SEVENTH MEETING OF THE COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL VII

DECEMBER 9, 2020

COMMENCE MEETING

Suzon Cameron, DFO

Opening Remarks

Charlotte Field, Chair

PRESENTATION

REPORT ON REVIEW AND RECOMMENDATIONS ON OPTIONAL SECURITY FEATURES IN 3GPP STANDARDS IMPACTING 5G NON-STANDALONE ARCHITECTURE

Kathy Whitbeck, Chair
Working Group 2

REVIEW AND RECOMMENDATIONS ON OPTIONAL SECURITY FEATURES IN 3GPP STANDARDS IMPACTING 5G NON-STANDALONE ARCHITECTURE

Working Group 2: Managing Security Risk in the Transition to 5G

Kathy Whitbeck, Chair WG2, Nsight

December 9, 2020

Deliverables/Schedule

Report 1 **June 2020** - ***Complete***

Report on Risks to 5G from Legacy Vulnerabilities and Best Practices for Mitigation

Report 2 **December 2020 – Submitting today for Council consideration**

Report on Recommended Updates to 3GPP Standards and Comparison Risk and Remediation Expenses for 5G Vulnerabilities (including identification of optional features in 3GPPstandards that can diminish the effectiveness of 5G security and recommendations to address these gaps)

Agenda

- Working Group 2 Background & Objectives
- Approach 5G Non-Standalone Architecture (NSA)
- 3GPPP Optional Features
- Findings
- Recommendations

Working Group 2 Members

Kathy Whitbeck (Chair)*	Nsight
Brandon Abley*	NENA
Jason Boswell	Ericsson
Paul Diamond	CenturyLink
Charlotte Field*	Charter Communications
Mohammad Khaled	Nokia Bell Labs
Farrokh Khatibi*	Qualcomm
John Marinho	CTIA
Susan M. Miller*	ATIS
Drew Morin	T-Mobile
Jitendra Patel	AT&T
Krisztina Pusok*	American Consumer Institute
Travis Russell*	Oracle Communications
Sandeep Shrivastava	Orchestra Technology
Brian Trosper*	Verizon
David Villyard	CISA DHS
Fei Yang	Comtech

FCC Liaison: Kurian Jacob

*Also CSRIC Member

Working Group 2 Alternates†

Steve Barclay	ATIS
Mike Geller	ATIS
Jeff Matisohn	Charter Communications
Scott Poretsky	Ericsson
Andrew Schnese	Nsight
Greg Schumacher	T-Mobile
Yousif Targali	Verizon

† Alternates are not a member of the Working Group and may not vote.

Working Group 2: Background

Working Group Description:

As Fifth Generation (5G) wireless technology is widely deployed by wireless service providers in the United States and around the world, its evolutionary design will incorporate a number of existing standards from previous generations. This approach risks the persistence in 5G of security issues that exist in currently deployed networks. For example, researchers have identified several vulnerabilities in the attach, detach, and paging procedures of earlier generation wireless technology that may negatively affect the confidentiality, integrity, and availability of wireless networks and continued challenges in avoiding fake base stations in 5G networks.

Working Group 2: Objectives

- The FCC directs CSRIC VII to review risks to 5G wireless technologies that may carry over from existing vulnerabilities in earlier wireless technologies that can lead to the loss of confidentiality, integrity, and availability of wireless network devices. CSRIC VII will recommend best practices to mitigate the risks for each vulnerability it identifies and address recently proposed solutions by security researchers.

Working Group 2: Objectives (Cont)

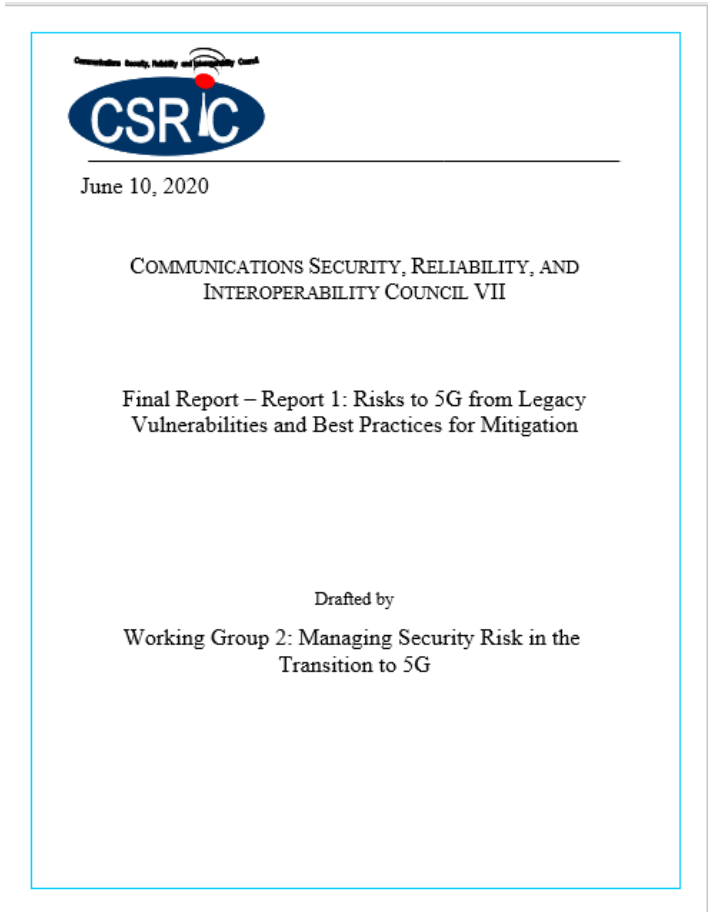
- Additionally, the FCC directs CSRIC VII to recommend any updates, if appropriate, to the 3GPP SA3 (security working group) standards, including digital certificates and pre-provisioned Certificate Authorities, to mitigate these risks and then place the vulnerabilities on a scale that accounts for both risk level and remediation expense.
- Finally, the FCC directs CSRIC VII to identify optional features in 3GPP standards that can diminish the effectiveness of 5G security, and recommendations to address these gaps.

Building Upon Report 1

Report 1

Focus on 5G-NSA

Adding elements of the 5G RAN to the LTE network core



June 10, 2020

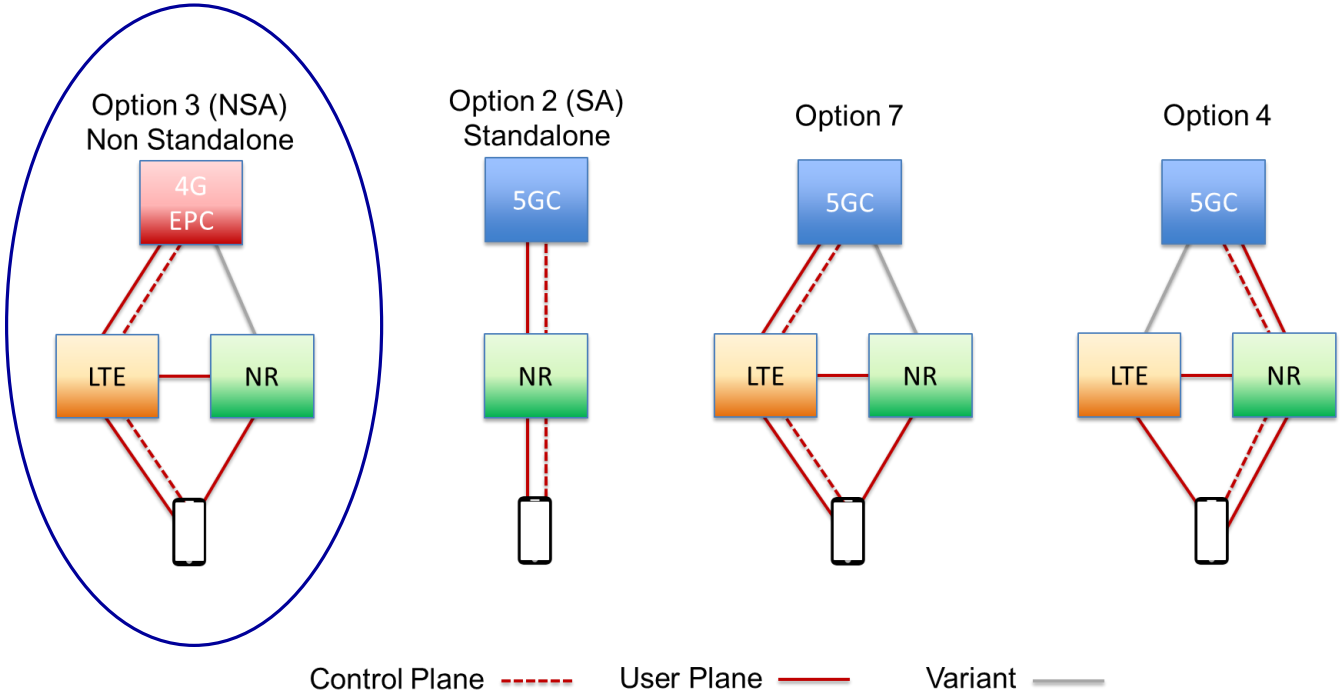
COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL VII

Final Report – Report 1: Risks to 5G from Legacy Vulnerabilities and Best Practices for Mitigation

Drafted by

Working Group 2: Managing Security Risk in the Transition to 5G

Working Group 2: Scope

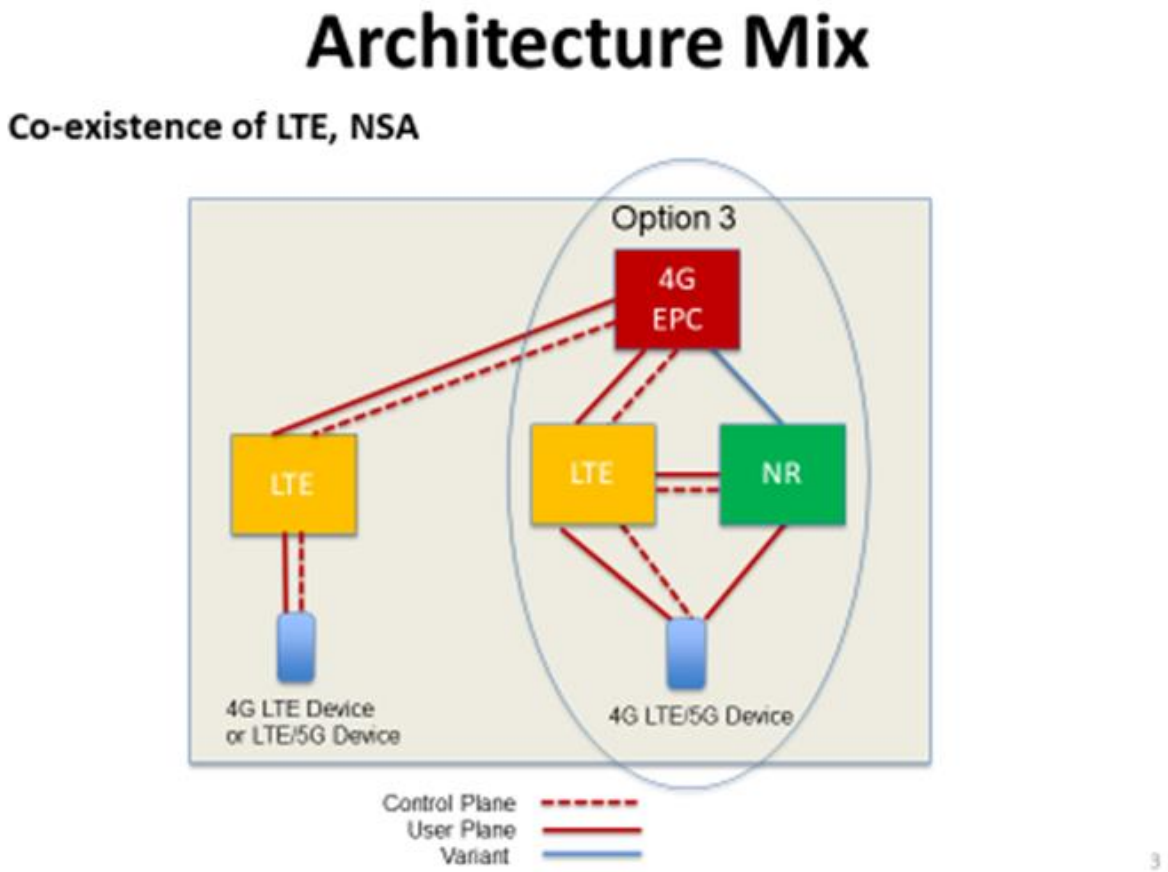


The primary focus of WG2 is on Option 3 (NSA)

5G NSA Architecture

- Utilizes 4G LTE Radio access network (RAN) for control plane traffic
- Retains use of 4G Evolved Packet Core (EPC) elements
- Enables introduction of 5G New Radio (NR) into 4G LTE infrastructure
- Offers a migration path to 5G SA while extending LTE useful life and investment

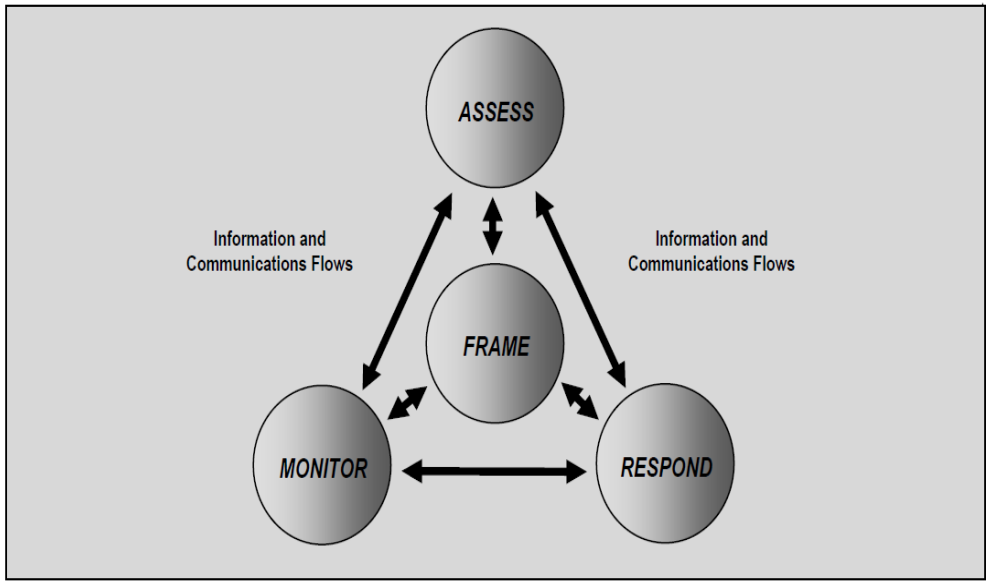
Co-Existence of LTE and 5G NSA



Co-Existence of LTE and 5G NSA (Option 3)

Working Group 2 Methodology

- Mapping to security categories
- Detailed look at individual requirements
- Risk-based *and* impact-based analysis
- Recommendations



NIST SP 800-39 Managing Information Security Risk

Optional Features

- **Network Relevance**
- **Equal but different paths**
- **Global needs**
- **Legal/export limitations**
- **Integration path/interdependencies**

Findings

Findings indicate potential risk is low and that the case-by-case nature of the decision to implement should be left to the operator.

6.1.1 Authentication

6.1.2 Control Plane RRC UE

6.1.3 NAS & AS Security Contexts Confidentiality and Integrity Algorithms Selection

6.1.4 Isolation Operations for Public Safety (IOPS)

6.1.5 Inter-PLMN Roaming Scenarios

6.1.6 RRC KeNB and Token Calculation

Recommendations for the FCC

7.1 Transition to 5G SA

7.1.1.1 5G RAN in NSA

As carriers connect 5G RAN to an existing LTE core and 3GPP continues to innovate on 5G SA-related standards, CSRIC VII recommends no new or additional regulations to address conformity to a particular core network design during this period of rapid development. The FCC should emphasize that carriers follow the guidance in CSRIC VII's previous report, CSRIC VII Report on "Risks to 5G from Legacy Vulnerabilities and Best Practices for Mitigation", as well as other previous CSRIC Reports.

Recommendations for the FCC

7.1 Transition to 5G SA

7.1.1.2 Timely Transition

CSRIC VII recommends that the FCC continue to support the industry's focus on the flexible and unimpeded deployment of secure next-generation networks. The FCC should leverage its unique role within government and continue to support the market-driven advances towards 5G, which will carry forward enhanced mitigations and address risks in an efficient manner.

Recommendations for the FCC

7.1.2 Future CSRIC Efforts

CSRIC VII recommends that future CSRIC efforts focus on the 5G SA architecture, as industry pushes ahead aggressively to innovate and deploy 5G in the US.

Recommendations for Industry

7.2.1 CSRIC Recommendations and Best Practices

Communications sector members should use CSRIC best practices 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, see CSRIC V Working Group 6 Report.

Recommendations for Industry

7.2.2 User Plane Confidentiality and Integrity

As per CSRIC VII Report titled" Risk to 5G from Legacy Vulnerabilities and Best Practices for Mitigation", CSRIC VII recommends higher layer security protections, such as TLS, to mitigate user plane threats. For NSA deployments, CSRIC VII recommends higher layer security protections to mitigate user plane threats.

Based on a risk analysis and use-case requirements, the operator should decide whether to use IPSec ESP, or an equivalent encryption technology such as MACSec, on untrusted links to provide confidentiality over the S1-U interface.

Recommendations for Industry

7.2.3 NAS Signaling Confidentiality and Integrity

It is recommended that the operator decide whether to add more security for signaling messages based on their specific customer requirements. Security can be enhanced by adding confidentially and/or integrity protection on unprotected signaling messages. Such changes would break many critical functions/features requiring resolution by adding significant complexity in mobile devices and network systems.

The operator should decide whether to use IPSec ESP, or an equivalent encryption technology such as MACSec, on untrusted links to provide confidentiality over the S1-MME, and management interfaces based upon risk analysis and the use case.

Recommendations for Industry

7.2.4 IPSEC

The following subsections provide recommendations for IPSec configuration options, when IPSec is used.

7.2.4.1 Tunnel Mode versus Transport Mode

Based on a risk analysis and use-case requirements, when using IPSec, the operator should decide whether to deploy IPSec Tunnel Mode or Transport Mode over the S1-MME, S1-U, and management interfaces.

7.2.4.2 SEG termination for IPSec

Based on a risk analysis and use-case requirements, when using IPSec, the operator should decide whether to deploy a SEG for IPSec termination on the core network side per their network design.

Questions?


CSRIC
Communications Security, Reliability and Interoperability Council

The members of Working Group 2 respectfully request that the CSRIC VII Council accept this CSRIC VII Report: *Review and Recommendations on optional security features in 3GPP standards impacting 5G Non-Standalone Architecture.*

Thank you.

Glossary of terms

- 3GPP 3rd Generation Partnership Project
- 5G Fifth Generation
- 5GC 5G core
- AS Access stratum
- eNB Evolved Node B
- EPC Evolved Packet Core
- FCC Federal Communications Commission
- IPSec Internet Protocol Security
- KeNB eNodeB Key
- LTE Long-term evolution

Glossary of terms

- MME Mobility management entity
- NB Node B
- NAS Non-Access Stratum
- NIST National Institute of Standards and Technology
- NR New radio
- NSA Non-standalone
- PLMN Public Land Mobile Network
- RAN Radio access network
- RRC Remote resource control
- SA Standalone
- UE User equipment

DISCUSSION

REPORT ON REVIEW AND RECOMMENDATIONS ON OPTIONAL SECURITY FEATURES IN 3GPP STANDARDS IMPACTING 5G NON-STANDALONE ARCHITECTURE

Kathy Whitbeck, Chair
Working Group 2

CALL FOR VOTE

REPORT ON REVIEW AND RECOMMENDATIONS ON OPTIONAL SECURITY FEATURES IN 3GPP STANDARDS IMPACTING 5G NON-STANDALONE ARCHITECTURE

Charlotte Field, Chair
CSRIC VII

Update on Progress

Working Group 1: Alert Originator Standard Operating Procedures

Craig Fugate, Chair
Working Group 1

Working Group 1:
Alert Originator Standard Operating Procedures
&
Recommendations to Resolve the Duplicate NWS Alert Issue

December 9, 2020

Craig Fugate, Chair WG1,
America's Public Television Stations (APTS)

Working Group 1: Background

- **Report #1 -** The FCC directs CSRIC VII to recommend model emergency alerting communications SOPs that emphasize engagement with all entities that contribute to the dissemination of fast and reliable emergency information to the public.
  - **Completed September 2020**
- **Report #2 -** The FCC tasks CSRIC VII to recommend the overall best solution(s) to resolve the duplicate NWS alert issue. CSRIC VII should comprehensively consider all aspects of the duplicate NWS alert issue, taking into consideration all relevant stakeholders' concerns (including alert originators, EAS participants, NWS, FEMA, as well as EAS equipment manufacturers and the public, the recipients of such alerts), and recommend the solution(s) that is the most effective, balancing the costs and benefits, for the majority of stakeholders. As part of this process, CSRIC VII should involve all stakeholders in the alert initiation and transmission process in order to research and assess possible solutions, including the method proposed by CSRIC III.
  - **Report expected completion March 2021**

Working Group 1: Report 2 Description

- Under certain conditions, the public receives duplicate National Weather Service (NWS) alerts issued over the Emergency Alert System (EAS).
  - Duplicate alerts occur due to technical differences in the processes for generating, distributing and broadcasting of alerts between the NWS systems and EAS.
  - EAS devices are required to reject “duplicate” alerts when operating in automated mode, which is the typical mode of operation.
  - Some NWS alerts generated for a single weather event, however, can be received by broadcast stations and other entities that transmit EAS alerts to the public from multiple sources with variations (primarily with respect to the geographic areas to which the alert applies) that appear to EAS devices as discrete alerts rather than duplicate alerts covering the same weather event.
  - EAS devices identify duplicate alerts by comparing the EAS header code information – which specifies the alert event type, alert originator, affected geographic areas and other information – against alerts previously received. If an alert contains identical EAS header code information when compared to a prior alert, the EAS device will reject that subsequent alert as a duplicate.
  - Any variation of the information in the product /alert when the comparison is made will result in the alert not being viewed as a duplicate.

Deliverables/Schedule

- The WG will evaluate the dissemination channels that contribute to EAS activation
- The WG will identify potential causes of duplicate NWS alerts
- The WG will provide recommended mitigation solutions for receiving duplicate alerts
- Final Report planned completion March 2021

Working Group 1 Members

Craig Fugate (Chair)*	APTS
Mark D. Annas*	City of Riverside Fire Department OEM
Terri Brooks	T-Mobile
Sulayman Brown	OEM, Fairfax County, VA
Wade Buckner*	International Association of Fire Chiefs
Dana M. Carey	Office of Emergency Services, County of Yolo, CA
Edward Czarnecki	Digital Alert Systems, Inc.
Brian K. Daly*	AT&T Services Inc.
Ashruf El-Dinary	Xperi Corporation
Matthew Gerst	CTIA
Robert Gessner*	ACA Connects
Dana Golub	PBS
Mark Hess*	Comcast
Antwane Johnson*	FEMA
Chandra Kotaru*	AWARN Alliance
Jordan Vilwock*	Laguna Beach Police Department
Jeff Littlejohn*	iHeartMedia Inc.
Michelle Mainelli-McInerney*	National Weather Service
Alex McHaddad	Blue Mountain Translator District (OR)
Michael Nix	Georgia Emergency Communications Authority
Donna Platt	North Carolina Department of Health and Human Services
Krisztina Pusok*	American Consumer Institute
Pat Roberts*	Florida Association of Broadcasters
Craig Saari	Charter
Francisco Sanchez Jr.*	OHSEM
Mark Schutte	Cox
Leslie Stitch	State of Minnesota
John Williamson*	Nez Perce Tribal Police Department
Jeff Wittek	Motorola Solutions, Inc
Clay Freinwald	Washington State SECC
Harold Price	Sage Alerting Systems Inc
Joe Berry	California Broadcasters Association
Tim Romero	Sonoma County, CA

FCC Liaisons: James Wiley (Task 1), **David Munson** (Task 2)

*Also CSRIC Member

Working Group 1 Alternates†

John Davis	T-Mobile
Charles P. (“Peter”) Musgrove	AT&T Services Inc.
Brian Hurley	ACA Connects
Jerry Parkins	Comcast
Michael Gerber	National Weather Service
Timothy Schott	National Weather Service
Mark Lucero	FEMA
John Dooley	State of Minnesota

† Alternates are not a member of the Working Group and may not vote.

Working Group 1 Conclusions

- The WG is currently on track to complete the report on time.

Discussion

Presentation of Working Group 1: Alert Originator Standard Operating Procedures

Craig Fugate, Chair
Working Group 1

UPDATE ON PROGRESS

WORKING GROUP 3: MANAGING SECURITY RISK IN EMERGING 5G IMPLEMENTATIONS

Farrokh Khatibi, Chair
Working Group 3

Working Group 3:
Managing Security Risk in Emerging 5G Implementations

December 9, 2020

Dr. Farrokh Khatibi, Chair WG3
Qualcomm Technologies, Inc.

Working Group 3: Background

Working Group Description:

3GPP Release 16, a set of standards which address core elements of the 5G architecture, was finalized in 2020. The potential risks introduced into core 5G network elements by weaknesses in the relevant 3GPP standards must be understood so that appropriate mitigation can be undertaken.

Working Group 3: Objectives

The FCC directs CSRIC VII to evaluate the 3GPP Releases 15 and 16 standards, identify areas of risk, and develop risk mitigation strategies to minimize risk in core 5G network elements and architectures.

In addition, the FCC directs CSRIC VII to identify optional features in proposed or work-in-progress 5G standards that can diminish their effectiveness.

Working Group 3: Report 1

Report on Risks Introduced by Releases 15 and 16 5G Standards

The Working Group will review Reports from CSRIC VI WG3 “Network Reliability and Security Risk Reduction” as well as the relevant 3GPP specifications to develop a new report on “Risks Introduced by Releases 15 and 16 5G Standards”.

Working Group 3: Report 2

Recommendations to Mitigate Risks Introduced by Releases 15 and 16 Standards

Furthermore, WG3 will make recommendations to mitigate risks introduced by Releases 15 and 16 Standards. This report will also include identifying optional features in proposed 3GPP standards that can diminish the effectiveness of 5G security, and recommendations to address these gaps.

Deliverables/Schedule

Report 1 - September 2020 Completed

CSRIC VII Report on Risks Introduced by 3GPP Releases 15 and 16 5G Standards. (September 16, 2020)

Report 2 - March 2021 progressing

Recommendations to Mitigate Risks Introduced by Releases 15 and 16 Standards. This report will also include identifying optional features in proposed 3GPP standards that can diminish the effectiveness of 5G security, and recommendations to address these gaps

Working Group 3 Members

Farrokh Khatibi (Chair)*	Qualcomm
Billy Bob Brown, Jr	CISA DHS
Brian K. Daly*	AT&T Services Inc.
Christopher(Chris) Joul	T-Mobile
Mohammad Khaled	Nokia Bell Labs
Michael Liljenstam	Ericsson
John Marinho	CTIA
Danny McPherson*	Verisign
Susan M. Miller*	ATIS
Krisztina Pusok*	American Consumer Institute
Travis Russell*	Oracle Communications
D.J. Shyy	MITRE
Kathy Whitbeck*	Nsight
Brian Trosper*	Verizon
Steve Watkins*	Cox Communications
Jeffrey Wirtzfeld	CenturyLink
Fei Yang	Comtech

FCC Liaison: Steven Carpenter

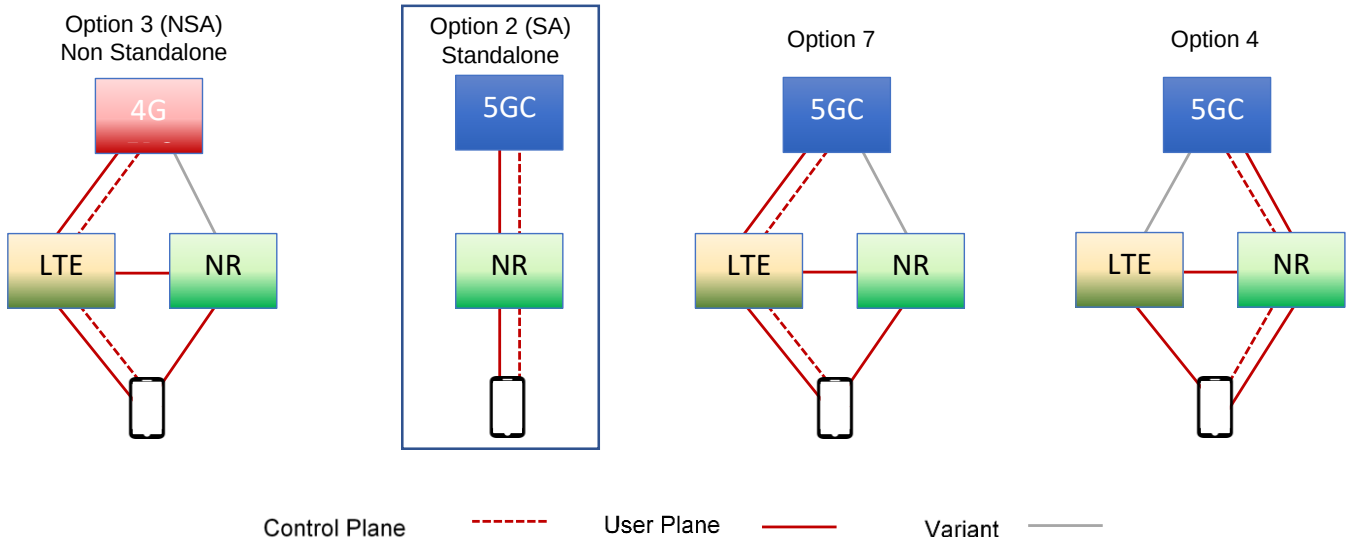
*Also CSRIC Member

Working Group 3 Alternates†

Steve Barclay	ATIS
Vinod Choyi	Verizon
Martin C. Dolly	AT&T Services Inc.
Yong Kim	Verisign
Andrew Schnese	Nsight
Greg Schumacher	T-Mobile

† Alternates are not a member of the Working Group and may not vote.

Working Group 3 Scope



The primary focus of WG3 is Option 2 Standalone (SA)

Working Group 3 Status and Next Steps

- Analyzing optional security features that can diminish the effectiveness of 5G security
- Continue our baseline report development
- Conduct regular conference calls
  - Review existing work in the area
  - Develop new Recommendations
- Provide periodic status updates to the CSRIC Council

Discussion

Presentation of Working Group 3: Managing Security Risk in Emerging 5G Implementations

Farrokh Khatibi, Chair
Working Group 3

Update on Progress

Working Group 4: 911 Security Vulnerabilities During the IP Transition

Mary Boyd, Chair
Working Group 4

Working Group 4:
911 Security Vulnerabilities During the IP Transition

December 9, 2020

Mary A. Boyd, Chair WG4
Intrado Life & Safety

Working Group 4: Background

Working Group Description:

The transition from legacy to IP-based networks, may result in hybrid system settings that commingle legacy and IP network elements. While in this hybrid state, the 911 systems operate at higher risk. For example, security functions (like data encryption) to protect data traversing through the IP-based networks do not function or are unavailable as the data travels through legacy network elements.

Working Group 4: Objective

The FCC directs CSRIC VII to survey the current state of interoperability for the nation's 9-1-1 system, including for legacy 911 networks, transitional 911 networks, and Next Generation 911 (NG911).

The FCC further directs CSRIC VII to identify security risks in legacy 911 networks, transitional 911 networks, and NG911 networks and recommend best practices to mitigate risks in these three areas.

In addition, CSRIC VII will place the vulnerabilities on a scale that accounts for both risk level and remediation expense. (Report 3)

Working Group 4: Report 1

The Working Group will survey the current state of interoperability for the nation's 911 systems, including for legacy 911 networks, transitional 911 networks, and Next Generation 911 (NG911); and,

- ❑Remain mindful and compliant of federal rules governing "surveying of information";
- ❑Identify and review existing 911 reports on the current states of interoperability as data sources; and,
- ❑Identify public safety associations and local 911 Program Offices as additional data sources for completion of the deliverables for the report.

COMPLETED

Working Group 4: Report 2

The Working Group will review hybrid 911 system architectures that commingle legacy and IP network elements and:

- ❑Will identify and study historical 911 outages caused by security risks to a 911 network;
- ❑Study networks security risks during the transition of 911 networks for hybrid vulnerabilities;
- ❑Identify security functions to protect data traversing through the IP based networks and impacts through legacy network elements;
- ❑Evaluate existing best practices and develop recommendations to minimize security risks to the legacy 911 networks, transitional 911 networks, and NG911 networks; and
- ❑Evaluate barriers to implementation of security recommendations.

COMPLETED

Working Group 4: Report 3
Measuring Risk Magnitude and Remediation Costs in 911 and NG911 Networks – Finalize By: February 17, 2021

In addition to the review of hybrid 911 system architectures that commingle legacy and IP network elements, the Working Group will:

- ❑ Identify and place vulnerabilities on a scale that accounts for risk level;
- ❑ Study risk levels and develop remediation expense;
  - ❑ Identify any economic disadvantages or risks;
  - ❑ Identify any barriers to implementing mitigation measures;
- ❑ Review Best Practices and make recommendations to reduce vulnerabilities; and
- ❑ Publish a report measuring risk Magnitude and Remediation costs in 911 and NG911 Network.

Working Group 4: Members

Mary A. Boyd (Chair)*	West Safety Services
Brandon Abley*	NENA
Daryl Branson	Colorado State 911 Program
Roger Marshall	Comtech
Gerald "Jay" English*	APCO
Laurie Flaherty*	US DOT, NHTSA
Jay Gerstner	Charter
James D. Goerke*	Texas 9-1-1 Alliance
Stacy Hartman	CenturyLink
Michael (Mike) Hooker	T-Mobile
Gerald Jaskulski	CISA DHS
William Leneweaver	Washington State 9-1-1 Coordination Office
Tim Lorello*	SecuLore
Krisztina Pusok*	American Consumer Institute
Theresa Reese	Ericsson
Charlie Sasser	NASTD
Andre Savage	Cox
Dorothy Spears-Dean*	NASNA
Leslie Stitch	State of Minnesota
Mark A. Titus	AT&T
Brian Trosper*	Verizon
Jeff Wittek	Motorola Solutions, Inc
Jackie Wohlgemuth	ATIS

FCC Liaison: Rasoul Safavian

*Also CSRIC Member

Working Group 4 Alternates†

Jeanna Green	T-Mobile
Tom Breen[ϕ]	SecuLore
Bill Mertka	Verizon
Steve Barclay	ATIS
Richard Muscat	Texas 9-1-1 Alliance

† Alternates are not a member of the Working Group and may not vote.
ϕ Tom Breen represented Comtech from 07/2019 to 07/2020

WORKING GROUP 4
REPORT 3 UPDATE:

CSRIC Report Measuring Risk Magnitude and Remediation Costs in 9-1-1 and NG9-1-1 Networks

Report 3 Structure

- Executive Summary
- Includes Normal Introductory Sections
- Analysis Includes:
  - General Impacts of Cyber Attacks
  - Impact On Public Safety Entities
  - Best Practices
- Findings Will Include
  - What Can Be Done To Mitigate Impacts
  - Estimated Costs to Mitigate
  - Basic Cybersecurity Controls At Lower Cost
  - Need For New Best Practices
- Recommendations
- Conclusions

Working Group 4 Status

- Established Two Sub-teams Focused on :
  - Technical Review and Recommendations
  - Best Practices Review and Recommendations
- Conduct weekly conference calls to:
  - Review and Edit Contributions
- Draft Report Is In Development
- On Schedule to Meet February 17th Schedule


CSRIC
Communications Security, Reliability and Interoperability Council

Questions?

DISCUSSION

PRESENTATION OF WORKING GROUP 4: 911 SECURITY VULNERABILITIES DURING THE IP TRANSITION

Mary Boyd, Chair
Working Group 4

UPDATE ON PROGRESS

WORKING GROUP 6: SIP SECURITY VULNERABILITIES

Danny McPherson, Chair
Working Group 4

Working Group 6: SIP Security Vulnerabilities Update

December 09, 2020

Danny McPherson, Chair WG6
Verisign

Working Group 6: Background

- Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences. Because SIP is used to initiate voice sessions, it is also important for 911 service. The FCC directs CSRIC VII to review the security vulnerabilities affecting SIP that affect the provision of communications service. CSRIC VII should outline how industry is addressing these vulnerabilities, identify any gaps in industry action, update any existing best practices relevant to SIP, and develop additional ones that, if implemented, would address such vulnerabilities and mitigate their associated risks, including the promotion of end-to-end-security

Working Group 6: Objectives

The SIP security vulnerabilities working group will:

- review the security vulnerabilities affecting SIP that affect the provision of communications service
- examine how industry is addressing these vulnerabilities
- identify any gaps in industry action
- update any existing best practices relevant to SIP
- develop additional best practices that, if implemented, would address such vulnerabilities and mitigate their associated risks, including the promotion of end-to-end-security

Working Group 6 Update

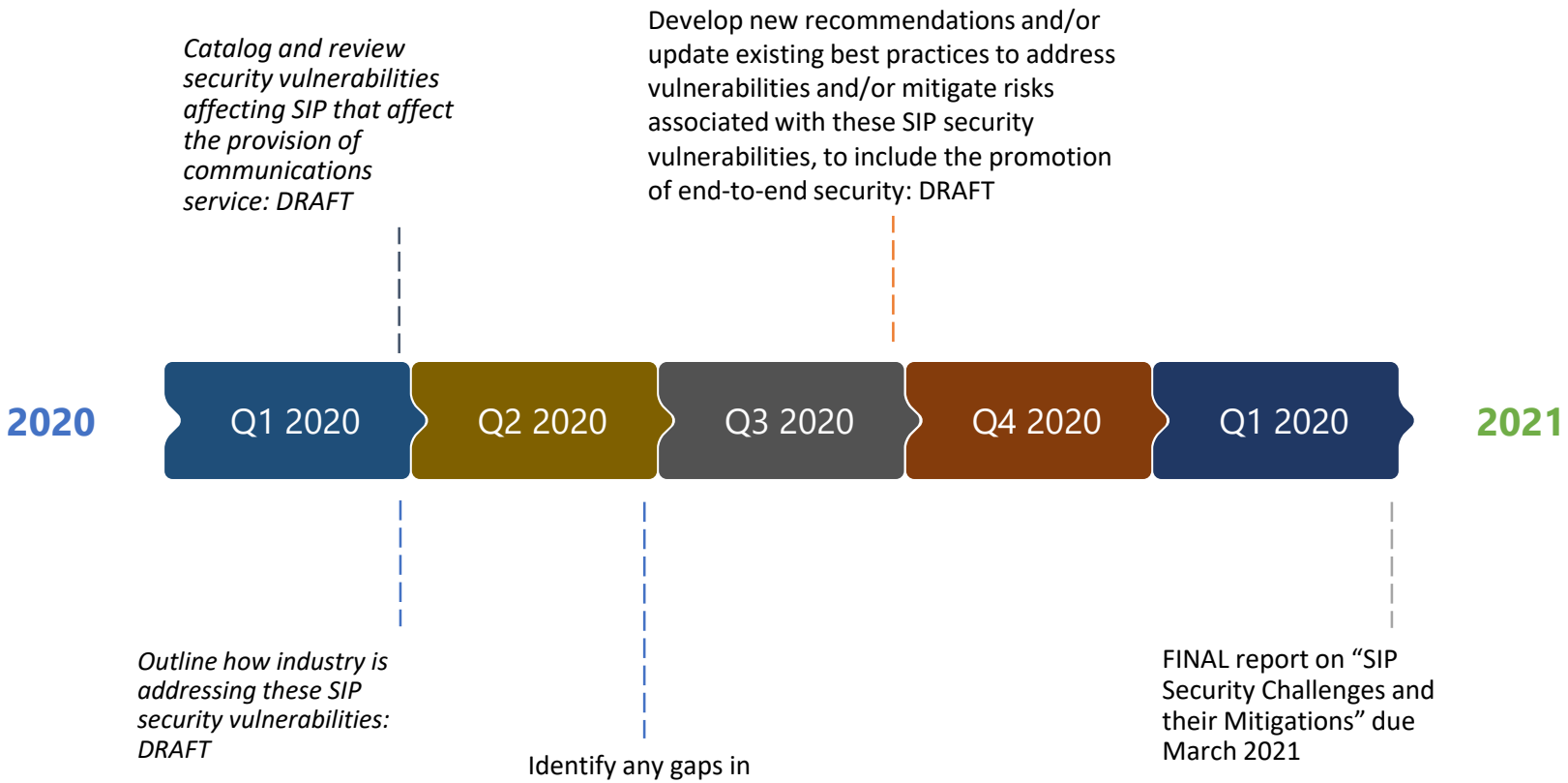
Complete

- Working Group Membership: Finalized
- Working Group Meeting Kickoff: November 13, 2019
- Convey Working Group ground rules
- Identify task teams and leaders
- Establish communications lists and repositories
- All SME briefings
- Catalog and review security vulnerabilities affecting SIP that affect the provision of communications service: DRAFT by end of Q1 (Vladimir Wolstencroft and Jon Peterson to lead effort)
- Outline how industry is addressing these SIP security vulnerabilities: DRAFT by end of 1Q2020
- Identify any gaps in industry action related to SIP security vulnerabilities: DRAFT by end of 2Q2020
- Develop new recommendations and/or update existing best practices to address vulnerabilities and/or mitigate risks associated with these SIP security vulnerabilities, to include the promotion of end-to-end security: DRAFT by end of 3Q2020

In Progress

- GMSA briefing
- Section leads to drive content development and review materials with the larger workgroup during the bi-weekly conference calls
- Deliver final report & recommendations by March 2021

Deliverables/Schedule



Working Group 6 Members

Danny McPherson (Chair)	Verisign
Jamal Boudhaouia	CenturyLink
Pierce Gorman	T-Mobile
Mark Hess	Comcast
Zeeshan Jahangir	T-Mobile
Susan M. Miller	ATIS
Thomas B. Nachbar	SGE
Richard E. Perlotto II	The Shadowserver Foundation

FCC Liaison: Ahmed Lahjouji

Jon Peterson	Neustar
Krisztina Pusok	American Consumer Institute
Evans Roberts Jr.	AT&T
Brian Rosen	NENA
Dorothy Spears-Dean	NASNA
John Totura	Comtech
Brian Trosper	Verizon
Steve Watkins	Cox Communications
Vladimir Wolstencroft	Twilio

*Also CSRIC Member

Working Group 6 Alternates†

Steve Barclay	ATIS
Ramone Torres	ATIS
Chris Wendt	Comcast
Damien Whaley	Cox
Shaun Slatton	Cox
Yong Kim	Verisign
Eric W. Kroymann	Verizon
Matt Thomas	Verisign

† Alternates are not a member of the Working Group and may not vote.

Next Steps

- Continue to review research documents/presentations from standard organizations, government agency and academia
- Section leads to drive content development and review materials with the larger workgroup during the bi-weekly conference calls
- Continue updates to Steering Committee and Council
- Deliver final report & recommendations by March 2021

Working Group 6:
SIP Security Vulnerabilities

Questions?

Discussion

Presentation of Working Group 6: SIP Security Vulnerabilities

Danny McPherson, Chair

FINAL CSRIC VII MEETING

MARCH 10, 2021

CLOSING REMARKS

CHARLOTTE FIELD, CHAIR

ADJOURN MEETING

Suzon Cameron, DFO