Q.1 Name :

Total responses 3

Total skipped 0

Ahmed Omer

Dr Hazza Alshamsi

Subasic Bojan

Q.2 Email :

Total responses 3

Total skipped 0

ahmed.omer@apple.com

h.alshamisi@adpolice.gov.ae

Bojan.subasic@urbanandmainlines.com

Q.3 Organization and position :

Total responses 3

Total skipped 0

Apple Product Regulatory Compliance

Abu Dhabi Police GHQ

Design Authority Telecom

Q.4 **What are the key factors that have influenced the deployment of private 5G networks in other Countries/regions?**

Total responses 2

Total skipped 1

1. The deployment of private 5G networks for public safety and police forces in various countries and regions has been influenced by several key factors: 1. Spectrum Availability and Regulation: o Spectrum Allocation: Availability of dedicated spectrum for public safety use is crucial. Regulatory Authority need to allocate specific bands that can be used exclusively for public safety purposes. o Regulatory Support: Favorable regulatory frameworks that support the deployment and operation of private 5G networks are essential. 2. Collaboration and Partnerships: o Inter-agency Cooperation: Effective communication and collaboration between various public safety agencies (e.g., police, fire departments, emergency medical services) are necessary for a unified approach to network deployment and usage. 3. Use Cases and Applications: o Critical Use Cases: Identifying and prioritizing critical use cases such as real-time video surveillance, situational awareness, drone-based monitoring, mission-critical push-to-talk (MCPTT) services and assist first responder with critical information. o Innovative Applications: Leveraging 5G capabilities for emerging applications such as augmented reality for training and operations, autonomous vehicles, and smart city integrations enhances the network's value. 4. Technology and Infrastructure: o Advanced Technology: Utilization of advanced technologies such as network slicing, edge computing, and enhanced security features ensures that the network meets the high reliability and low latency requirements of public safety applications and provide ease of deployment for last mile first responder. 5. Cybersecurity and Data Privacy: o Robust Security Measures: Ensuring robust cybersecurity measures to protect sensitive data and maintain the integrity of public safety operations is paramount. o Data Privacy Regulations: Adhering to data privacy regulations and ensuring that personal data is protected and handled responsibly. Examples of countries that have made significant strides in deploying private 5G networks for public safety include the United States, South Korea, Japan, and several European nations such as the United Kingdom and Germany. These deployments often serve as benchmarks for other regions considering similar initiatives.

2. Performance, standardization, security

Q.5 **Can you provide examples of successful private 5G network deployments and the technologies used?**

Total responses 2

Total skipped 1

1. United States: New York Police Department (NYPD) Deployment Overview: • The NYPD has been piloting private 5G networks to enhance their communication and operational capabilities. This initiative includes the deployment of 5G infrastructure in key areas of the city. Technologies Used: • Network Slicing: To provide dedicated and secure bandwidth for different public safety applications.

• Edge Computing: To enable real-time data processing and reduce latency for critical applications such as live video streaming from body cameras and drones. • Enhanced Mobile Broadband (eMBB): To support high-speed data transfer for applications like HD video surveillance and data sharing between officers in the field. 2. United Kingdom: Emergency Services Network (ESN) Deployment Overview: • The UK's Emergency Services Network (ESN) is transitioning to a 4G LTE-based network with plans to integrate 5G capabilities. This network will support police, fire, and ambulance services across the country. Technologies Used: • Mission-Critical Push-to-Talk (MCPTT): For reliable voice communication among emergency responders. • Internet of Things (IoT) Devices: Such as connected sensors and wearable technology to monitor the health and location of officers. • Enhanced Security Protocols: To ensure data integrity and protection from cyber threats. 3. South Korea: Seoul Metropolitan Police Agency Deployment Overview: • South Korea has been at the forefront of 5G technology adoption. The Seoul Metropolitan Police Agency has implemented a private 5G network to support various smart policing initiatives. Technologies Used: • Artificial Intelligence (AI) and Machine Learning (ML): For real-time crime prediction and data analysis. • Smart Surveillance Systems: Incorporating facial recognition and anomaly detection to enhance situational awareness. • Autonomous Drones: For monitoring large public gatherings and providing aerial support during emergencies. 4. Japan: Tokyo Metropolitan Police Department Deployment Overview: • The Tokyo Metropolitan Police Department has been leveraging private 5G networks to improve their operational efficiency and response times. Technologies Used: • Augmented Reality (AR): For training and situational awareness, providing officers with real-time information overlays during operations. • Vehicle-to-Everything (V2X) Communication: To enhance the coordination of patrol cars and other emergency vehicles. • High-Definition (HD) Video Streaming: For live monitoring and rapid sharing of critical information during incidents. 5. Germany: Bavarian Police Deployment Overview: • The Bavarian Police have implemented a private 5G network to support their public safety operations, particularly in urban areas like Munich. Technologies Used: • Edge Computing and IoT: For managing smart city infrastructure and integrating public safety applications. • Next-Generation GIS (Geographic Information Systems): To provide real-time mapping and tracking of incidents and resources. • Robust Encryption Standards: To ensure secure communication and data exchange within the network. These examples illustrate how advanced technologies such as AI, edge computing, IoT, and enhanced security protocols are being integrated into private 5G networks to support public safety and police operations. The successful deployment of these networks relies on a combination of technological innovation, strategic partnerships, and robust regulatory frameworks.

2. Urban Railway CBTC

Q.6 **What best practices (regulatory model) should be considered for deploying private 5G networks in the UAE?**

Total responses 2

Total skipped 1

1. Deploying private 5G networks in the UAE involves considering best practices and regulatory models. Here are some best practices to consider: 1. Spectrum Allocation and Management • Dedicated Spectrum Bands: Allocate specific frequency bands for public safety use to avoid

interference with commercial networks. • Regulatory Framework: Establish clear regulations governing the use of the allocated spectrum, ensuring it is used efficiently and effectively. 4. Cybersecurity and Data Privacy • Robust Security Protocols: Implement strong encryption and authentication mechanisms to protect sensitive data. • Regular Audits and Assessments: Conduct regular security audits and assessments to identify and mitigate potential vulnerabilities. • Data Privacy Regulations: Ensure compliance with data privacy laws and regulations to protect citizens' personal information. 6. Training and Capacity Building • Regular Training Programs: Conduct regular training programs for police officers and other public safety personnel on the use and benefits of the 5G network. Regulatory Model Examples 1. United States: FirstNet • FirstNet Authority: An independent authority within the U.S. Department of Commerce to oversee the deployment and operation of a nationwide public safety broadband network. • Public Safety Advisory Committee (PSAC): Involves stakeholders from various public safety disciplines to provide input and guidance. 2. United Kingdom: Emergency Services Network (ESN) • Home Office Oversight: The UK Home Office oversees the ESN, ensuring it meets the needs of all emergency services. • Strategic Supplier Partnerships: Partnerships with telecom providers and technology firms to deliver and maintain the network. 3. South Korea: Public Safety LTE (PS-LTE) • Ministry of the Interior and Safety: Oversees the deployment and operation of PS-LTE, ensuring interoperability and compliance with national standards. • Integrated Approach: Combines LTE and 5G technologies to provide robust and reliable communication services.

2. Lightly licensed model

Q.7 **How do these private 5G deployments ensure high Quality of Service (QoS) and what metrics are used to measure it?**

Total responses 2

Total skipped 1

1. Ensuring high Quality of Service (QoS) in private 5G deployments is crucial for maintaining the reliability and efficiency required for public safety operations. Here are the strategies and metrics used to ensure and measure QoS: Strategies for Ensuring High QoS 1. Network Slicing: o Dedicated Slices: Allocate dedicated network slices for different public safety applications to ensure they receive the required resources and bandwidth. o Priority Levels: Implement priority levels within slices to ensure critical communications are given precedence over less critical data. 2. Edge Computing: o Local Processing: Deploy edge computing nodes to process data locally, reducing latency and improving response times for mission-critical applications. o Data Offloading: Offload less critical data processing to the edge, freeing up core network resources for high-priority tasks. 3. Advanced Traffic Management: o Dynamic Resource Allocation: Use AI and machine learning algorithms to dynamically allocate network resources based on real-time demand and priority. o Quality Monitoring: Continuously monitor network traffic to detect and address congestion, ensuring smooth operation during peak usage. 4. Redundancy and Reliability: o Redundant Infrastructure: Implement redundant network components to ensure continuous operation in case of failures. o Failover Mechanisms: Establish automatic failover mechanisms to switch to backup systems seamlessly if primary systems fail. Metrics for Measuring QoS 1. Latency: o Round-Trip Time (RTT): Measure the time it takes for data to travel from the source to the destination and back. o

Application-Specific Latency: Monitor latency for specific applications such as video streaming or voice communication to ensure they meet the required thresholds. 2. Throughput: o Data Transfer Rate: Measure the amount of data transmitted successfully over the network per second. o Application Throughput: Assess throughput for critical applications to ensure they receive sufficient bandwidth. 3. Reliability: o Uptime: Track the percentage of time the network is operational and available. o Mean Time Between Failures (MTBF): Measure the average time between network failures to assess reliability. 4. Packet Loss: o Packet Delivery Ratio: Measure the percentage of packets successfully delivered compared to those sent. o Application Impact: Evaluate the impact of packet loss on specific applications, especially those requiring high reliability. 5. Jitter: o Variation in Latency: Measure the variation in packet arrival times, which can affect real-time applications like voice and video. o Consistent Performance: Ensure jitter remains within acceptable limits to maintain application performance. 6. Availability: o Service Availability: Measure the percentage of time the network services are available and accessible to users. o Redundancy Effectiveness: Assess the effectiveness of redundancy mechanisms in maintaining service availability. 7. User Experience: o Quality of Experience (QoE): Gather feedback from users on their experience with the network, including aspects like clarity of voice calls, quality of video streams, and overall satisfaction. o Service Level Agreements (SLAs): Monitor compliance with SLAs that define the expected QoS parameters and performance levels. 8. Response Times: o Emergency Response Time: Measure the time taken to respond to emergencies, leveraging the 5G network for communication and coordination. o Incident Resolution Time: Track the time taken to resolve incidents from the moment they are reported until they are closed.

2. Latency, jitter, handover kpi’s

Q.8 **What are the challenges of utilizing the existing non-private (commercial) 5G networks?**

Total responses 2

Total skipped 1

1. Utilizing existing non-private (commercial) 5G networks for public safety and police operations presents several challenges. These challenges primarily relate to security, reliability, priority access, and customization needs specific to public safety operations. Here are the key challenges: 1. Security Concerns • Data Privacy: Public safety operations often involve sensitive and confidential information. Commercial networks may not provide the same level of data privacy and security as private networks. • Cybersecurity Risks: Commercial networks are more susceptible to cyberattacks, which can compromise the integrity and availability of public safety communications. 2. Reliability and Resilience • Network Congestion: During emergencies or large public events, commercial networks can become congested, leading to degraded service quality and potential communication failures. • Service Outages: Commercial networks may experience outages due to maintenance, technical issues, or other factors, which can be unacceptable for critical public safety operations. 3. Priority Access • Lack of Priority: In commercial networks, public safety communications may compete with regular consumer traffic. Ensuring priority access for emergency services can be challenging without dedicated network slices. • Preemption Issues: Preempting commercial traffic to prioritize public safety communications can be difficult to implement and manage effectively on

commercial networks. 4. Customization and Control • Limited Customization: Commercial networks are designed to cater to a wide range of users and applications, limiting the ability to customize network configurations specifically for public safety needs. • Control and Management: Public safety agencies may have limited control over network management, making it harder to ensure the network meets their specific operational requirements. 5. Quality of Service (QoS) • Inconsistent QoS: Ensuring consistent QoS for public safety applications can be challenging on commercial networks, especially during peak usage times. • Latency and Jitter: Commercial networks may not always meet the low latency and jitter requirements necessary for real-time applications like video surveillance and mission-critical push-to-talk (MCPTT). 6. Interoperability and Integration • Compatibility Issues: Integrating public safety applications with commercial network infrastructure can pose compatibility issues. • Standardization: Commercial networks may not fully comply with the specific standards and protocols required for public safety communications, such as those set by 3GPP for mission-critical services. 7. Economic Considerations • Cost of Services: Using commercial networks for public safety communications can incur significant ongoing costs, especially for dedicated or priority services.

2. Security, nw parameters not optimized for mission critical services like cbtc

---

Q.9 **What are the main regulatory challenges associated with deploying private 5G networks in the UAE?**

Total responses 2

Total skipped 1

1. Spectrum Availability: Ensuring the availability of suitable spectrum bands for private 5G networks without causing interference with existing commercial networks and other private networks.

2. No frequency band allocation, no clear rules

Q.10

How can the current telecommunications regulatory framework be improved to facilitate private 5G network deployment?

Total responses 2

Total skipped 1

1. Improving the Telecommunications and Digital Government Regulatory Authority (TDRA) regulatory framework in the UAE to facilitate private 5G network deployment involves several key areas. These include spectrum management, security and privacy and infrastructure regulations. Align the regulatory framework with the UAE's broader digital transformation goals and Vision 2021 objectives, ensuring that private 5G networks contribute to the country's strategic ambitions.

2. Analyze and apply models from other countries

Q.11

Are there any specific compliance requirements that must be addressed to facilitate the deployment of private 5G networks?

Total responses 2

Total skipped 1

1. Yes, deploying private 5G networks involves adhering to several specific compliance requirements to ensure security, reliability, interoperability, and alignment with national and international standards. Here are the key compliance requirements: 1. Spectrum Compliance • Spectrum Licensing: Obtain the necessary spectrum from TDRA. • Interference Management: Ensure compliance with regulations to prevent harmful interference with other spectrum users. This may involve coordination with other spectrum holders and adherence to technical specifications. 2. Security and Privacy Compliance • Encryption and Authentication: Implement strong encryption and authentication mechanisms to protect data integrity and prevent unauthorized access. • Data Privacy Laws: Comply with data privacy regulations to ensure the protection of personal and sensitive information transmitted over the network. This includes adherence to the UAE's data protection laws and any relevant international standards. • Security Audits: Conduct regular security audits and assessments to identify and mitigate potential vulnerabilities. Compliance with standards such as ISO/IEC 27001 (Information Security Management) may be required. 3. Technical and Operational Standards • 3GPP Standards: Adhere to 3rd Generation Partnership Project (3GPP) standards for 5G networks, ensuring interoperability and compatibility with other networks and devices. • ITU Regulations: Follow International Telecommunication Union (ITU) regulations and recommendations for radio communications and network operations. • QoS Requirements: Meet Quality of Service (QoS) requirements as specified by the TDRA, including metrics for latency, throughput, reliability, and availability.

2. Full 3GS compliance, local spectrum policy and rules

Q.12 **How will you distinguish and segregate between the different private networks? What is the mechanism used?**

Total responses 2

Total skipped 1

1. 1. Dedicated Private MNC: • Networks that use a specific MNC allocated exclusively for private network purposes. 2. Dedicated Spectrum: • Networks that use spectrum specifically allocated for private network use. • These allocations are often made by regulatory bodies to ensure that the private network has exclusive use of the spectrum, without interference from other users.

2. Non networks are not providing service to public, commercial users

Q.13 **Is a Public Land Mobile Network ID (PLMNID) necessary for private 5G networks in the UAE, and how should it be managed?**

Total responses 2

Total skipped 1

1. Whether a PLMNID is necessary for a private 5G network in the UAE depends largely on its operational scope and requirements. For purely internal deployments without shared access or roaming needs, a PLMNID may not be mandatory. However, if the network requires interaction with public networks or operates in shared environments, obtaining and managing a PLMNID becomes crucial for regulatory compliance, network identification, and interoperability purposes. Operators should consult with TDRA and adhere to local regulations to determine the specific requirements and procedures for managing PLMNIDs in the UAE.

2. Yes, follow ITU recommendations

Q.14

How will such PLMNID be utilized? What is the expected demand on such resources? Provide your recommended reuse mechanism of such resources if applicable

Total responses 2

Total skipped 1

1. A Public Land Mobile Network ID (PLMNID) is utilized primarily for identification and routing purposes within mobile telecommunications networks.

2. 3GS Rel 17 methodology and ITU

Q.15 **What measures should be implemented to ensure data security and privacy in private 5G networks?**

Total responses 2

Total skipped 1

1. Ensuring robust data security and privacy in private 5G networks involves implementing comprehensive measures across various aspects of network infrastructure, operations, and compliance. Here are key measures that should be considered: 1. Encryption and Authentication • End-to-End Encryption: Encrypt data both in transit and at rest to protect against unauthorized access and interception. • Strong Authentication: Implement multi-factor authentication (MFA) and strong password policies to secure access to network resources and devices. 2. Access Control and Authorization • Role-Based Access Control (RBAC): Define and enforce access policies based on roles and responsibilities within the organization. • Least Privilege Principle: Limit access permissions to only those necessary for individuals to perform their duties. 3. Network Segmentation and Isolation • Virtual Private Networks (VPNs): Use VPNs to create secure tunnels for data traffic between different parts of the network and remote devices. • Network Slicing: Segment the network into virtual slices with dedicated resources and security policies for different applications or user groups. 4. Security Monitoring and Incident Response • Real-Time Monitoring: Implement continuous monitoring of network traffic, devices, and systems for suspicious activities or anomalies. • Incident Response Plan: Develop and regularly update a plan to quickly respond to security incidents, including containment, mitigation, and recovery procedures. 5. Data Protection and Privacy Compliance • Compliance Frameworks: Adhere to relevant data protection regulations and frameworks such as GDPR, UAE Data Protection Law, and industry-specific standards. • Data Minimization: Collect and retain only necessary data, and anonymize or pseudonymize where possible to reduce privacy risks. 6. Physical Security and Environmental Controls • Secure Facilities: Ensure physical security measures are in place to protect network infrastructure and sensitive data storage locations. • Environmental Monitoring: Monitor environmental factors such as temperature and humidity to ensure optimal operation of equipment and prevent physical tampering. 7. Vendor and Supply Chain Security • Vendor Risk Management: Assess and manage security risks associated with third-party vendors and suppliers, including contractual obligations for security practices. • Supply Chain Integrity: Verify the security posture of components and software used in the network to prevent supply chain attacks. 8. Employee Training and Awareness • Security Awareness Programs: Conduct regular training sessions to educate employees about security best practices, phishing awareness, and incident reporting procedures. • Role-Specific Training: Provide specialized training for IT and security teams on managing 5G-specific security challenges. 9. Audits and

Compliance Assessments • Regular Audits: Conduct periodic security audits and vulnerability assessments to identify and address potential weaknesses in the network infrastructure. • Compliance Checks: Ensure ongoing compliance with security standards and regulatory requirements through regular assessments and certifications. By implementing these measures, operators of private 5G networks can enhance data security, protect user privacy, and build trust among stakeholders, ensuring the network remains resilient against evolving cyber threats and regulatory scrutiny.

2. Integrity, cyphering, authentication must be turned on

Q.16 **What are the preferred frequency bands for deploying private 5G networks in the UAE, and what is the expected bandwidth (BW) for these networks?**

Total responses 1

Total skipped 2

1. N78/77, n79, 50-100Mhz

Q.17 **What are the most promising use cases for private 5G networks in the UAE?**

Total responses 2

Total skipped 1

1. PowerPoint presentation attached. (Confidential)

2. Public transportation, industry 4.0, oil&gas

Q.18

How can private 5G networks drive business innovation and growth in the UAE?

Total responses 2

Total skipped 1

1. PowerPoint presentation attached. (Confidential)

2. New capabilities

Q.19 **Which industries or sectors would benefit the most from private 5G networks, and how?**

Total responses 2

Total skipped 1

1. PowerPoint presentation attached. (Confidential)

2. Public transportation cbtc, mission critical voice and data, remote driving

---

Q.20 **What are the anticipated infrastructure costs for deploying private 5G networks?**

Total responses 2

Total skipped 1

1. (Confidential)

2. Depend on size and type of deployment

Q.21 **What are the expected operational costs and ongoing expenses?**

Total responses 2

Total skipped 1

1. (Confidential)

2. <15

Q.22 **What regulatory and compliance costs should be considered?**

Total responses 2

Total skipped 1

1. (Confidential)

2. <10k usd

Q.23 **What are the potential revenue streams and business models for private 5G networks?**

Total responses 2

Total skipped 1

1. (Confidential)

2. Internal use

Q.24

What technical challenges might impact the economic viability of private 5G networks?

Total responses 2

Total skipped 1

1. (Confidential)

2. Qualified personal

Q.25 How should security and data privacy concerns be addressed?

Total responses 2

Total skipped 1

1. (Confidential)

2. Government audits

Q.26 What are your overall impressions of the proposed deployment of private 5G networks in the UAE?

Total responses 2

Total skipped 1

1. The proposed deployment of private police 5G networks in the UAE represents a strategic initiative aimed at enhancing public safety, operational efficiency, and emergency response capabilities. Private police 5G networks in the UAE holds significant potential to transform law enforcement operations, enhance public safety, and improve emergency response capabilities. Addressing challenges through comprehensive planning, stakeholder collaboration, and technological innovation will be crucial to successfully integrating these networks into the broader public safety infrastructure while ensuring privacy and security.

2. Na

Q.27 Do you have any additional recommendations or suggestions to enhance the study?

Total responses 3

Total skipped 0

1. Public regulatory allocation of an MNC, or MNCs, for private network use by enterprises within a country provides all OEM’s clear guidance on which to plan support to maximize device compatibility. In addition to requesting clear regulatory references for private network MNC's, Apple has documented network and SIM configuration guidance that ensures our devices work best on private 5G and LTE networks:
https://support.apple.com/guide/deployment/support-for-private-5g-and-lte-networks-depac6747317/web

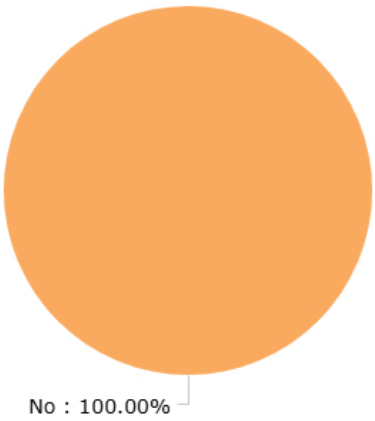
2. To enhance the study and facilitate the regularization of sideline 5G technology, consider the following additional recommendations and suggestions: 5G sidelink, also known as device-to-device (D2D) communication, is a key feature introduced in 3GPP Release 16 that enhances the capabilities of 5G networks by allowing direct communication between user devices without the need for a base station (e.g., a cell tower) to relay the information. 5G sidelink refers to a communication channel that enables direct transmission of data between devices. This capability is especially valuable in scenarios where traditional network infrastructure is unavailable, unreliable, or when low-latency communication is critical. Key Features of 5G Sidelink 1. Direct Device Communication: o Devices can communicate directly with each other, bypassing the base station, which reduces latency and enhances communication reliability in certain scenarios. 2. Enhanced Reliability: o Sidelink improves the reliability of communications, particularly in mission-critical applications such as public safety, emergency response, and vehicular communications (V2V). 3. Low Latency: o By eliminating the need to route data through a base station, sidelink communication significantly reduces the end-to-end latency, which is crucial for real-time applications. 4. Network Offloading: o Sidelink helps in offloading traffic from the core network, which can alleviate congestion and improve overall network performance. Policy and Regulatory Framework • Dedicated Sideline 5G Policy: Develop a specific policy framework tailored to sideline 5G deployments, considering their unique characteristics and operational requirements. • Regulatory Clarity: Provide clear guidelines on spectrum allocation, technical standards, and operational practices specific to sideline 5G networks. By incorporating these recommendations into the study and regulatory framework, policymakers and stakeholders can effectively regulate and promote the responsible deployment of sideline 5G technology in the UAE.

3. Na

Q.28 **Do you have any additional issues which you feel are relevant for consideration in this consultation?**

Total responses 3

Total skipped 0



No 100 %

Q.29 **Please provide specific support and/or explanation of your viewpoints as well as recommendations regarding how such issues might be resolved.**

Total responses 1

Total skipped 2

1. Na
