Response to 5G Notice of Inquire from

National Telecommunications and Information Administration on 01/11/2021

Leveraging the U.S. Army CMOSS Ecosystem for Open 5G Stack Development and DoD Insertion

This proposed effort leverages the existing research and development (R&D) partnership and collaboration on CMOSS with the U.S. Army Team Aberdeen Proving Ground (APG), through Cooperative Research Development and Agreement (CRADA). This CRADA effort is managed by U.S. Army Command, Control, Communications, Cyber, Intelligence, Surveillance and Reconnaissance Center (C5ISR CTR), in coordination with Program Executive Office, Command, Control, Communications Tactical (PEO C3T)

About Spectranetix

Spectranetix is a leading developer of C5ISR Modular Open Suite of Standards (CMOSS) and Sensor Open Systems Architecture™ (SOSA) aligned hardware and software solutions for the US Department of Defense. We have mature CMOSS aligned offerings that are already core subsystems in programs of record and are built to open architecture standards with highly flexible modular designs. In 2020, Spectranetix was acquired by Pacific Defense, which brought on a highly experienced team of executives and opened new partnership opportunities for capability and market expansion and high-volume production. Spectranetix has forged a strategic partnership with Regal Technology Partners that focuses on volume manufacturing process.

Contact Information

Niraj Srivastava
Vice President, Pacific Defense
Niraj.Srivastava@pacific-defense.com
508-364-4818

Daniel Kilfoyle
Chief Technology Officer, Pacific Defense
Dan.Kilfoyle@pacific-defense.com
508-274-1197

Paul Terzulli
US Army PEO C3T – PM I2S
paul.l.terzulli.civ@mail.mil
410-459-6785

Leveraging the U.S. Army CMOSS Ecosystem for Open 5G Stack Development and DoD Insertion

Executive Summary

The Department of Defense has sought open architecture weapon and sensor system solutions for well over 10 years. Within those effort, the C5ISR Modular Open Suite of Standards (CMOSS) stands out as a success. Our partnership (Spectranetix with the U.S. Army) matured CMOSS and realized the sought-after benefits of an open architecture for RF systems. In fact, CMOSS is a threshold requirement in multiple programs of record, speaking to that readiness. Based on this, we offer the lessons we learned for the Open 5G Stack Challenge. Our key messages are:

1- **The true measure of a successful open architecture is how finely distributed the components of a solution can be amongst different vendors.** One vendor's modular design that cannot be replicated by anyone else is not open.
2- **The flexibility, growth, and performance benefits of a software defined stack is best leveraged with an open, modular hardware baseline that allows re-architecting.** Physical layers and network layers supportable by separate, modular hardware enable rapid, incremental capability growth and various approaches to disaggregation. Military solutions may need varying degrees of local stack instantiation.
3- **The DoD has a unique need for communication solutions that integrate tightly with a multi-waveform and multi-function framework.** Multifunction goals drive spectrum cooperation and optimization rather than just deconfliction as spectrum co-use implies. Multifunction RF is central to the CMOSS architecture. We discuss specific 5G mission use cases that illustrate the unique needs of the DoD.
4- **Building the DoD open 5G capability on the successful and mature DoD CMOSS ecosystem will accelerate transition to and integration with the warfighter.** The DoD has an urgent need to confront national threats. Insertion of 5G technology into a deployed CMOSS infrastructure can happen far faster than possible with a conventional, standalone acquisition. Furthermore, our international allies (Australia, Canada, and the United Kingdom) are incorporating CMOSS into their RF modernization programs further enabling the rapid uptake of CMOSS based Open 5G.

We recommend that the NTIA include a Challenge component that explicitly seeks a CMOSS-integrated 5G demonstration. We further recommend that the Challenge provide selected participants with sufficient funds to adapt, integrate, and demonstrate their existing 5G technology into the U.S. Army Future Command's premier multi-disciplinary demonstration event, Project Convergence. By leveraging CMOSS and Project Convergence, NTIA will jumpstart adoption of 5G technology by the DoD.

Challenge Structure and Goals

The greatest barrier to a robust, mature open 5G ecosystem (note the explicit extension beyond an open 5G stack) is a weak and narrow concept of openness. The DoDs experience with modular open system architectures (MOSA) includes numerous failed efforts where the openness merely meant a published standard from a single vendor. A successful open system has a diverse vendor base with a single, enforced set of interfaces at a granular enough level that key system components can be separately competed and replaced with interoperability assured. A recent article discussing Dr. Jette's (Army Acquisition Executive (AAE)) statements said,

"Companies have been able to classify unique proprietary systems that other companies do not have the ability to manufacture as open systems by releasing the details, Jette said. He named data buses as an example of this trend. When this happens, market forces prevent actual competition for the nominally open system, Jette said. Potential competitors would have to invest significant sums to compete on formerly proprietary systems, so they cannot match the market leader on price and cannot actually compete for contracts."

These interfaces must be drawn from broadly available standards when possible. For instance, hardware standards based on specific instantiations of OpenVPX and software standards based on existing data interfaces such as VITA49.2 ensure small teams of innovators can bring their ideas into the system without insurmountable investment or development barriers. As an example of how CMOSS enables the insertion of innovation, we have built a fully CMOSS-aligned hardware baseline, provided interfaces between common software defined radio frameworks and the specific "MORA" messaging service and even connected the open system into the existing U.S. Army user interface and command/control infrastructure (**Figure 1**). This existing infrastructure would also minimize the need for Open 5G Stack innovators to understand the DoD product model which is substantially different than a commercial product model.

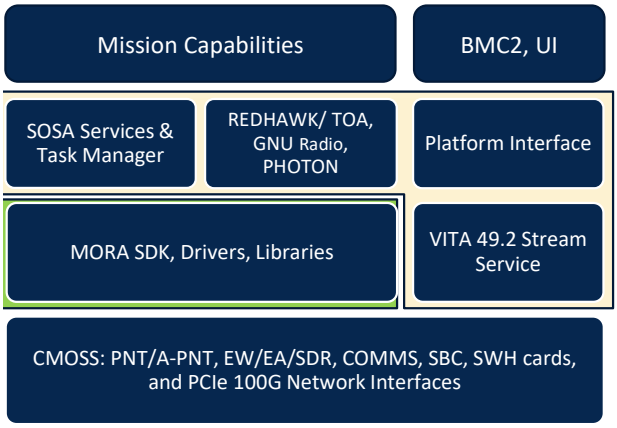

Figure 1. Our CMOSS initiative provides a mature, rigorously defined multifunction RF infrastructure framework for an Open 5G stack that enables frictionless, innovative insertions.

The CMOSS and the Air Force variant, Sensor Open System Architecture (SOSA), have garnered a diverse vendor base (**Figure 2**). That base confirms this open architecture will continue to expand throughout the DoD. Structuring the Open 5G Stack Challenge to explicitly rely upon CMOSS/SOSA will facilitate rapid integration of innovation and integration into DoD missions.

Processing scalability is another challenge for a DoD relevant Open 5G Stack. The DoD will face unique challenges for a 5G deployment that are not even addressed by the standard such as a mobile BTS, adapting the physical layer to a dynamic spectrum in unlicensed bands, and resource management for shared apertures. The ability of CMOSS to easily scale processing by adding more single board computers, digital signal processors or graphics processing units to a system provides the architectural agility that stove-piped proprietary hardware baselines cannot.

The inexorable increase of virtualization will continue to make specialized hardware irrelevant while a general software defined radio and commodity processing platforms become the preferred hardware basis. Intended to support a plethora of RF sensor and processing missions, the CMOSS vendor base is developing these commodity SDRs and processing cards. The CMOSS architecture explicitly envisions the SDR as a powerful digitizer and coarse channelizer, routing data samples to processors for everything above layer 1. That matches well with the trend towards virtualization of the Open 5G Stack.

Figure 2 The CMOSS/SOSA ecosystem is diverse, robust, and an ideal basis for grounding the Open 5G Stack to facilitate innovation and rapid DoD uptake.

A further advantage of grounding the Challenge in CMOSS/SOSA is the ability to apply DoD mission relevant metrics to both proposal content and Challenge outcomes. Candidate Stack technologies can be exercised in the context of actual DoD missions by embedding the Challenge into an existing CMOSS demonstration event such as Project Convergence 21/22 where the demands of spectrum co-use are quite evident. As the full military context of these demonstration is otherwise provided, this integration is a cost-effective way to illuminate the full DoD benefit of the Challenge.

Incentives and Scope

Spectranetix and the U.S. Army are providing this response not as contributors to the Open 5G Stack but as contributors to the Challenge infrastructure and context. As central figures in the DoD movement to open architectures, we suggest incentives and scope reflect unique DoD circumstances.

Unlike the commercial world, DoD industrial research, development, and prototype activities are typically funded through a mix of internal and government sources. A successful Open 5G Stack Challenge for the DoD will involve both commercial companies and defense base companies. To ensure adequate representation of DoD vendors familiar with tactical communication missions, technology, and unique constraints, we recommend funding the adaptation, integration, and demonstration of defense technology directly through the Challenge while the underlying technology remain an in-kind contribution from the companies. Absent that funding coupled with the perceived uncertainty on return on investment, a robust defense company participation is unlikely.

To ensure the Challenge results in capabilities that will be rapidly adopted and deployed by the DoD, we further recommend that mission use cases figure prominently as context for the Challenge demonstrations and evaluations.

Lessons learned from the shortcomings of previous generation tactical cellular technologies (to include 4G solutions) have been proven to degrade the military operational lethality and survivability of combat platforms. The root causes of this are manyfold. First and foremost, recurring gaps in the solutions made available from industry (1) result in an inadequate soldier user experience (UX), (2) add complexity and impede operational support of vehicle electronic combat networks, and (3) exceed size, weight, power, and cooling (SWaP-C) resources that are already oversubscribed in modern vehicle electronic combat networks. A CMOSS-enabled 5G solution set deliberately overcomes these limitations of previous generation tactical cellular products and technologies. CMOSS leverages a Soldier Centered

Design (SCD) approach, and drastically improves the soldier User Experience (UX) through simplified design and improved automation. CMOSS further simplifies and optimizes the design of military vehicle electronic networks, through elimination of duplicative components disjointed products, to include antennae, power amplifiers, power supplies and other ancillary equipment. Lastly, through the consolidation of vehicle electronic combat network capabilities into a unified, common physical envelope and form factor, SWaP-C resources become unencumbered. The precious SWaP-C resources enable the commander to leverage the platform to greater lethality and survivability, through carrying additional soldiers, additional munitions, and additional combat support materiel (ex. battery power sources). Giving the 5G Challenge a strong CMOSS focus, will increase the likelihood of an enduring capability transition.

Timeframe and Infrastructure

Technology transition to the DoD is a difficult process where operationally relevant demonstration and validation is always required. To lower barriers to small, innovative software stack developers seeking to contribute, a single open, accessible software defined radio infrastructure with a clear path to service-led demonstration should be provided. This will ensure rapid evaluation and a "level playing field" that doesn't favor large commercial cellular original equipment manufacturers (OEMs). By leveraging the growing CMOSS based ecosystem as hardware infrastructure to quickly instantiate Open 5G Stack candidates and already planned demonstration events such as Project Convergence 21 and Project Convergence 22, an accelerated schedule of 9 – 12 months is feasible. This allows for a rapid 5G-tailored CMOSS module development (leveraging existing digital host card with a to be developed 5G specific RF mezzanine) in parallel with participants porting their Challenge solutions into a CMOSS software environment. A bench level evaluation structured to align with the mission use cases described above would support a down select to the promising solutions for participation in a broader Army CMOSS demonstration event such as NetModX or Project Convergence.

Conclusion

While the open architecture imperative is strong and driven from the highest levels in the DoD, successful adoption of any Open 5G Challenge require more than a principle of open architecture. DoD uptake will be more likely if the Challenge is structured to use the specific, mature CMOSS ecosystem and is embedded within already planned CMOSS DoD demonstrations. The inherent modularity of CMOSS will enable the virtualization for DoD applications and the scalability will provide for the additional resources that multifunction tasking, mobile cores, and dynamic spectrum usage will undoubtedly require. Finally, participation of DoD contractors, with different R&D investment models than most commercial entities, will be enhanced if the costs of adapting, integrating, and demonstrating technology is provided by the Challenge.