DELL Technologies

Technical Paper

SECURE FEDERAL COMMUNICATIONS:
The Need for Dedicated Private 5G Networks

June 2025

Author

Marissa Borrego
Senior Principal Engineer, Telecom Systems Business
Dell Technologies

Bob Kerr
Product Management , Telecom Systems Business
Dell Technologies

Michael Rash
Senior Distinguished Engineer, Telecom Systems Business
Dell Technologies

Chris Wallace
Director Software Engineering, Telecom Systems Business
Dell Technologies

Table of Contents

Introduction

The federal government's communication needs are unlike most other sectors, and include demands for unparalleled levels of security, reliability, and flexibility. With national security hinging on fortified and reliable communication networks, it is crucial to adopt solutions tailored to the specific needs of federal agencies. This white paper highlights key federal mandates that guide network modernization efforts within the U.S. government. It then focuses on examining dedicated private 5G networks and their suitability compared to commercial carrier-based alternatives in addressing a select class of federal use cases.

For the purpose of these discussions, a dedicated 5G network will refer specifically to a standalone private 5G network deployment that does not interact with a public network. These dedicated networks are particularly well suited for meeting the specialized needs of federal deployments, where security and strict access control are of utmost importance, such as for agencies focused on intelligence, national defense, and homeland security. In addition to enabling tight security controls, dedicated private networks can provide the tailored configurability and feature enablement needed to meet critical mission demands. This will be exemplified through several key Department of Defense (DoD) use cases.

Deployment Options

This section provides a high-level overview of 5G network deployment options and sets the stage for the discussions presented in the subsequent sections. In general, there are three main approaches for deploying 5G networks: Public, Hybrid, and Dedicated Private.

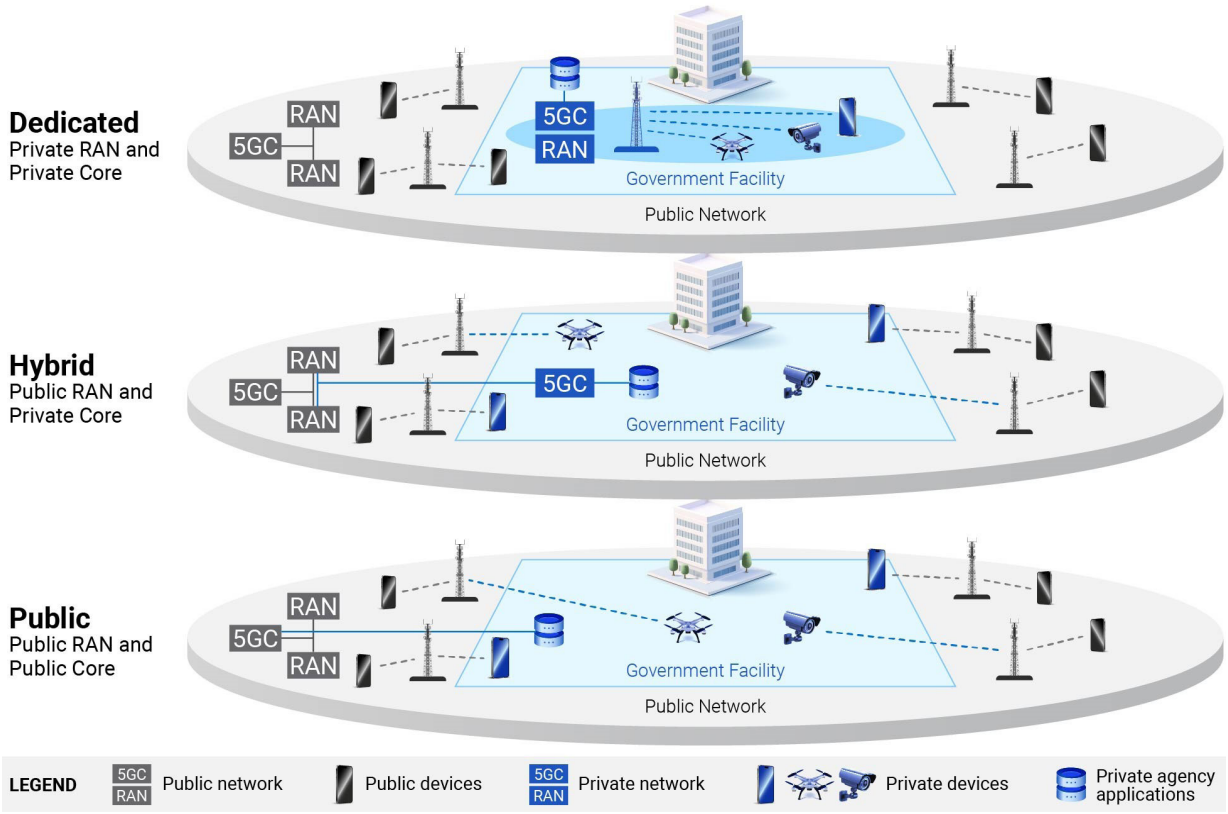
1. **Public Networks:** Public 5G network deployments are fully operated by major telecom providers and run entirely on their public Radio Access Network (RAN) and core infrastructure. All 5G network hardware and software is owned by the telecom provider and used by both the general public (commercial customers) and agency-specific network devices. This option provides broad coverage and scalable services over existing public networks, and does not require dedicated infrastructure investments. Ensuring compliance with strict federal security requirements across a public network can be challenging.

2. **Hybrid Networks:** Hybrid networks leverage public 5G RAN network infrastructure combined with private Core. This option provides broad connectivity while maintaining a private core for enhanced security and control. While agency-specific devices continue to use the telecom-owned public RAN infrastructure alongside commercial users and face similar federal compliance requirements, this model adds key advantages. It enhances security and provides tailored controls at the Core, while ensuring seamless interoperability with public networks for non-sensitive operations.

3. **Dedicated Private Networks:** A dedicated private 5G network is built using private RAN and private Core. They allow for highly tailored configurations, enabling compliance with stringent federal security standards, including Zero Trust architecture and Trade Agreements Act (TAA) requirements.These networks deliver secure communication environments isolated from commercial users and under the full control of the federal agency. They provide exclusive, on-premises connectivity tailored to specific operational requirements, ensuring the highest levels of security, customization, and specialized feature enablement.

It is important to highlight that, rather than being mutually exclusive, these three deployment options provide complementary solutions for varying connectivity demands. Overall, they provide a comprehensive set of strategies that meet the diverse needs of the federal government.

Figure 1. 5G Network Deployment Models



Alignment to Federal Mandates

The U.S. government has developed a comprehensive framework of mandates and strategies to secure and advance wireless communications, encompassing a wide range of initiatives, including:

- Secure 5G and Beyond Act of 2020 [1]
- "Department of Defense Private 5G Deployment Strategy" [2]
- "NTIA National Strategy to Secure 5G Implementation Plan" [10]
- "DoD 5G Strategy Implementation Plan" [11]
- "Fulcrum: The Department of Defense Information Technology Advancement Strategy" [12]
- National Defense Authorization Act (NDAA) FY 2022 [13]
- Executive Order on America's Supply Chain [15]
- Executive Order on Improving the Nation's Cybersecurity [16]

Main 5G Directives

This section highlights several of the most significant directives, with a particular focus on those that address the deployment of private 5G networks. The Secure 5G and Beyond Act of 2020[1] and the ***"DoD 5G Strategy Implementation Plan"*** [11] establish the foundation for these 5G efforts, requiring a national strategy to address vulnerabilities, safeguard supply chains, and protect against foreign adversaries.

The ***"Department of Defense Private 5G Deployment Strategy"*** (October 2024) [2] focuses on deploying secure, scalable private 5G networks at military installations to enhance operational capabilities, resilience, and mission-specific communication needs. It "recommends the use of Open Radio Access Network (RAN) solutions, whenever possible and appropriate" and outlines the "types of private networks and the associated security and performance considerations" that are necessary [2].

Complementary guidance, such as the General Services Administration's (GSA) ***"Acquisition Guidance for Procuring 5G Technology"*** [3], addresses related security themes, including compliance with Open Radio Access Network (O-RAN) standards. Together, these mandates outline that a "key aspect to DoD's modernization effort is to leverage 5G networks, both commercial and private, to deliver ubiquitous high-speed connectivity for mobile capabilities" [2], as well as highlight the criticality of ensuring secure, robust communication infrastructure for maintaining national security and driving technological leadership.

Dedicated Private Network Trade-offs

In general, federal mandates call out key advantages of dedicated private wireless 5G networks compared to solutions based on commercial carrier agreements. Both the DoD and the GSA have stressed that, unlike public networks, dedicated private 5G networks can be "tailored to the specific installation's mission needs, security, and military-unique capabilities" [2], and thus deliver:

- enhanced operational controls
- strengthen data sovereignty
- improve remote support for advanced technologies

such as autonomous systems, edge computing, and AI. These networks can closely align with stringent federal security requirements, including Zero Trust architecture and Trade Agreements Act (TAA), compliance, making them well positioned to minimize risks in numerous areas including data interception, unauthorized surveillance, dependence on external personnel, and exposure to non-compliant vendors.

However, these vital benefits come with the trade-off of higher upfront costs and initial deployment efforts. As a result, while dedicated private wireless solutions are well suited for DoD and other federal agencies with use cases that require strict security compliance, stringent access control, enhance adaptability or unique performance demands, they are not the best choice in all cases.

Public and Hybrid Network Trade-offs

Conversely, public and hybrid solutions can be more advantageous and cost effective than dedicated wireless 5G networks in meeting federal communications for numerous scenarios, and there are recommendations for leveraging "commercial networks to the maximum extent possible" [2]. This is most applicable to federal scenarios that are less concerned with national security, but rather focus more on enabling communication for a broad range of users. Examples include agencies focused on education, administration, or human services.

These networks are also ideal for operations requiring broad geographic coverage, such as disaster response across multiple regions, where public telecommunication providers can offer immediate access to existing infrastructure. They can also enable rapid deployment in emergencies, provide a cost-effective solution for low-bandwidth applications, and are based on an attractive Operating Expenditures (OpEx) pricing model that does not require upfront Capital Expenditures (CapEx) investment. Additionally, commercial networks serve as a practical choice for redundancy, support a diverse device ecosystem, and ensure reliable international communication through roaming agreements.

Public and hybrid solutions provided by commercial telecom companies provide many notable benefits, including:

- Extensive coverage
- Established infrastructure
- OpEx-based costing
- Rapid scalability

making commercial carriers one of the key solutions for U.S. federal communication strategies. However, despite the many strengths and broad applicability of existing public networks, federal policymakers have flagged the risks associated with relying solely on commercial carriers, especially for critical operations. Concerns include vulnerabilities such as:

- Unauthorized surveillance
- Data breaches
- Limited autonomy

Furthermore , telecom providers can lack the flexibility to fully address specialized federal use cases and face challenges with prioritization between commercial and government demands. Another concern is the ability for commercial carriers to align their offering to meet rigorous federal compliance standards, particularly for DoD deployments. The extensive global supply chains supporting these carrier networks frequently involve non-compliant vendors, introducing serious risks that can threaten our national security. These security issues will be examined in greater detail later.

Key Takeaway

The federal government recognizes the need for a **combination of public, hybrid, and private 5G networks** as part of its infrastructure modernization efforts. Each deployment approach provides valuable benefits. Determining which to select should be based on the specific federal use case requirements.

The following section outlines several DoD use cases where dedicated wireless solutions are a good fit. They require enhanced security, , autonomy and specialized mission-critical communication and align well with the strategic capabilities that can be delivered by dedicated private networks.

Deployment Considerations for DoD Use Cases

When evaluating the three different models of 5G deployment for U.S. Military Base coverage, Public RAN/Core, Public RAN with Private Core, and Private RAN and Core, it is important to consider the intended use cases of the 5G service. Above all else, the purpose of the network deployment is to ensure mission success with 5G modernization to support the readiness, safety, and performance of the fighting force. These considerations play a key role in the following DoD use cases:

Train Like You Fight: Align Domestic Training and Tactical Deployment Readiness

When the objective is modernization and readiness of the fighting force with 5G capabilities, it is important to maintain consistency between how forces train and how they fight. For example, while a public RAN could be used domestically across a public carrier's network, all devices connected domestically would no longer use the same service, infrastructure, frequencies, orchestration, and management when deployed to a battle zone Outside the Continental United States (OCONUS). In support of our war fighters, while it is possible to switch networks between training and fighting, it is not a proven paradigm for readiness or seamless transition.

Compatible Communications Across Military Branches and Allied Forces

One of the strengths of the U.S. military is the integrated command and control and the inter-communication and coordination between U.S. and allied forces. Robust communications in theater can typically leverage different frequencies for communications, depending on the use case. There is significant value, however, in ensuring a common band of frequency across the branches of the military. This is evident when considering equipment maintenance and support, DoD procurement & deployment scale, aligned device and network performance, and compatibility. This concept similarly extends to allied fighting forces.

Use of domestic public networks and associated specialized frequency bands would not support this mission objective. One option is to government-allocated spectrum that is available for both government and military use across the United States, as well as NATO countries. In some cases such spectrum is also assigned for use in Japan for private networks, which can extend to U.S. military base use. Due to commercial use in Japan and South Korea, a robust eco-system of major brand devices and chipsets exists that can be used to support DoD use cases.

Balancing Personal and Operational Communications

The needs and use cases across U.S. military bases and installations is not limited to official DoD work. Like any other area, those who work on base need personal communications capability to connect and support their personal life. This is where the extension of the domestic public network onto the base is important.

While it would be ideal to share one network, the above considerations of train like you fight and inter-force commonality of communication technology, along with security concerns around using public networks (ex. Salt Typhoon cellular network attack), weigh against using public networks or public RAN for DoD use cases.

One strategy to accommodate the disparate use cases on base and OCONUS could be different devices on different networks. Forexample, tactical, training, and official DoD use cases supported on a fully private network versus personal devices supported on an extension of the surrounding public network. In this case, it may be possible to use security software such as Hypori Halo to separate traffic and protect communications.

A 5G network architecture and deployment approach is fundamental when evaluating the impact on the effectiveness of "train like you fight," OCONUS mission readiness, and in ensuring maximum compatibility with the branches of the U.S. military, as well as NATO and Asia Pacific allies. Control over deployable services, frequencies, devices, applications, and supported use cases will weigh heavily on the chosen network design.

Recommendations for Base Coverage

There is no one solution that meets the customer end needs of affordability, deployability, mission fit, and security with Public or Private networks alone. In fact, a hybrid approach is needed. For coverage areas and communication demands that require civilian, family, and non-mission related access, the use of a Public RAN and Multiple Operator Core Network (MOCN) Core may provide the best fit for cost and ease of deployment, using a commercial service provider subscription model. For coverage areas supporting DoD related mission communications, the use of a Private 5G network specific to the DoD using Government spectrum would ensure that the specific security and performance needs of the mission are supportable.

Holistically, the two networks can operate alongside each other and allow each to be separately deployed and optimized where used. To link the user experience together for devices that straddle both networks under different use cases, dual SIM devices and specific apps can be linked to each network.

Network Security Considerations

The major public telecommunications providers have been under persistent attack for many years. In several cases, threat actors have been successful in compromising carrier networks and siphoning off massive troves of customer and administrative data. Affected carriers have included all the well-known entities based in the United States. These attacks have consistently resulted in the compromise of both customer and employee data, and have demonstrated the dire need for telecommunications entities to strengthen network security.

Example: Salt Typhoon

More recently, attacks from nation-states against telecom networks have culminated in the frightfully successful "Salt Typhoon" incident [7]. Although the large public carriers have invested massive amounts of capital in securing their sprawling infrastructure, the persistence and ingenuity of the computer offense broke down these defenses and caused massive loss of trust across the telecom landscape. The Salt Typhoon compromise of telecom infrastructure was so severe that it prompted CISA to change its general security guidance to recommend end-to-end encryption of communications on public networks, among other changes [8]. Further, CISA's guidance identified the perpetrators of Salt Typhoon as likely state-backed actors from the People's Republic of China (PRC). Some users must now assume that China had, and may still have undue levels of access to their communications as they traversed public carrier networks. Although public carriers have responded with high urgency to Salt Typhoon, an important conclusion can be drawn from this incident: in the security vs. usability trade-off there is much more room for better security. For high-value assets and use cases where security is paramount, stronger security control is provided by taking 5G connectivity into dedicated standalone networks.

Dedicated 5G Networks—A Naturally Air-Gapped Environment

From the perspective of the large telecom carriers, dedicated 5G solutions are essentially air-gapped environments that do not touch their public networks. These private 5G networks give operators control. Operators have control over who attaches to the dedicated 5G network, who can monitor user traffic and behavior, the security posture of the entire private 5G stack, and policy restrictions that may need to be in place. Taken together, these aspects allow dedicated 5G operators to align much more closely with Zero Trust and defense-in-depth principles than possible on public carrier networks. Further, as discussed above in the section on federal mandates, stronger control helps to align dedicated private 5G networks to required security capabilities as defined via executive order, 5G procurement guidance, O-RAN security guidelines, and more. These are important considerations for a vast set of DoD use cases that mandate extremely high levels of security. Air-gapped networks are not impervious to attack – the most famous example is probably the Stuxnet operation against Iranian centrifuge SCADA networks. However, an air-gap boundary significantly raises the bar for would-be adversaries.

Supply Chain Security

It would be hard to pick a subdomain of computer security more impactful than the security of the supply chain. This is an area where dedicated private 5G deployments have a massive advantage over public carrier networks, and it is easy to see why. Given the expansive hardware and software footprint of large public carriers, it is exceedingly difficult for them to produce comprehensive Software Bill of Materials (SBOMs) and Hardware Bill of Materials (HBOMs) for every device that handles user traffic. For networks as large and complex as those maintained by public carriers, this translates to a nearly impossible task. Furthermore, some carriers (especially in Europe) still have devices from sanctioned entities, such as Huawei. For the U.S. Government, this is entirely untenable. In essence, fully assessing the complete supply chain of the large public carriers is virtually infeasible, and this challenges the notion that meaningful security is achievable – let alone something as rigorous as Zero Trust or O-RAN security mandates. In contrast, the supply chain of dedicated private 5G deployments is far more constrained, making it significantly easier for providers to produce a complete accounting via SBOM and HBOM data for every constituent component. Above all, the supply chain specifics of every device involved in network communications for sensitive use cases should be known, accounted for, and made part of any broader security strategy..

Configurability & Control

The most important consideration when applying any technology is its suitability for purpose – can it get the job done? Public mobile networks are designed, deployed, and optimized for their primary mission to deliver mobile broadband Internet service to subscribers. Although recent generations of cellular technology have allowed more customization to broaden the applicability of the public network, there are still limitations that may render a public network unsuitable to deliver the characteristics needed for the federal use case.

1	Tailored Coverage	Specialized use cases, such as perimeter security and device tracking, may need to be limited to specific geographical locations. Customizing physical characteristics of radio network deployments, such as site location, transmission power, and antenna patterns may be impractical for a public network optimized for uniform wide area coverage.
2	Performance Optimization	The successful operation of specific use cases requires that the network provides sufficient resources to meet requirements on throughput, latency, or other characteristics. The configuration of private networks allows for much more customization to ensure that the mission's performance characteristics can be delivered to the end devices. Being able to modify parameters such as the balance of uplink and downlink radio resources and carrier channel bandwidths may be impossible in a public network, but necessary to ensure that private network use cases can be achieved without compromise
3	Individual Device control	Data sovereignty implies much more than just keeping user plane data within the realm of the government organization. Information about which devices connect and disconnect to the network, where they are physically located, and traffic patterns can be inferred from shared RAN telemetry.
4	RF Spectrum Considerations	Although national spectrum management agencies have allocated large amounts of spectrum to mobile operators, the non-public government agencies are uniquely positioned to access additional spectrum reserved for government use. The ability to effectively support "train as you fight" use cases would be degraded if devices and spectrum characteristics change fundamentally between the "train" activities at home and "fight" activities abroad. Dedicated private networks operating independently of surrounding public networks may enable a level of consistency that cannot be achieved otherwise.

Ultimately, having a network that delivers the required performance and flexibility to deliver on the required mission is the most important factor determining its suitability. Dedicated private networks may be the only practical way to ensure that critical applications can be supported without compromise.

Cost Considerations

While cost considerations are inherently complex, encompassing both upfront investments and long-term operational expenses and depreciation, this section provides an overview of important financial factors that should be evaluated when determining any network deployment. There are different financial models to consider, such as using public carrier subscriptions in a recurring monthly subscription model per user/device through OpEx, or a CapEx centric approach of building a Private Network suited to the specific DoD mission needs. As discussed in earlier sections, a reasonable approach may be a hybrid approach of subscriptions with Private Networks for official military base operational use cases and public service for base coverage.

When assessing cost, it is important to look at the upfront deployment cost of a network, as well as the downstream cost of the network on the mission. For example, dedicated 5G networks enable "train like you fight" readiness by better preparing war fighters through training environments that emulate real battlefield conditions, but also reduce costs by allowing them to use the same equipment in both training and tactical deployments, eliminating the need to purchase and manage separate technologies. Furthermore , this type of unified approach also streamlines the cost and effort needed to safeguard the security of communications for both types of deployments.

Specific items directly tied to cost for CONUS and OCONUS 5G coverage deployment and downstream costs over a multi-year period include:

- Avoid vendor lock-in, which can prevent control over downstream service deployment and costs.
- Avoid a collage of domestic networks versus a unified communication strategy to minimize 5G equipment and services retooling costs as soon as an OCONUS tactical deployment occurs.
- Economies of scale derived from a holistic DoD 5G strategy for U.S. installations CONUS and OCONUS (build and strengthen a shared eco-system focused on supporting DoD use cases)
- Cost of time and expense when trying to fit a public network design into the strict confines of federal compliance to address security versus a product defined for federal government secure communications use.
- Choosing a flexible network solution that allows ease of deployment and operational simplicity for both domestic and OCONUS use cases.

Ultimately, the multi-year cost must be looked at from an upfront and post deployment CapEx and OpEx perspective, as well as the downstream consideration of mission efficiency.

Conclusion

For the U.S. federal government, particularly the DoD, communication networks are far more than a utility – they are critical infrastructure of paramount importance to national security. While the DoD continues to lead the push for private 5G, it is imperative to strike the right balance between private and public network solutions. Public and hybrid commercial carrier networks remain a practical solution for a wide set of agencies, particularly those not tied to mission-critical applications. However, they fall short in meeting the specialized capabilities required for agencies centered around national security or with distinct performance and compliance requirements. Dedicated private 5G networks have emerged as a crucial mobile communication solution, offering unmatched control, security, and adaptability to meet the demands of critical installations.

Dedicated private networks can excel in safeguarding sensitive communications through stringent security controls, adherence to Zero Trust principles, and compliance with federal mandates. Their isolation from public infrastructure minimizes vulnerabilities, such as unauthorized surveillance and data breaches, which have become increasingly prevalent on public carrier networks. They are uniquely positioned to address strategic DoD use cases, such as:

- Enabling seamless "train like you fight" environments
- Interoperable communications between military branches and allied forces
- Flexibility to operate on shared military frequency bands for cohesive, secure coordination
- Safeguarding mission-critical traffic while allowing personal connectivity on military bases

These capabilities make dedicated private 5G networks an essential component in the U.S. federal government's effort to modernize its communication infrastructure, strengthen national security, and maintain technological leadership.

References

1. **Secure 5G and Beyond Act of 2020, Public Law No: 116-129:** https://www.congress.gov/116/plaws/publ129
2. ***"Department of Defense Private 5G Deployment Strategy",*** October 2024: https://dodcio.defense.gov/Portals/0/Documents/Library/Private5GDeploymentStrategy_508.pdf
3. ***The GSA "Acquisition Guidance for Procuring 5G Technology",*** March 2023: https://buy.gsa.gov/api/system/files/documents/GSA%20Acquisition%20Guidance%20for%20Procuring%205G%20Technology%20508_0.pdf
4. ***"AT&T Addresses Illegal Download of Customer Data":*** https://about.att.com/story/2024/addressing-illegal-download.html
5. ***"Verizon Data Breaches: Full Timeline Through 2024"***: https://firewalltimes.com/verizon-data-breaches/
6. ***"T-Mobile Confirms it Was Hacked in Recent Wave of Telecom Breaches"***: https://www.bleepingcomputer.com/news/security/t-mobile-confirms-it-was-hacked-in-recent-wave-of-telecom-breaches/
7. ***"Salt Typhoon" incident***: https://www.wsj.com/tech/cybersecurity/typhoon-china-hackers-military-weapons-97d4ef95?st=YMdezA&reflink=desktopwebshare_permalink
8. The CISA ***"Mobile Communications Best Practice Guidance"***, December 2024 : https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf
9. **"XZ backdoor"**: https://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094
10. 10. The NTIA ***"National Strategy to Secure 5G Implementation Plan"***, January 2021: https://www.ntia.gov/other-publication/2021/national-strategy-secure-5g-implementation-plan
11. ***"Department of Defense 5G Strategy Implementation Plan",*** December 2020: https://dodcio.defense.gov/Portals/0/Documents/Library/Private5GDeploymentStrategy_508.pdf
12. ***"Fulcrum: The Department of Defense Information Technology Advancement Strategy",*** June 2024: https://dodcio.defense.gov/Portals/0/Documents/Library/FulcrumAdvStrat.pdf
13. **National Defense Authorization Act (NDAA) FY2022,** Section 242(b)(3): https://www.congress.gov/bill/117th-congress/house-bill/4350
14. The NIST ***"Secure Software Development Framework (SSDF)"***: https://csrc.nist.gov/Projects/ssdf
15. Executive Order on America's Supply Chains: https://www.govinfo.gov/content/pkg/FR-2021-03-01/pdf/2021-04280.pdf
16. **Executive Order on Improving the Nation's Cybersecurity:** https://www.govinfo.gov/content/pkg/CFR-2022-title3-vol1/pdf/CFR-2022-title3-vol1-eo14028.pdf
17. ***"O-RAN Security Requirements Specification"***: https://www.o-ran.org/specifications