



CSRIC IV - Working Group 4: Cybersecurity Best Practices Status Update

March 20, 2014

Co-Chair: Robert Mayer, US Telecom

Co-Chair: TBD

Agenda

- Background and Perspectives
- Objectives
- Planned Approach
- Working Group 4 Leadership and Members
- Status
- Next Steps

Background and Perspectives

- In March 2011, CSRIC II, Working Group 2A, Cyber Security Best Practices, delivered their final report¹ containing 397 Best Practices across 9 focus areas including: Wireless, IP Service, Network, People, Legacy Services, Identity Management, Encryption, Vulnerability Management, and Incident Management.
- In February 2014, NIST delivered their Cybersecurity Framework v1.0², in response to the President's Executive Order 13636, "Improving Critical Infrastructure Cybersecurity"³. This CSRIC Working Group effort was timed to coincide with the release of the February 2014 Cybersecurity Framework which is focused on five core areas of risk management: Identify, Protect, Detect, Respond, and Recover.

¹ <http://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf>

² <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>

³ <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>



Background and Perspectives (cont.)

- “I commend NIST and the many stakeholders who helped develop the Cybersecurity Framework, a significant first step that lays the groundwork to further secure America’s critical infrastructure. The FCC was pleased to participate in this process. Now the next phase of hard work begins. It is time to operationalize the framework within the communications sector to keep America’s information economy strong.”

FCC Chairman, Tom Wheeler, February 12, 2014

- “The Framework allows organizations – regardless of size, degree of cyber risk or cybersecurity sophistication to apply the principles and best practices of risk management to improve the security and resilience of critical infrastructure... The development of this Framework has jump-started a vital conversation between critical infrastructure sectors and their stakeholders. They can work to understand the cybersecurity issues they have in common and how those issues can be addressed in a cost-effective way without reinventing the wheel.”

NIST Director, Patrick D. Gallagher, February 12, 2014



WG4 Objectives

- Evaluate CSRIC's most critical existing cybersecurity best practices and determine how best to improve them to account for changes in cybersecurity practice and the threat landscape.
- Harmonize and update these best practices with the recently released NIST Cybersecurity Framework.
- Identify aspects of a business environment in which cybersecurity-specific practices will be effective, efficient, and sustainable.
- Identify barriers to implementing cybersecurity best practices and recommend actions the Commission can take to mitigate those barriers.
- Produce a final report in March 2015 for communications providers of all size and scope who may use the material to evaluate and improve their cybersecurity posture and communicate needs and expectations internally and with external stakeholders throughout the broader ecosystem.

WG4 Planned Approach

- We organized WG4 around five communications sector segments:
 - Broadcast
 - Cable
 - Wireless
 - Wireline
 - Satellite
- Each subgroup segment has strong industry representation including representation from small and mid-sized entities.
- The industry segments will review existing CSRIC cybersecurity BPs and produce a streamlined set of technical and operational BPs that align with the Cybersecurity Framework's five core functions.



WG4 Planned Approach (Cont.)

- The Framework recognized the critical need for executive level engagement to ensure that critical elements of the entire organization are aligned around security best practices. The WG4 Cyber Risk Management subgroup will explore the different organization elements that must work together to achieve a desired security state and the critical factors that lead to a successful and sustainable risk management process.
- Previous work in CSRIC III Working Group 7 developed an analytical framework to identify barriers to implementing a set of recommendations associated with the U.S. Anti-Bot Code. WG4 will refine that effort to understand how specific practices may be impacted by various considerations (e.g., technology, process, people) and what incentives may be required to address economic hurdles.

WG4 Planned Approach (Cont.)

- It has become increasingly evident that the challenges associated with managing cyber risk are global in nature and involve a diverse set of stakeholders with varying degrees of accountability, capabilities, resources, and motives.
- In the communications and IT sectors in particular, convergence has created a multitude of shared infrastructures, platforms, and services, which fundamentally alters the balance of responsibilities among service providers, content providers, e-commerce providers, equipment vendors, software and application developers and end-users.
- WG4 will look at the dynamics in the ecosystem from a carrier/ISP perspective to understand how different communities can work together to support common interests and to consider the appropriate venues for such activity to occur.
- WG4 will recommend that the FCC adopt a revised and updated set of best practices based on the outcome of the analyses across the sub-groups and any other recommendations associated with future activities.

Leadership Team

We have assembled a highly-regarded team of advisors, thought-leaders, and senior cybersecurity practitioners to lead this effort.

WG4 Stakeholder Leads

- NIST/CSRIC Alignment - Segment Leads
 - Broadcast, Kelly Williams, NAB
 - Cable, Matt Tooley, NCTA
 - Wireless, John Marino, CTIA
 - Wireline, Chris Boyer, AT&T
 - Satellite, Donna Bethea Murphy, Iridium
- Cyber Risk Management, Jack Whitsitt, EnergySec
- Ecosystem – Shared Responsibilities, Co-Leads, Tom Soroka, USTelecom, Brian Scarpelli, TIA
- Mids/Smalls – Co-Leads, Susan Joseph, Cable Labs, Jesse Ward, NTCA

WG4 Senior Advisors

- Donna Dodson, WG4 Senior Technical Advisor, NIST, Deputy Chief Cybersecurity Advisor & Division Chief for Computer Security Division
- Samara Moore, WG4 Senior Policy Advisor, White House Director of Critical Infrastructure
- Emily Talaga, WG4 Senior Economic Advisor, Economist, FCC International Bureau



WG4 Membership Team

65 members representing the communications sector, and representatives from the energy, financial and IT sectors, standards bodies, vendors, as well as federal and state departments and agencies.

Robert Mayer (Chair)	Kate Dean	Susan Joseph	Michael Mosher	Danna Valsecchi
Samara Moore (Sr. Policy Advisor)	Martin Dolly	Merike Kaeo	Donna Bethea Murphy	S. Rao Vasireddy
Donna Dodson (Sr. Technical Advisor)	Russell Eubanks	Kevin Kastor	Paul Nguyen	Phil Venables
Emily Talaga (Sr. Economic Advisor)	Paul Ferguson	John Kelly	Jorge Nieves	Joe Viens
Vern Mosley (FCC Liaison)	Kevin Frank	Scot Kight	Mike O'Hare	Jessie Ward
Adrienne Abbott	Craig Froelich	Kate Kingberger	Ron Roman	Errol Weiss
Brian Allen	Chris Garner	Rick Krock	Chris Roosenraad	Jack Whitsitt
Chris Boyer	Michael Geller	Jeremy Larson	Harold Salters	Kelly Williams
Lois Burns	Jessica Gulick	Greg Lucak	Brian Scarpelli	Pamela A. Witmer
Ingrid Caples	Stacy Hartman	Ethan Lucarelli	Karl Schimmeck	
Joel Capps	Chris Homer	John Madden	Tom Soroka	
William Check	Charles Hudson, Jr	Daniel Madsen	Myrna Soto	
Nneka Chiazor	Wink Infinger	John Marinho	Matt Tooley	
Edward Czarnecki	Chris Jeppson	Beau Monday	Bill Trelease	



WG4 Status

- WG4 has held a kick-off conference call with the Leadership team as well as its working group members to discuss the updated working group description, a preliminary approach reflected in this presentation, and expectations of members participating in this effort.
- WG4 has established various administrative capabilities (e.g., list-serve, membership contact information), and is working to confirm scheduled conference calls to discuss progress on sub-group tasks and inter-sub-group coordination.

Next Steps

- Firm up WG4 leadership and membership.
- Reach WG4 consensus on approach, work plan, and make adjustments as necessary.
- Schedule first face-to-face meeting.
- Schedule Leadership, Sub-group and Working Group conference calls.
- Provide periodic status updates to Steering Committee and Council.