INTRODUCTION

DISH is a connectivity company. Since 1980, it has served as a disruptive force, driving innovation and value on behalf of consumers. Through its subsidiaries, the company provides television entertainment and award-winning technology to over eleven million customers with its satellite DISH TV and streaming SLING TV services. In 2020, the company became a nationwide U.S. wireless carrier through the acquisition of Boost Mobile. DISH continues to innovate in wireless, building the nation's first cloud-native, Open-RAN-based 5G broadband network.

DISH has invested over $21 billion in wireless spectrum assets with the goal of entering—and disrupting—the wireless industry. DISH was excited to acquire the prepaid wireless service Boost in July of 2020 and currently has over 9 million subscribers through that brand. Meanwhile, the company has been hard at work building the nation's first Open-RAN, virtualized, standalone 5G broadband network. DISH's emergence as a competitor in the wireless industry means that it will be a critical participant in the United States' "race to 5G" against other countries.

DISH, a Fortune 200[1] company, was founded in 1980. In 2008 EchoStar, a Fortune 1000 company, was spun off and later acquired Hughes Communications in 2011. Hughes Network Systems is the leading provider of satellite broadband services and brings broadband to the most remote areas of the United States. DISH and EchoStar are both headquartered outside of Denver and together employ approximately 18,000 people throughout the United States. The DISH family also includes thousands of independent retailers and distributors – local small businesses that are on the ground promoting and installing DISH products in every state, including the country's most rural areas.

Just as we were challenged to offer satellite television services, we are challenged once again to offer unparalleled wireless services on our 5G network across the U.S. We are pleased to participate in this RFI by lending our expertise and experience in 5G.

RFI QUESTIONS

DISH provides the following responses to the RFI questions:

3.A How could DoD own and operate 5G networks for its domestic operations? What are the potential issues with DoD owning and operating independent networks for its 5G operations?

DISH respectfully opposes any proposal to create a nationalized, government-owned and operated 5G network. We believe that the task for DOD to build and deploy all of the equipment and systems, including, but not limited to: hardware, software, power systems,

[1] This includes the acquisition of Boost Mobile.

physical towers, optical fiber cable systems and microwave radios, is an inefficient use of DoD resources.

Figure A.1 below depicts a scenario in which the DoD owns and operates a 5G network for its domestic operations.

It may be possible for the DoD to deploy a dedicated network within each DoD facility and interconnect with national commercial operators to roam onto the commercial networks for additional coverage and capacity. However, the device interoperability between the different networks will be limited and expensive, depending on the scale of the device ecosystem.

There are also limited controls available to the DoD through traditional commercial roaming agreements and certain security considerations that need to be considered. The device ecosystem to support DoD specific spectrum allocated and deployed within the DoD facilities also represents a significant challenge. A cost-effective device ecosystem is achievable, when spectrum is deployed at scale across a national network, specifically when the device development can be amortized across a large customer base.

Figure A.2 below shows a scenario in which the DoD owns and operates a network within each DoD facility, but interconnects with commercial operators for national coverage and roaming arrangements.

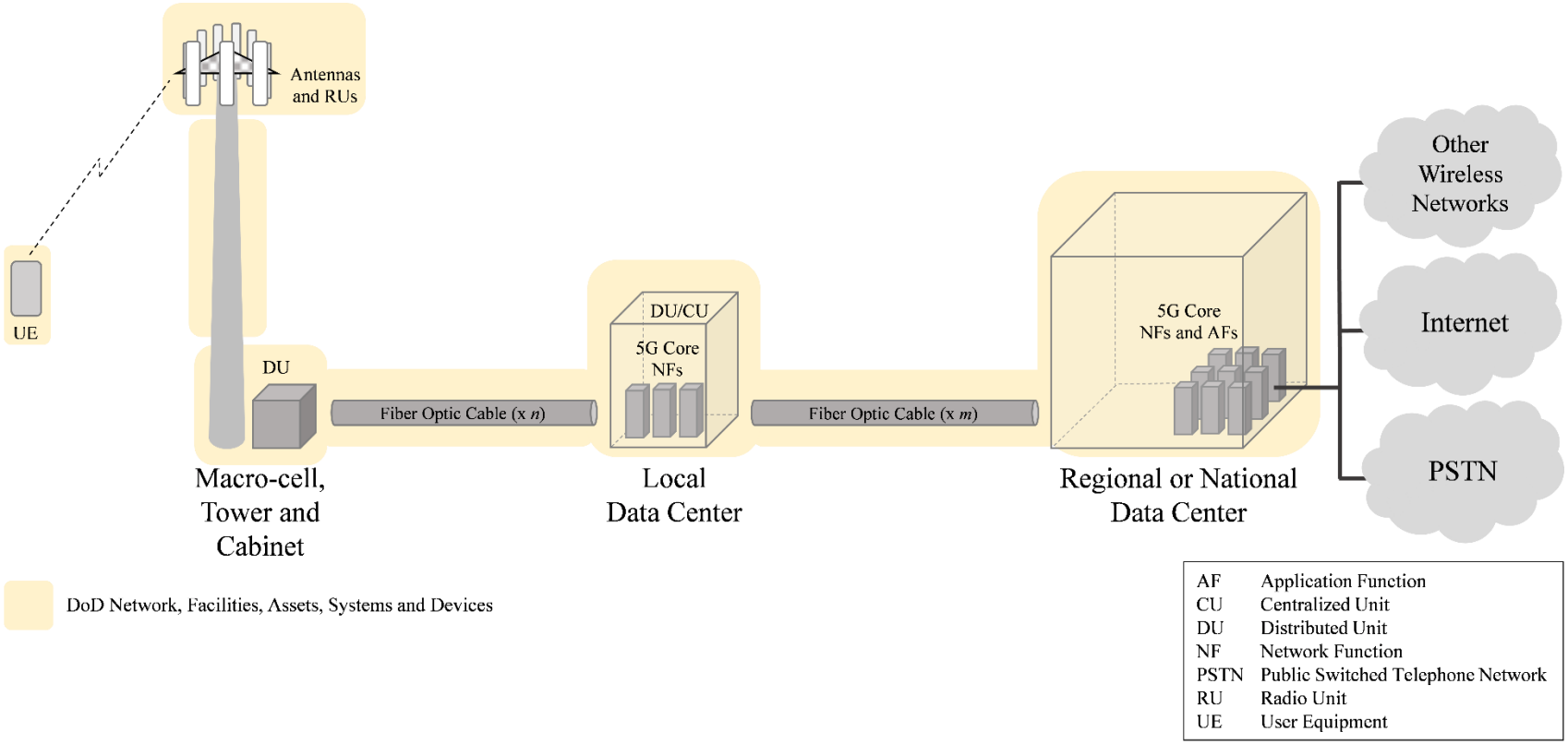

Figure A.1: A DoD owned and operated 5G network.

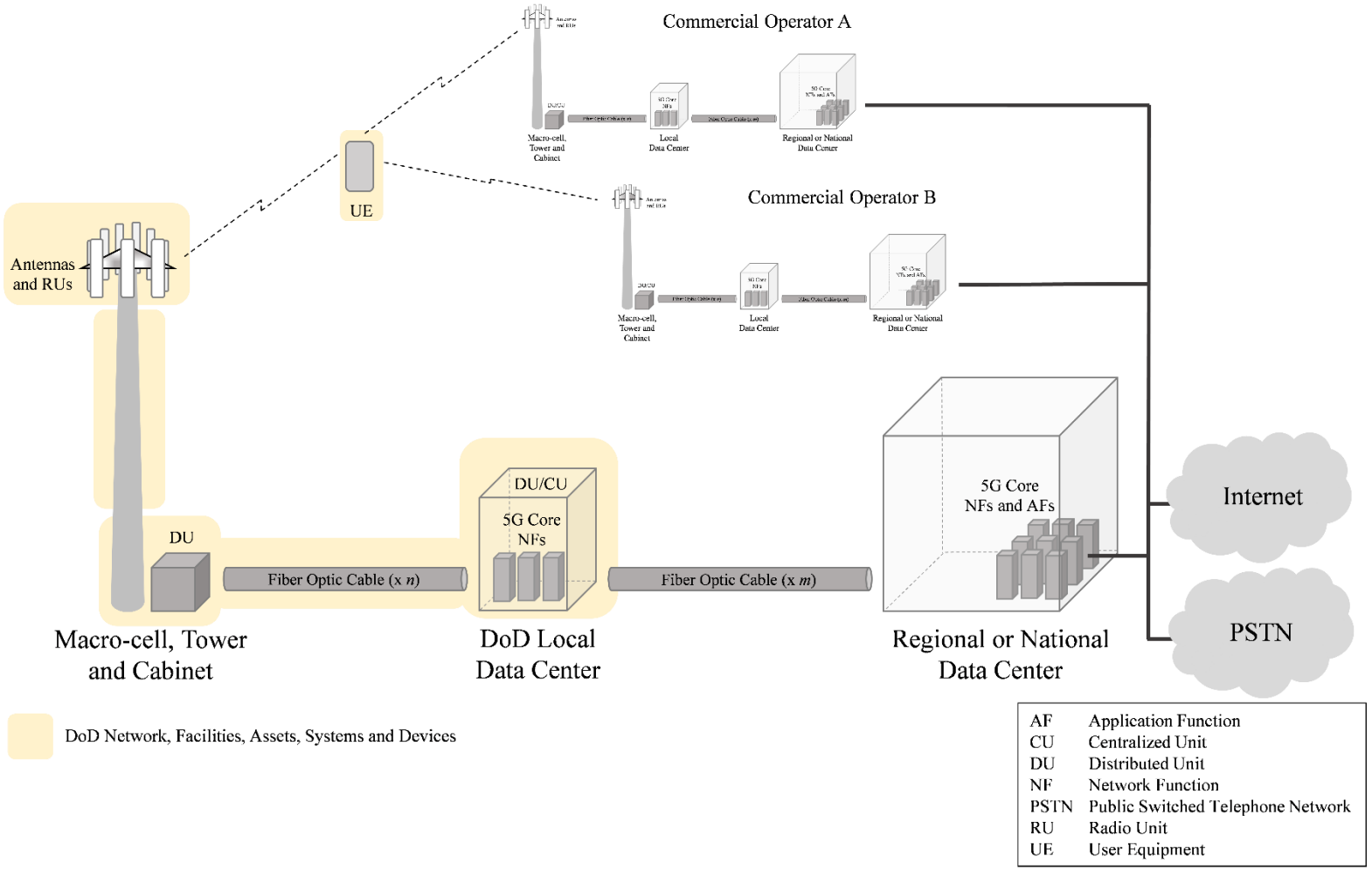

Figure A.2: A DoD owned and operated 5G network within DoD facilities, with national commercial roaming.

Network operators in the U.S. today share certain infrastructure to reduce the cost of their services, while maintaining operational control over network services, the radios and the spectrum. ***Figure A.3*** shows a typical configuration for operators sharing facilities, while maintaining operating control of the network services.

There is a precedent for how the DoD can take advantage of shared physical assets and network resources, while maintaining operational control and flexibility to support the DoD's objectives. One example is the use of satellite transponder capacity on commercial satellites. The DoD can lease these transponders and then use DoD controlled ground systems, terminal equipment, hardware and software without compromising operational flexibility or capabilities.

FIRSTNET is another example of a commercial network deployment where the public safety spectrum has been deployed on a commercial network with preemptive access for public safety purposes. FIRSTNET and the commercial deployment each retain their own core network in this model and share access to spectrum and other network resources, including the radio at a cell site within the AT&T network. In order to meet the coverage requirements for FIRSTNET, AT&T has continued to add macro-sites to their network. This capability utilized the deployment of LTE technology and Multi-Operator Core Network (MOCN) standards.

The functionality available within 5G standards allows network function disaggregation and sharing of resources to be taken to a new level. 5G provides more robust capability to provide the DoD with any number of dedicated network slices.

DISH's first-of-a-kind network deployment will be uniquely positioned to take full advantage of the next generation of mobile connectivity. The functionality available to a cloud–native, software-based 5G Open-Radio Access Network (O-RAN)[2] enables significantly more control over all network resources from the spectrum to the core, which allows us to provide enterprise and wholesale customers a dedicated network slice[3].

The DoD can securely control and operate a 5G network enabled network slice for its domestic operations, across a nationally-scaled DISH 5G cloud-native network.

This next generation network effectively enables the DoD to manage and control a slice of DISH's network, together with specific spectrum resources, while reducing the cost and accelerating the availability of secure 5G services for the exclusive use of the DoD. The high-level architecture of this type of a network is shown in ***Figure A.4***. This network can take advantage of dedicated DoD spectrum, commercial spectrum and shared spectrum.

The deployment of Citizen Broadband Radio Service (CBRS) spectrum and the use of a Spectrum Access System (SAS), with the appropriate sensor network in place, is one example of how spectrum can be shared between the military and commercial operators. The recent success of Auction 105 highlights the value commercial operators are

[2] "Towards an Open and Smart RAN", O-RAN Alliance, October 2018.
[3] "An Introduction to Network Slicing", GSMA White Paper, 2017.

willing to place on shared-use spectrum, which can also be deployed for commercial services.

DISH supports the findings of the NTIA report[4] on the technical feasibility of sharing Federal spectrum with commercial operations in the 3450-3550 MHz band; more specifically that dynamic, time-based sharing is a technically feasible approach to protecting federal systems while providing access to the DoD spectrum for commercial operations.

The proposed solution in this response addresses the potential issues with DoD owning and operating a separate and independent network for its 5G operations.

[4] "Technical Feasibility of Sharing Federal Spectrum with Future Commercial Operations in the 3450-3550MHz Band", NTIA Technical Report 20-546, January 2020.

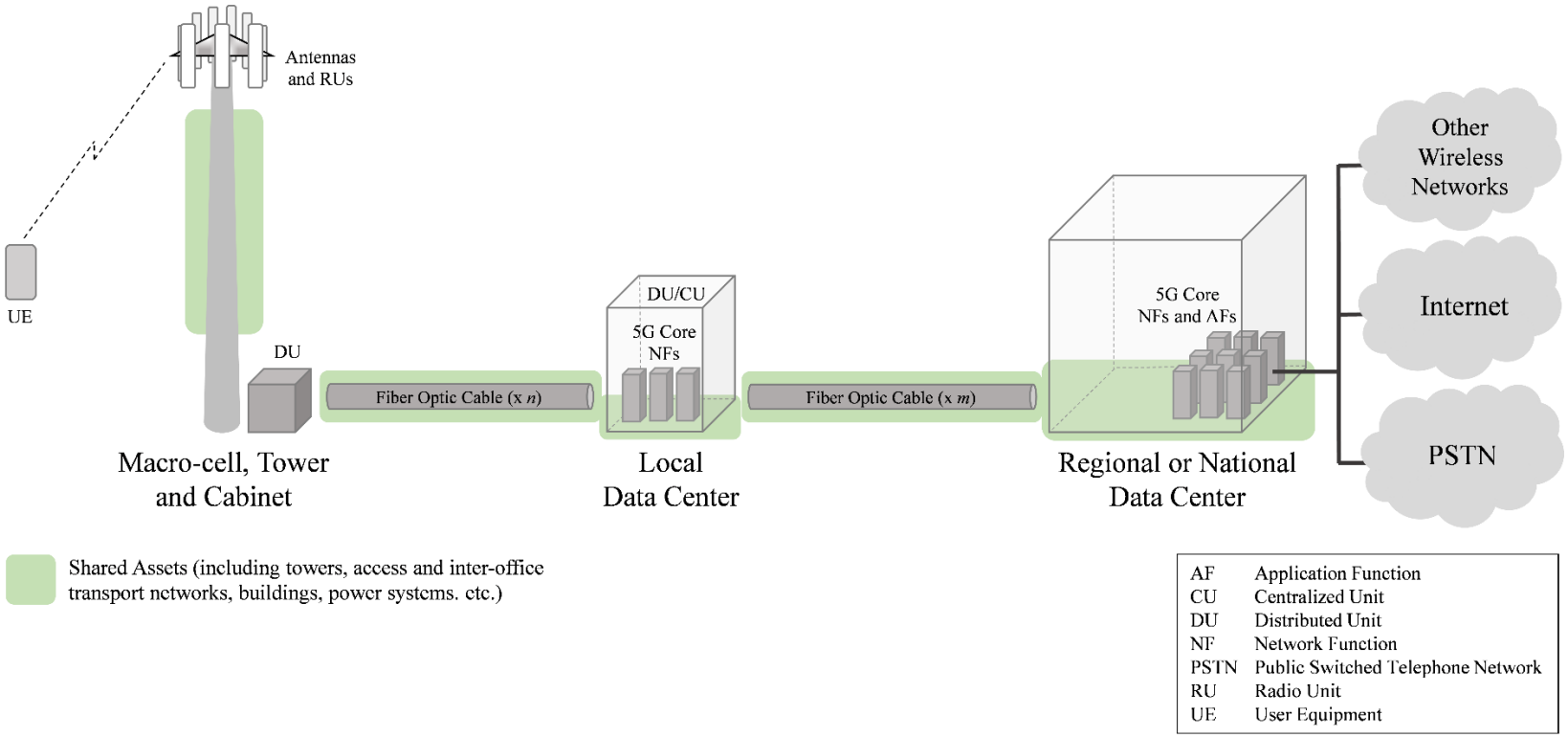

Figure A.3: Typical network operations for a national wireless operator.

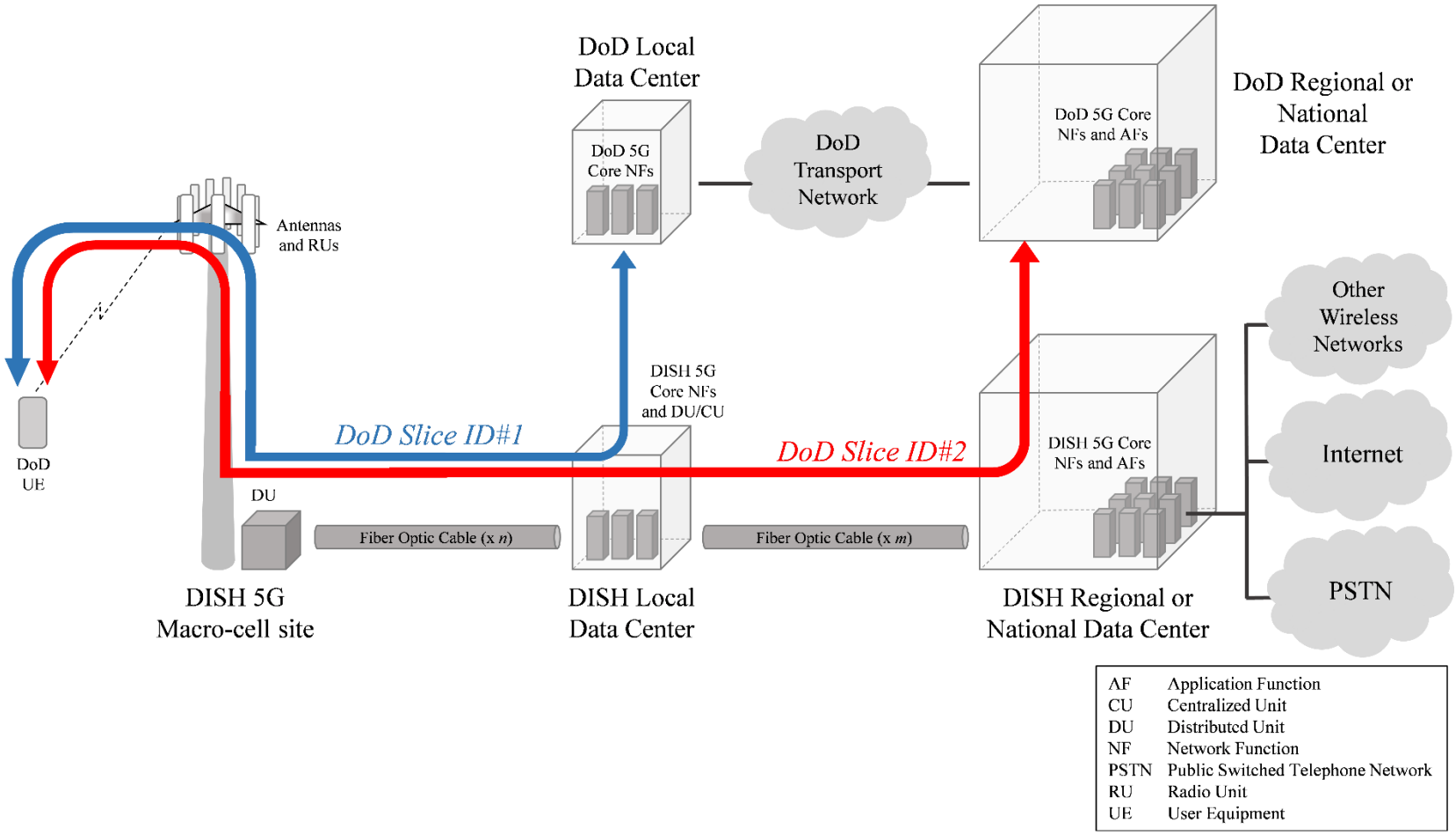

Figure A.4: DoD dedicated network slices, enabled through the DISH 5G Network.

3.B While the Department has made available the 3450-3550 MHz spectrum band for 5G, are there new technologies or innovative methods as to how additional mid-band spectrum currently allocated to DoD can be made available for 5G faster?

By utilizing an O-RAN model, with standardized, open and interoperable interfaces between the Radio Unit (RU), Central Unit (CU) and Distributed Units (DU), DoD could enable a more rapid deployment of new spectrum. In order for spectrum to be utilized, new RUs will need to be developed and deployed to take advantage of additional mid-band spectrum.

Through advances in radio and antenna technologies as well as disaggregated hardware and software, radios are able to carry multiple spectrum bands. This allows 5G infrastructure to be leveraged and additional spectrum to be deployed and integrated into the 5G core network.

In a distributed software-defined architecture, such as the one DISH is deploying, new technologies and features specific to new spectrum bands can be added as upgrades to applications without disrupting existing operations.

Additional mid-band DoD spectrum could be made available through a similar approach to the solutions which have been deployed for CBRS.

A combination with the DISH 5G network, which includes substantial low-band and mid-band spectrum, offers a more robust and cost-effective solution than a single frequency band network.

3.C What are other innovative ideas as to how 5G can share spectrum with high-powered airborne, ground-based and ship-based radar operations in the 3100-3550 MHz spectrum band?

One approach would be to leverage the CBRS hierarchical Dynamic Spectrum Sharing (DSS) model along with other licensed spectrum to meet the needs of customers in the 3100-3550 MHz band. DoD spectrum could be deployed across the DISH 5G network and dynamically managed by the DoD, based on its operational needs. This could be achieved with a DoD controlled incumbent-informing SAS.

The DoD could utilize commercial spectrum bands deployed throughout DISH's network when the 3100-3550 MHz DoD spectrum is unavailable due to the use of high-powered airborne, ground-based and ship-based radar systems. Access to the commercial bands could be facilitated by provisioning DoD dedicated network slices.

DISH's software architecture will allow the DoD to create a policy-based approach to autonomously manage its users in terms of when, where and how they access the spectrum.

Private DoD dedicated network slices represent an end-to-end solution that can be used to guarantee a level of service. While there are many flavors of network slicing, the ability to guarantee a level of service through a slice specific Service Level Agreement (SLA) is only

possible through the cloud-native, standalone 5G network architecture DISH is deploying. Each DoD network slice could have its own performance characteristics along with an associated SLA, that can be securely managed by the DoD. Separate networks do not have to be constructed to support each network slice, thereby making this a scalable and cost-effective solution.

3.D Are there other spectrum bands that can be made available to share quickly in the low and high band spectrum ranges?

As explained above, DISH is deploying a cloud-native, next generation, standalone 5G network using multiple commercial nationwide spectrum bands (between 600 MHz and 2 GHz) and CBRS spectrum. By bringing together innovations such as the distributed cloud, edge computing and network slicing, our software-based network could provide the DoD a customizable, secure network solution on our commercially-deployed spectrum bands, in addition to new DoD spectrum. Access and capacity to the network resources could be either dedicated or shared, or multiple network slices could be established with different service level agreements, as described in C above.

The time taken to deploy new spectrum bands will be constrained by the development time for the new radios and device ecosystem. The O-RAN architecture adopted by DISH facilitates the timely integration of new spectrum bands and there are many more options available to the DoD and DISH to securely source radios to support the additional spectrum.

The network functionality enables the DoD to manage and control their slice of the network and allocated spectrum as if it were a private DoD operated network. The advantage of access to commercially-deployed spectrum is the availability of a robust commercial device ecosystem and the coverage available through the entire DISH network.

Additional spectrum that may be acquired by DISH could also be made available to the DoD through dynamic provisioning and reconfiguration of the DoD 5G network slices. The network slices are not static and can be dynamically updated based on the needs and requirements of the DoD.

Figure D.1 shows an example for how a combination of existing commercial bands supported on the DISH network, and new undefined spectrum bands, can be made available to DoD devices. In the proposed solution, the DoD can manage the DoD spectrum through a dedicated SAS, providing control over the spectrum allocation on the RUs.

As other spectrum bands are made available, additional RUs associated with the new spectrum can be integrated into this network.

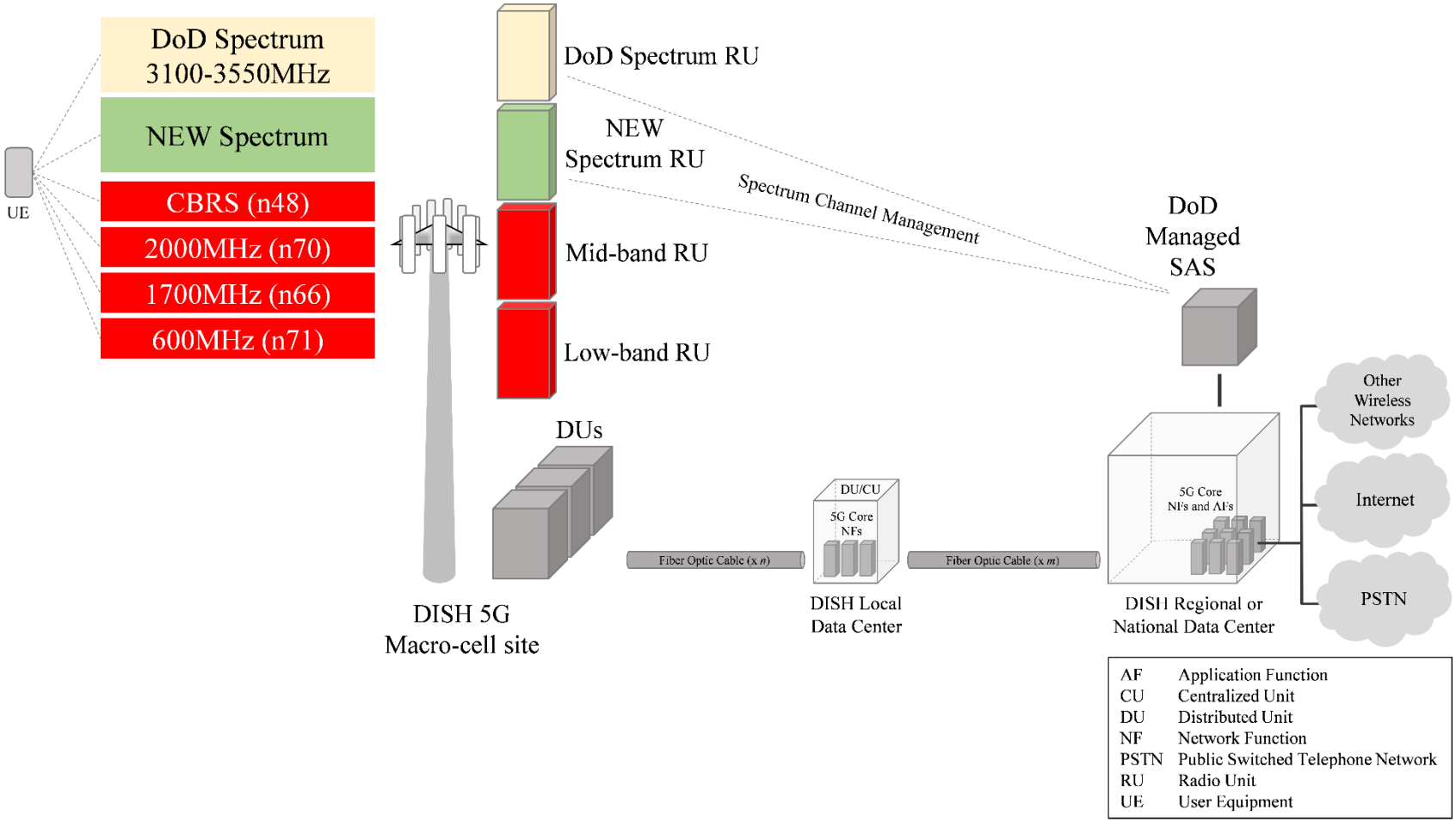

Figure D.1: Shared access to existing commercial spectrum, DoD spectrum and new bands on the DISH 5G Network.

3.E What types of technologies exist, or are anticipated, that will allow civilian users to share spectrum faster?

In order to provide access to spectrum, it is critical for a radio and antenna to be deployed at each site to enable expedited access to shared spectrum. The physical deployment of the radio and antennas at each site across the network will limit the speed at which a civilian user can access shared spectrum. Aside from the timing for the build-out, a robust commercial device ecosystem supporting the shared spectrum and features such as carrier-aggregation is a prerequisite for timely access to this spectrum.

From the point at which spectrum is made available, it can take five to seven years for a robust device ecosystem to be in place to allow for commercial and civilian use of the spectrum, unless the band is either adjacent to an existing commercial system or there is an existing global ecosystem to leverage.

Most operator networks today are limited to using existing and incumbent vendors in the radio access network. It is technically challenging for an incumbent operator to combine different radio vendors with existing baseband systems.

The 5G O-RAN-based network DISH is deploying will provide a platform to allow multiple vendors to be integrated and deployed at a site, supporting different spectrum allocations. An example of this configuration is shown below in ***Figure E.1.***

By deploying an open-RAN, cloud-native architecture, U.S.-based vendors can develop software and hardware that can be integrated and deployed at scale more rapidly than a vertically integrated environment with incumbent wireless vendors.

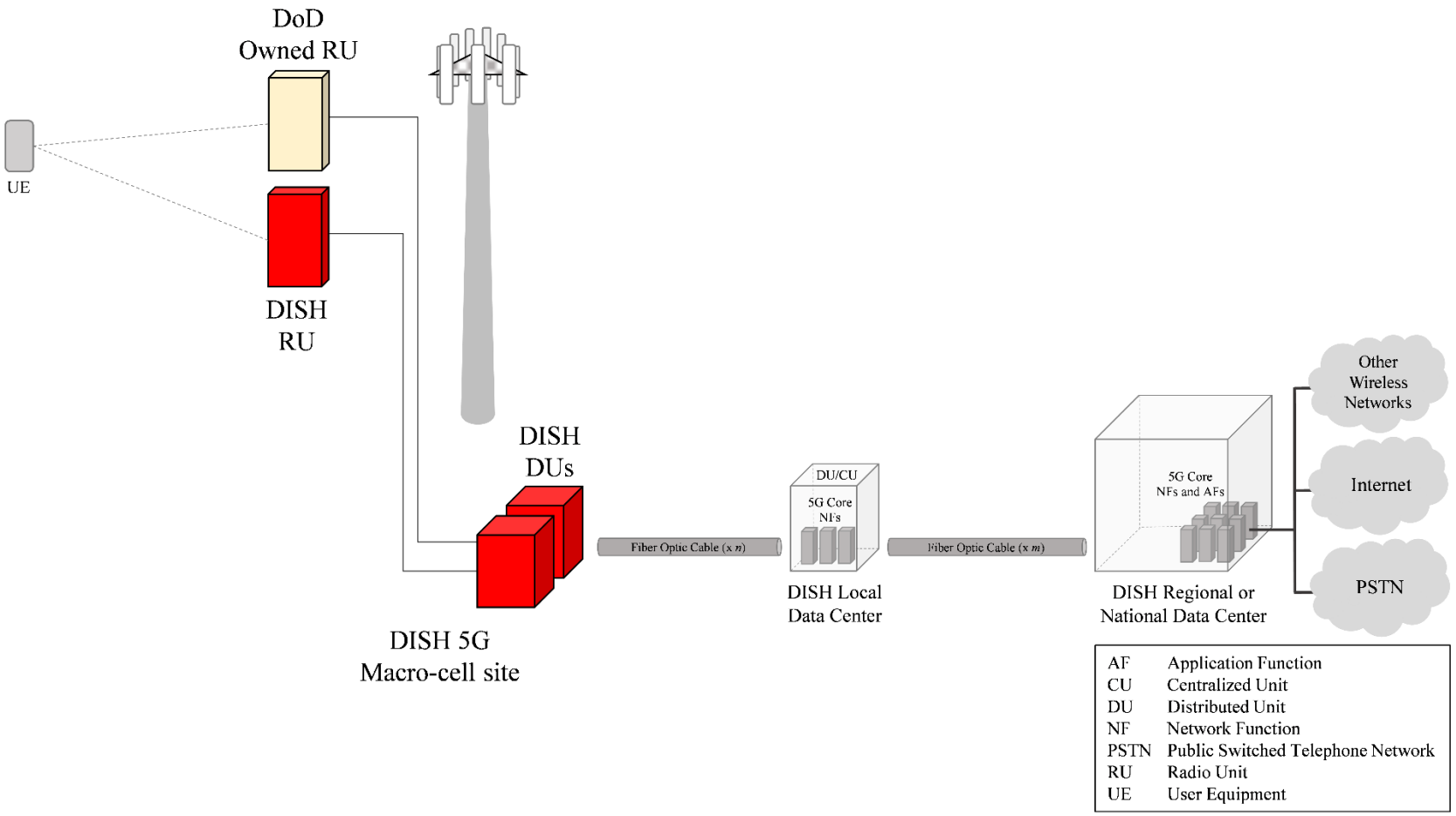

Figure E.1: Example of Adding New Radios and Multiple Vendors to an Existing DISH Site.

3.F Do you foresee any national security concerns with DoD sharing with commercial 5G?

The DoD can operate and manage their own secure network slices together with an incumbent-informing SAS system, with a DoD controlled access for all shared DoD spectrum, with a time-based sharing mechanism, consistent with the approach described in the NTIA report.

The dedicated DoD network slices and this system would address the challenges to potential operational security, continuity of operations and the specific cyber security posture of the DoD. The DISH 5G cloud-native network and the proposed solution take into consideration the national security concerns and the need for operational security.

National Security considerations for DoD sharing with commercial 5G providers

The United States National Cyber Strategy has stated that: "The Administration will facilitate the accelerated development and rollout of next generation telecommunications and information communications infrastructure here in the U.S., while using the buying power of the Federal Government to incentivize the move towards more secure supply chains. The U.S. Government will work with the private sector to facilitate the evolution and security of 5G, examine technological and spectrum-based solutions, and lay the groundwork for innovation beyond next-generation advancements."

The DISH security strategy aligns with the U.S. National Cyber Strategy and is committed to providing the most advanced and fully secure standalone 5G network to support this directive.

Foreign and legacy equipment risks

According to U.S. government authorities, equipment made by foreign states may pose a national security risk through unauthorized exfiltration of data flowing through the equipment or a disruption of service. In addition, the use of legacy telecom infrastructure augmented with 5G capabilities may expose additional vulnerabilities and diminish the security benefits associated with a standalone, fully virtualized 5G network architecture.

Given the sensitivity of the information traversing 5G networks, it is important that the below recommendations are taken into consideration when evaluating this proposal.

Fully virtualized standalone 5G core

As published by the Intelligence and National Security Alliance, recommendations for regaining U.S. leadership in wireless technology include the development of containerized security functions, virtualized 5G networks, zero trust concepts and the use of artificial intelligence. The DISH 5G network, based on the O-RAN architecture, combined with our fully virtualized standalone architecture supports these security imperatives.

Any DoD network slice would be built on virtual network functions (vNFs) designed by companies who operate within the U.S. or other allied countries, and are controlled by U.S.

entities or those of other allied countries. DISH is deploying this type of a network and can provide network slices with the ability to fully isolate these slices from other commercial or government customers within the network. The DISH architecture is based on cloud native principles that can allow the DoD to add additional security and monitoring measures, as needed, to the DoD slices. The core vNFs, as well as any backups or copies, reside within the U.S. Critical intellectual property and core source code are also within the U.S. The DISH network design is based on an O-RAN topology that allows for interoperability of different radio unit providers through an open architecture. This limits the dependency and supply chain risk of a single vertically integrated provider, and supports the quick isolation of affected segments of the network.

An O-RAN architecture provides added security benefits and monitoring capabilities.

Separate security posture for a DoD

DoD network slices will be able to maintain an advanced security posture that differs from the standard security posture of other commercial network slices. This helps ensure that a domestic attacker could not use their commercial 5G provider to test for vulnerabilities or attack vectors of the DoD network slice. The functionality within the network will provide the capability to quickly instantiate a new network slice and seamlessly absorb traffic from a compromised slice.

End-to-end encryption

The DoD network slices can be supported with sophisticated end-to-end encryption of the user plane traffic. The encryption keys shall be owned or held solely by the DoD. The encryption mechanism will include the ability to enable multipathing of encrypted traffic to increase the resilience and protection of sensitive data.

Advanced threat intelligence through AI and Big Data

Any DoD network slice can include the ability to collate, manage and interpret the security and operations logs. The solution can support the use of sophisticated AI and ML algorithms to autonomously identify patterns, behaviors and anomalies within these large datasets, and initiate automated incident response through the security orchestrator to swiftly and dynamically resolve security incidents or events.

Continuous and independent threat hunting / penetration testing

Components of the network are changing and threats are continually evolving. The solution proposed includes a security slice that can be used to continuously test the security posture of a production state through a combined internal threat hunting and external penetration testing model. In addition, a dedicated security slice allows for new software and solutions to be tested in a production mode without the risk of impacting operations.

User equipment (UE) protection

UE protection is established as close to the edge as possible to prevent authorized devices on the network from becoming compromised and attacking the network from within. The DoD network slice will have the ability to protect UE through AI and behavioral pattern analysis. In addition, a root of trust can be established to ensure that a device on the network is authorized to be attached to the DoD network slice.

Security controls embedded in the design of the DoD network slice

Security controls can be embedded into the DoD network slice and they can include: UE protection, denial of service protection, identity and access management, behavioral anomaly detection, endpoint protection, certification lifecycle management, firewalls and gateways, container security, zero trust architecture, mutual authentication, management of network function communications, and an integrated security incident and event management platform supported by a security operations center.

3.H What are other current and perceived barriers that industry is aware of to DSS?

DISH does not believe there are technical limitations with the deployment and use of DSS, with the proposed solution, using time-based and DoD controlled access to the DoD spectrum. The requirement for any traditional commercial operator is the need for predictable and deterministic access to capacity for customers.

The capital investment and marginal operating cost required to deploy new radios and systems with a new spectrum band across a national network is significant. To achieve a reasonable return on this investment, an operator requires a sufficient margin on the incremental usage. DSS can add uncertainty and risk to the available capacity.

Given the relative fixed cost structure of the network, the effective cost per unit of capacity increases with this uncertainty. The additional risk and operational uncertainty increases the commercial cost to adoption of DSS and shared spectrum. A similar dynamic exists within the satellite industry with on-demand and time-based access to transponder capacity.

FIRSTNET and the commercial deployments of CBRS have demonstrated how operators can deploy shared use of new spectrum. These two examples highlight two different approaches, which balance the needs of different stakeholders, while allowing for dynamic access to the spectrum.

3.I How would DSS work with existing commercial spectrum bands?

The use of DSS for specific DoD spectrum, in conjunction with dynamic network slice management, would provide the DoD with both predictable and on-demand access to network resources. The capacity within the commercial network can be set up through a network slice to provide the DoD with a number of private networks with a predictable performance.

DoD spectrum that is not being used for other DoD-specific purposes could be added through a DoD controlled DSS platform to the commercial network, either for use by DoD or the commercial operator. An example of this is shown in ***Figure I.1.***

Between the user equipment and the network, it is possible to utilize either the commercial spectrum, or the DoD spectrum, if available. The proposed adoption of DSS is only applicable to the DoD spectrum.

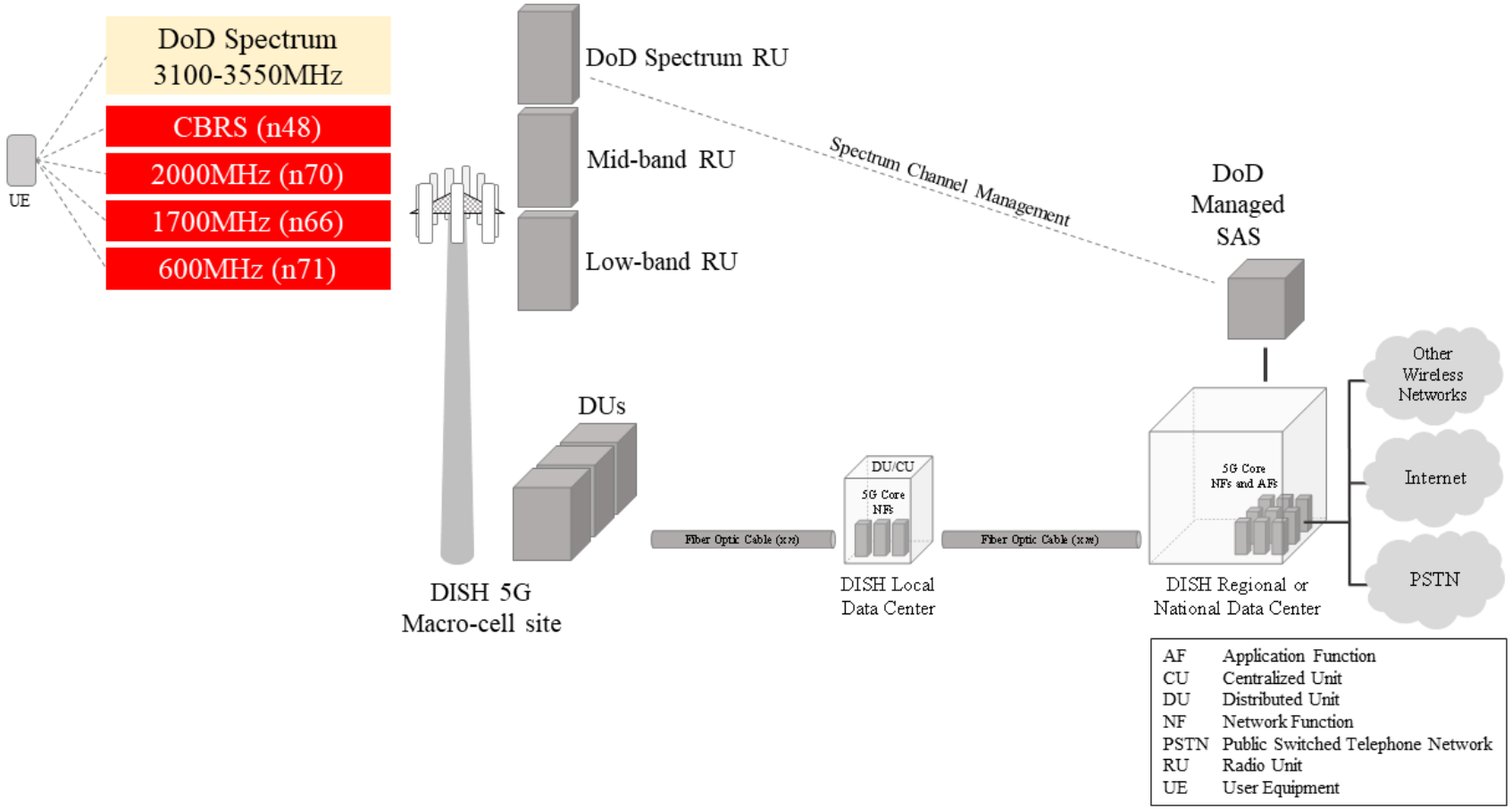

Figure I.1: The use of DoD controlled DSS with existing commercial spectrum bands.

3.J Could multiple DSS technical solutions coexist and under what conditions?

There are multiple shared spectrum solutions that have been deployed in the market. Most of the solutions fall into one of five categories. The below tables provides a summary of the different solution categories:

	DSS Technical Solution Categories	Description
1	Open Access model	Unlicensed spectrum access to all users, such as Wi-Fi 2.4 GHz, 5 GHz and High-band mmWave 60 GHz.
2	Licensed Assisted Access model	Licensed Assisted Access (LAA) is currently a feature of 4G LTE that leverages unlicensed spectral bands in combination with licensed spectrum to deliver increased net performance for mobile device users. The most common example is the use of carrier aggregation (downlink) to combine 4G LTE in unlicensed 5 GHz band with 4G LTE in a licensed band to provide increased overall bandwidth and a better user experience.
3	Licensed Shared Access model	License Shared Access (LSA), in which license holders can sub-license specific spectrum to other users in a controlled way. Carrier A (license holder) may sub-license or provide access to non-license holders (Partner X) under a business arrangement or a government-authorized program.
4	Hierarchical model	CBRS (3,550-3,700 MHz) in the U.S. utilizes a Spectrum Access System (SAS) to monitor and manage spectral access across licensed and unlicensed spectrum.
5	Cooperative Shared Access model	Also known as Concurrent Shared Access (CSA), licensed spectrum partners can agree to share use of same spectral bands in the same geographic location to increase coverage or services.

Any combination of the shared spectrum categories may be theoretically possible, yet the business and technical feasibility is dependent on a number of factors. Business factors include but are not limited to market demand, geographic considerations, business case justification, partner arrangements and investment requirements. Technical factors include but are not limited to solution compatibility across networks and users, network component compatibility, system integration and coordination, chipset and device compatibility, geographic considerations and spectral interference mitigation.

Each approach is spectrum band dependent and to achieve operational efficiency. It is DISH's recommendation to adopt a standardized approach and adoption of one solution for DSS in the

DoD spectrum band. A fractured approach to sharing and dynamically allocating spectrum resources within a band will drive inherent inefficiencies and create barriers to deployment.

3.K How can spectrum modernization, including spectrum Information Technology (IT) modernization and automation, help facilitate faster spectrum sharing?

The device ecosystem, chipset support, and modem and filter development is the key challenge to wide-scale adoption and cost-effective use of any new spectrum band. The development cost and the time to launch new bands are significant. The more certainty and duration of access to spectrum will result in lower risks to this investment.

Once an ecosystem is in place, spectrum can be managed and shared dynamically through multiple approaches, as discussed above. Systems exist today that can be enhanced as software and hardware continue to evolve. DISH's 5G network is based on Open APIs allowing ML algorithms to perform pattern recognition and application analysis that can help to optimize spectrum sharing. The capability of the algorithms can improve with the increasing compute available in both devices and radios. The speed at which systems can adapt to changing conditions will also increase in line with the continuing evolution of processors.

3.L Are there standards, including data standards, which could accelerate spectrum repurposing decisions? If so, what are they?

While industry standards are critical to achieve economies of scale, the time it takes to move through the standardization process is a constraint on the speed at which the wireless industry moves. Unfortunately, even when systems are compliant with industry standards, there are often configurations or parameters that are undefined and can lead to a lock-in with certain vendors and suppliers.

Moving away from a vertically integrated, closed ecosystem is a critical first step to accelerating the adoption of new technologies and deploying new spectrum faster in a network. This is a contributing factor in the decision DISH made to deploy an O-RAN-based network. An open and interoperable architecture with standards based interfaces enables multi-vendor competition and innovation to be unlocked in areas that were traditionally constrained.

New radios can be developed by suppliers for new spectrum bands, potentially working with the DoD, and integrated more rapidly into the DISH network.

As mentioned above, the radio and the network are only a part of the solution; a device ecosystem needs to be put into place in parallel. This development can take considerably longer for cost effective devices to be introduced into the market. The development time and the cost for any commercial device can be influenced by many factors.