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

SEPTEMBER 16, 2020

COMMENCE MEETING

Suzon Cameron, DFO

OPENING REMARKS

Charlotte Field, Chair

PRESENTATION

REPORT ON STANDARD OPERATING PROCEDURES FOR EMERGENCY ALERTING COMMUNICATIONS

Craig Fugate, Chair
Working Group 1

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

September 16, 2020

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

Working Group 1: Background

- 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.

Working Group 1: Objectives

This report documents the examination by CSRIC VII, Working Group 1 with respect to the following:

- 1) Establishing and maintaining communications between industry stakeholders (e.g., broadcasters, cable providers, wireless providers), government partners, and alert originators;
- 2) Developing and maintaining relationships between communications providers and alert originators that can readily be leveraged during emergencies;
- 3) Establishing redundant and effective lines of communication with key stakeholders during emergencies, including Government Emergency Telecommunication Service (GETS) and the Wireless Priority Service (WPS); and
- 4) The important elements that should be included in alert message that retract or correct false alerts.

Deliverables/Schedule

- Final Report Due September 2020

Working Group 1 Members

Craig Fugate (Chair)*	APTS
Mark D. Annas*	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
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

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

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

Working Group 1 Conclusions

- Recommendations and next steps included in this report will continue to improve the current alert systems by assisting all personnel in their tasks and supporting their ability to reach out, work as part of a greater team, and share knowledge. The False Alert Handling recommendations will decrease stress in both the alert personnel and public by reducing the number of false alerts and bringing a more automated structure to the reactions following a false alert.

The members of Working Group 1 respectfully request that the CSRIC VII Council adopt the Report on Standard Operating Procedures for Emergency Alerting Communications .

(Next Slide, Please)

DISCUSSION

REPORT ON STANDARD OPERATING PROCEDURES FOR EMERGENCY ALERTING COMMUNICATIONS

Craig Fugate, Chair
Working Group 1

CALL FOR VOTE

REPORT ON STANDARD OPERATING PROCEDURES FOR EMERGENCY ALERTING COMMUNICATIONS

Charlotte Field, Chair
CSRIC VII

PRESENTATION

REPORT ON RISKS INTRODUCED BY 3GPP RELEASES 15 AND 16 5G STANDARDS

Farrokh Khatibi, Chair
Working Group 3

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

September 16, 2020

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 Completed

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

Report 2 - March 2021 started

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
Chandra Kotaru*	AWARN Alliance
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*

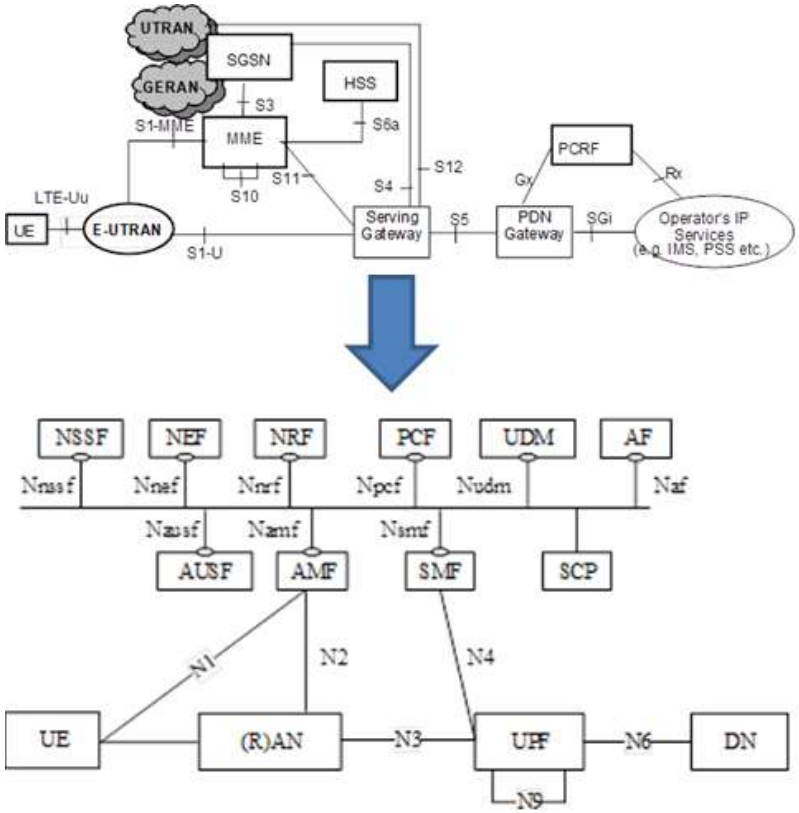
Steve Barclay	ATIS
Vinod Choyi	Verizon
Martin C. Dolly	AT&T Services Inc.
Yong Kim	Verisign
Andrew Schnese	Nsight
Greg Schumacher	T-Mobile

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

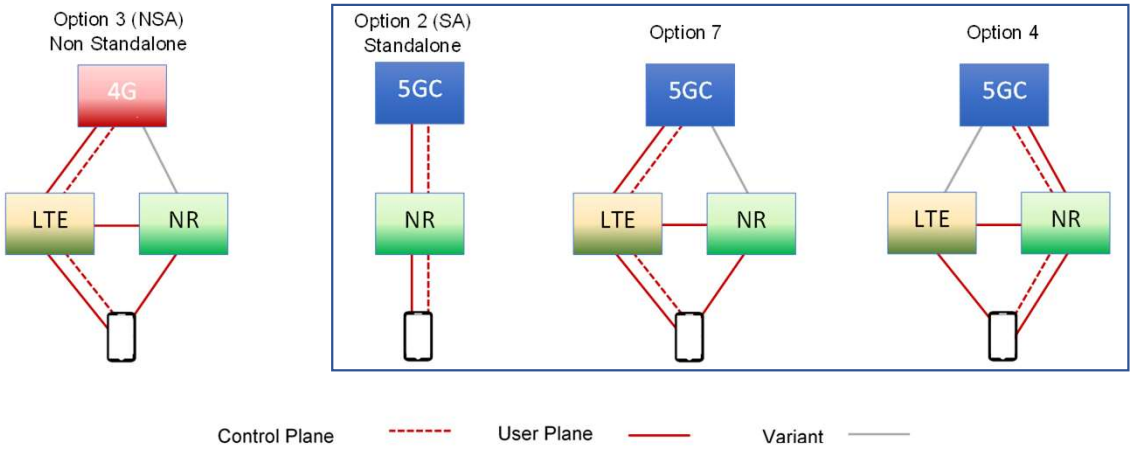
5G Background

- 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



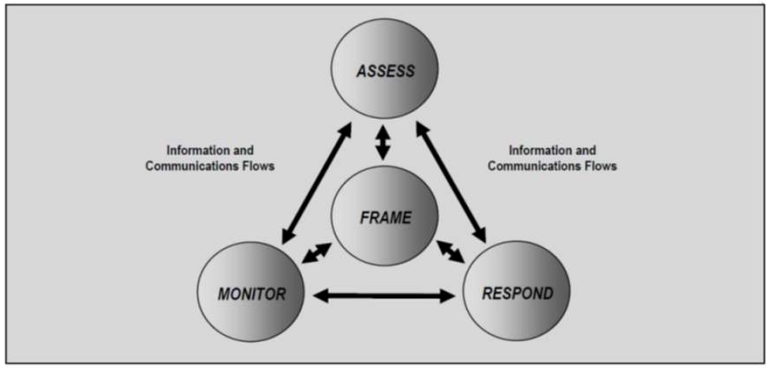
Working Group 3 Scope



The primary focus of WG3 is Option 2 Standalone (SA) and related options with 5G Core network (5GC)

Working Group 3 Methodology

- The WG relied upon several sources to compile the data to identify and evaluate the emerging security risks anticipated in the transition to 5G, including:
  - Industry SME presentations
  - Standards bodies and industry associations
  - Individual contributor research gathered by Working Group members
  - Academic papers
- The WG also considered NIST SP 800-39 methodology as shown below:



Recommendations to the FCC

Previous CSRIC Recommendations

The working group commends the FCC's efforts to support CSRIC recommendations as shown by previous Public Notices (PNs). WG3 recommends that the FCC encourage industry for continued implementation of CSRIC's prior recommendations and continue to promote awareness.

Recommendations to the FCC

Supply Chain Recommendations

CSRIC VI WG3 published an addendum to their final report regarding supply chain recommendations.

CSRIC VII WG3 reiterates the recommendation that the FCC continue to actively participate in the ICT SCRM Task Force, engage with NIST on the review of SP 800-161 rev 1 and continue as an active member of the ATIS 5G Supply Chain Working Group. These Supply Chain Risk Management (SCRM) programs represent strong public and private partnerships that are working to develop the framework for trusted 5G networks.

Recommendations to the FCC

Network Slicing

Network Slice is a logical network that provides specific network capabilities and network characteristics. It is defined within a Public Land Mobile Network (PLMN) and includes the Core Network Control Plane and User Plane Network Functions as well as the 5G Access Network (AN).

The working group recommends that the FCC consider further investigation the security implication of Network Slicing for a future CSRIC task.

Recommendations to the FCC

5G Private Networks

Private Networks, also called Non-Public Networks (NPN) in 3GPP specifications, are intended for the sole use of a private entity such as an enterprise, and may be deployed in a variety of configurations, utilizing both virtual and physical elements. Specifically, they may be deployed as completely standalone networks, they may be hosted by a PLMN, or they may be offered as a slice of a PLMN.

5G Private Networks is briefly discussed in section 5.4 of the Report, but with limited conclusion due to the pending activities in 3GPP. The working group recommends that the FCC consider further investigation of 5G Private Network security for a future CSRIC task.

Recommendations to the FCC

5GC Support of Different Access Technologies

The working group recommends that FCC consider further investigation of other access technologies that enable 5G deployment and delivery for a future CSRIC task. Additional work should be accomplished toward wireline, satellite, as well as other wireless access technologies concerning security and capacity as well as specific potential vulnerabilities.

Recommendations to Industry

Previous CSRIC Recommendations

The working group 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

Protection of legacy protocols

The protection of legacy protocols (Diameter, GTP) and associated interfaces shall be supported according to Network Domain Security IP network layer security (NDS/IP) as specified in 3GPP TS 33.210. In case of intermediaries (e.g., hop-by-hop), it does not ensure end-to-end message authenticity and confidentiality protection. Additionally, protection of Diameter interfaces shall use recommendations described in CSRIC VI WG3.

Recommendations to Industry

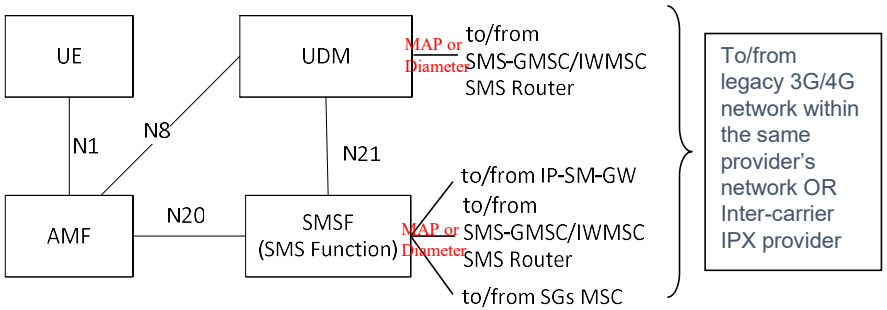
Security Concerns of Using Legacy Protocols

The Unified Data Management (UDM) may be prone to known HLR/HSS specific attacks that exist on legacy 3G/4G inter-carrier SS7 or Diameter roaming links.

The SMS Function (SMSF) may be prone to known MSC/VLR specific SS7 or Diameter attacks that exist on the inter-carrier SS7 or Diameter roaming links.

The Charging Function (CHF) may be prone to attacks that exploit vulnerabilities that exist in base Diameter protocol implementation without transport layer protection.

The Session Management Function (SMF) and User Plane Function (UPF) may be prone to attacks that may exploit GPRS Tunnelling Protocol (GTP) and Packet Forwarding Control Protocol (PFCP) that are generally deployed without any message authentication, integrity and confidentiality protection



N8: Reference point for SMS function address retrieval and SMS over NAS service authorization between AMF and UDM

N20: Reference point for SMS transfer between AMF and SMS Function

N21: Reference point for SMS subscription retrieval between SMS Function and UDM

Recommendations to Industry

Security Concerns of Using Legacy Protocols

The Unified Data Management (UDM) and SMS Function (SMSF) may be prone to attacks similar to what was seen in earlier generations on the HLR/HSS. Attacks via SS7/Diameter in 3G/4G networks could be repeated in a 5G network using the InterWorking Function (IWF), or through new attacks against the HTTP protocol.

The working group recommends that remediation against known SS7/Diameter attacks be implemented at the IWF, and that safeguards for the UDM be implemented.

The working group recommends that remediation against known SS7/Diameter attacks be implemented at the IWF, and that safeguards for the SMSF be implemented.

Recommendations to Industry

Workforce

The working group recommends that industry leverage CSRIC's collection of Best Practices to ensure the workforce is prepared to operate and maintain carrier grade reliability and security in a 5G SA environment. This includes workforce training on network elements introduced in the 5G SA architecture such as virtualization and network slicing.

Recommendations to Industry

Open Source in 5G

One of the common misconceptions about an open source architectures is that open interfaces introduce security risk. In fact, these same open interfaces, defined in technical specifications, provide a foundation and architecture for improving security.

An open architecture opens the ecosystem to new suppliers, increasing the diversity of virtualized solutions, inherently increasing the security of a network vs. a proprietary, single vendor network. Standards play an important role in 5G security and an open source.

The working group recommends the industry continue to advance open architectures for 5G and continue to address security as a fundamental consideration of all open source architectures.

Recommendations to Industry

Network Slicing Security

WG3 recommends that the industry should consider the following factors to ensure security in Network Slicing.

Slicing Isolation:

- Isolation is the crucial security aspect in network slicing. It is important to make sure that resources dedicated to one slice cannot be consumed by another slice. Also, data/traffic cannot be intercepted/faked by entities of another slice.

- Slice isolation needs to be achieved assuming sound implementations in the cloud, SDN transport and non-virtualized equipment.
  - The cloud infrastructure that host the slices needs to provide adequate protection and isolation at the platform level, hypervisor level and at individual virtual machine (VM) or Containers levels with proper configuration and monitoring tools.
  - The SDN transport infrastructure needs to achieve isolation by using VPNs.
  - The non-virtualized equipment (e.g., RAN) should achieve isolation by equipment-specific mechanisms.

Recommendations to Industry

Network Slicing Security

WG3 recommends that the industry should consider the following factors to ensure security in Network Slicing.

Automated Slicing Security Management and Orchestration tools:

- Automated Security Management and Orchestration is needed to cope with the dynamic nature of slicing. Some security tools may only run within one slice, not aware of other slices, but there must be others that have the complete network view.

Slice-specific assurance level:

- Network functions may have diverse security assurance levels. All network functions used in a slice (as well as the platform on which they are deployed) must meet the assurance level required for the services deployed in the slice.
- This may also allow fast, lightweight deployment of experimental services in slices without a high security assurance level.

Recommendations to Industry

Network Slicing Security

WG3 recommends that the industry should consider the following factors to ensure security in Network Slicing.

Protection of slicing-specific procedures (such as slice selection, slice-specific authentication and authorization, or slice management access by third party tenants):

- Current and future state-of-the-art protection measures for such interfaces and procedures must be applied.
- Use standardized security measures to standardized slicing-specific procedures (e.g., 3GPP TS 33.501)

Recommendations to Industry

Network Slicing Security

WG3 recommends that the industry should consider the following factors to ensure security in Network Slicing.

Per slice network security measures: A slice is a virtual network, so general network security measures must be applied per slice:

- “Legacy” measures applied to a virtualized network: virtual firewall, zoning and traffic separation by virtual networking, intrusion detection, authentication, cryptographically protected protocols, access control etc.
- Integrity protection for platform and virtualized functions using remote attestation based on strong trust anchors
- “Modern state-of-the-art”: Pervasive Monitoring, AI/ML based analytics, automated response loop, automated threat intelligence sharing etc.

Recommendations to Industry

Network Slicing Security

WG3 recommends that the industry should consider the following factors to ensure security in Network Slicing.

Automated Slicing Security Management and Orchestration tools:

- Automated Security Management and Orchestration is needed to cope with the dynamic nature of slicing. Some security tools may only run within one slice, not aware of other slices, but there must be others that have the complete network view.

Slice-specific assurance level:

- Network functions may have diverse security assurance levels. All network functions used in a slice (as well as the platform on which they are deployed) must meet the assurance level required for the services deployed in the slice.
- This may also allow fast, lightweight deployment of experimental services in slices without a high security assurance level.

Working Group 3 Chairman's Note:

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

I would also like to wish the WG2 chairman emeritus, Mr. Lee Thibaudeau, happy and healthy days in his retired years.

The members of Working Group 3 respectfully request that the CSRIC VII Council adopt the *Report on Risks Introduced by Releases 15 and 16 5G Standards.*

Thank You

(Next Slide, Please)

DISCUSSION

REPORT ON RISKS INTRODUCED BY 3GPP RELEASES 15 AND 16 5G STANDARDS

Farrokh Khatibi, Chair
Working Group 3

CALL FOR VOTE

REPORT ON RISKS INTRODUCED BY 3GPP RELEASES 15 AND 16 5G STANDARDS

Charlotte Field, Chair
CSRIC VII

PRESENTATION

REPORT ON SECURITY RISKS AND BEST PRACTICES FOR MITIGATION IN 911 IN LEGACY, TRANSITIONAL, AND NEXT GENERATION 911 IMPLEMENTATIONS

Mary Boyd, Chair
Working Group 4

Working Group 4:
911 Security Vulnerabilities During the IP Transition

September 16, 2020

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 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.

Working Group 4: Report 3

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;
- ❑Review Best Practices and make recommendations to reduce vulnerabilities;
- ❑Identify any economic disadvantages or risks;
- ❑Identify any barriers to implementing mitigation measures; and
- ❑Publish a report measuring risk Magnitude and Remediation costs in 911 and NG911 Network.

Deliverables/Schedule

Report 1 Title:

- Current State of Interoperability for the nation's 911 systems, including for legacy 911 networks, transitional 911 networks, and Next Generation 911 (NG911)
  - Finalized: March 2020

Report 2 Title:

- Security Risks and Best Practices for Mitigation in 911 in Legacy, Transitional, and NG911 Implementations
  - Finalize By: September 2020 – Today's Report

Report 3 Title:

- Measuring Risk Magnitude and Remediation Costs in 911 and NG911 Networks – Finalize By: March 2021

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	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 2:

REPORT ON SECURITY RISKS AND BEST PRACTICES FOR MITIGATION IN 9-1-1 IN LEGACY, TRANSITIONAL, AND NG 9-1-1 IMPLEMENTATIONS

Report 2 Structure

- Executive Summary
- Includes normal introductory sections
- Introduction to NG911 Cybersecurity Considerations
  - Focus On Threat Surface & Attack Vectors
- Discussion of Threat Protection & Mitigation Strategy Recommendations
  - Identify Functions (6 Use Cases)
  - Protect, Detect, Respond and Recover Functions
  - Use of Controls During Transition
  - Mapping Asset Types to 911 Domains
  - Guidelines for Implementing Controls Through Transitions
- Conclusions
- Recommendations

Report 2 Overview: Methodology

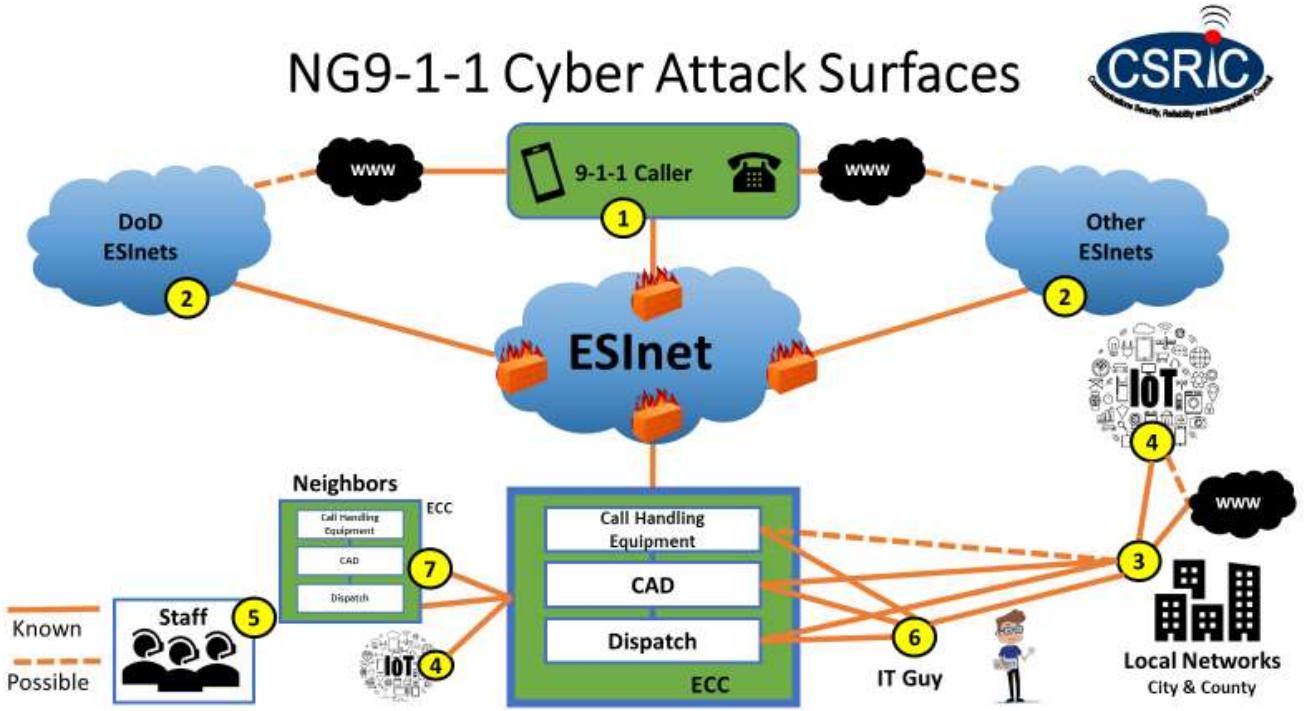
- Explored the TFOPA Maturity States for transitional network phases of NG911 (2015)

- 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*

- Report is designed to address security considerations and is also intended to address the larger threat landscape and how industry and public safety can work together to implement appropriate measures based on a combined threat analysis and approach.

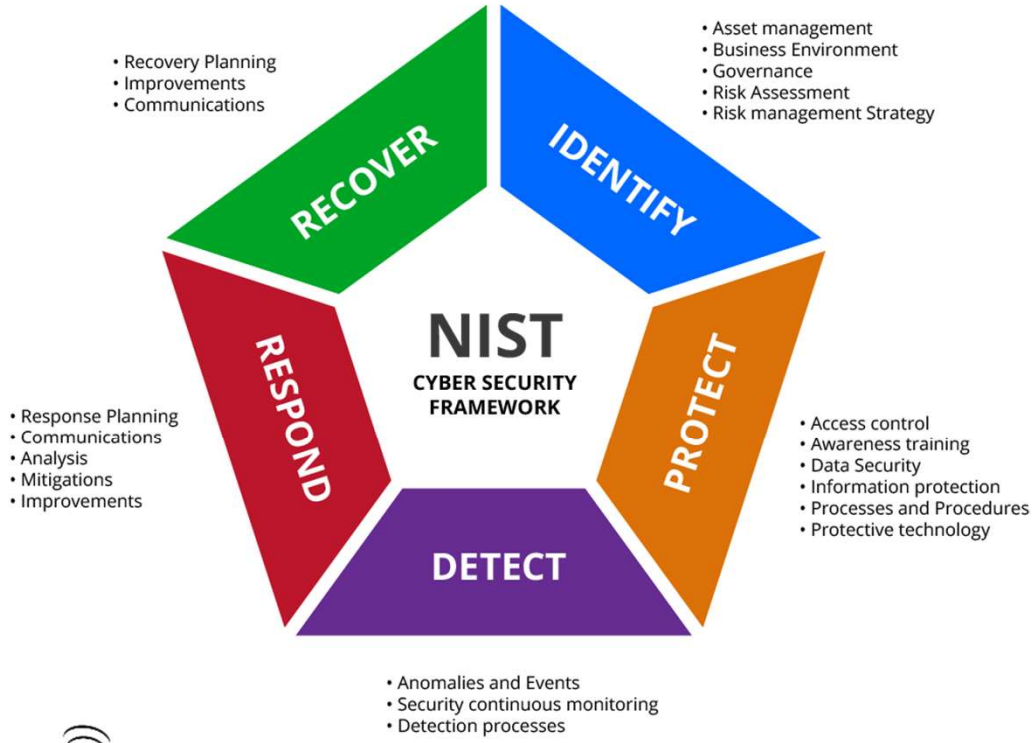
Introduction to NG911 Cybersecurity Considerations:

7 Cyber Attack Surfaces (Section 6)

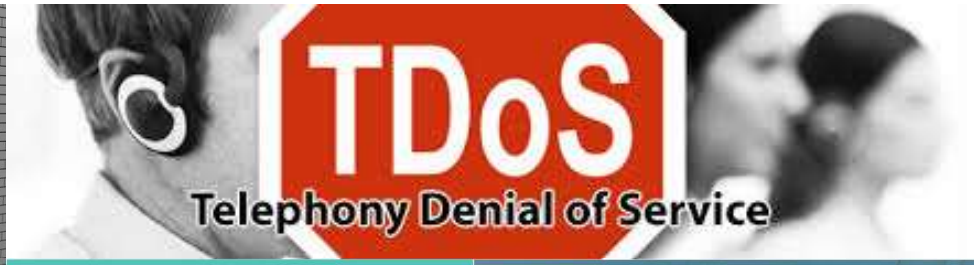


Threat Protection & Mitigation Strategies (Section 7)

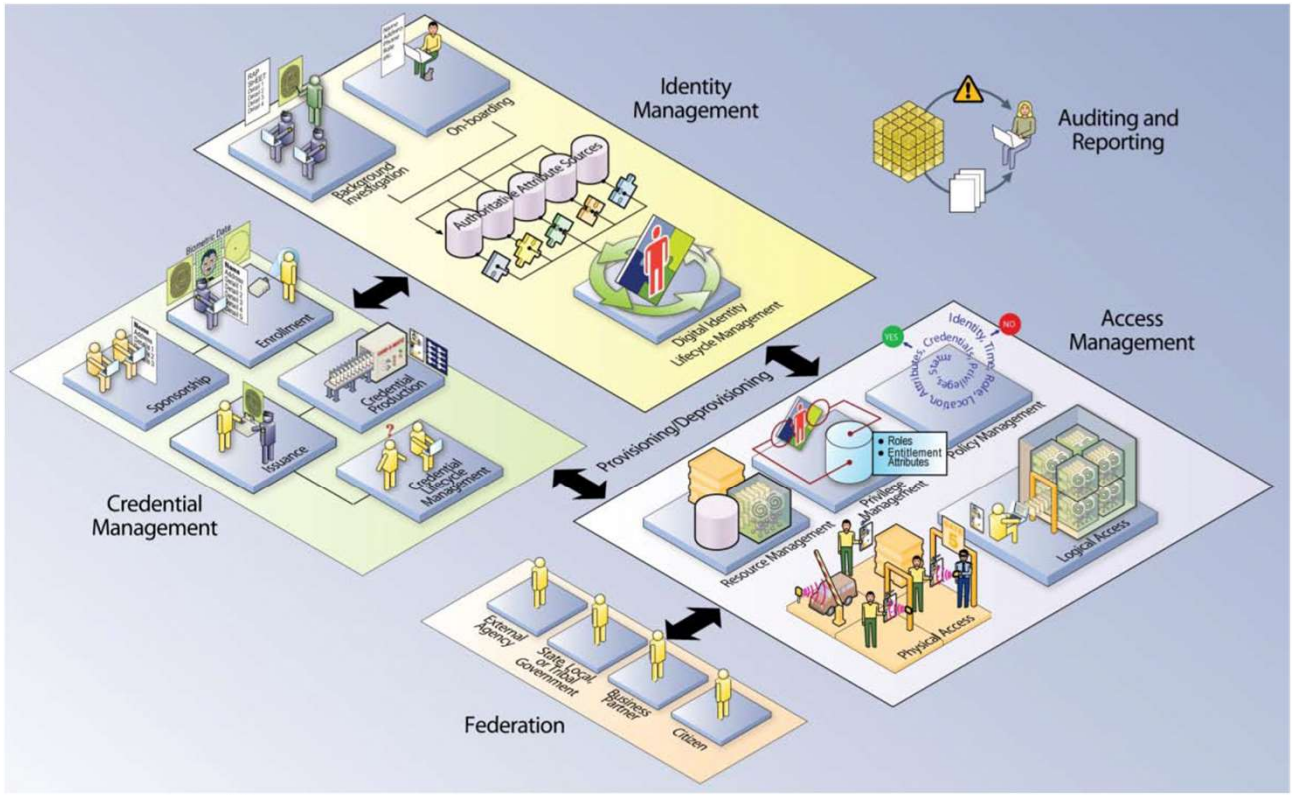
Threat Protection & Mitigation Strategies: NIST Framework



Report 2 Review & Recommendations: Use Cases



ICAM: The Big Picture



Conclusions (Section 8)

In 2015 TFOPA Working Group 1, identified that "A lack of cybersecurity poses a clear and present danger to ECC's and emergency communication system(s) in the United States…"

In 2020 WG4 concluded that an approach to managing 9-1-1 cybersecurity should include:

- Public/private partnerships;
- Cooperation's is needed in all levels of public safety both operationally and financially;
- Maintain environments to identify threats and recommend to ECC's the importance and how to mitigate; and
- Sharing of intelligence, practices for defending 911 networks and cooperative architectures to defend transitional states is needed until fully deployed NG911 networks is achieved.

Recommendations (Section 9)

In addition to the Use Case recommendations from Section 7, CSRIC VII also recommends the following:

- Implement appropriate industry-recognized cybersecurity controls in their entirety where possible, and in phases if necessary, during the transition;
- Organizations implement basic security controls, regardless of size, in a legacy environment;
- NG9-1-1 networks implement foundational security controls and some of the organizational security controls and;
- Implement Best Practices as indicated in Report 2 and Report 3.

Recommendations (cont.)

CSRIC VII also provides recommendations to the Commission for future initiatives:

- Going forward, review and revise this report to accommodate changes in cybersecurity advancements, improving on the security recommendations for 9-1-1 systems;
- Review cybersecurity aspects of future technologies impacting Public Safety:
  - Over-the-top network solutions, such as Text To 9-1-1 (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 target,
  - Smart Cities,
  - 5G, and
  - Other cybersecurity topics as they become known.

Request for Motion for Adoption of Report on Security Risks and Best Practices for Mitigation in 9-1-1 in Legacy, Transitional, and NG 9-1-1 Implementations

(Next Slide, Please)

Discussion

Report on Security Risks and Best Practices for Mitigation in 911 in Legacy, Transitional, and Next Generation 911 Implementations

Mary Boyd, Chair
Working Group 4

CALL FOR VOTE

REPORT ON SECURITY RISKS AND BEST PRACTICES FOR MITIGATION IN 911 IN LEGACY, TRANSITIONAL, AND NEXT GENERATION 911 IMPLEMENTATIONS

Charlotte Field, Chair
CSRIC VII

UPDATE ON PROGRESS

WORKING GROUP 2: MANAGING SECURITY RISK IN THE TRANSITION TO 5G

Kathy Whitbeck, Chair

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

September 16, 2020

Kathy Whitbeck, Chair WG2,
Nsight

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

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.

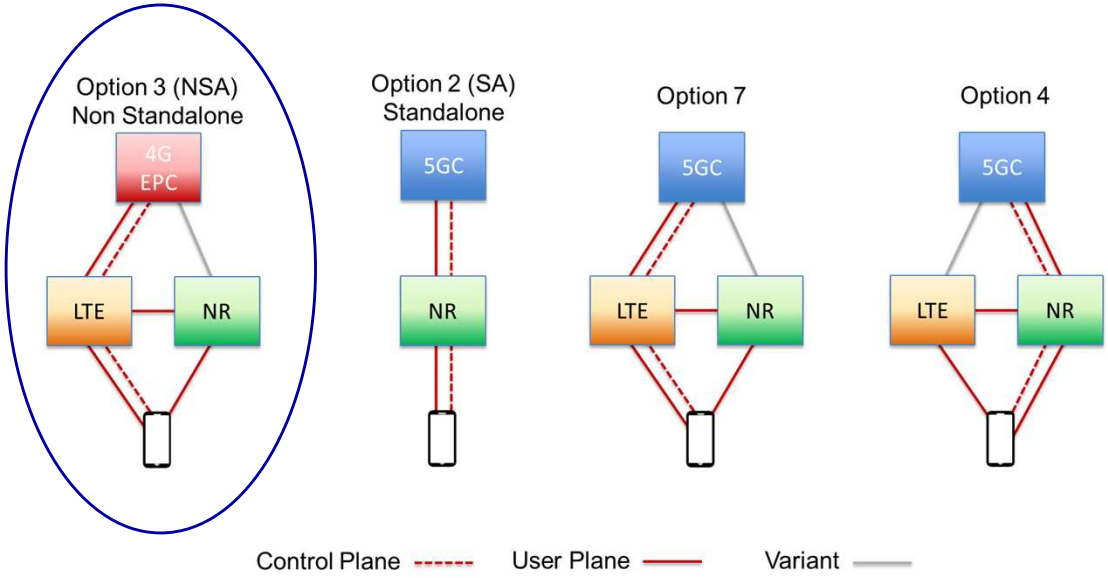
Working Group 2: Objectives

- 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.

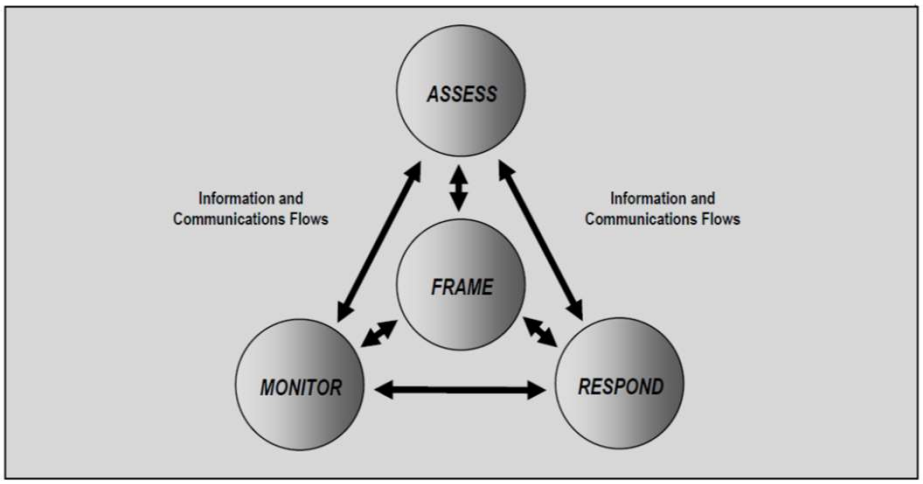
Working Group 2: Scope



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

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

Deliverables/Schedule

Report 1 June 2020 - *Complete*

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

Report 2 December 2020

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)

Working Group 2 Status

- Work toward completion of Report 2 – Due in December.
- Continue weekly Working Group conference calls
- Continue coordinating work effort with WG3:
  - Reduce potential gaps or overlap
  - Support efforts of both teams to conduct a thorough project
- Initiated discussion with WG4 on Public Safety-related requirements

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

Questions?

(Next Slide, Please)

DISCUSSION

PRESENTATION OF WG2: MANAGING SECURITY RISK IN THE TRANSITION TO 5G

Kathy Whitbeck, Chair

UPDATE ON PROGRESS

WORKING GROUP 6: SIP SECURITY VULNERABILITIES

Danny McPherson, Chair

Working Group 6: SIP Security Vulnerabilities Update

September 16, 2020

Danny McPherson, Chair
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

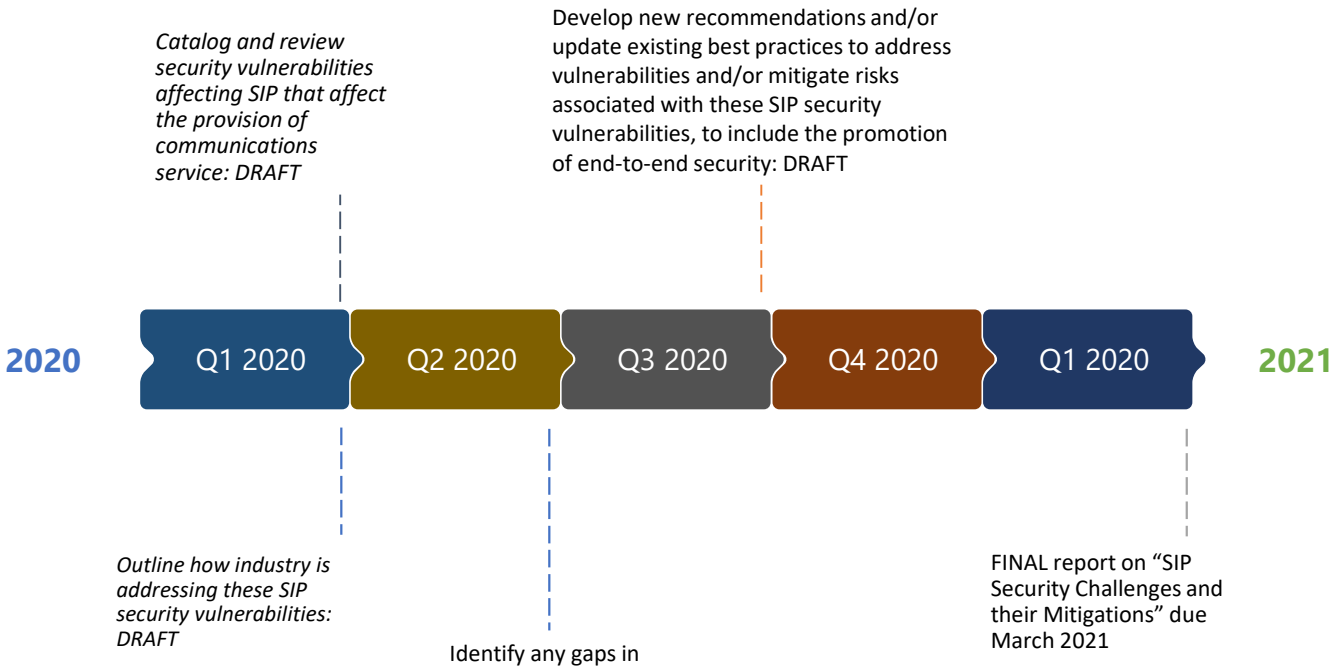
Complete

- 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

In Progress

- Access to GSMA for non-members of the workgroup
- 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
- Publish report for Council review

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

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

Next Steps

- Gain access to GSMA for non-members of the workgroup (IN PROGRESS)
- 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
- 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

Working Group 6:
SIP Security Vulnerabilities

Questions?

(Next Slide, Please)

Discussion

Presentation of Working Group 6: SIP Security Vulnerabilities

Danny McPherson, Chair

NEXT CSRIC VII MEETING
IS

WEDNESDAY
DECEMBER 9, 2020

CLOSING REMARKS

CHARLOTTE FIELD, CHAIR

ADJOURN MEETING

Suzon Cameron, DFO