White Paper

Considerations for Secure and Resilient Private 5G

ATARC Secure 5G Working Group

September 2023

ATARC

Advanced Technology Academic Research Center

ATARC would like to take this opportunity to recognize the following Secure 5G Working Group members for their contributions:

Christian Williams, *General Services Administration (GSA)*

Katie Noyes, *Federal Bureau of Investigation (FBI)*

Rosie Pridemore, *MITRE*

Muddasar Ahmed, *MITRE*

Jianning Guo, MITRE

Narendra Mangra, *George Mason University*

Brian Daly, *AT&T*

Suro Sen, *Sentech Corporation*

John Cavanaugh, *Internet Infrastructure Services Corp.*

Randy Siegel, *Center Circle Consultants*

Sam Moser, *First Responder Network Authority*

Mike Vande Woude, *MVWConsultants*

Executive Summary

This executive summary provides an overview of the key considerations and recommendations for the governance of a Federal Government 5G network. As the deployment and management of 5G networks become critical for national security and economic competitiveness, it is essential for the federal government to establish effective governance mechanisms to ensure the successful implementation and operation of a secure and reliable 5G infrastructure.

In today's hyperconnected world, most people have an average of three mobile devices, with the number of network-connected devices fast approaching 29.3 billion this year, finds a report—"Accelerating enterprise innovation and transformation with 5G and Wi-Fi 6"[1] published by Deloitte. Next-generation wireless technologies such as 5G and Wi-Fi 6 are crucial parts of networks that link people and machines by offering faster speeds, higher capacity, lower latency, precision location sensing, autonomous driving, telemedicine, collaboration, and a host of new and emerging use-cases that were previously unimaginable or unachievable via legacy networks such as 4G/LTE and Wi-Fi. Today, leaders of organizations view advanced wireless technologies such as 5G and Wi-Fi 6 as foundational to their efforts to implement innovative technologies in their digital transformation journeys involving data analytics, artificial intelligence (AI), massive internet of things (mIoT), cloud and edge computing, etc.

The COVID-19 pandemic caused a massive surge for better connectivity to support remote workers, online learning, automation, security, and high-quality connectivity to reduce onsite personnel and build continuity of operations and foster virtual employee interactions and engagements. As a result of COVID-19, a technology progression that normally would have taken a few years was compressed into a few intense months. IT executives increased spending to build resiliency, accommodate new usage scenarios, while maintaining or improving network security, and protecting data privacy.

In the interest of national security, the establishment of a secure and resilient private 5G network infrastructure mitigates potential risks and protects critical infrastructure. Private networks are an important component of the larger goal of securing national infrastructure.

Public and private networks using a secure standards-based approach enables both economies of scale and scope. Private networks augment or introduce new capabilities for exclusive entities within a defined geographical service area or premises.

[1] https://www2.deloitte.com/cn/en/pages/technology-media-and-telecommunications/articles/global-5g-transformation.html

Table of Contents

Purpose and Scope....4
What is a Private Network?....4
Types of 5G Non-Public Networks....5
Benefits of a Non-Public Network....6
Federal Use Cases to Consider When Implementing a 5G Non-Public Network....7
Privacy/Security/identity, Credential, and Access Management (ICAM)....11
Operations And Maintenance....14
Key Considerations....15

Purpose and Scope

To meet the ever-increasing connectivity demands of users and staff, IT executives might leverage rather than "must" leverage the capabilities of advanced wireless technology solutions to blend indoor and outdoor usage scenarios, blend of fixed and mobile networks, and enhance workplace communications and collaboration. Organizations can use Wi-Fi 6 for indoor, on-campus, and ad-fixed network situations as well as 5G for outdoor, off-campus, and mobile network environments to extend beyond or between non-public environments. Organizations will continue to adopt 5G and Wi-Fi 6 in parallel to meet their needs. Wi-Fi has lower barriers/cost to entry given its use of unlicensed spectrum and legacy adoption within enterprises, while 5G could potentially have slower adoption due to upfront implementation of infrastructure costs and lack of dedicated spectrum ownership for private or non-public networks (NPNs). Public networks offer mobile network services to the general public, whereas NPNs are intended for the sole use of a private entity in a specific geographic area within the entity's defined premises. NPNs utilize both virtual and physical network functions and may be deployed in a stand-alone NPN (SNPN) operated by an NPN operator and do not rely on network functions provided by a PLMN, or a public network integrated NPN (PNI-NPN that is deployed with the support of a PLMN[2].

NPN's are custom built networks for federal or enterprise buildings, campuses, and factories, with dedicated resources to achieve mission communications objectives of performance, security, scalability, and usability.

This paper will explore the types of Non-Public Networks (NPN), use-cases, security, privacy, and performance implications, in deploying a private network in a federal building or enterprise campus.

What is a Private Network?

Unlike mobile network services offered to the public, a Non-Public 5G Network (NPN), also called a Private 5G Network, provides 5G network services to a clearly defined and approved user group like workers in a federal agency/building. Such private networks are built for a targeted purpose with specific performance, access, and security in mind. These networks may or may not be dependent on wireless carriers and could be standalone. For example, a 5G non-public network can be deployed in a federal GSA building or campus. Figure 1[3], below depicts a high-level example of how a private 5G network can be deployed in a government building.

[2] 3GPP TR 28.807: Study on management of Non-Public Networks (NPN)

[3] Credit: Suro Sen, 2023

Figure 1: GSA Building Private Network Example

Benefits of an NPN:

- **Quality-of-Service (QoS):** Higher QoS via dedicated key performance indicators (KPI)
- **Security:** Higher security requirements achieved by dedicated security credentials
- **Reliability:** Isolation from public networks, thereby providing more reliability, performance, security, privacy, and safety
- **Accountability:** A non-public network makes it easier to identify responsibility for availability, maintenance, and operation

Types of 5G Non-Public Networks

When the federal government considers implementing a 5G NPN there are several approaches offering different levels of inherent security and cost tradeoffs. In a closed network (standalone NPN), the network operator owns all core and RAN (Radio Access Network) services. This offers the greatest control given the total ownership of end-to-end infrastructure components. However, this approach limits the users to only the services and extensions of the network. This approach limits mobile devices from roaming across other closed networks. An alternative approach is sharing resources between public and non-public networks. In this approach, NPN shares access to public RAN and/or Core services. There are a wide range of opportunities in this hybrid approach given the commercial industries' investments. The federal government could own the core and license/lease access to commercial RANs beyond the government perimeter while maintaining some small cells for gap areas within various federal campuses or military bases. The final approach is licensing access to services from commercial providers via virtual NPNs. This approach leverages network slicing where the traffic is external to the NPN but treated as a completely separate network from public traffic. Below lists some tradeoffs associated with each approach:

Network Approach	Advantages	Disadvantages
Standalone NPN	Full control of end-to-end Dedicated radio spectrum	Lack of roaming beyond perimeter Requires greater economies of scale
Hybrid (shared resources)	Most flexible for usability and security	Complex security controls
Virtual NPN (hosted by public network)	Least up front cost	100% dependent on network provider

Benefits of a Non-Public Network

- **Public-private collaboration:** Foster partnerships with private sector entities for global roaming across closed and open mobile network operators including public and federal networks.
- **Quality-of-Service (QoS):** Higher QoS via dedicated key performance indicators (KPI), which includes performance, priority, and preemption.
- **Security:** Enhance national security: Establish a secure and resilient 5G network infrastructure that mitigates potential risks and protects critical infrastructure. Higher security requirements are achieved by dedicated security credentials. Individual agency security needs depend on their risk tolerance.
- **Assuredness:** Isolation from public networks, thereby providing enabling dedicated resources that improve, performance, security, privacy, and safety
- **Network Operations Management:** A non-public network makes it easier to identify responsibility for availability, maintenance, and operation.

With the deployment of commercial 5G networks, the federal government will gain additional capabilities not previously available in 4G. With the enhanced Mobile Broadband (eMBB) feature the edge devices benefit from an increase in throughput by the networks using higher frequencies, wider channels, and more efficient spectrum utilization. An increase in throughput means the edge devices receive greater speeds for their applications. With Ultra-reliable and Low Latency Communications (URLLC) the devices experience an improvement in connectivity and a reduction in latency. This enables improvements to applications that stream media, voice/video communications, and other services dependent on reliable connectivity (without latency). With massive Machine Type Communications (mMTC) the network can increase the density of access points which translates to supporting more simultaneous endpoints thus improving the scalability of mIoT. 5G is intended to serve one million devices in a square kilometer versus 100,000 per square kilometer for 4G. These three new features offer an opportunity to significantly improve end-user capabilities but are limited in applicability towards improving the security of the infrastructure.

The 3GPP standards have made major improvements in 5G security compared to 4G with network slicing, multi-level of services and multi-connectivity network capabilities. Although to leverage all the security improvements, the network operator needs to connect 5G RANs with 5G Cores (standalone mode) as opposed to 5G RANs connected with 4G Cores (non-standalone mode). As published by GSMA[4] and 3GPP[5], some key security advantages of 5G include:

- Primary (mutual authentication) is controlled by the NPN and secondary authentication is integrated into the 5G architecture.
- Enhanced subscriber identity protection (privacy)
- Inter-operator security – built-in protection for roaming across networks (e.g., mitigations against key-theft and re-routing attacks)
- Integration of service-based architecture enabling security enhancements
- Key-separation and integrity of user plane
- Independence between mobile and security anchors

Federal Use Cases to Consider When Implementing A 5G Non-Public Network

In the world of 5G, the environments are no longer just mobile networks, but rather a combination of heterogenous networks enabling ubiquitous connectivity with highly dense nodes for massive computing power.

4 https://www.gsma.com/security/securing-the-5g-era/

5 https://www.3gpp.org/news-events/3gpp-news/sec-5g

1. **Smart Building Management:** 5G technology, with its high capacity for device connectivity, enables the integration of a larger number of IoT sensors and devices into a building's infrastructure. This allows building systems like HVAC and lighting to be controlled more efficiently in real-time, resulting in energy and cost savings. For example, sensors can provide data on room occupancy, adjusting heating and lighting automatically to save energy when rooms are unoccupied. Moreover, predictive maintenance can be implemented, where building systems can be monitored to detect and address issues before they lead to system failures.
2. **Security:** 5G can revolutionize security systems within federal buildings. High-definition security cameras can stream real-time video over 5G networks, reducing delays and allowing security personnel to respond more quickly to incidents. Biometric systems can use 5G's high-speed data transmission to process facial recognition or fingerprint scans more quickly, enhancing building access controls. Furthermore, IoT devices can be integrated into a building's security system, allowing for real-time tracking of assets and personnel within the building.
3. **Virtual and Augmented Reality:** 5G's low latency and high data transmission rates make it an ideal technology for virtual and augmented reality (VR/AR) applications. For training, VR can be used to simulate emergency situations, allowing employees to practice their response in a safe environment. AR can be used for maintenance tasks, overlaying digital information on physical systems to guide technicians through complex repairs. These technologies could also be used to enhance accessibility in federal buildings, providing virtual tours or guides for visitors who may not be able to physically access certain areas.
4. **Remote Work and Collaboration:** The COVID-19 pandemic highlighted the importance of remote work capabilities. 5G technology can greatly enhance remote work and collaboration tools, such as video conferencing, by reducing delays and improving video quality. This can make remote work more efficient and support continuity of operations during emergencies.
5. **IoT and Automation:** 5G's high device capacity is perfect for IoT applications. Sensors can be integrated into a building's infrastructure to monitor everything from structural health to air quality. Automated systems, like robotic cleaners or delivery drones, can be managed over 5G networks, improving efficiency and reducing the need for human intervention. These applications can improve building safety, efficiency, and sustainability.
6. **Emergency Response:** In emergency situations, 5G can support communications and response within federal buildings. Real-time video feeds can guide first responders, and IoT devices can provide vital data on things like building occupancy and structural integrity. Furthermore, 5G can support public safety communications systems, ensuring that first responders can communicate effectively during emergencies.
7. **Data Centers and Cloud Services:** For federal buildings that house data centers, 5G can enhance performance by allowing for faster data processing and transmission. This can support a range of applications, from machine learning algorithms that can analyze large amounts of data to improve building operations, to cloud-based software that can be accessed from anywhere within the building.

8. **Public Services:** In federal buildings that serve the public, 5G can support a range of services. For instance, virtual queues could be implemented, allowing visitors to wait their turn without physically standing in line. Digital information kiosks can provide real-time information to visitors, and improved accessibility features, such as AR guides for visually impaired visitors, could be implemented.
9. **Precision Agriculture:** For federal buildings that house agriculture-related departments, 5G can enable the use of precision agriculture technologies, such as drones and IoT sensors, for real-time monitoring of crops and livestock. These technologies can help improve yields, reduce waste, and enhance sustainability.
10. **Mobile Offices:** With 5G, federal employees could effectively work from anywhere within or even outside the building, thanks to the high-speed, reliable connection. This could allow for more flexible work arrangements and make it easier for employees to collaborate with colleagues in other locations.
11. **Telemetry:** For federal buildings involved in scientific research or monitoring, 5G can enable real-time telemetry, allowing for faster and more reliable collection, processing, and transmission of data. This could be used for everything from environmental monitoring to space exploration.
12. **Telemedicine:** In federal buildings that provide health services, 5G could support telemedicine applications, allowing healthcare providers to consult with patients remotely, share high-resolution images and video, and even perform remote surgeries using robotic systems.
13. **Smart Parking:** 5G can support smart parking applications, allowing employees and visitors to find available parking spots more easily. Sensors in parking spaces can transmit data over the 5G network, and an app can guide drivers to available spots, reducing the time and frustration involved in finding parking.
14. **Digital Signage:** 5G could support digital signage systems within federal buildings. These could provide real-time information to employees and visitors, and the content could be easily updated over the 5G network.
15. **Energy Management:** 5G can enable real-time energy management within federal buildings. Sensors can provide data on energy usage, and intelligent systems can use this data to optimize energy consumption, reducing costs and environmental impact.
16. **Disaster Management:** In the event of natural disasters or other emergencies, 5G can support disaster management efforts. High-speed, reliable communication can be crucial in coordinating response efforts, and IoT devices can provide real-time data on the situation.
17. **Asset Tracking:** For federal buildings with valuable assets, 5G can support real-time asset tracking. Sensors attached to assets can transmit data over the 5G network, allowing for real-time location tracking and theft prevention.
18. **Land Port Entry (POE) Screening Operations:** A large POE with advanced screening including video processing, massive sensor array (IoT) and other technologies to rapidly screen vehicles, people, and cargo traversing a border crossing. 5G capabilities such as Enhanced Mobile Broadband (EMBB) will deliver higher data rates with a peak data rate of 20 Gbit/second. Typical applications include 4K/8K ultra-high- definition (UHD) video, fiber

replacement, augmented reality (AR), and virtual reality (VR). EMBB, which is currently being deployed, offers more bandwidth and faster download speeds compared to 4G, making it ideal for data-heavy uses such as video monitoring for situational awareness. 5G capability for Massive Machine-Type Communications (MMTC, or Massive Internet of Things (IOT)) requires the design of low complexity, low power consumption devices which translates to longer battery life. MMTC extends current IoT and machine-type communications served by Low Power Wide Area (LPWA) technologies to meet the needs of extremely high-density deployments. 5G is intended to serve one million devices in a square kilometer versus 100,000 per square kilometer for 4G.

19. **Converging Network Architecture:** The Fixed Mobile Convergence (FMC) concept aims to provide users with universal access to subscribed services from both fixed and wireless networks, such as DOCSIS, Ethernet, PON, Wi-Fi, MVNO 4/5G, CBRS 5G, and partner networks. This convergence is to be implemented in two domains within a telecom operation. The first domain involves the network at the 5G core, enabling devices connected to fixed lines to access services through 5G residential gateways seamlessly. This allows for uninterrupted movement between 5G wireless, Wi-Fi, and fixed networks, often simultaneously using Dual Sim, Dual Standby (DSDS) technology. The second and more significant convergence occurs through a new Business/Operation Support System, which empowers Multiple System Operators (MSOs) to rapidly capitalize on multi-network access. This enables the efficient delivery of applications and services at a large scale without needing to overhaul existing complex IT systems.

While implementing 5G technology has many benefits, it's important to remember that it also increases the potential for cyber attacks due to increased connectivity. Therefore, robust cybersecurity measures need to be in place to protect the networks in federal buildings. Each of these applications could significantly enhance the efficiency, safety, and sustainability of federal buildings. However, they would also require careful planning and implementation to ensure network security and privacy.

Figure 2[6]: Federal 5G Use Cases

6 https://www.cio.gov/2020-11-18-Federal-Mobility-Group-Unveils-5G-Testbed-Framework/

Use Cases	eMBB	URLLC	mMTC
Autonomous Vehicle Proving Grounds		X	
Backhaul Using Slices	X	X	
Cellular Drone Delivery/UAS		X	
Continuous Multifactor Authentication		X	
FWA for Bases	X	X	
Installation-Level Micro-Grid			X
Last-Mile In-Port Cutter Connectivity	X		
Multi-Access Edge Computing	X	X	
Secure Interoperable Emergency Comms	X	X	X
Single Device/Multiple Classification Levels	X	X	
Tactical Edge Communication System	X	X	X

Source: Federal Mobility Group (FMG) Framework To Conduct 5G Testing

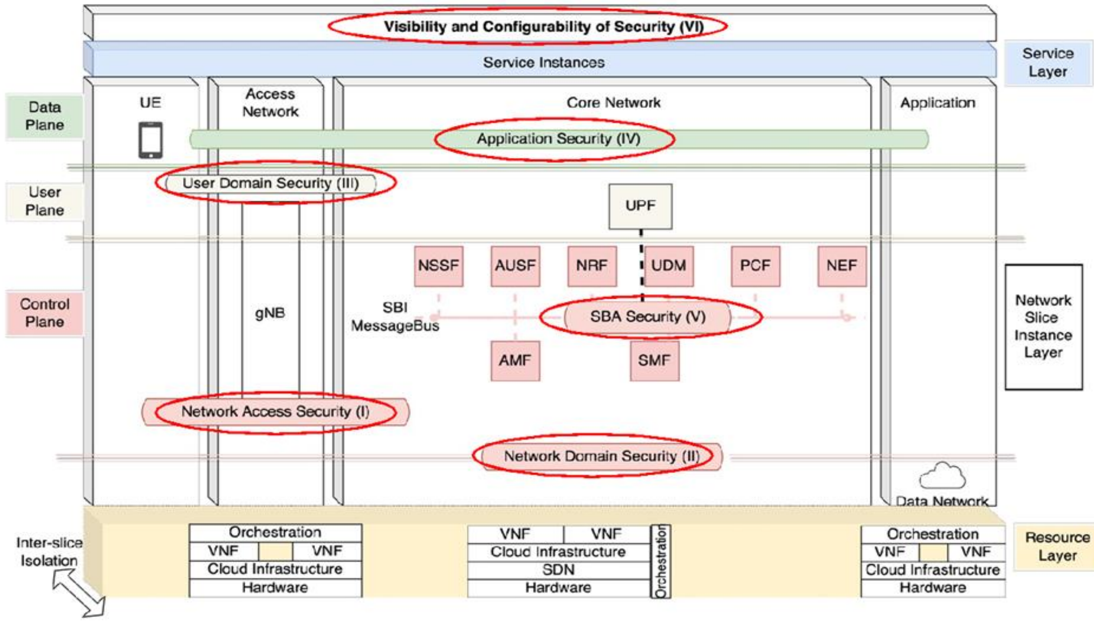
Privacy/Security/Identity, Credential, and Access Management (ICAM)

5G enables new and enhanced applications and services to be used by mobile network consumers. In order to ensure that 5G fulfills its promise, all security matters accompanying the 5G architecture need to be addressed. The 5G network must support high level security and privacy for its entities (not just humans, but also devices, applications, etc.) and its traffic. At the same time, the 5G network must be resistant to cyber-attacks. To address this two-fold challenge, security requirements for 5G cannot be regarded as an add-on; instead, security must be built into the 5G network design right from the beginning. This approach will protect subscribers, devices, applications, and their communications, as well as the integrity of the network itself.

3GPP is a partnership project that brings together Standard Development Organizations - SDOs - from around the world focusing on technical standards and specifications.3GPP TS 33.501 is the key document providing a detailed description of ‘security architecture and procedures for 5G system’. The specification defines a model of a security architecture, consisting of six security domains, as shown in Figure 3[7].

Figure 3: Security Domain for 5G

[7] TS 33.501 - 5GS Security Architecture and Procedures, https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-i20.zip



The six security zones are as follows:

1. **Network access security** – The set of security features that:
   - Enables UE to authenticate and access services via the network securely, including the 3GPP access and non-3GPP access, particularly to protect against attacks on the (radio) interfaces.
   - Enables the network to authenticate the user (via the Universal Subscriber Identity Module USIM) and mobile equipment accessing the network.
   - Provides security context delivery from the serving network to UE for the access security.
2. **Network domain security** - The set of security features that enables network nodes to securely exchange signaling data and user plane data. Network domain security defines security features for interfaces between access and CNs and between home and serving networks.
3. **User domain security** - The set of security features that secures user access to mobile equipment. Mobile equipment uses internal security mechanisms such as a personal identification number (PIN) code to ensure security between the mobile equipment and USIM.
4. **Application domain security**- The set of security features that enables applications in the user domain and in the provider domain to exchange messages securely. Security mechanisms of the application domain should be transparent to the entire mobile network and should be provided by application providers. 3GPP TS 33.501 specifications **do not cover** application domain security.
5. **Service Based Architecture (SBA) domain security**- The set of security features that enables network functions of the SBA architecture to securely communicate within the

serving network domain and with other network domains. SBA domain security is a new security feature in 5G. An SBA forms the basis of the 5G CN.

Figure 4: 5G Security Assurance Attributes

6. **Visibility and configurability of security**– The set of security features that enables the consumer and provider to be informed regarding which security features are in operation or not. Can be used to configure security features.

The main purpose of a 5G network operator's security architecture is to provide security assurance characterized by four key **attributes** as shown in Figure 4[8]: Confidentiality, Integrity, Availability and Accountability.

3GPP Release 16 specifications address enhanced security measures in 5G. However, some details – such as those pertaining to network configuration -- are still left to the individual operator. Other standards bodies (e.g., Global System for Mobile Communications Association (GSMA), European Telecommunications Standards Institute (ETSI), Open Radio Access Network Alliance, etc.) may bring specifications and guidelines to fill in some of these details. As the 3GPP 5G security specifications establish optional security features and provide degrees of freedom for implementation and operation as per local regulations, 5G users may encounter different security contexts.

Standards groups such as 3GPP suggest the following key functionalities:

- 3GPP Standards Based Confidentiality.
  - Authentication and encryption framework in 5G standards (AKA, Key hierarchy) provides authentication, authorization for user equipment (UEs) and keys for encryption of user communication sessions. It is a required element of 5G network and user devices.
  - Network function communication security (SCP, SEPP, NEF, Interfaces to use TLS) is also specified. 3GPP does not go in details required for hardened security posture. Consideration must be made to enforce granular access controls via application firewalls or service mesh mechanisms.
- 3GPP Standards Based Integrity.
  - Functions and slice isolations mechanism are part of the architecture, but it is left to implementation of such capabilities.

[8] MITRE Corporation

    - Network slices is introduced in the architecture, offers custom networks for enterprise users based on SLA, but granular details of such measures are also implementation decisions.
    - Encryption is a key element, encryption offers digital signatures, message authentication and message encryptions to offer assurance that message was sent from authenticated NF/Users and have not been tempered in transit.
- Availability
    - Availability is provided by Area of service, session continuity, UE Access policy. This measure is also implementation dependent to offer any node and network failures.
- Accountability
    - NWDAF, charging function and CDRs, supporting systems and control information from the infrastructure offers accountability in 5G service. This only extends to 5G application layer, it does not cover Cloud, host or network levels records.

- Non-3GPP Security considerations
    - Special attention should be paid to supporting technologies such as Cloud/NFVI, IP network, SDN, OSS/BSS tools[9], and supply chain. These technologies make it possible to create efficient and dynamic 5G networks. There are security best practices available for each one of these supporting technologies, following such guidance will ensure benefits from 5G are implementations are achieved without inheriting risk from added threat surfaces.
    - Roles and Responsibility of Network and Security OPS- the roles and responsibilities of network and security operations teams are vital to ensure the reliable, secure, and efficient operation of private 5G networks. Their efforts contribute to maintaining network integrity, protecting sensitive data, adhering to regulations, and delivering seamless connectivity for critical applications within an organization.
    - **Access, Privacy, Security, ICAM** can be improved by enablers such as AI/ML and security can be integrated in each technology or tool set to increase visibility and reduce response time. In a high-speed network, detection, analysis, and response needs to happen in real time before any negative impact on user data or network.

[9] https://www.tmforum.org/oda-interactive-map/

Operations and Maintenance

Operation and Management, also known as Service Operations (SO), are the activities and procedures that provide effective IT services and be included in the buildout, especially in a secure architecture and services that are consistent with service level agreements. Known as Service Operations which performs the duties and encompasses all day-to-day operations, modernization, infrastructure, and procedures required for efficient delivery, operations and management of IT services, security, and capabilities.

Service Operations 4 essential functions should include:

- **Service Desk is t**he principal point of interaction for end-user and IT service provider activity synchronization for customer issues especially for IT, security, and cyber incidents.
- **Technical Management provides** the in-depth expertise and resources capabilities needed to assist the organization's ongoing activities in the IT domain.
- **IT Operation Management** is responsible for carrying out the operational duties necessary to oversee, maintain, modernize and lifecycle the organization's IT and cybersecurity architecture regularly.
- **Application Management** oversees as to whether to build or acquire a service and of building, testing, and improving applications.

A Service Operations plan and build must include the resources to standup, sustain, lifecycle and modernize to optimize service operations, maintenance, lifecycle, and modernization such as:

- **Long-Term Incremental Improvement which** entails assessing the performance, modernization, security needs of equipment and systems software and hardware end of life and end of support to modernize with resources before change is required.
- **Short-Term Ongoing Improvement** is focused on minor improvements in working practices in service operation procedures that do not require large changes to a process or technology.

Best Practices in Service Operation

Choosing and implementing best practices assist enterprises throughout the Service Operation phase:

1. The principles of daily service operation tasks improve overall business efficiency because it allows for quick and easy access to standard services, allowing employees to boost efficiency or the performance of business services and products without the need for additional assistance.
2. The lifecycle is concerned with the effective and efficient delivery and support of agreed-upon IT services that meet SLA. When followed it allows the effective handling

of service disruptions and identify root causes, eliminating unplanned labor, and cost avoidance of additional labor or material costs.
3. Efficient service operation helps operators and consumers maximize the value of service provided by minimizing the duration and frequency of service problems.
4. Provides a better customer service experience and, higher retention of customers.
5. Service Operation will enhance security by limiting access to IT services to those in the organization only to those that are permitted to use them.

Key Considerations

When implementing a 5G NPN for use by Federal Government organizations a few considerations are suggested.

- Standards and interoperability - Encourage the adoption of international standards and promote interoperability to enable seamless connectivity and the integration of diverse 5G technologies.
    - Stay in-line with commercial standards and roadmaps to maximize investments from commercial R&D, minimize total cost of ownership, and support interoperability with global roaming across heterogeneous networks.
    - Since completely replacing 4G infrastructure is not efficient, the federal government should consider an approach to augmenting existing infrastructure with the addition of 5G technologies.
    - Securely roaming between internal and external networks and on top of trusted and untested infrastructure
    - Deployment scalability from small cells to macro core networks that address federal mobility use cases.
- Spectrum management - Develop policies and regulations to effectively allocate and manage the use of radio frequencies, ensuring efficient and coordinated spectrum allocation for 5G networks. To increase reliability and availability utilize white space where possible.
- Infrastructure development - Allocate sufficient resources and funding to support the development and deployment of 5G infrastructure, particularly in underserved areas and regions of strategic importance.
- Infrastructure sustainment - Simplify and expedite permitting, zoning, and rights-of-way processes to facilitate the timely deployment of 5G infrastructure while ensuring compliance with safety and environmental regulations.
- Security and privacy - Implement robust security standards and privacy protections to safeguard sensitive data and prevent unauthorized access or breaches.
    - Conduct comprehensive risk assessments to identify vulnerabilities, threats, and potential impacts on national security, and establish risk mitigation strategies and protocols.

  - Establish strict security requirements and vetting processes for vendors and suppliers, considering their trustworthiness, adherence to security standards, and potential risks associated with foreign entities.
  - Adoption of zero-trust architectures supports lower upfront costs than requiring trusted-supplier procurements.
  - Countermeasures that address the emergence of post-quantum encryption
  - Verifiable components with trusted identities, consider trusted HW/SW and services supply chains.
  - Defense in depth for energy flexibility and agility
- Workforce development – plan for architecture, design, deployment, and optimal operations. 5G and some of the supporting technologies may require skills that organization does not have. A holistic plan to partner, outsource or develop resource for lifecycle phases will avoid unexpected security exposure and cost creeps.
- Public engagement - Conduct public awareness campaigns to educate citizens about the benefits, risks, and responsible use of 5G technology, promoting understanding and acceptance.
  - Foster open dialogue and collaboration with industry stakeholders, consumer advocacy groups, and the public to address concerns, gather feedback, and ensure transparency in decision-making processes.
  - Promote digital literacy that also removes barriers to access digital services[10].

By adopting these governance recommendations, the federal government can establish a robust framework for the deployment and management of a secure, reliable, and inclusive 5G network. This will enable the country to harness the full potential of 5G technology, drive innovation, and safeguard national security while ensuring equitable access and benefiting all citizens.

Disclaimer*: This document was prepared by the members of the ATARC Secure 5G Working Group in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated with, and shall not be used for advertisement or product endorsement purposes.*

[10] EU reference - https://digital-strategy.ec.europa.eu/en/library/digital-skills-all-europeans-brochure