June 2023

COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL VIII

REPORT ON RECOMMENDATIONS ON THE ROLE OF THE FCC IN PROMOTING THE AVAILABILITY OF STANDARDS FOR MORE SECURE, RELIABLE 5G ENVIRONMENT THROUGH THE USE OF VIRTUALIZATION TECHNOLOGY

DRAFTED BY
WORKING GROUP 3: LEVERAGING VIRTUALIZATION TECHNOLOGY TO PROMOTE SECURE, RELIABLE 5G NETWORKS

Table of Contents

1 Executive Summary

This report provides recommendations to the Federal Communications Commission (FCC) on how to promote collaboration, facilitate innovation, and ensure interoperability in the virtualized 5G space. The virtualized 5G space is seeing the emergence of many standards bodies working to ensure interoperability. While the FCC should refrain from direct involvement in the standards development process, it should closely monitor relevant standards development forums and work with industry and outside parties, including the FCC TAC[1] and NIST, to identify the most relevant standards bodies and the most efficient way to stay abreast of their progress. The FCC should track the standards development and understand the implications. The FCC should also work with relevant Executive Branch agencies and Congress to incentivize US participation and leadership in standards bodies.

To promote collaborations to achieve innovation in virtualized 5G technologies, the FCC should serve as a catalyst and facilitator to bring the relevant communities and organizations together and encourage the allocation of FCC resources necessary to establish and sustain meaningful collaborations. Specific examples of opportunities for enhanced collaboration include establishing means to facilitate user groups, vendors, and standards/guidance developers to share advanced requirements with the research funding organizations to help shape the direction of future research.

To build confidence in virtualized 5G solutions, the FCC should ensure that security is built into the system from the outset, rather than being bolted on as an afterthought. The FCC should work with NIST and CISA to develop a concise co-branded specification of the United States Government (USG) security requirements for virtualized 5G telecommunication environments. The FCC should also work with relevant USG agencies to support the development of open-source test and evaluation tools for USG security requirements and test and evaluate specific open-source virtualization platforms for their support of USG security requirements.

Summary of Key Findings and Recommendations:

1. Extensive deliberations were conducted to develop the report and formulated recommendations within the FCC's remit, considering industry-wide recommendations for enhanced outcomes.
2. The work group emphasizes the value of CSRIC programs and recommends the FCC to continue pursuing this path while expanding participation to address emerging inter-agency dynamics and complex technology ecosystems.
3. The use of the Memorandum of Understanding (MOU) vehicle between departments, is recommended to improve inter-agency collaboration, information sharing, and coordination. All stakeholders must collectively contribute to solving this problem.
4. The FCC should enhance collaboration with industry, FCC TAC, and NIST to identify relevant standards bodies and stay informed about their progress and implications for interoperability in the virtualized 5G space.
5. Relevant Executive Branch agencies and Congress should be encouraged to incentivize US participation and leadership in standards bodies, and tax policies should be adjusted to correct disincentives for international standards work.
6. The FCC can promote innovation in the virtualized 5G ecosystem by establishing means for user groups, vendors, and developers to share requirements, enhance open-source platforms, facilitate testing, and contribute to standards development.
7. To build confidence in virtualized 5G solutions based on open-source cloud computing software, the FCC could support a testing and validation framework, foster a culture of collaboration, and

[1] *FCC Technological Advisory Council (TAC),* https://www.fcc.gov/general/technological-advisory-council

create incentives for network operators to adopt these solutions.

8. The FCC should consider the overall health of the virtualized 5G solutions ecosystem, including diversity, productivity, security, and resilience, when making regulatory decisions. Industry, government, and academia must all participate to achieve this goal.

2 Introduction

The fifth generation (5G) of wireless networks has the potential to transform many industries, including healthcare, transportation, and entertainment, by providing high-speed connectivity, lower latency, and increased reliability. To ensure the smooth operation of 5G, it is essential to have coordination and interworking among different standards and open-interface community efforts. This interoperability can be achieved through collaboration among various standard bodies, including 3GPP, ATIS, O-RAN Alliance, Small Cell Forum, IETF, ETSI, NIST, and GSMA. However, this process may require coordination, and the Federal Communications Commission (FCC) could play a crucial role in promoting collaboration and innovation in the virtualized 5G space. In this context, the FCC could take several steps to help coordinate formal and informal standards and collaborative open-interface community efforts to ensure interoperability in the virtualized 5G space. This report provides recommendations for the FCC to promote collaborations to achieve innovation in virtualized 5G, build confidence in virtualized 5G solutions using open-source cloud computing software, and other relevant actions.

This report documents the cross industry expert collaboration to inform CSRIC VIII on Recommendations on the role of the FCC in promoting the availability of standards for more secure, reliable 5G environment through the use of virtualization and cloud-native technologies. This set of recommendations is informed by the US National Cybersecurity Strategy published on March 2, 2023[2].

To effectively tackle this extensive and intricate subject matter, the report has organized its chapters to align with the four critical inquiries presented by the FCC. Chapter 8 further consolidates these insights into aggregate recommendations, providing a comprehensive overview of the report's findings.

Chapter 4	Steps that the FCC should take (if any) to help coordinate formal standards, informal standards, and any collaborative open-interface community efforts to ensure interoperability in the virtualized 5G space.
Chapter 5	Recommendations on how the FCC can promote collaborations to achieve innovation in virtualized 5G.
Chapter 6	Recommendations on actions the FCC can take to build confidence in virtualized 5G solutions based upon open-source cloud computing software.
Chapter 7	Any other ways in which FCC can promote a diverse, competitive 5G environment.
Chapter 8	Recommendations.

2.1 CSRIC Structure

[2] U.S. Department of State, *Announcing the Release of the Administration's National Cybersecurity Strategy*, (March 2, 2023), https://www.state.gov/announcing-the-release-of-the-administrations-national-cybersecurity-strategy/

CSRIC VIII was established at the direction of the Chairperson of the Federal Communications Commission (FCC) in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App. 2. The purpose of CSRIC VIII is to provide recommendations to the FCC regarding ways the FCC can strive for security, reliability, and interoperability of communications systems. CSRIC VIII's recommendations will focus on a range of public safety and homeland security-related communications matters. The FCC created informal subcommittees under CSRIC VIII, known as working groups, to address specific tasks. These working groups must report their activities and recommendations to the Council as a whole, and the Council may only report these recommendations, as modified or ratified, as a whole, to the Chairperson of the FCC.

Communications Security, Reliability, and Interoperability Council (CSRIC) VIII					
CSRIC VIII Working Groups					
Working Group 1: 5G Signaling Protocols Security	Working Group 2: Promoting Security, Reliability, and Interoperability of Open Radio Access Network Equipment	Working Group 3: Leveraging Virtualization Technology to Promote Secure, Reliable 5G Networks	Working Group 4: 911 Service Over Wi-Fi	Working Group 5: Managing Software & Cloud Services Supply Chain Security for Communications Infrastructure	Working Group 6: Leveraging Mobile Device Applications and Firmware to Enhance Wireless Emergency Alerts
Co-chairs: Brian Daly, AT&T & Travis Russell, Oracle	Co-chairs: Mike Barnes, Mavenir & George Woodward, RWA	Co-chairs: Micaela Giuhat, Microsoft & John Roese, Dell	Co-chairs: Mary Boyd, Intrado & Mark Reddish, APCO	Co-chairs: Todd Gibson, T-Mobile and Padma Sudarsan, VMware	Co-chairs: Farrokh Khatibi, Qualcomm & Francisco Sanchez, SBA
FCC Liaison: Ahmed Lahjouji	FCC Liaison: Zenji Nakazawa	FCC Liaison: Jeff Goldthorp	FCC Liaison: Rasoul Safavian	FCC Liaison: Zenji Nakazawa	FCC Liaison: James Wiley, Tara Shostek

Table 2-1 - Working Group Structure

2.2 Working Group 3 Team Members

Working Group 3 consists of the members listed below.

Name	Company
Marla Dowell	NIST
Andrew Drozd	ANDRO Computational Solutions, LLC
Bob Everson	Cisco
Michael Gallagher	Verizon
Micaela Giuhat	Microsoft Corporation
Martin Goldberg	National Security Agency (NSA)
Jeff Goldthorp	FCC
Javed Khan	Altiostar Networks

Douglas Knisely	Qualcomm Incorporated
Jennifer Manner	CSRIC Access
Serge Manning	T-Mobile USA
Timothy May	NTIA
Martin McGrath	Nokia
William Mikucki	Comtech Telecommunications Corp.
Keith O'Brien	Palo Alto Networks
Jitendra Patel	AT&T
Leo Popokh	Hewlett Packard Enterprise
John Roese	Dell Technologies
Tom Sawanobori	CTIA
Scott Poretsky	Ericsson
Jane Shen	Mavenir
Santiago Rodriguez	Motorola Solutions
Frank Suraci	Cybersecurity and Infrastructure Security Agency (CISA ECD)
Peter Tomczak	FirstNet
Claire Vishik	Intel Corporation
Damien Whaley	Cox Communications
George Woodward	Rural Wireless Association

Table 2-2 - List of Working Group Members

Alternates for members are listed below.

Name	Company
Reza Arefi	Intel Corporation
Kevin Green	FirstNet
Bryan Larish	Verizon
Doug Montgomery	NIST
Vishwamitra Nandlall	Dell Technologies
Stere Preda	Ericsson
Rowland Shaw	Dell Technologies
Matthew Sneed	EchoStar
Darrell Stogner	Motorola Solutions
Ryan Stokes	Rural Wireless Association
Megan Stapleton	Comtech Telecommunications Corp.
Richard Tenney	Cybersecurity and Infrastructure Security Agency (CISA ECD)
Afeite Dadja	CTIA
Timothy Woods	ANDRO Computational Solutions, LLC

Table 2-3 - List of Working Group Alternates

2.3 Subject Matter Expert Contributors

Name	Company
Michael Gallagher	Verizon

Table 2-3 - List of Subject Matter Experts

3 Objective, Scope, and Methodology

3.1 Objective

The Chairwoman of the FCC directs CSRIC VIII to develop recommendations on how virtualization technology can be used to promote the availability of secure, reliable 5G technologies and services solutions from a diverse market of 5G equipment vendors.
Most 5G network product sets are vertically integrated and proprietary - factors that contribute to important communications supply chain risks.
CSRIC VIII will develop recommendations for how vendor-agnostic, horizontal stack solutions for 5G can be promoted to foster a diverse, competitive, and more secure 5G environment despite the wider attack surface presented. These recommendations should address ways to provide opportunities for smaller vendors that cannot yet manufacture all parts of a vertically integrated, traditional 5G stack.

3.2 Scope

The objective is to be addressed in two reports and should be read in conjunction with CSRIC VIII WG2.

The first report on How Virtualization Technologies can be Used to Promote 5G Security and Reliability, for CSRIC VIII included recommendations on:

- Ways in which funding and non-funding methods can be deployed to promote virtualized environments that result in improved 5G security and reliability.
- Recommendations on ways to promote and overcome obstacles and increase 5G vendor diversity for virtualized systems including Distributed Unit (DU), Central Unit (CU), Radio Unit (RU)Radio Access Networks (RAN) and Service Based Architectures (SBA).
- Best practices for reliability and interoperability by enabling the 5G ecosystem to be open and create interworking between small and large vendors in the same 5G system. These recommendations should also broadly focus on reducing the cost of entry for 5G and making it more accessible to smaller adopters of the technology.
- CSRIC VIII will also identify whether any additional work is needed from a broad landscape of IT, Cloud and Telecom standards and initiatives that virtualized 5G is dependent on.

This second report on Recommendations on the Role of the FCC in Promoting the Availability of Standards for More Secure, Reliable 5G Environment Through the Use of Virtualization Technology, for CSRIC VIII includes recommendations on:

- Steps that the FCC should take (if any) to help coordinate formal standards, informal standards, and any collaborative open-interface community efforts to ensure interoperability in the virtualized 5G space
- Recommendations on how the FCC can promote collaborations to achieve innovation in virtualized 5G
- Recommendations on actions the FCC can take to build confidence in virtualized 5G solutions based upon open-source cloud computing software
- Any other ways in which FCC can promote a diverse, competitive 5G environment.

3.3 Methodology

CSRIC VIII WG3 is comprised of numerous industry experts across the domains of Telecom, Wireless, IT, and Security from both the demand and supply sides. For the purposes of this CSRIC VIII report, the deep technical insight and knowledge of the team was elevated to provide policy level insight.

Specifically, the team:

- Generated and published a first report titled "The Communications Security, Reliability and Interoperability Council VIII Report on How Virtualization Technologies Can be Used to Promote 5G Security and Reliability" which:
  - Reviewed industry lessons learned from the use of virtualization and increased vendor diversity in strengthening security, increasing competition, and creating a more secure supply chain. Gathered insights and input from researchers, technologists, thought leaders and standards development organizations on availability of solutions, and technical issues to be addressed. Performed an assessment of implementation best practices and reviewed results from test labs or real-life deployments around the world. Performed comparison between virtualized and non-virtualized security vulnerabilities in a 5G network. Identified issues to be addressed by the commission and provided high level recommendations on how best to support a secure diverse vendor ecosystem.

    This second report should be considered as a continuation of our previous work, with a specific emphasis on addressing the four questions posed by the FCC. In Chapter 8, we have compiled a comprehensive set of recommendations that build upon our earlier findings and insights.

4 Steps that the FCC should take (if any) to help coordinate formal standards, informal standards, and any collaborative open-interface community efforts to ensure interoperability in the virtualized 5G space

The virtualized 5G space is seeing the emergence of many standards bodies working to ensure interoperability. While 3GPP and the O-RAN Alliance are the most significant standards-setting bodies in the 5G virtualized RAN/Open RAN spaces, there are diverse groups, including ATIS, IETF, ETSI, NIST, GSMA, Small Cell Forum, and many more, working collaboratively to build upon each other's work. This process has been successful in driving innovation and joint commitment of the industry towards this important technology. Therefore, we recommend that the FCC refrain from direct involvement in the standards development process, except through the facilitation of rules that encourage ecosystem development inclusive of virtualized environments which include the setting of RAN and Open RAN-friendly spectrum policies.

However, we recommend that the FCC closely monitor relevant standards development forums and understand their implications, especially regarding standards impacting open-source technologies. To achieve this, the FCC should collaborate with industry, outside parties, including the FCC TAC and NIST, to identify the most relevant standards bodies and the most efficient way to stay abreast of their progress. The FCC should track the standards' development and be able to understand their implications.

As the FCC understands these implications, it should encourage relevant Executive Branch agencies and Congress to incentivize US participation and leadership in standards bodies, consistent with the US Government National Standards Strategy for Critical and Emerging Technology. For instance, correcting

the disincentive in US tax policies with regard to R&D tax credits for international standards work, which is currently limited to domestic work[3], would be a step in the right direction.

5 Recommendations on how the FCC can promote collaborations to achieve innovation in virtualized 5G.

The ecosystem required to foster innovation in virtualized 5G technologies necessitates multiple communities to collaborate in a more direct and cohesive manner than they typically do presently. These communities include:

- **Users** – who must be able to articulate current and future requirements for network capabilities and properties (e.g., security, resilience, performance) in technology agnostic terms to shape the future research directions, and technology specific terms to enable precise acquisition of the systems and services necessary to meet current needs.
- **Standards and Guidance Developers** – who develop base technology standards and policy guidance / requirements that refine / enhance base specifications for specific use cases and user groups.
- **Open-Source Developers** – who evolve and maintain the open-source platforms and oversee the life cycle management of a sustained community resource.
- **Vendors / Operators** – who develop and deploy commercial platforms and services in response to business demands and applicable standards.
- **Testers** – who provide test and measurement tools and services to characterize virtualized network technologies along various dimensions.
- **Researchers** – who lead the design and evaluation of fundamentally new virtualized network technologies typically guided by the programmatic objectives of their respective funding organizations.

Many of these communities collaborate today. For example, other sections of this report discuss the important role of open-source platforms to foster innovation and diversity in vendor and operator community. But in most cases the collaboration and/or influence between groups is somewhat haphazard and lacks a sustained focus and/or resources necessary to ensure and institutionalize processes that would lead to richer collaboration and expedited innovation.

Specific examples of opportunities for enhanced collaboration include:

1. Establishing means to facilitate user groups, vendors, and standards / guidance developers to share advanced requirements / open issues with the research funding organizations to help shape the direction of future research.
2. Establishing means to facilitate enhancement of select open-source platforms to implement key standards and/or specific capabilities called out in subsequent guidance documents.
3. Establish means to facilitate a rich testing ecosystem of tools, test specifications and testing services that are accessible to the user, open-source, and research community as well as the vendor and operator community.
4. Establish means to facilitate direct contributions of the research community to standards development and established open-source communities.

[3] *IRS Sec 41, Credit for increasing research activities,* https://www.irs.gov/pub/irs-regs/research_credit_basic_sec41.pdf

5. Establish means to facilitate the development of acquisition profiles by user groups – enabling easy translation of specific use case requirements into technical specifications to shape the direction of product and service offerings.

In the above examples, the FCC could play a crucial role as a facilitator, bringing together relevant communities and organizations. This can be achieved through platforms like this Communications Security, Reliability, and Interoperability Council (CSRIC) or similar initiatives, with the aim of encouraging the allocation of necessary resources to establish and maintain meaningful collaborations. In most cases, other government agencies that have direct engagement with specific areas and activities will also be involved in these collaborative efforts.
An illustrative instance of a collaboration facilitated by the FCC is the promotion of partnerships between the USG standards and guidance, testing, and open-source communities. The aim being to foster the availability of open-source platforms that effectively support USG security requirements. To accomplish this objective, the FCC should undertake the following actions:

- Collaborate with industry and NIST through ATIS. Together, they should develop specifications for virtualized 5G functions and deployment environments within the United States. This collaborative effort should draw insights from resources like the National Security Agency's ESF/DHS CISA's "Security Guidance for 5G Cloud Infrastructures[4]," as well as other industry bodies such as ETSI, 3GPP, and the O-RAN Alliance.
- Work with relevant USG agencies to support the development of open-source test and evaluation tools that align with USG security requirements.
- Collaborate with relevant USG agencies to conduct testing and evaluation of specific open-source virtualization platforms, assessing their compliance with USG security requirements.
- Collaborate with relevant USG agencies to facilitate the development of enhancements for select open-source platforms, ensuring they meet the defined security requirements.

By adopting these steps, the FCC can actively contribute to the advancement of secure open-source platforms and promote collaboration among various stakeholders within the USG.

6 Recommendations on actions the FCC can take to build confidence in virtualized 5G solutions based upon open-source cloud computing software

Open-source software is an integral component to continued software innovation. According to research published last year by McKinsey & Company[5], open-source adoption was the biggest differentiator for top-performing organizations. Modern software projects are increasingly dependent on open-source software and components. This can range from whole operating systems to user interfaces, to back-end data analysis, and front-end graphics.

Like most technology and software innovations, Open-source software has some benefits and is also sometimes accompanied by security risks that must be understood and mitigated. For the most part, it is important to understand these risks apply when using any third-party software component, regardless of whether it is open-source or closed source software.

[4] *Security Guidance for 5G Cloud Infrastructures* (Dec 16, 2021), https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2875523/esf-members-nsa-and-cisa-publish-the-fourth-installment-of-5g-cybersecurity-gui/
[5] Srivastava, S., Trehan,K, Wagle, D. and Wang, J., *Developer Velocity: How software excellence fuels business performance, McKinsey & Company,* (Apr. 2020).

Open-source software lowers the barrier to entry both for consumers of the software, who may be leveraging the software to build new U.S.-based 5G products, and for contributors who wish to improve the software by adding new features, improving performance, or fixing a software defect. Open-source fundamentally enables and accelerates research and development and the creation of new technology products, which is why, according to Synopsys' 2023 Open-source Security and Risk Analysis Report, 96[6]% of new codebases include open-source software, and open-source software made up 76% of the codebases themselves. Put differently, almost all new audited software not only uses open-source, but most of the software is open-source components. This same report revealed that of the 99% of codebases containing open-source components, 49% contained high-risk vulnerabilities of which the top 10 most common high-risk vulnerabilities were in open-source components.

Mature open-source software development practices have been shown to produce more secure software. To build confidence in open-source, the FCC should encourage best security practices to ensure that the consumption of open-source software follows all the security tenets for secure software. Industry security best practices for 5G virtual and cloud infrastructure should be based upon publicly available sources, including Open Worldwide Application Security Project (OWASP) Top 10 lists, Center for Internet Security (CIS) Benchmarks, Cloud Security Alliance (CSA) Top Threats to Cloud Computing, NIST Special Publications, National Security Agency Enduring Security Framework (ESF) reports, and DHS CISA guidance. As industry increases its attention on security for open-source software in 5G critical infrastructure, software development best practices should follow NIST guidance, including the Cybersecurity Framework (CSF) and Secure Software Development Framework (SSDF).

The FCC could take several actions to promote the use of virtualized 5G solutions using open-source cloud computing software.

- Increase confidence in open-source by actively speaking to and encouraging the use of software bills of material (SBOM).
- Promote industry collaboration with the Linux Foundation[7], CNCF, and other open-source communities to ensure better incorporation of virtualized 5G use cases in their open-source initiatives.
- Solicit a mechanism for timely intervention in case of disruptive incidents caused by open-source software. This could involve assigning a new responsibility and facilitating collaboration between CISA and FCC to effectively identify and mitigate potential risks.

- Promote the availability of relevant open-source projects by providing incentives for the open-source community to create availability of open-source implementation of the 5G standards

Other possible actions:

FCC could collaborate with industry at international standards bodies to encourage open-source implementation of standards.

1. The FCC should support the establishment of a testing and validation framework that can be used to verify the performance, security, and reliability of virtualized 5G solutions using open-source cloud computing software. This framework should include a set of standard test cases that can be used to evaluate the solutions against a set of predefined criteria.

[6] Synopsys' 2023 *Open-source Security and Risk Analysis Report*, https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html
[7] *The Linux Foundation*, https://www.linuxfoundation.org/

2. Encourage a collaborative culture among developers, vendors, and users of virtualized 5G solutions using open-source implementations of relevant 5G standards. This goal can be accomplished by establishing online communities or forums where stakeholders can exchange information, work together on projects, and promote the sharing of code and other valuable resources.

3. Creating incentives for operators to adopt virtualized 5G solutions using open-source implementation of 5G standards. The FCC could help accelerate the deployment of these solutions and promote greater innovation in the 5G space. Additionally, by promoting the secure use of open-source 5G software, the FCC could help foster an ecosystem of interoperable and affordable solutions that benefit consumers and the broader economy.

7 Any other ways in which FCC can promote a diverse, competitive 5G environment

Technology ecosystems comprising small, medium, and large companies have become essential for emerging industries, particularly in virtualized 5G solutions, due to their ability to accelerate innovation, disperse costs, and reduce maintenance costs. To shift the industry from proprietary closed to open technology, several ecosystem elements are required, including technology building blocks such as the radio supply chain, operating models and practices, and business models.

To ensure the health of a virtualized 5G solution ecosystem, it should provide durably growing opportunities for its members, work efficiently, survive crises, generate innovation, and help its firms achieve financial goals better than those not in the ecosystem. Evaluating the health of the ecosystem relies on four primary categories of assessment: diversity, productivity, robustness, and security and resilience.

1. Diversity measures the ability to create value by putting new functions into operation to increase meaningful diversity in the ecosystem. Modularity and use case coverage are metrics applied in this category. Modularity promotes element standardization and “Open Interfaces,” while use case coverage captures the number, maturity, and diversity of established use cases that can be addressed by the architecture. The FCC could open a study period to open the dialog with the industry and coordinate with other USG entities to encourage the availability of open and accessible testing laboratories capable of supporting conformance, interoperability and integration testing for small companies and startups.

2. Productivity measures the return on investment, or the economic value added from tangible and intangible assets created from the development and operation of virtualized 5G equipment. Financial wellness and satisfaction are metrics applied in this category. Financial wellness measures the growth of ecosystem profits in terms of market share, while satisfaction evaluates the overall satisfaction through customer complaints, parity of features, performance, reduced operator cost of ownership, and overall ease of use for the elements in the ecosystem.

3. Robustness measures the survival rate of the ecosystem’s members, either in relation to other ecosystems or over time. Security and privacy and commercial scale are metrics applied in this category. Security and privacy evaluate the number of known vulnerabilities outstanding in the ecosystem and the ability to quickly respond to remediate any identified threat. Commercial scale addresses the scale and size of the contributing companies involved in the ecosystem.

4. The evolution of 5G critical infrastructure, including Open RAN, to virtualized and cloud-native

deployments requires a Zero Trust Architecture (ZTA) approach to security, as NSA ESF and DHS CISA describe in its series "Security Guidance for 5G Cloud Infrastructures[8]". The FCC with CISA should use their influence to encourage software vendors and operators to pursue its recommendations for a ZTA. The FCC can accelerate industry's efforts to achieve a ZTA by voicing support for standardization and innovation in areas such as continuous monitoring to detect lateral movement, secure API design, and security configuration validation and checking.

In summary, virtualized 5G solutions rely on ecosystems to meet their technological or business needs, and a healthy ecosystem can provide several advantages. Evaluating the health of the ecosystem relies on four primary categories of assessment: diversity, productivity robustness, and security and resilience, which are measured through various metrics. The work group fully recognizes that to achieve these recommendations it requires actions and participation from industry, Government, and academia.

8 Recommendations

Collectively the working group acknowledged the importance of improving the inter-agency collaboration process and recommends the creation of an effective mechanism to address this. To this end, a Memorandum of Understanding (MOU) vehicle or a similar instrument between departments can facilitate information sharing, better collaboration, and coordination. Establishing an ongoing mechanism can provide a framework for addressing gaps and ensure continuous improvement. It is important to note that the FCC cannot solely solve this problem and hence requires a collective effort from all stakeholders.

To help coordinate formal standards, informal standards, and any collaborative open-interface community efforts to ensure interoperability in the virtualized 5G space the FCC should:

1. Establish sustained collaboration with industry, outside parties, including the FCC TAC and NIST, to identify relevant standards bodies and how to stay informed of their progress and understand their implications.
2. Encourage relevant Executive Branch agencies and Congress to incentivize US participation and leadership in standards bodies consistent with The US Government National Standards Strategy for Critical and Emerging Technology[9].
3. The disincentive in US tax policies about R&D tax credits for international standards work should be corrected to encourage US participation in standards bodies.

The FCC can promote collaborations to achieve innovation in the virtualized 5G ecosystem necessary to support innovation across the somewhat disjointed communities to collaborate in more direct and sustained ways than they typically do today by:

1. Establishing means to facilitate user groups, vendors, and standards / guidance developers to share advanced requirements / open issues with the research funding organizations to help shape the direction of future research.
2. Establishing means to facilitate enhancement of select open-source platforms to implement key standards and/or specific capabilities called out in subsequent guidance documents.

[8] *NSA and CISA provide cybersecurity guidance for 5G cloud infrastructures* (Oct. 28, 2021) https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2825412/nsa-and-cisa-provide-cybersecurity-guidance-for-5g-cloud-infrastructures/

[9] *The US Government National Standards Strategy for Critical and Emerging Technology*, (May 2023) https://www.whitehouse.gov/wp-content/uploads/2023/05/US-Gov-National-Standards-Strategy-2023.pdf

3. Establish means to facilitate a rich testing ecosystem of tools, test specifications and testing services that are accessible to the user, open-source, and research community as well as the vendor and operator community.
4. Establish means to facilitate direct contributions of the research community to standards development and established open-source communities.
5. Establish means to facilitate the development of acquisition profiles by user groups – enabling easy translation of specific use case requirements into technical specifications to shape the direction of product and service offerings.

For actions the FCC can take to build confidence in virtualized 5G solutions based upon open-source cloud computing software they could:

1. Support the establishment of a testing and validation framework that can be used to verify the performance, security, and reliability of virtualized 5G solutions using open-source cloud computing software. This framework should include a set of standard test cases that can be used to evaluate the solutions against a set of predefined criteria.

2. Foster and where applicable coordinate a culture of collaboration among developers, vendors, and users of virtualized 5G solutions using open-source implementation of 5G standards. This can be achieved by supporting online communities or forums where stakeholders can share information and collaborate on projects, and by encouraging the sharing of code and other resources.

3. Creating incentives for network operators to adopt virtualized 5G solutions using open-source implementation of 5G standards. The FCC could help accelerate the deployment of these solutions and promote greater innovation in the 5G space. Additionally, by promoting the use of open-source 5G software, the FCC could encourage an ecosystem of interoperable and affordable solutions that benefit consumers and the broader economy.

To further promote a diverse and competitive 5G environment, the FCC can enhance its approach by considering the overall health of the virtualized 5G solutions ecosystem in regulatory motions. Evaluating the ecosystem's health involves assessing four key categories: diversity, productivity, robustness, and security, and resilience, using a range of metrics. The work group fully recognizes that to achieve this requires actions and participation from industry, Government, and academia.

9 Conclusion

During the process of developing the report and formulating recommendations, extensive deliberations took place regarding the optimal implementation and deployment of recommendations falling within the remit of the FCC. These considerations were juxtaposed with industry-wide type recommendations to ensure enhanced outcomes. Consequently, the work group decided to emphasize the significant value of the CSRIC programs and urge the FCC to persist in pursuing this path, while simultaneously expanding participation, particularly in response to emerging inter-agency dynamics across these complex and converged technology ecosystems and solutions.

10 Appendix A – Glossary of Acronyms

Abbreviation	Definition
3GPP	3rd Generation Partnership Project, https://www.3gpp.org/
5G	Fifth Generation
AI/ML	Artificial Intelligence / Machine Learning
API	Application Programming Interface
CISA	Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/
CONUS	Continental United States
CSRIC	Federal Communications Commission's Communications Security, Reliability, and Interoperability Council
DHS	Department of Homeland Security https://www.dhs.gov/
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FCC TAC	FCC Technological Advisory Council https://www.fcc.gov/general/technological-advisory-council
GSMA	Global System for Mobile Communications Association, https://www.gsma.com/
IETF	Internet Engineering Task Force, https://www.ietf.org/
NFV	Network Function Virtualization
NIST	National Institute of Standards and Technology, https://www.nist.gov/
OCONUS	Outside of the Continental United States
ORAN	Open Radio Access Network
RAN	Radio Access Network
RF	Radio Frequency
R&D	Research and Development
SDO	Standards Developing Organization
TAC	Technical Advisory Council
USG	United States Government
VNF	Virtual Network Function
ZT	Zero Trust
ZTA	Zero Trust Architecture