Angela	McKay	**Microsoft**

First Name	Last Name	Organization
Matt	Tooley	**National Cable and Telecommunications Association**
Jon	Boyens	**National Institute of Standards & Technology**
Bryanna	Evans	**Nokia**
Andrew	McGee	
Rao	Vasireddy	
Kazu	Gomi	**NTT America**
Kimura	Masato	
Shinichi	Yokohama	
Franck	Journoud	**Oracle**
Richard	Perlotto	**Shadow Server**
Patrick	Koethe	**Sprint**
Jeff	Greene	**Symantec**
Chris	Roosenraad	**Time Warner Cable**
Joe	Viens	
Darren	Kress	**T-Mobile**
Michelle	Rosenthal	
Robert	Mayer	**USTelecom Association**
Tom	Soroka	
Nadya	Bartol	**Utilities Telecom Council**
Al	Bolivar	**Verisign**
Tomofumi	Okubo	
Heath	McGinnis	**Verizon**
Dorothy	Spears-Dean	**Virginia Information Technologies Agency and National Association of State 911 Administrators**
Ethan	Lucarelli	**Wiley Rein (Iridium)**
Peter	Ruffo	**ZTE USA**

Table 2 - List of Working Group Members

3 Objective, Scope, and Methodology

3.1 Objective

CSRIC V's Working Group 6 was tasked with providing recommendations to help ensure the security of the supply chain for critical communications infrastructure. The supply chain consists of several distinct segments: design and development, distribution, and maintenance- each of which has its own risks and vulnerabilities. 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 hardware and software in the core public communications network.

In addition, Working Group 6 has been tasked with developing a means to assure the FCC and the public that the identified recommended security capabilities are being implemented by network equipment vendors. To provide this assurance, in a future report, this Working Group will identify voluntary mechanisms that demonstrate the success of these recommendations and best practices.

3.2 Scope

The capabilities recommended by this Working Group make use of security-by-design principles and processes that enable network equipment manufacturers to make the core communications network more secure, resilient, and defendable from attacks. For the purposes of this exercise, the Working Group relied on the National Sector Risk Assessment's (NSRA's) definition of "core network," which was also relied upon in the CSRIC IV Working Group 4 report. The Working Group 4 report provides the following guidance regarding the core network:

> "The core network transports a high volume of aggregated traffic over large distances; typically via fiber or satellite and interconnects with access networks across the country. The core network is global, connecting all continents except Antarctica using submarine fiber optic cable systems and land-based fiber and copper facility networks. The converged core network uses various technologies for the physical (layer 1) and transport layers (layer 2) for the transport of the services.
>
> "Multiple service providers operating distinct core networks traversing the entire country provide the communications core infrastructure. These networks are primarily composed of wireline networks. The voice, video, and data services typically require some kind of routing translation query such as a host name look up or toll-free number query and are provided as part of operating the core network. In addition, the Network Operations Center (NOC), customer care centers, and data centers for all the access networks reside on the core network.
>
> "The access networks connect the end users to the core network. Traffic may originate and terminate with an access network without connecting to the core network."[4]

Further, the NSRA depicts the core network visually as follows:[5]

[4] CSRIC Working Group 4 report at pgs. 68-70.

[5] http://info.publicintelligence.net/commsector2012.pdf

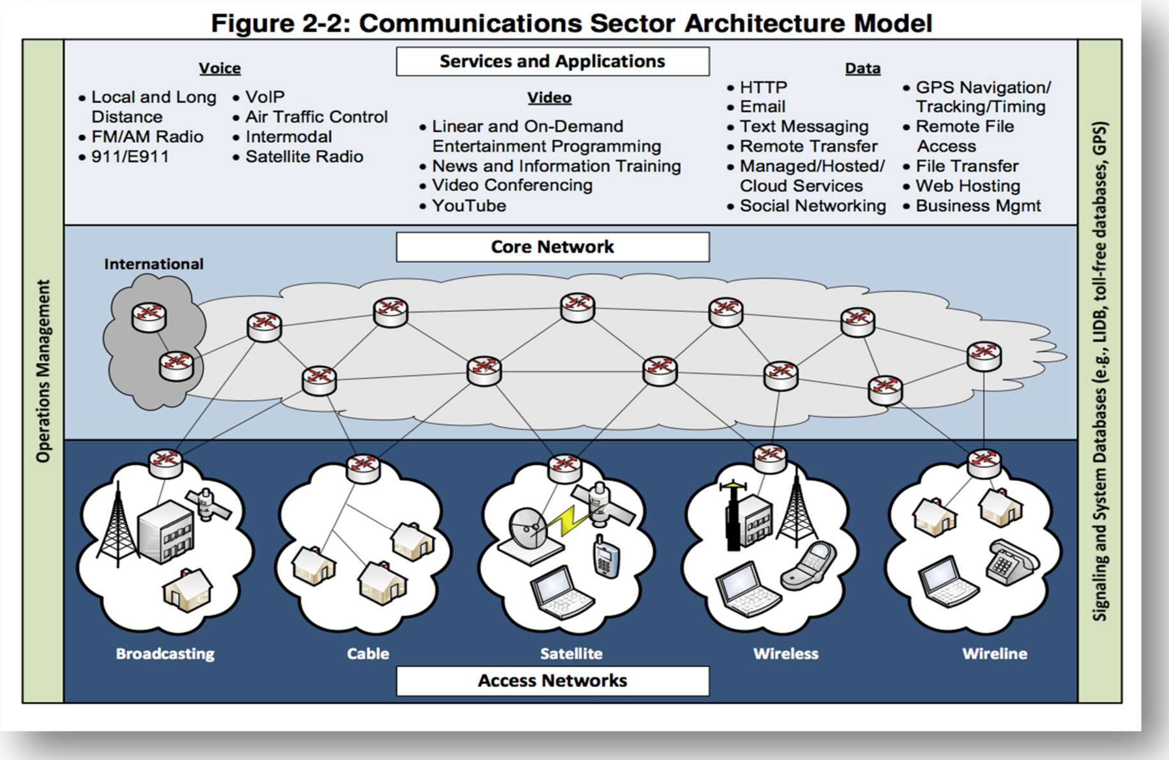

Figure 1:2012 NSRA Depiction of the Communications Sector Architecture Model

This document is intended to address best practices for service providers seeking to manage cybersecurity risks associated with technology obtained from third party vendors, suppliers, and or integrators for use in their core networks.

3.3 Methodology

In order to provide the recommended capabilities to better ensure the security of the supply chain for critical communications infrastructure, a three-phased approach was undertaken to complete the above deliverables:

- **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-monthly conference calls and in-person meetings to produce the above deliverables.

The Working Group 6 members agreed to the following framing concepts:

- The deliverable should incorporate both perspectives related to service providers who require secure practices by their vendors, and the vendors who should incorporate secure development life cycle practices to manage risk.
- The deliverable should be at the principle level, and should be technology- and origin-neutral, so that the recommendations can remain relevant as technologies evolve (e.g., the recommendations should be useful for traditional and software-defined networks).
- The principles in this deliverable should draw from the existing body of standards and best practices developed for security-by-design.

With these framing concepts in mind, Working Group 6 reviewed current industry security-by-design standards/best practices. Informed by this exercise, an assessment of these standards/best practices was then undertaken using the NIST CSF to determine key security-by-design practices, from both the service provider and vendor perspectives. Members of Working Group 6 then evaluated the NIST CSF in the context of companies' vendor security management programs and best practices. The result was a compendium of macro, process level best practices for core network owners and operators to use as they evaluate and deploy hardware and software products.

4 Findings and Recommendations

4.1 Findings

As noted above, Working Group 6 conducted a review of standards bodies and consortia published materials related to managing cybersecurity risk, as well as individual company approaches to security-by-design. Through its analysis the Working Group determined the following:

- A rich body of information exists to help companies evaluate and manage cybersecurity risk, and the development of security-by-design principles. The communications sector should leverage these proven, industry-accepted reference materials and existing standards/best practice recommendations. A non-exclusive list of these existing efforts is included in this report as Appendix 1.
- Given the diverse type and functions of vendors and suppliers serving core network providers, any risk management recommendations should be at a macro level and process-based, so as to allow for their extensibility and utility across technologies and services.
- Through its analysis, the Working Group found that the NIST CSF presented the strongest foundation for best practices. The following table comprises the Working Group's assessment of measures that a communications sector member should utilize to review security-by-design protections with vendors and suppliers. The items discussed are not intended to be a checklist that a sector member must build into supplier contracts. Rather, the best practices are intended to be set of prioritized voluntary controls that communications providers may use as a reference in working with vendors and suppliers to mitigate supply chain cybersecurity risk. It should be noted that depending upon the supplier and the specific functions being provided, these measures should not be viewed

as appropriate in all instances. Moreover, the NIST CSF may be updated to more specifically address hardware assurance and other supply chain-related cybersecurity matters; thus, while this list provides recommended areas of focus, organizations may want to consult the NIST CSF as it is updated over time.

- It is important for service providers to establish upfront which party will be responsible for managing risks associated with the operation of the technology. The answer may vary depending upon whether the technology is delivered as a physical product or as a subscription-based service. In a traditional product sales model, vendors could reasonably be expected to employ a secure development lifecycle that would include mechanisms for communicating information about mitigations or patches to known vulnerabilities. However, vendors would not typically be positioned to operate the technology --or to directly manage risks associated with its operation. By contrast, where service providers have contracted for a vendor-managed service, the agreement may very well require vendors or other operators of the service to assume compliance obligations for managing security risks on an ongoing basis.

The table below summarizes the recommended best practices for communications sector members to use to assess and manage supply chain cybersecurity risk.

SECURITY-BY-DESIGN		
FUNCTION & CATEGORIES	**BEST PRACTICE**	**SAMPLE SUBCATEGORIES FROM NIST CSF**
IDENTIFY **ID.GV, ID.RA**	**Governance, Risk Assessment and Risk Management.** Ensure that suppliers have an organizational security policy that governs design, development, and production of the products and services. Examples include: • Following policies, procedures, and processes to manage and monitor the organization's cybersecurity risks to ensure that suppliers understand the cybersecurity risk to both their operations and to their customers; • Following governance and risk management policies; • Identifying vulnerabilities, threats and the likelihoods and impacts to determine risk; • Ensuring that a baseline configuration of information systems is created; • Defining a life cycle to manage systems; • Putting in place change control processes; • Conducting, maintaining and periodically testing the backup of information; • Destroying data according to policy; • Putting in place and managing incident response and recovery plans and developing and implementing a vulnerability management plan.	**ID.GV-1, ID.GV-4, ID.RA-1, ID-RA.3, ID.RA-5, ID.RA-6. PR.IP-1, 2,3,4,6,9, 12**

SECURITY-BY-DESIGN		
FUNCTION & CATEGORIES	**BEST PRACTICE**	**SAMPLE SUBCATEGORIES FROM NIST CSF**
PROTECT **PR.AC**	**Access Controls.** Ensure that suppliers limit access to (1) assets and associated facilities used to design, develop, and produce applicable solutions, and (2) the products and services, to authorized users, processes and devices and limit access to only authorized activities and transactions. Steps may include: • Suppliers establishing user account credentials and account management processes, • Establishing password requirements; • Ensuring that identities and credentials are managed for authorized devices and users; • Managing and protecting physical access to assets; • Managing remote access ; • Managing access permissions to systems impacting sector member information assets incorporating the principles of least privileged and separation of duties; and • Protecting network integrity incorporating network segregation where appropriate.	**PR.AC-1, PR.AC-2, PR.AC-3, PR.AC-4, PR.AC-5**

SECURITY-BY-DESIGN		
FUNCTION & CATEGORIES	**BEST PRACTICE**	**SAMPLE SUBCATEGORIES FROM NIST CSF**
PROTECT **PR.DS**	**Data Security.** Ensure that information and records (data) relevant to products and services residing on applicable solutions are managed to protect and ensure the confidentiality, integrity and availability of information. This may include steps by supplier to ensure that data-at-rest and data-in-transit are protected, including; • Using strong encryption, • Implementing protections to prevent data leaks, and • Using integrity checking mechanisms to verify software, firmware and information integrity. Additional steps may involve: • Isolating relevant products and services from other customer's or suppliers own products and services, • Having documented procedures for secure backup, recovery and destruction of sector member's information, and • Limiting access to such information to only authorized personnel.	**PR.DS-1, PR.DS-2, PR.DS-5, PR.DS-6, PR.DS-7**
PROTECT **PR.MA**	**Maintenance**. Ensure that suppliers have in place mechanisms to ensure: • Performing maintenance and repair of relevant products and services in a timely manner, and • Approving, logging and performing remote maintenance of products and services in a manner that prevents unauthorized access.	**PR.MA-1,2**

SECURITY-BY-DESIGN		
FUNCTION & CATEGORIES	**BEST PRACTICE**	**SAMPLE SUBCATEGORIES FROM NIST CSF**
PROTECT **PR.PT**	**Protective Technology.** Ensure that supplier's information resources that may impact applicable products and services are sufficiently hardened which may involve disabling unused networking or other computing functionality. Supplier may also ensure that technical security solutions are managed to ensure the security and resilience of supplier's information resources relevant to products and services including that: • Controlling access to systems and assets, incorporating the principle of least functionality, • Protecting communications and control networks, • Protecting removable media and restricting its use according to policy, and • Maintaining audit and log records. When providing Internet accessible services to sector members, supplier should ensure that adequate Distributed Denial of Service (DDoS) protections are in place and that supplier requires strong authentication for any remote access to such systems.	**PR.PT-1, 2,3,4**
DETECT **DE.AE**	**Anomalies and Event Detection**. Ensure that: • Supplier has tools in place to detect anomalies and events relevant to products and services, and • Such events are analyzed to understand attack targets and methods. The impact of events or anomalies should be determined and supplier should notify sector members according to a documented procedure.	**DE.AE-2, 4**

SECURITY-BY-DESIGN		
FUNCTION & CATEGORIES	**BEST PRACTICE**	**SAMPLE SUBCATEGORIES FROM NIST CSF**
DETECT **DE.CM**	**Security Continuous Monitoring**. Ensure that supplier information system and assets relevant to products and services are monitored to identify cybersecurity events and verify the effectiveness of cybersecurity measures. This may include that: • Baselining and monitoring the network to detect potential cybersecurity events, • Monitoring the physical environment to detect potential cybersecurity events, • Detecting malicious code, • Detecting authorized mobile code, • Performing vulnerability scans on a routine basis, and • Monitoring for unauthorized personnel, connections, devices and software. Supplier may also actively monitor industry resources for timely notification of applicable security alerts related to sector member's information resources, as defined via contract, to take prompt action.	**DE.CM-1,2,4,5,7**
DETECT **DE.DP**	**Detection Processes**. Ensure that suppliers have in place detection processes and procedures for identifying security events that may impact products and services; for example intrusion detection or intrusion detection and prevention systems, that monitors traffic interacting with sector member's information resources, that are maintained to ensure timely awareness of anomalous events. This may include event detection and Supplier should ensure they have a documented procedure to be followed in the event of an actual or suspected attack and promptly notify sector member whenever there is a successful attack upon, intrusion upon, unauthorized access to, loss to or other breach of sector member's information resources.	**DE.DP-4**

SECURITY-BY-DESIGN		
FUNCTION & CATEGORIES	**BEST PRACTICE**	**SAMPLE SUBCATEGORIES FROM NIST CSF**
RESPOND **RS.RP** **RS.CO**	**Response Planning and Communications** Ensure that supplier has in place a documented process to remediate security vulnerabilities relevant to products and services to detected cybersecurity events and that response activities are coordinated with customers and external stakeholders (as appropriate), which may include support from law enforcement or other agencies.	**RS.RP-1, RS.CO-4**
RESPOND **RS.AN** **RS.MI**	**Analysis and Mitigation.** Ensure that supplier is conducting analysis to ensure adequate response and support recovery activities relevant to products and services including determining the impact of the incident, forensics, and notifications as appropriate and that activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident or contain its impact.	**RS.AN-1,2,3** **RS.MI-1,2**
RECOVER **RC.RP**	**Recovery Planning**. Ensure that suppliers have in place recovery processes and procedures covering the products and services that can be executed and maintained to ensure the timely restoration of relevant systems and assets affected by cybersecurity events.	**RC.RP-1**

4.2 Recommendations

Working Group 6 recommends the following:

- Communications sector members should use the best practices detailed in this report as a reference for working with vendors and suppliers to reduce cybersecurity risk within the core network. Communications sector stakeholders that provide hardware and software products and services for the core network should reference the best practices to help ensure security-by-design principles are collaboratively addressed.
- To enable network stakeholders to keep pace with the dynamic nature of threats to the core network, the voluntary approach embodied by the NIST CSF and available technical approaches to securing the core network should be leveraged to drive future development of security-by-design standards and best practices.
- Public-private coordination and collaboration in advancing security-by-design should be encouraged and enabled in order to avoid inconsistencies in approaches to security-by-

design. This also ensures increased intelligence sharing. Information sharing about supplier risk between government and industry is recommended as well.

5 Conclusions

Communication network organizations that follow security-by-design principles are foundational to secure communications and are also part of a larger ecosystem that faces increasing security threats. A diversity of consensus-driven voluntary standardization bodies and consortia are engaged in efforts to address security-by-design today and are referenced in the NIST CSF. Further, public-private coordination and collaboration in advancing security-by-design will help avoid inconsistencies in approaches to security-by-design. The introduction of the NIST CSF represents a major breakthrough in the ability to communicate cybersecurity risk management principles and processes and can be effectively employed by the communications sector and applied to other critical infrastructure sectors.

Communications sector stakeholders that provide hardware and software products and services for the core network are encouraged to utilize this report and the NIST CSF to improve their security-by-design practices, which may contribute to a more secure core network. The communications sector's public and private members have demonstrated their commitment to improving the use and enhancement of security-by-design practices. While this report is an important step forward in this space, core network stakeholders will need to continue to refine and expand the use of security-by-design practices.

6 Acknowledgments

Working Group 6 would like to acknowledge the significant contributions of each of its members. Without their expertise, participation, analysis, and contributions throughout the process, the report findings, conclusions, and recommendations contained herein would not have been possible. Member insight, focus, and outreach across the communications sector, and leadership throughout the Working Group 6 process is evidenced by the quality of this report's analysis, recommendations, and conclusions. In particular, Working Group 6 would like to thank Nadya Bartol, Chris Boyer, Chris Roosenraad, and Matt Tooley for their expertise and dedication in guiding this Working Group through using the NIST CSF to formulate the security-by-design findings and recommendations in this report.

Working Group 6 would also like to acknowledge and thank our FCC liaisons Steven McKinnon and Emily Talaga, for their support and contributions, as well as their thoughtful advice, and encouragement throughout the process.

Working Group 6 would also like to acknowledge the skill and dedication of Stacy Hartman for her leadership and attention to detail in the drafting of the final report, without which the Final Report would not have been possible.

Finally, Working Group 6 would like to acknowledge and thank co-chairs Joel Molinoff and Brian Scarpelli for their helpful insight on security-by-design practices, as well as their efforts to include a broad array of stakeholders in the Working Group 6 process as well as their work to

build consensus amongst the Working Group members.

7 Appendix 1 – Security-by-Design Efforts Reference List

Refer to attachment: *FCC CSRIC WG6 Reference List*

CSRIC Working Group 6: Secure Hardware and Software - Security-by-Design
Reference List

Short Title	Title	Year of Issuance	Abstract	Link
	Cybersecurity Procurement Language for Energy Delivery Systems	2014	In order to help energy sector asset owners and operators communicate expectations and requirements in a clear and repeatable manner, the Energy Sector Control Systems Working Group (ESCSWG) built upon DHS (2009) to develop the baseline cybersecurity procurement language provided in this document. This language is tailored to the specific needs of the energy sector in order to provide a starting point for energy sector cybersecurity procurements.	http://energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf
	DHS 'Build Security In' - Improve Security and Software Assurance: Tackle the CWE Top 25 Most Dangerous Software Errors		The Top 25 CWEs represent the most significant exploitable software constructs that have made software so vulnerable. Addressing these will go a long way in securing software, both in development and in operation.	https://buildsecurityin.us-cert.gov/
NIST SP 800-160	DRAFT Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems		This publication addresses the engineering-driven actions necessary for developing a more defensible and survivable information technology (IT) infrastructure—including the component products, systems, and services that compose the infrastructure. It starts with and builds upon a set of well-established International Standards for systems and software engineering published by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronic Engineers (IEEE) and infuses systems security engineering techniques, methods, and practices into those systems and software engineering processes. The ultimate objective is to address security issues from a stakeholder requirements and protection needs perspective and to use established organizational processes to ensure that such requirements and needs are addressed early in and throughout the life cycle of the system.	http://csrc.nist.gov/publications/drafts/800-160/sp800_160_draft.pdf
	Financial Services Information Sharing and Analysis Center (FS-ISAC), Appropriate Software Security Control Types for Third Party Service and Product Providers (version 2.1.3)	2015	This white paper aims to further improved controls operating in concert with vendor management practices to advance the relationship between security and third party software service providers and commercial off-the-shelf software (COTS) vendors.	http://docs.ismgcorp.com/files/external/WP_FSISAC_Third_Party_Software_Security_Working_Group.pdf

CSRIC Working Group 6: Secure Hardware and Software - Security-by-Design
Reference List

Short Title	Title	Year of Issuance	Abstract	Link
ISO/IEC 20243:2015	Information Technology -- Open Trusted Technology ProviderTM Standard (O-TTPS) -- Mitigating maliciously tainted and counterfeit products	2015	This standard is intended to help commercial off-the-shelf (COTS) information and communication technology (ICT) providers prevent the introduction of tampered or counterfeit product components at any stage of the product life cycle to mitigate risk.	http://www.iso.org/iso/catalogue_detail.htm?csnumber=67394
ISO/IEC 27002	Information technology -- Security techniques -- Code of practice for information security controls	2013	ISO/IEC 27002:2013 gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).	http://www.iso.org/iso/catalogue_detail?csnumber=54533
	NDIA Engineering for System Assurance (version 1)	2008	This guidebook provides process and technology guidance to increase the level of system assurance. This guidebook is in tended primarily to aid program managers (PMs) and systems engineers (SEs) who are seeking guidance on how to incorporate assurance measures into their system life cycles. Assurance for security must be integrated into the systems engineering activities to be cost-effective, timely, and consistent. In systems engineering, the activities for developing and maintaining the assurance case enable rational decision making, so that only the actions necessary to provide adequate justification (arguments and evidence) are performed. This guidebook is a synthesis of knowledge gained from existing practices, recommendations, policies, and mandates. System assurance activities are executed throughout the system life cycle.	http://www.acq.osd.mil/se/docs/SA-Guidebook-v1-Oct2008.pdf
	NIST CSF	2014	The Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.	http://www.nist.gov/cyberframework/index.cfm
O-TTPS Version 1.1	Open Group Trusted Technology Provider Standard (O-TTPS) Accreditation Program	2015	This standards is aimed at assuring both the integrity of commercial off-the-shelf (COTS) information and communication technology (ICT) products and the security of their supply chains. It helps to safeguard the products and their global supply chains against the increasing sophistication of cybersecurity attacks.	http://www.opengroup.org/news/press/OTTPS-approved-as-ISO-IEC-international-standard

CSRIC Working Group 6: Secure Hardware and Software - Security-by-Design
Reference List

Short Title	Title	Year of Issuance	Abstract	Link
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations	2013	This publication provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors. The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. The controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure, derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs. The publication also describes how to develop specialized sets of controls, or overlays, tailored for specific types of missions/business functions, technologies, or environments of operation. Finally, the catalog of security controls addresses security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability).	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
	Software Integrity Controls, An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain	2010	This paper is focused on examining the software integrity element of software assurance and provides insight into the controls that SAFECode members have identified as effective for minimizing the risk that intentional and unintentional vulnerabilities could be inserted into the software supply chain.	http://www.safecode.org/publication/SAFECode_Software_Integrity_Controls0610.pdf
NIST SP 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations	2015	This publication provides guidance to federal agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels of their organizations. The publication integrates ICT supply chain risk management (SCRM) into federal agency risk management activities by applying a multitiered, SCRM-specific approach, including guidance on assessing supply chain risk and applying mitigation activities.	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

CSRIC Working Group 6: Secure Hardware and Software - Security-by-Design
Reference List

Short Title	Title	Year of Issuance	Abstract	Link
ISO/IEC/IEEE 15288:2015	Systems and software engineering – System life cycle processes	2015	ISO/IEC/IEEE 15288:2015 establishes a common framework of process descriptions for describing the life cycle of systems created by humans. It defines a set of processes and associated terminology from an engineering viewpoint. These processes can be applied at any level in the hierarchy of a system's structure. Selected sets of these processes can be applied throughout the life cycle for managing and performing the stages of a system's life cycle. This is accomplished through the involvement of all stakeholders, with the ultimate goal of achieving customer satisfaction.	http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=63711
	The Software Supply Chain Integrity Framework, Defining Risks and Responsibilities for Securing Software in the Global Supply Chain	2009	This paper assesses software supply chain integrity in the context of software engineering, providing a framework and common taxonomy for evaluating the associated risks and defining the industry’s role in addressing them. This framework will serve as the foundation for subsequent work aimed at describing and analyzing software integrity best practices.	http://www.safecode.org/publication/SAFECode_Supply_Chain0709.pdf