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

MARCH 10, 2021

COMMENCE MEETING

Suzon Cameron, DFO

WELCOME

Lisa Fowlkes, Chief,
PSHSB, FCC

Opening Remarks

Charlotte Field, Chair

PRESENTATION

REPORT ON RECOMMENDATIONS TO RESOLVE DUPLICATE NWS ALERTS

Michelle M. Mainelli
Terri Brooks
Co-Chairs
Working Group 1

Working Group 1:
Alert Originator Standard Operating Procedures
&
Duplicate National Weather Service Alerts

March 10, 2021

Terri L. Brooks (Co-Chair)
T-Mobile USA

Michelle M. Mainelli (Co-Chair)
National Weather Service

Working Group 1: Description

- **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.
  - **Approved and Released 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 and recommend the solution(s) that is the most effective, balancing the costs and benefits, for the majority of stakeholders.
  - **Submitting today for full council consideration**

Agenda

- WG1 Background
- Approach, Analysis and Conclusions
- Recommendations
- Expectations for Next Steps

Working Group 1 Members

Michelle Mainelli-McInerney* (Co-Chair)	National Weather Service
Terri L. Brooks (Co-Chair)	T-Mobile USA
Mark D. Annas*	City of Riverside Fire Department OEM
Joe Berry	California Broadcasters Association
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
Clay Freinwald	Washington State SECC
Craig Fugate	APTS
Matthew Gerst	CTIA
Robert Gessner*	ACA Connects
Dana Golub	PBS
Mark Hess*	Comcast
Antwane Johnson*	FEMA
Chandru Kotaru*	AWARN Alliance
Jeff Littlejohn*	iHeartMedia, Inc.
Alex McHaddad	Blue Mountain Translator District (OR)
Michael Nix	Georgia Emergency Communications Authority
Donna Platt	North Carolina Department of Health and Human Services
Harold Price	Sage Alerting System, Inc.
Krisztina Pusok*	American Consumer Institute
Pat Roberts*	Florida Association of Broadcasters
Tim Romero	Sonoma County, CA
Craig Saari	Charter
Francisco Sanchez Jr.*	OHSEM
Mark Schutte	Cox
Leslie Stitch	State of Minnesota
Jordan Villwock*	Laguna Beach Police Department
John Williamson*	Nez Perce Tribal Police Department
Jeff Wittek	Motorola Solutions, Inc

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

*Also CSRIC Member

Working Group 1 Alternates**

John Davis	T-Mobile USA
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: Report 2 Background

Under certain conditions, the public receives duplicate National Weather Service (NWS) alerts.

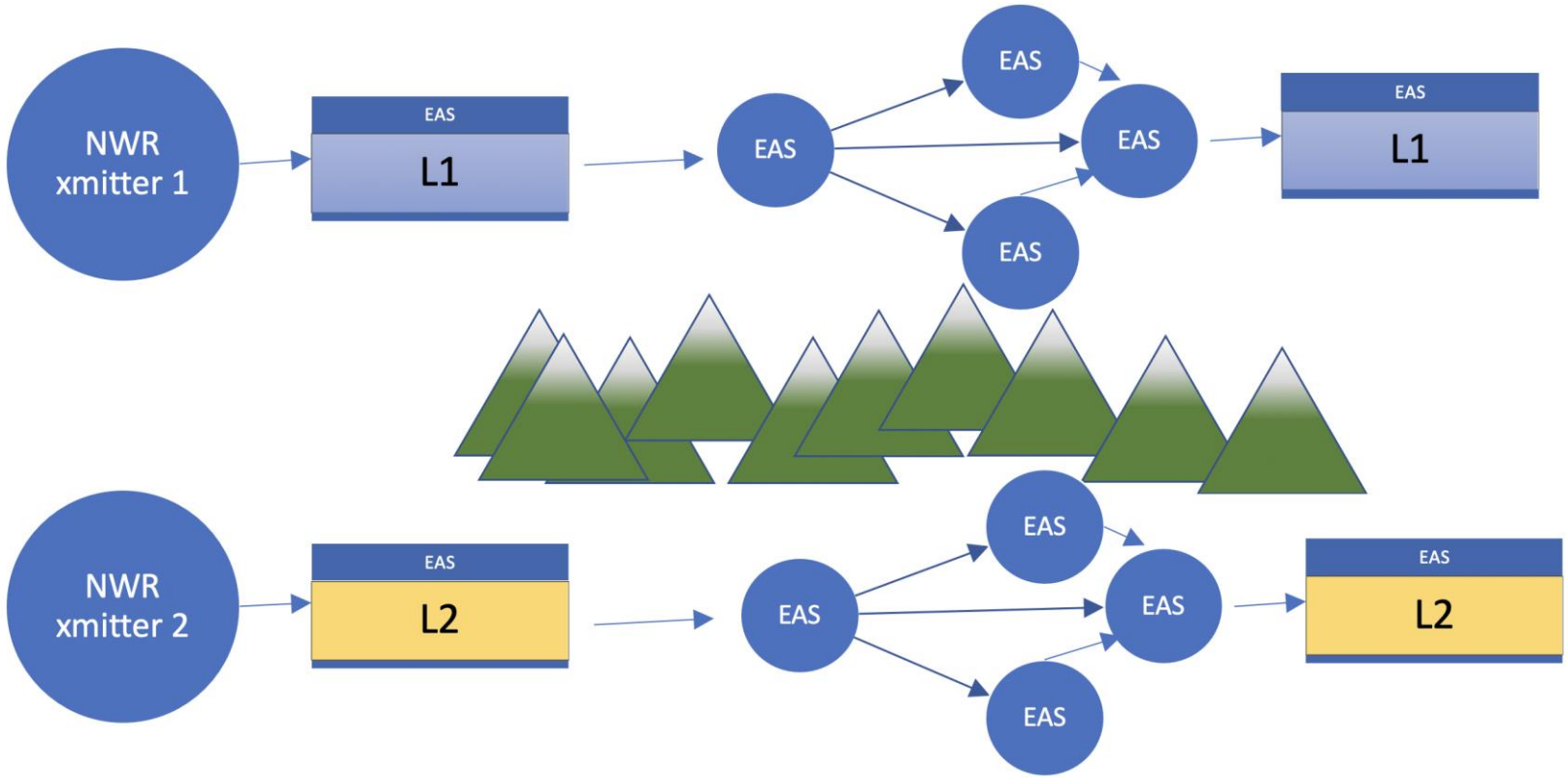
Variations may occur as the alert traverses the NOAA Weather Radio All Hazards (NWR) system using Specific Area Message Encoding (SAME) and is modified, creating two or more EAS versions of the original alert. Any change detected by a byte-by-byte comparison in any of the five EAS header fields will cause the EAS equipment to view the variations as distinct alerts.

The most common variation occurs when localized encoding changes the length or order of the Location Codes list.

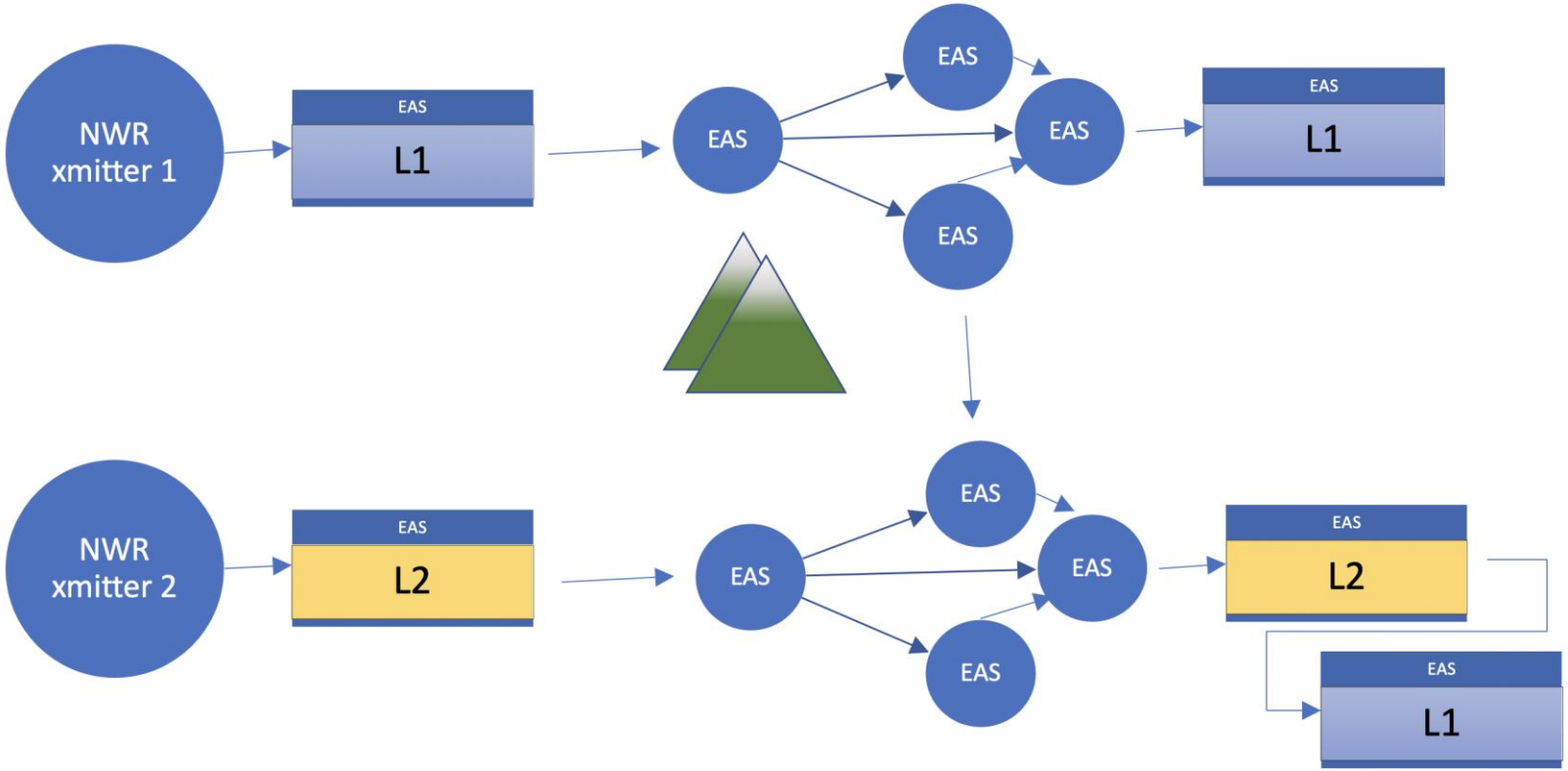
Definition of “Duplicate Alert”

For the purposes of this report, a “duplicate alert” is defined as the inability of EAS encoder/decoder equipment to disambiguate between two (or more) received variations of the same alert.

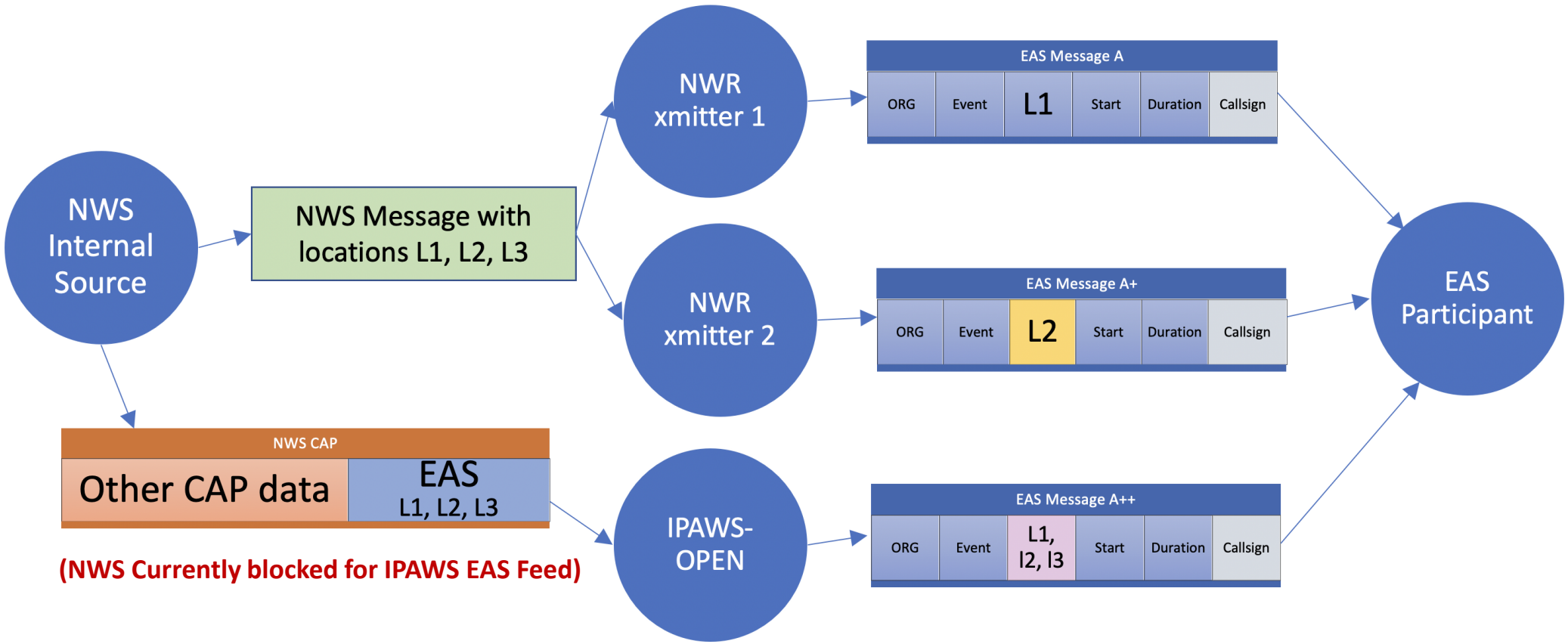
SAME Message Flow via NWR: Natural Barriers



SAME Message Flow via NWR: Break in Natural Barriers



NWS Alerts via IPAWS and NWR



Working Group 1: Approach

- WG1 Activities for Report 2:
  - Evaluated dissemination channels that contribute to EAS activation
  - Identified potential causes of duplicate NWS alerts
  - Identified potential improvements and solutions
  - Quantified* extent of improvements and solutions
  - Identified and quantified* potential impacts

- Key goals during these activities included both mitigation of the identified duplication problem and increasing access to NWS Alerts via IPAWS CAP EAS Feed.

*Quantified to the extent possible with available data

Working Group 1: Analysis

Six proposals were identified and analyzed. These lend themselves to two categories:

1. Improvements to CAP EAS Access 2-3 years
2. Full, or near full, solutions 5+ years

For each proposal, the report includes a description, identified impacts/tasks per stakeholder, and Pros/Cons. Where applicable, quantifying field numbers and other criteria for next steps (e.g., testing and verification) have been included.

Working Group 1: Proposals Analyzed

Potential Improvements in a 2 - 3 year timeframe:

- Unblock NWS Alerts for distribution on the CAP EAS Channel for only the Limited Set of Geographic Areas where NWR is not available
- Unblock NWS Alerts for distribution on the CAP EAS Channel for Single Geocode Alerts (CAP EAS Alerts with only one FIPS Code)
- Unblock NWS Alerts for distribution on the CAP EAS Channel and Remove/Eliminate NWR as a source for EAS
- Unblock NWS Alerts for distribution on the CAP EAS Channel: Establish CAP as the Primary NWS EAS Source with NWR Backup

Potential Solutions in a 5+ year timeframe:

- Additional Data Tag
- NWS NOAA Weather Radio Sites Provide Complete and Consistent Ordering of SAME Location (Local Area Codes) in all Alert Broadcast Messages

Working Group 1: Conclusions

Following review and analysis of the findings of the prior CSRIC WGs, new proposals, and current field knowledge, CSRIC VII WG1 concludes that the best approach is to **follow two parallel paths**, including a near-term improvement to CAP EAS Access and a longer-term solution that directly supports the ability to accurately identify variations of the same alert.

Working Group 1 Recommendations: Long-Term Solution

Section 6.1 Additional Data Tag is the preferred long-term solution. This solution adds a data tag to uniquely identify each alert, directly supporting the ability to detect separate instances of the same alert, both the NWR-sourced and CAP-sourced, removing the need to block NWS weather alerts from proceeding through the CAP EAS Channel. This solution is considered to be the *most complete solution* if all EAS stakeholders comply.

Section 6.6 Complete and Consistent Ordering of SAME Location Codes should also be considered due to the limited impact to most stakeholders, though it does not address the possibility of CAP-sourced EAS duplicates for alerts that must be broken down due to limits defined by the protocols (e.g., greater than 31 FIPS codes or WEA 10/100 limits).

Working Group 1 Recommendations: Near-Term Improvement

In parallel with the work on a long-term solution, the FCC should consider interim guidelines that will facilitate the passage of some NWS CAP messages via IPAWS:

Section 6.3 Unblock the EAS Channel for Single Geocode Alerts is the preferred near-term improvement with minimal impacts to EAS stakeholders.

Section 6.5 Establish CAP as the Primary NWS EAS source with NWR backup may be considered as an interim approach; however, more significant EAS stakeholder impacts exist, and this solution has a chance of generating CAP-sourced EAS duplicates for alerts that must be broken down due to limits defined by the protocols (e.g., greater than 31 FIPS codes or WEA 10/100 limits).

Next Steps

- Final decisions need to be made as to the exact improvement and/or solution to fully pursue, and the implementation details. These decisions require further analysis by the affected stakeholders.

- Where applicable and known, the need for additional quantifying information, testing, and specific criteria (e.g., testing and verification) for making subsequent decisions are included in each section describing an improvement or solution.

- All recommendations for improvements and solutions will require close coordination (testing, hardware/software changes) throughout the entire dissemination value chain and any implementation of these recommendations will follow appropriate notification timelines.

Working Group 1

Questions?

Discussion

Report on Recommendations to Resolve Duplicate NWS Alerts

Michelle M. Mainelli
Terri Brooks
Co-Chairs
Working Group 1

CALL FOR VOTE

REPORT ON RECOMMENDATIONS TO RESOLVE DUPLICATE NWS ALERTS

Charlotte Field, Chair
CSRIC VII

PRESENTATION

REPORT ON RECOMMENDATIONS FOR IDENTIFYING OPTIONAL SECURITY FEATURES THAT CAN DIMINISH THE EFFECTIVENESS OF 5G SECURITY

Farrokh Khatibi, Chair
Working Group 3

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

March 10, 2021

Dr. Farrokh Khatibi, Chair
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

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

Report 2 - March 2021

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	Lumen
Fei Yang	Comtech

FCC Liaison: Steven Carpenter

*Also CSRIC Member

Working Group 3 Alternates*

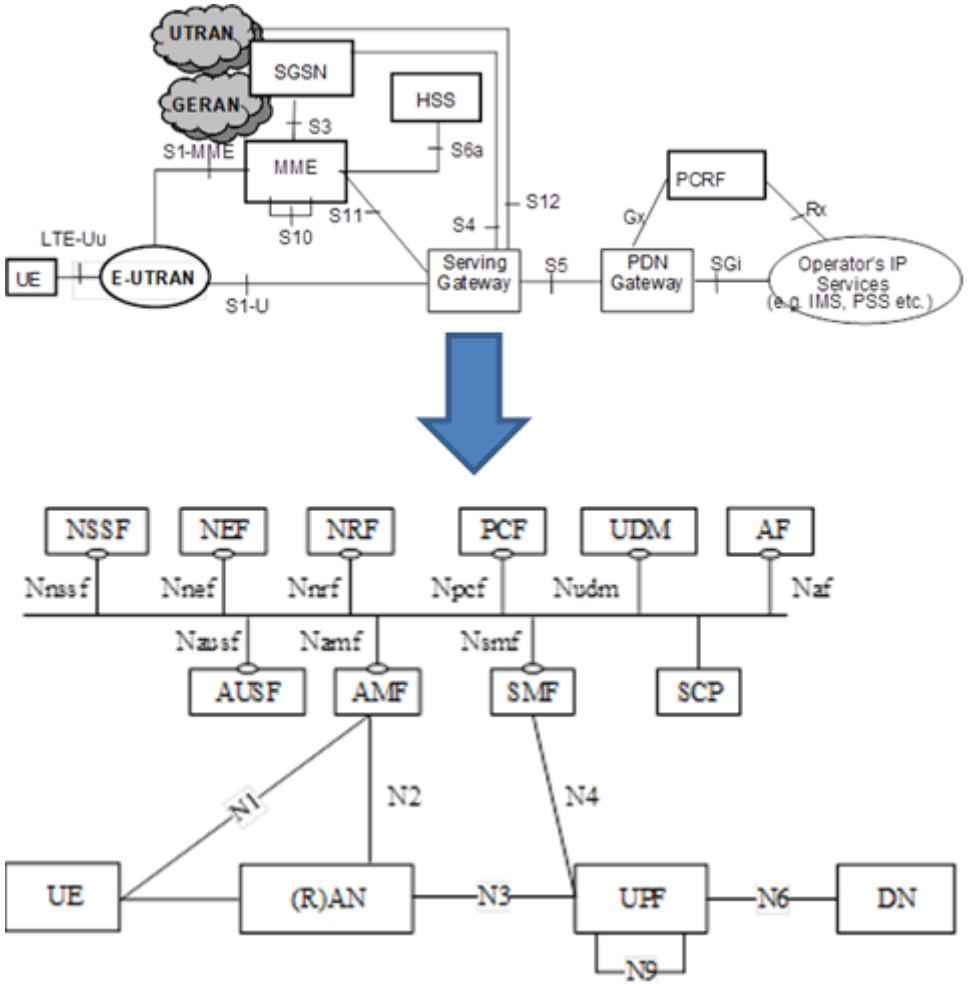
Steve Barclay	ATIS
Vinod Choyi	Verizon
Martin C. Dolly	AT&T Services Inc.
Yong Kim	Verisign
Andrew Schnese	Nsight
Greg Schumacher	T-Mobile

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

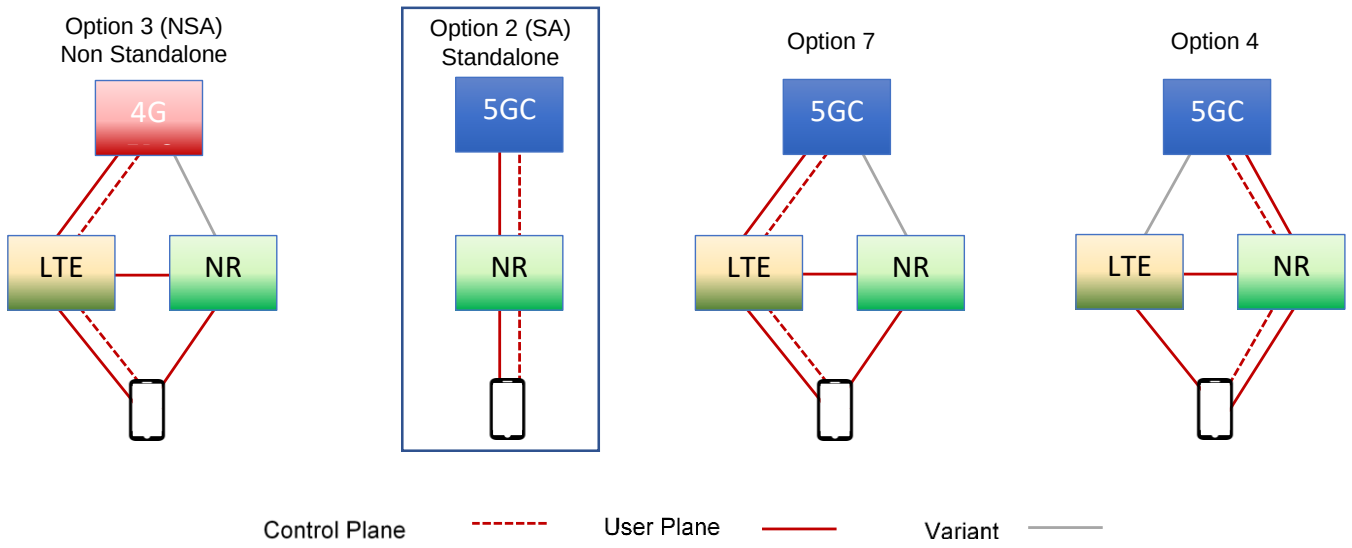
5G Background

- 5G wireless and network technology is enabling a new wave of innovation that will impact many aspects of people's lives from connected vehicles to healthcare and internet of things.
- 5G New Radio (NR) is the global standard for a unified, more capable 5G wireless air interface. It will deliver significantly faster and more responsive mobile broadband experiences and extend mobile technology to connect and redefine a multitude of new industries.
- 5G Core network (5GC) has been defined that allows many different functions to be built, configured, connected, and deployed at the required scale in a programable and flexible manner, to meet the need at any given time.
    - "Service-Based Architecture" (SBA) is centered around services that can register themselves and subscribe to other services. This enables a more flexible development of new services, as it becomes possible to connect to other components without introducing specific new interfaces.

5G Core Network Evolution



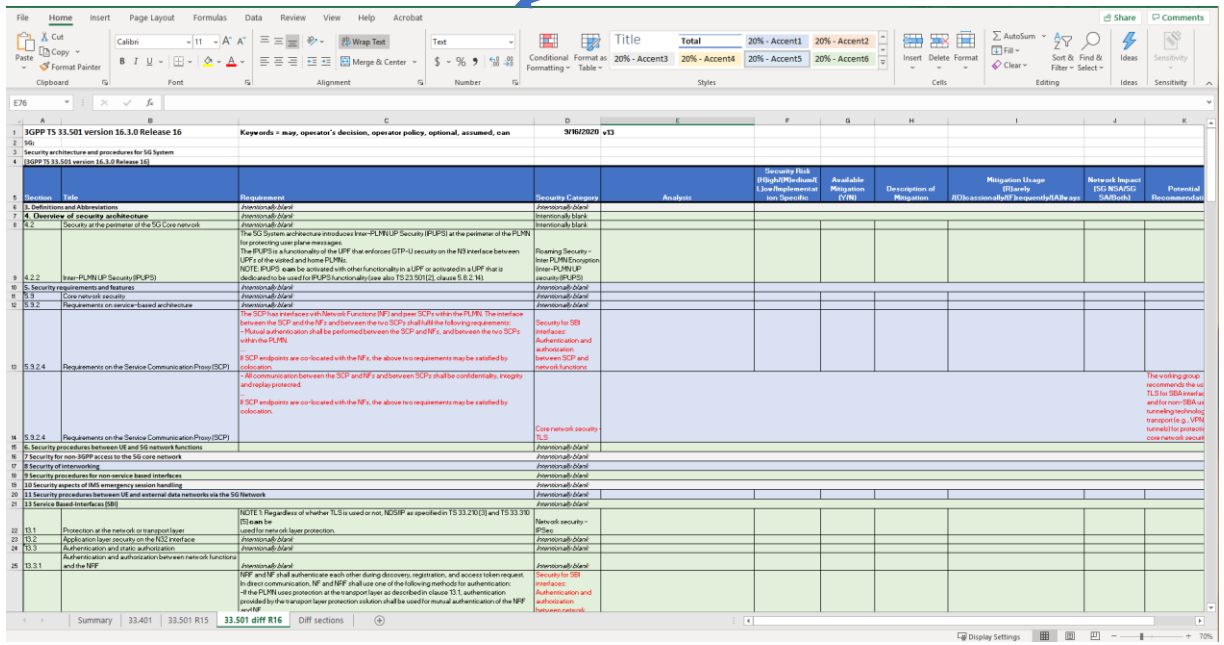
Working Group 3 Scope



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

Working Group 3 Methodology

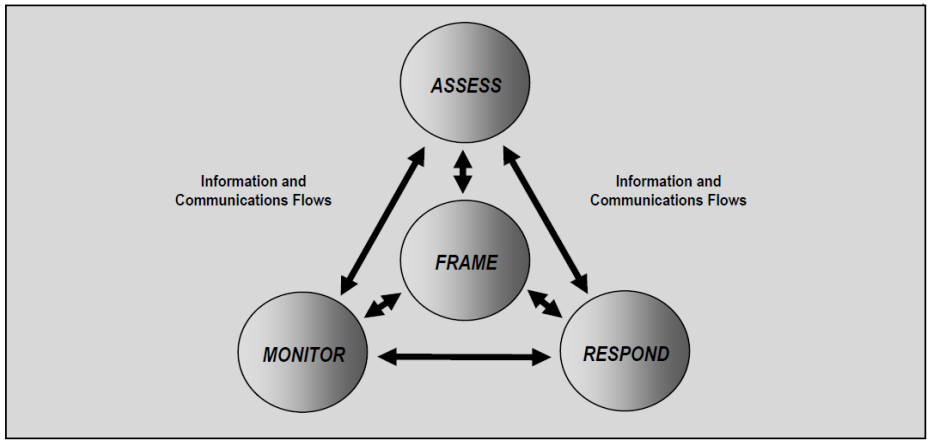
The WG performed both bottoms-up and top-down analysis of 5G security



Security Category	5G in R-15 (3GPP TS 33.501)	5G in R-16 (3GPP TS 33.501)
NAS[i] signaling confidentiality	Optional	Same
NAS signaling integrity	Mandatory	Same
User plane confidentiality	Optional	Same
User plane integrity	Optional	Same [9]
RRC[ii] signaling confidentiality	Optional	Same
RRC signaling integrity	Mandatory	Same
SUPI/IMSI privacy	SUPI[iii] encryption is optional (has exceptions)	Same
Primary Subscriber Authentication (5G AKA / EAP-AKA')	Has optional features	Same
Network slice specific authentication and authorization function (NSSAAF)[10 11 12]	Does not exist	Optional [13]
Certificates – gNB enrollment[14]	Optional [iv]	Same
Certificates – IPSec [10]	Mandatory (with some optional implementation mechanisms [v])	Same
Certificates – TLS [10]	Mandatory (with some optional implementation mechanisms [vi])	Same
Network security – IPSec	Optional	Same
Core network security – TLS	Optional	Same
Security for SBI interfaces[15]: TLS protection for direct connection between NF and SEPP	Mandatory	Mandatory [16 17]
Security for SBI interfaces [11]: Protection between SEPPs	Mandatory	Mandatory [12]
Security for SBI interfaces [11]: Authentication and authorization between network functions and the NRF	Mandatory	Mandatory [12]
Security for SBI interfaces [11]: Authentication and authorization between network functions	Does not exist	Mandatory [12 18]
Security for SBI interfaces [19]:	Does not exist	Mandatory [12]

Working Group 3 Methodology

The WG also considered NIST SP 800-39 methodology as shown below:



Recommendations to the FCC

Previous CSRIC Recommendations

CSRIC VII commends the FCC's efforts to support CSRIC recommendations as shown by previous Public Notices (PNs). CSRIC VII recommends that the FCC encourage industry for continued implementation of CSRIC's prior recommendations and continue to promote awareness.

Recommendations to the FCC

As described in Section 4.2 (Scope) of the report, the work of this CSRIC was not exhaustive. CSRIC VII therefore recommends that the FCC consider further CSRIC work to expand the security analysis coverage of 5G SA.

CSRIC VII recommends future CSRICs consider:

- Security of capabilities still being developed in 3GPP future Releases 17 and 18, such as interworking between 5G SA and 4G networks.
- Existing optional security capabilities which were brought forward to 5G from 4G which have not been addressed in previous CSRICs or warrant revisiting for 5G SA. Examples include Network Domain Security and IMS Security
- Mandatory security features to deploy with a choice between several defined approaches can be analyzed for which choice may be recommended. Some examples are in the following areas: optional co-location of functions, where Subscription Concealed Identifier (SUCI) is calculated in UE, storage and handling of keys, priority of crypto algorithms, conditions for primary reauthentication and frequency of key setting, UICC properties, logging of certain events. More specific examples of these are given in Annex A.
- Network Slice-Specific Authentication and Authorization (NSSAA): Additional authentication and authorization that is performed beyond primary authentication is based on an operator or enterprise's risk associated with access to a dedicated slice. Different slices may have different associated risks and therefore while access to a dedicated slice may require the services of NSSAA Function (NSSAAF), while access to a different dedicated slice with a different risk profile may not need the additional authentication services provided by the NSSAA. Evaluate risks associated with specific dedicated slices and provide guidance accordingly on the use of NSSAA by operators and enterprises.

Recommendations to Industry

Previous CSRIC Recommendations

CSRIC VII recommends that industry rely upon CSRIC recommendations to mitigate threats to the 5G SA system, specifically CSRIC VI, V, and IV Reports.

Recommendations to Industry

NAS Signaling Confidentiality

3GPP TS 33.501 specifies mandatory (e.g., requires vendor implementation) support for protection of the NAS signaling confidentiality, but optional for service providers to use.

Given this standards requirement, CSRIC VII recommends only non-user identity related information shall be conveyed prior to security context is established.

Note, after security context is established all NAS messages are encrypted according to 3GPP TS 33.501.

Non-access stratum

Recommendations to Industry

User Plane Confidentiality

3GPP TS 33.501 specifies mandatory (e.g., requires vendor implementation) support for protection of the User plane confidentiality, but optional for service providers to use.

Given this standards requirement, CSRIC VII recommends User plane confidentiality protection over the access stratum be done at PDCP layer.

Confidentiality protection for UP is applied at the PDCP layer, and no layers below PDCP are confidentiality protected. User data sent via UPF may be confidentiality protected.

PDCP: Packet Data Convergence Protocol
UPF: User Plane Function

Recommendations to Industry

User Plane Integrity

3GPP TS 33.501 specifies mandatory UE support of integrity protection and replay protection of user data between the UE and the gNB, but the data rates at which it is supported is different between Release 15 and 16, and it is optional for service providers to use.

CSRIC VII recommends that device OEM and network infrastructure vendors support the Release 16 full rate capability, along with 128-NIA3 as defined in Annex D of 3GPP TS 33.501, and for operators to implement according to the service requirement.

CSRIC VII recommends that user data integrity is mandatory for Release 16 U.S. deployments.

While the goal is for mandatory user data integrity in Release 16 U.S. deployment, CSRIC VII recognizes that during operator network transitions to consistent and ubiquitous 5G SA availability and coverage, operators may defer deploying user plane data integrity protection during this transition period. Examples of impacts to providing seamless integrity protection include:

- Significant user base of Release 15 UEs not supporting user plane integrity protection at full rate.
- 4G/LTE overlay networks unable to support user plane integrity protection.

gNB: gNodeB is a base station that supports 5G NR

Recommendations to Industry

RRC Signaling Confidentiality

3GPP TS 33.501 specifies mandatory (e.g., requires vendor implementation) support for protection of the RRC signaling confidentiality, but optional for service providers to use.

Given this standards requirement, CSRIC VII recommends protection of the RRC-signaling confidentiality. Only non-identity related information shall be conveyed prior to security context is established.

RRC: Radio Resource Control

Recommendations to Industry

Subscription Permanent Identifier/ International Mobile Subscriber Identity (SUPI/IMSI) Privacy

3GPP TS 33.501 specifies mandatory (e.g., requires vendor implementation) support for protection of the SUPI/IMSI privacy, however 3GPP allows for some exceptions where the Subscription Concealed Identifier (SUCI) may use null scheme (i.e., the identity is not protected).

CSRIC VII recommends that devices and networks in the U.S. use IMSI privacy (SUCI), and do not use null encryption scheme except when the UE is requesting emergency services.

It is recommended that no other exceptions allowed by 3GPP in Release 16 (for null encryption scheme SUCI) be used by devices or networks in the U.S. This may result in roaming 5G devices configured by operators from outside the U.S being unable to connect to 5G SA (option 2) networks. They can use 4G LTE networks instead.

Recommendations to Industry

Network Security – IPSec

3GPP TS 33.501 specifies mandatory (e.g., requires vendor implementation) support of protection of the network security – IPSec, but optional for service providers to use.

CSRIC VII recommends the use of IPSec or use of a tunneling technology for transport (e.g., VPN tunnels) for protection of network security.

Recommendations to Industry

Core Network Security – Transport Layer Security (TLS)

3GPP 33.501 specifies mandatory (e.g., requires vendor implementation) support of protection of the core network security – TLS, but optional for service providers to use.

CSRIC VII recommends the use of TLS for SBA interfaces and for non-SBA use of a tunneling technology for transport (e.g., VPN tunnels) for protection of core network security.

SBA: Service Base Architecture

Working Group 3 Chairman's Note:

I would like thank members of Working Group 3 for their diligence, critical thought, and professionalism in the development and submission of this Report.

I would also like to thank ATIS for providing the necessary support and tools to enable work progress.

The members of Working Group 3 respectfully request that the CSRIC VII Council accept *Recommendations for Identifying Optional Security Features that can Diminish the Effectiveness of 5G Security.*

DISCUSSION

REPORT ON RECOMMENDATIONS FOR IDENTIFYING OPTIONAL SECURITY FEATURES THAT CAN DIMINISH THE EFFECTIVENESS OF 5G SECURITY

Farrokh Khatibi, Chair
Working Group 3

CALL FOR VOTE

REPORT ON RECOMMENDATIONS FOR IDENTIFYING OPTIONAL SECURITY FEATURES THAT CAN DIMINISH THE EFFECTIVENESS OF 5G SECURITY

Charlotte Field, Chair
CSRIC VII

PRESENTATION

REPORT MEASURING RISK MAGNITUDE AND REMEDIATION COSTS IN 911 AND NG911 NETWORKS

Mary Boyd, Chair
Working Group 4

Working Group 4:
911 Security Vulnerabilities During the IP Transition –

Report 3: Measuring Risk Magnitude and Remediation Costs in 9-1-1 and NG9-1-1 Networks

March 10, 2021

Mary A. Boyd, Chair
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 9-1-1 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). (Report 1)

The FCC further directs CSRIC VII to identify security risks in legacy 911 networks, transitional 9-1-1 networks, and NG9-1-1 networks and recommend best practices to mitigate risks in these three areas. (Report 2)

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 9-1-1 systems, including for legacy 9-1-1 networks, transitional 9-1-1 networks, and Next Generation 9-1-1 (NG9-1-1), and,

- ❑Remain mindful and compliant with federal rules governing "surveying of information";
- ❑Identify and review existing 9-1-1 reports on the current states of interoperability as data sources; and,
- ❑Identify public safety associations and local 9-1-1 Program Offices as additional data sources for completion of the deliverables for the report.

COMPLETED

CSRIC
Communications Security, Reliability and Interoperability Council

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

CSRIC
Communications Security, Reliability and Interoperability Council

Working Group 4: Report 3:

Measuring Risk Magnitude and Remediation Costs in 9-1-1 and NG9-1-1 Networks – Seeking Adoption: March 10, 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 9-1-1 and NG9-1-1 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	Lumen
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	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.
† Tom Breen represented Comtech from 07/2019 to 07/2020

WORKING GROUP 4
REPORT 3 REVIEW:

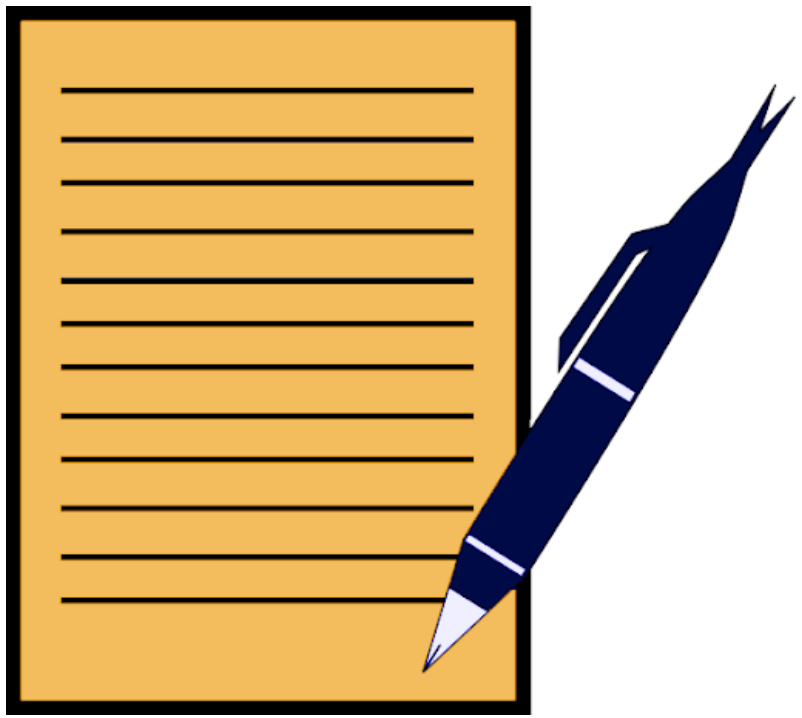
CSRIC Report *Measuring Risk Magnitude and Remediation Costs in 9-1-1 and NG9-1-1 Networks*

Past Schedule: Working Group 4

- Established Two Sub-teams Focused on :
  - Technical Review and Recommendations
  - Best Practices Review and Recommendations
- Conducted weekly conference calls to:
  - Review and Edit Contributions

Report 3 Structure

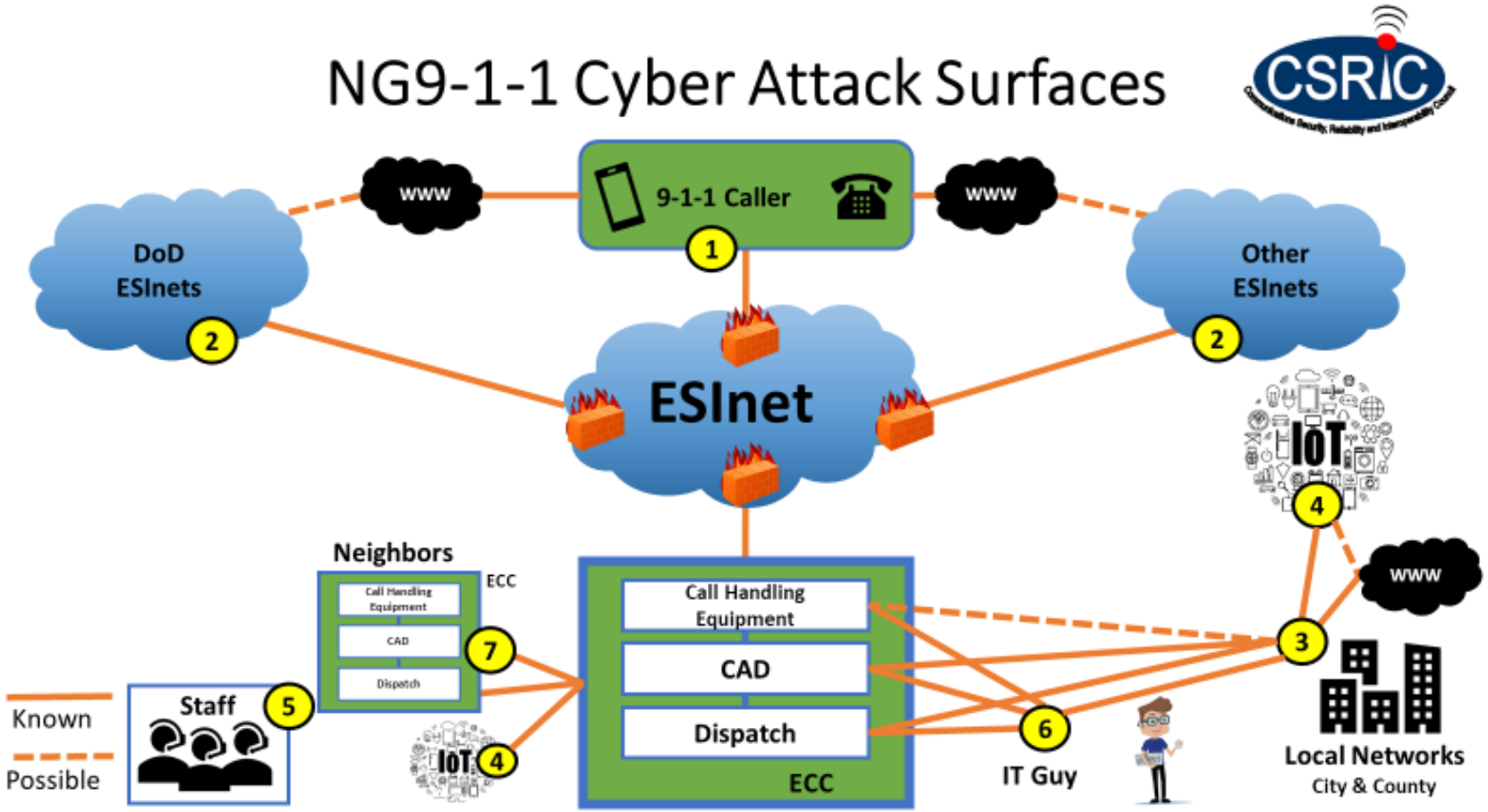
- Executive Summary
- Includes Normal Introductory Sections
- Analysis Includes:
  - General Impacts of Cyber Attacks
  - Impact On Public Safety Entities
  - Best Practices
- Findings Will Include
  - What Can Be Done To Mitigate Impacts
  - Estimated Costs to Mitigate
  - Basic Cybersecurity Controls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



Report 3 Overview: Methodology

- Report 3 Builds On Report 1 and 2 which:
  - Explored the TFOPA Maturity States for transitional network phases of NG911 (2016)
  - Determined that several of the transitional phases did not materially impact the nature of cybersecurity during the transition, and consolidated those stages focusing on:
    - *Legacy State*
    - *Transitional State*
    - *End State*
  - Addressed security considerations and larger threat landscape and discussed how industry and public safety can work together to implement appropriate measures based on a combined threat analysis and approach.
- Examined nature of attacks; attack mitigation and remediation strategies and associated costs. Resource information based on subject matter experts, and exploration of growing literature and documented experiences.
- Reviewed existing cybersecurity-related Best Practices; provided clarification; proposed deletions where appropriate; and developed new Best Practices based on Report 2 Use Case scenarios.

Introduction to NG9-1-1 Cybersecurity Considerations: 7 Cyber Attack Surfaces (Report 2)



2019 U.S. Ransomware : $7.5B

Ranks #3 in Top 10 Risks for Business

Quantifying Risks – 5.1.3

Benefits of Quantifying Risk

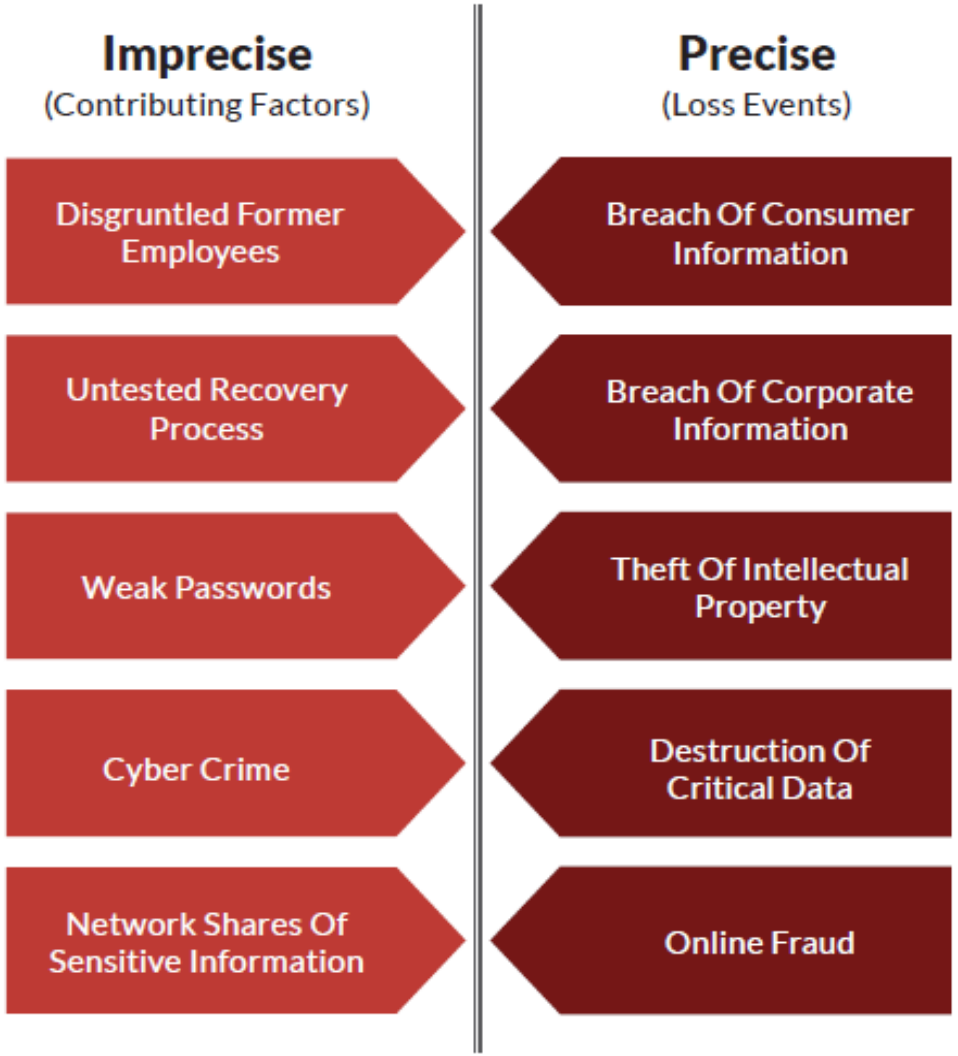
- Understanding Impacts of Risk
- Prioritization of Risks/Controls
- Accurate Risk Analysis

Impediments To Quantification/Mgt

- Limited Insight
- Failure To Prioritize
- Focus on Identification & Prevention
- Failure To Hire Talent
- Weak 3rd Party Management
- Lack of Security-Aware Culture
- Operational Stress

Quantifying Risks: 5.1.3

TERMINOLOGY FOR DEFINING CYBER RISKS:

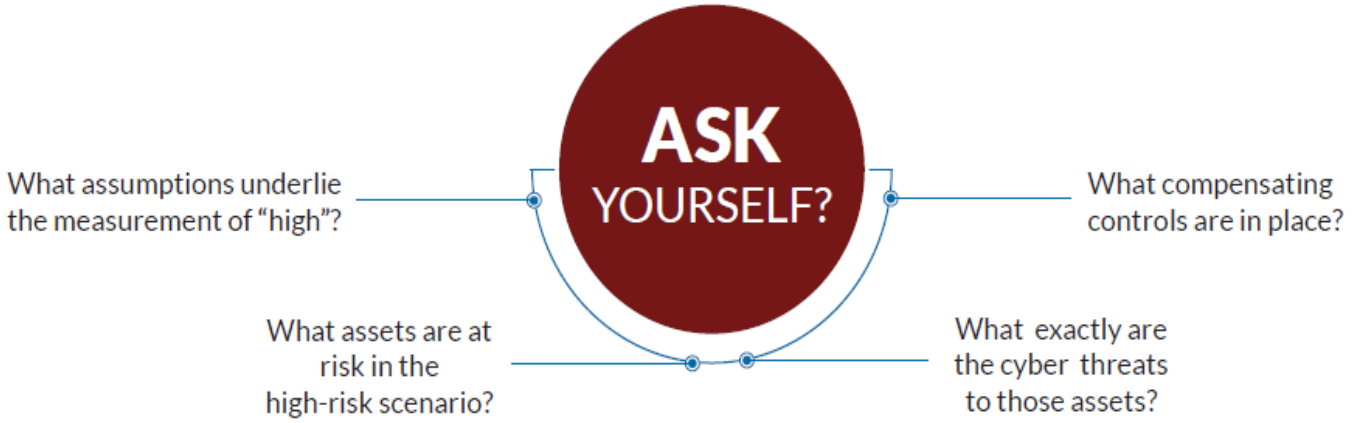


Based on A Clarification of "Risks"? white paper, the FAIR Institute[2]

Quantifying Risks – 5.1.3

Quantification Methodology

- Define Risk
- Scope Risk Clearly
- Apply Accurate Modeling



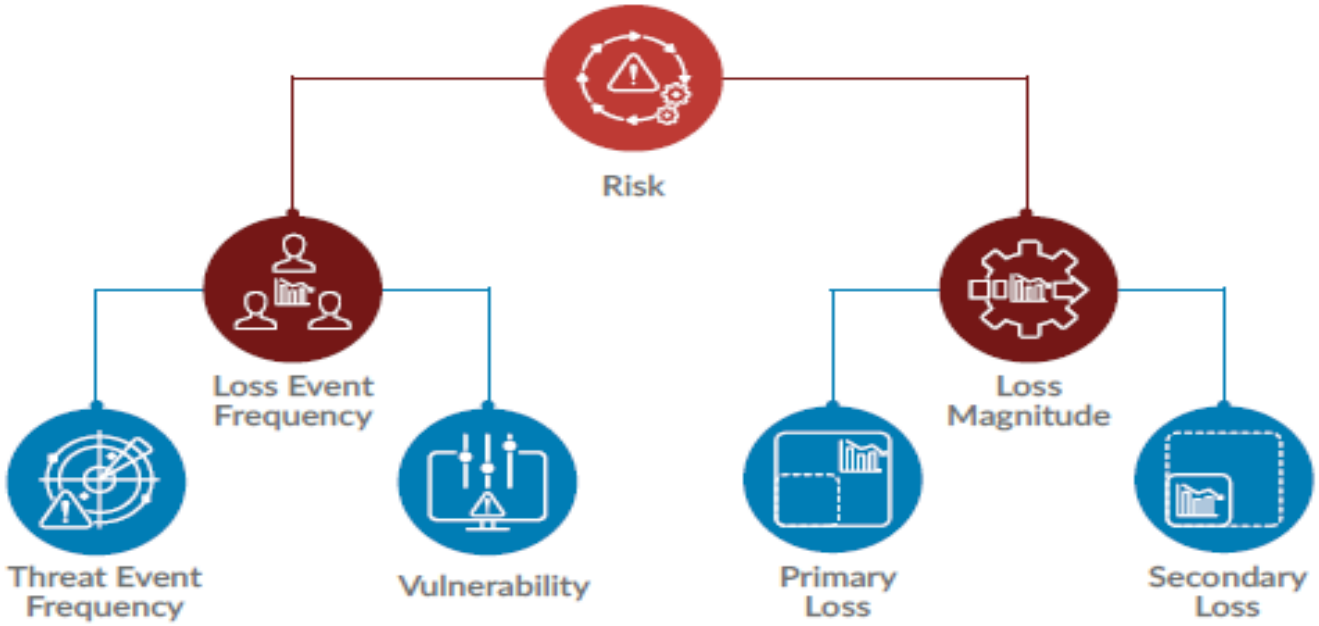
Scoping Risk with Precision

*From *RSA Ebook: 3 Essentials for Cyber Risk Quantification*

Quantifying Risks – 5.1.3

FAIR MODEL FOR RISK MANAGEMT

- Define Risk
- Models
- Framework
- Quantitative Analysis



Factor Analysis of Information Risk (FAIR) Model

*From *RSA Ebook: 3 Essentials for Cyber Risk Quantification*

9-1-1 Fees and Cybersecurity (5.1.4)

INVEST IN THE FUTURE

- Roles For FCC
- 9-1-1 Fee Diversion Impacts
- Cybersecurity Investment

PHOTO: Cybercrime Magazine.

FINDINGS (5.2)

- Mitigation
- Estimated Costs
  - Operations
  - Vulnerability Assessments
  - Written Cyber Response Plan
- Cybersecurity Investment
- Best Practices (Revisions & New)

Recommendations (5.3)

- **Public Safety Community**
  - Service Delivery Models
  - Cybersecurity as Eligible Use of Funds
  - Funding Allocation Decisions
  - Develop Cyber Response Plan
  - Work With Insurance Providers
  - All Emergency Call Path PSAP/ECC Data Meet Security Recommendations
  - IoT Smart Cities devices are isolated from 911 networks
  - Employ Methodologies like FAIR Model to quantify risk and remediation
  - Implement CIS Implementation Group controls

Recommendations (5.3 cont.)

- **Federal Communications Commission (FCC)**
  - Foster & facilitate the development of a written model for cyber response plan
  - Urge all organizations to implement level of controls equivalent, or similar, to CIS IG1
  - Encourage call authentication mechanism for 911 calls in legacy and transitional environments
  - Update TFOPA Report specific to Emergency Communications Cybersecurity Center (EC3) cost assessment
  - Foster communication with cybersecurity entities (ISO, CIS, NIST, NASCIO) to adopt NG911 Best Practices important to security and reliability of public safety agencies
  - Collect data from 9-1-1 community about cybersecurity maturity; reference control models which include maturity states and maps to NIST framework
  - Support spending of 9-1-1 Fees on cybersecurity as a matter of public policy

Recommendations (5.3 cont.)

- **Federal Communications Commission (FCC) – Future Initiatives**

  Continue to support research into cybersecurity considerations for:

  - Over-the-top network solutions, such as Text-To-911 (including examination and consideration of TTY architectures)
  - Delivery of supplemental data and use of handset-based applications for vulnerabilities and exposures to cyber threats
  - IoT as a cyber attack target
  - Smart Cities
  - 5G
  - Dealing with encrypted data destined for the PSAP/ECC
  - Other cybersecurity topics as they become known

Report 3: Measuring Risk Magnitude and Remediation Costs in 9-1-1 and NG9-1-1 Networks

Questions / Seek Adoption

Discussion

Report Measuring Risk Magnitude and Remediation Costs in 911 and NG911 Networks

Mary Boyd, Chair
Working Group 4

CALL FOR VOTE

REPORT MEASURING RISK MAGNITUDE AND REMEDIATION COSTS IN 911 AND NG911 NETWORKS

Charlotte Field, Chair
CSRIC VII

PRESENTATION

REPORT ON SIP SECURITY CHALLENGES AND MITIGATION

Danny McPherson, Chair
Working Group 6

Working Group 6:
SIP Security Vulnerabilities

March 10, 2021

Chair: Danny McPherson, 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 Members

Members

Name	Company
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
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

Alternates

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

FCC Liaison: Ahmed Lahjouji
*Also CSRIC Member

Working Group 6: Final Report

- Provides a background of how SIP-based infrastructures are designed, commonly deployed, and how their components interact.
- Codifies known SIP issues and vulnerabilities into a threat model that divides a mnemonic for security threats into various categories.
- Presents a Gap Analysis of on-going work efforts in various standardization groups to address SIP security issues.

Working Group 6: STRIDE

- Report follows Microsoft STRIDE threat model methodology.
- Issues are grouped into attack classes:
  - Spoofing
  - Tampering
  - Repudiation
  - Information Disclosure
  - Denial of Service
  - Elevation of Privilege

Working Group 6: Key SIP Actions

- Use TCP transport protected by TLS exclusively, with a PKI based authentication scheme. This requires upgrades to many existing systems.
- Keep components up to date with security patches. Many systems are unable to be patched rapidly or at all. Those systems should be replaced.
- Deploy STIR/SHAKEN more widely (e.g. non-carrier and international).
- For systems where massive TDoS would cause severe repercussions (e.g. emergency services), deploy high volume DDoS mitigation services. This should include call processing as well as packet processing mitigations.

Working Group 6: Recommendations

- The FCC should support SIP operators adopting and deploying well-established security frameworks.
- Industry should implement basic hygiene best practices to ensure that their SIP networks are secure.
- The working group urges the commission to study the potential trade-offs between caller privacy and law enforcement requirements to find a balance point that increases confidence in the confidentiality of calls.
- Working Group recommends the FCC to further study if and or when downgrades from more secure protocols, such as TCP with TLS, should be allowed in SIP.

Working Group 6:
SIP Security Vulnerabilities

Questions?

Discussion

Report on SIP Security Challenges and Mitigation

Danny McPherson, Chair
Working Group 6

CALL FOR VOTE

REPORT ON SIP SECURITY CHALLENGES AND MITIGATION

Charlotte Field, Chair
CSRIC VII

CLOSING REMARKS

CHARLOTTE FIELD, CHAIR

ADJOURN MEETING

Suzon Cameron, DFO