MOSA Compliance for RF Data Systems

Architecting the Future of Spectrum Dominance

December 28, 2025

Executive Summary

The geopolitical landscape of the 21st century has undergone a tectonic shift, moving away from the asymmetric counter-insurgency operations that defined the post-9/11 era toward a volatile environment of near-peer competition. In this new strategic paradigm, the Electromagnetic Spectrum (EMS) has ascended to the status of a primary maneuver domain, equivalent in importance to land, sea, air, and space.[1] The ability to dominate this domain, through sophisticated Electronic Warfare (EW), precise Signals Intelligence (SIGINT), and resilient communications, relies not merely on the deployment of advanced sensors, but fundamentally on the architecture of the data systems that underpin them. Modern warfare has become irrevocably data-centric, yet the infrastructure supporting Radio Frequency (RF) operations remains dangerously antiquated, characterized by proprietary silos, chaotic data management, and a pervasive inability to leverage the power of Artificial Intelligence (AI) and Machine Learning (ML).[1]

This white paper, titled "MOSA Compliance for RF Data Systems," presents a comprehensive analysis of the operational and legal imperatives driving the adoption of the Modular Open Systems Approach (MOSA) within the Department of Defense (DoD). It specifically examines how **SigDrive**, an Enterprise RF Data Lake, utilizes an open architecture and the **Signal Metadata Format (SigMF)** to solve the critical "middle layer" bottleneck in spectrum operations. By decoupling data ownership from hardware vendors and normalizing disparate proprietary formats into a government-owned, queryable asset, SigDrive provides a turnkey pathway for Program Managers to demonstrate compliance with statutory mandates such as **Title 10 U.S.C. 2446a**.[3]

The analysis contained herein exposes the severe economic and operational costs of "vendor lock-in," a condition where the government is held hostage by proprietary interfaces that drive sustainment costs into an unsustainable "death spiral".[2] It contrasts this legacy model with the MOSA-centric approach, which leverages open standards to foster competition, accelerate technology refresh, and ensure "data readiness" for critical AI initiatives like the Army's **Project Linchpin** and the Joint All-Domain Command and Control (**JADC2**) framework.[6] Through a detailed technical examination of SigDrive's pluggable parser framework, canonical metadata schema, and air-gap-ready design, this report delineates the roadmap for achieving electromagnetic dominance through architectural openness.[1]

1. The Strategic Imperative: MOSA and the Legal Landscape

The transition to a Modular Open Systems Approach represents one of the most profound shifts in defense acquisition policy in decades. It is a transformation driven not by mere technical preference, but by the urgent necessity to curb escalating costs and the operational imperative to adapt faster than the adversary. MOSA has evolved from a discretionary best practice into a binding legal framework that dictates how the DoD designs, procures, and sustains its weapon systems.

1.1 The Statutory Mandate: Title 10 U.S.C. 2446a

The legal foundation for this architectural revolution is codified in **Title 10 U.S.C. 2446a**, titled "Requirement for modular open system approach in major defense acquisition programs".[3] Enacted by Congress to break the monopolistic hold of defense prime contractors on critical system interfaces, this statute mandates that all Major Defense Acquisition Programs (MDAPs) be designed and developed with a modular open system approach to the maximum extent practicable.[4] The law is explicit in its intent: to ensure that the government, rather than the vendor, controls the "key interfaces" that determine the long-term evolution of a platform.

Under this statute, a "major system interface" is defined as a shared boundary between major system components, characterized by various physical, logical, and functional attributes, including data formats and software protocols.[9] The law requires that these interfaces comply with widely supported and consensus-based standards, effectively rendering the use of closed, proprietary interfaces illegal for major subsystems unless a waiver is granted.[8] For an RF data system, compliance with 10 U.S.C. 2446a imposes three specific technical obligations that a solution like SigDrive is uniquely engineered to satisfy.

First, the system must be composed of "**severable modules**".[4] This requirement targets the monolithic software architectures traditionally provided by hardware vendors, where the analysis capabilities are inextricably hard-coded to the sensor hardware. In a MOSA-compliant architecture, the "ingestion" capability must be a distinct, severable module that can be upgraded or replaced without necessitating a complete system redesign.[11] SigDrive achieves this through its pluggable architecture, where the logic for parsing a specific file format is encapsulated in a discrete plugin that implements a standard Extractor interface.[1]

Second, the government must receive "**machine-readable definitions**" of the interface, including software-defined interface syntax and properties.[9] This provision precludes the delivery of "binary blobs", data files whose structure is known only to the vendor's proprietary software. Compliance requires that the data be described by a documented schema. SigDrive fulfills this by normalizing all data into a Canonical Metadata Schema based on the open SigMF standard, ensuring that the interface for data access is transparent, documented, and machine-readable.[1]

Third, the mandate explicitly favors **Open Standards**.[4] The reliance on proprietary file formats (such as X-DAT or proprietary binary streams) that require a specific vendor's software to read or process is fundamentally non-compliant if a suitable open standard exists. By standardizing on SigMF, SigDrive aligns with the "consensus-based standards" requirement of the statute, leveraging a format that is rapidly becoming the *de facto* standard across the industry and academia.[13]

1.2 The Cost of Vendor Lock-In

The economic rationale underpinning the MOSA mandate is the mitigation of "**vendor lock-in**," a pernicious condition where the government becomes dependent on a single supplier for a product or service and cannot transition to another vendor without incurring prohibitive costs or unacceptable delays.[2] In the domain of Electronic Warfare and RF engineering, lock-in is typically enforced not through hardware connectors, but through proprietary file formats and software licensing.

When a Program Office procures a high-performance spectrum analyzer or a software-defined radio (SDR) from a major incumbent vendor, the device often outputs data in a closed, proprietary format (e.g., .xdat, .tmp, or undocumented binary variants).[1] To visualize or analyze this data, the government is forced to purchase perpetual or subscription-based licenses for that specific vendor's analysis software suite. These licenses can cost between $2,000 and $10,000 per seat annually, creating a massive recurring revenue stream for the vendor while draining government resources.[1]

The table below illustrates the stark economic and strategic contrast between legacy proprietary architectures and the open architecture championed by SigDrive.

Cost Factor	Proprietary / Closed Architecture	Open / MOSA Architecture (SigDrive)	Strategic Impact
Data Ownership	Vendor retains effective control via format obscurity (e.g., X-DAT, proprietary binary).	Government owns data; format is open JSON/Binary (SigMF).	"Data sovereignty" allows competitive bidding for analysis tools.
Sustainment	High. Upgrades require sole-source contracts with the OEM.	Low. Modules can be upgraded by third parties.	Breaks the "death spiral" of rising O&S costs.
Interoperability	Siloed. Data cannot move between vendors (e.g., Keysight to R&S).	High. Universal translator (SigMF) bridges systems.	Enables JADC2 "sensor-to-shooter" data flows.
Upgrade Cycle	Tied to vendor hardware refresh cycles (5-10 years).	Software-defined; continuous integration (CI/CD).	Matches the speed of software development.
Flexibility	Rigid. "Black box" interfaces prevent integration with new AI tools.	Modular. Pluggable extractors allow rapid adaptation.	Facilitates immediate integration of new algorithms.

Table 1: The Economics of Proprietary vs. Open RF Systems

The Government Accountability Office (GAO) has repeatedly highlighted that a lack of technical data rights and reliance on proprietary interfaces are primary drivers of "sustainment cost growth" and operational readiness challenges.[5] A poignant example is the F-35 program's Autonomic Logistics Information System (ALIS), where proprietary data structures and limited government rights contributed to massive cost overruns, data inaccuracies, and significant readiness failures.[18] The inability of the government to access and manipulate the data generated by its own platforms forced a costly redesign and replacement effort. By contrast, adopting a MOSA-compliant data lake like SigDrive allows the DoD to "own the interface," thereby commoditizing the storage and retrieval layer and forcing vendors to compete on the quality of their analytics rather than the obscurity of their file formats.

1.3 Data Rights: Government Purpose vs. Limited Rights

Compliance with MOSA is inextricably linked to the legal framework of data rights, which is governed by the Defense Federal Acquisition Regulation Supplement (DFARS). Specifically, **DFARS 252.227-7013** outlines the rights in technical data for non-commercial items, while **DFARS 252.227-7014** covers computer software.[20] Understanding these distinctions is vital for any acquisition strategy involving RF systems.

- **Limited Rights:** This category is often asserted by vendors for "commercial" software or technical data developed exclusively at private expense. Under Limited Rights, the government can use the data internally but is restricted from releasing it to third parties (e.g., other defense contractors) without the vendor's permission.[20] This effectively cements vendor lock-in, as the government cannot hire a competitor to maintain or upgrade the system using the original data.
- **Government Purpose Rights (GPR):** This designation allows the government to use, modify, release, and disclose the data within the government and to third parties for "government purposes," which includes competition, maintenance, and sustainment.[22] GPR typically applies to mixed-funding development efforts and expires after a set period (usually five years), converting to Unlimited Rights.
- **Unlimited Rights:** The government possesses the right to use the data for any purpose whatsoever, including commercialization.

SigDrive is strategically designed to support the acquisition of **Government Purpose Rights** or better. Because the platform itself utilizes open-source schemas (SigMF) and standard APIs, the data stored within it is inherently untethered from the restrictive licensing that accompanies proprietary formats. The business plan explicitly positions SigDrive as a "Government Owned" data layer.[1] This architecture ensures that the government retains the rights to the *data*, the raw IQ samples and the associated metadata, even if it pays for the *software* license to manage it. This distinction is vital for Program Managers who must certify that they have secured sufficient data rights to allow for future competitive sustainment, a requirement emphasized in recent National Defense Authorization Acts (NDAAs) and the recommendations of the Section 813 Panel on Technical Data Rights.[5] By mandating the delivery of data in the SigMF format via SigDrive, the government ensures that the "technical data package" it receives is truly open and reusable, rather than a collection of locked proprietary files.

2. The Technical Crisis in RF Operations

To fully appreciate why a specialized "RF Data Lake" is a prerequisite for MOSA compliance, one must understand the unique and challenging characteristics of Radio Frequency data. Unlike structured textual data, logs, or standard multimedia, RF data possesses "volume," "velocity," and "variety" characteristics that defy traditional enterprise IT solutions and exacerbate the problems of lock-in.

2.1 The Phenomenon of Data Gravity

"Data Gravity" is a concept in big data architectures suggesting that as data accumulates, it acquires "mass," making it increasingly difficult, slow, and costly to move.[1] In the RF domain, this gravity is immense and dictates the operational tempo.

A single high-fidelity wideband IQ recording (e.g., 100 MHz bandwidth, 16-bit complex samples) can generate gigabytes of data per second. A recording session lasting just a few minutes can result in a file exceeding 500 GB. In traditional "stovepiped" architectures, these massive files are stored on local hard drives within the proprietary recorders or analysis workstations. When an analyst at a different location needs to process this data, the sheer size makes network transfer over bandwidth-constrained military networks (like SIPRNet) impractical.

This leads to the prevalence of "**Sneakernet**" logistics, the physical shipping of hard drives between test ranges, laboratories, and intelligence centers.[1] This manual handling is inefficient, insecure, and leads to version control chaos. Valuable signal recordings are effectively lost in unindexed storage cabinets, rendering them useless for future analysis or AI training.

SigDrive addresses the physics of data gravity by functioning as a centralized repository designed for **data-at-rest**. Its architecture supports:

- **Resumable Uploads:** Utilizing the **TUS.io** open protocol, SigDrive handles files up to 5TB, enabling reliable, chunked transfer over unstable networks.[1]
- **Decoupled Storage and Compute:** By storing the heavy binary data in cost-effective S3-compatible object storage while indexing the lightweight metadata in a high-performance PostgreSQL database, SigDrive allows users to query, search, and visualize data *in place*.[1] An analyst can view a spectrogram of a 1TB file in a web browser instantly, downloading only the specific segment of interest rather than the entire file.

This architecture aligns with the DoD's shift toward "Data-Centric" warfare, where the focus moves from platform-centric capabilities (e.g., a specific jet) to the data that enables the joint force to sense and make decisions.[24]

2.2 The Heterogeneity Problem: A Tower of Babel

The second major challenge inhibiting MOSA compliance is the proliferation of incompatible, vendor-specific file formats. The EW ecosystem is littered with a "Tower of Babel" of proprietary standards that prevent interoperability.

- **X-DAT / DAT:** These are proprietary formats used by **Keysight** (formerly Agilent) hardware.[1] While they may be technically documented in obscure user manuals, they are designed to be read primarily by Keysight's PathWave software. The metadata is often split between XML headers and binary payloads in a way that requires significant reverse-engineering to parse correctly without the vendor's SDK.
- **Midas Blue (X-Midas):** A legacy format widely used in the US intelligence community and by defense prime contractors.[1] It is characterized by a 512-byte binary header and often involves detached data files. While technically "open" to government users, the format is archaic, complex, and lacks the semantic richness of modern standards (e.g., JSON). It often leads to "detached head" syndromes where the metadata file is separated from the binary data, rendering the recording useless.[28]
- **Proprietary Binary Blobs:** Many SDR vendors output raw binary files with practically no metadata, or with metadata stored in separate, unlinked text files or proprietary sidecar files.[1]

This heterogeneity creates severe operational friction. An analyst using a Rohde & Schwarz analysis tool cannot easily open a file recorded by a Keysight spectrum analyzer. A machine learning engineer trying to train a classifier cannot ingest data from three different sensors without writing three different custom parsers. This lack of interoperability is a direct violation of the spirit, if not the letter, of MOSA mandates for "key interfaces".[29]

SigDrive solves this through its **Pluggable Ingestion Engine**, which acts as a universal translator. By implementing specific extractors for each of these formats, SigDrive normalizes the chaotic landscape of RF data into a single, unified Canonical Schema, effectively "washing" the data of its proprietary constraints and making it universally accessible.[1]

3. SigDrive Architecture: A MOSA-Native Design

SigDrive was architected from the ground up to meet the rigorous requirements of modularity, openness, and security mandated by the DoD. Its design reflects the principles of the "Twelve-Factor App" methodology while addressing the specific constraints of classified, air-gapped environments.

3.1 Pluggable Parser Framework

The cornerstone of SigDrive's MOSA compliance is its **Ingestion Service Plugin Architecture**. Unlike legacy systems that are hard-coded to support only a specific vendor's format, SigDrive defines an abstract Extractor interface that decouples the ingestion logic from the core system.[1]

- **Mechanism:** On startup, the system scans a designated plugin directory. Any class that implements the Extractor interface is automatically discovered and registered. This allows for dynamic extensibility.
- **Routing:** When a file is uploaded, the Ingestion Service inspects the MIME type or file extension and dynamically routes the data to the appropriate plugin.[1]
- **Extensibility:** This design means that if a new sensor with a novel data format is deployed next year, the government can simply commission a small Python plugin to parse that format. The core SigDrive infrastructure, database, user interface, security, and storage, requires no modification. This capability is the precise definition of "severable modules" required by 10 U.S.C. 2446a.[3]

Current implementations include parsers for **SigMF** (using the sigmf Python library), **WAV/RF64** (standard audio/RF), **Midas Blue** (legacy binary), and **Raw IQ** (manual entry).[1] This plugin architecture ensures that the system is never obsolete; it can evolve alongside the changing sensor landscape.

3.2 Canonical Metadata Schema

To make the data searchable and "understandable" (a key tenet of the DoD Data Strategy's VAULTIS framework [24]), SigDrive normalizes all incoming data into a **Canonical Metadata Schema**.

- **Foundation:** The schema is strictly based on the **SigMF specification**, ensuring that the internal data model complies with an open, consensus-based industry standard.[1]
- **Normalization Logic:** The extractors map vendor-specific fields (e.g., a "CenterFreq" field in a Midas header or an XML tag in an X-DAT file) to the standardized SigMF field (core:frequency).
- **Validation:** The system employs Pydantic models to enforce strict validation of this metadata before it is committed to the PostgreSQL database.[1] This ensures that the data lake remains clean and queryable.
- **Geospatial Indexing:** By converting location metadata into **PostGIS** geometries, SigDrive enables geospatial queries (e.g., "Find all signals recorded within 50km of this coordinate") that are impossible in file-based systems.[1]

This normalization process effectively transforms proprietary data into a vendor-neutral asset. The data is stored in **JSONB** columns within PostgreSQL, allowing for the flexibility of a NoSQL document store combined with the relational integrity and indexing power of a SQL database.[1]

3.3 Air-Gap Ready and Security Compliance

Compliance with DoD mandates extends beyond data formats to security architecture. SigDrive is designated as "**Air-Gap Ready**," a critical requirement for deployment on classified networks like SIPRNet and JWICS where internet access is strictly prohibited.[1]

- **Bundled Dependencies:** The system is delivered as a set of hardened Docker containers with all dependencies included. There is no requirement for runtime internet access to fetch libraries or updates.[1]
- **Offline Licensing:** License validation avoids "phone-home" mechanisms, which are non-starters in secure facilities (SCIFs). Instead, it uses cryptographically signed license keys that can be validated offline.[1]
- **Audit Service:** A dedicated microservice generates **immutable logs** of every user action, including metadata edits, file access, and deletions.[1] This supports the "Trustworthy" pillar of VAULTIS and provides the rigorous audit trail required for obtaining an **Authority to Operate (ATO)**.[1]
- **RBAC:** A Role-Based Access Control engine restricts data access based on user clearance and role, complying with strict "Need to Know" principles and data segregation requirements.[1]

4. SigMF as the Interoperability Enabler

The choice of **SigMF (Signal Metadata Format)** as the native language of SigDrive is a strategic differentiator that aligns directly with the open standards mandate of MOSA.

4.1 SigMF: The Standard for Data-at-Rest

SigMF is an open-source standard originally developed by GNU Radio and DeepSig researchers to solve the portability problem in RF engineering.[13] It fundamentally separates the metadata from the data, consisting of two files:

1. **.sigmf-data:** The raw binary IQ samples. This is the simplest possible representation of the signal.
2. **.sigmf-meta:** A JSON file describing the data (frequency, sample rate, geometry, annotations, hardware details).[30]

This separation is crucial. Unlike legacy formats that embed metadata in complex binary headers, SigMF's JSON metadata is human-readable and machine-parseable by any modern programming language.

Feature	SigMF	VITA 49	Midas Blue	Keysight X-DAT
Primary Use	Data-at-Rest (Storage/AI)	Data-in-Motion (Streaming)	Legacy Storage	Proprietary Analysis
Format	JSON + Binary	Packetized Binary	Binary Header + Data	XML + Binary
Openness	Open Source (GitHub)	Open Standard (VITA)	Govt. Open / Complex	Closed / Proprietary
AI Readiness	High (JSON is native to ML)	Medium (Requires parsing)	Low (Binary headers)	Low (Vendor tools needed)
SOSA Status	Recommended for Recording	Standard for Streaming	Legacy Support	Non-Compliant

Table 2: Comparison of RF Data Standards

While **VITA 49** is the standard for "data-in-motion" (transporting data from a radio to a processor in real-time), SigMF is designed for "data-at-rest" (archival, sharing, and analysis).[28] The DoD's **Sensor Open Systems Architecture (SOSA)** Technical Standard has increasingly recognized this distinction, referencing SigMF as the preferred standard for recording and datasets alongside VITA 49.[31]

4.2 Why SigMF Enables MOSA

Adopting SigMF allows the government to break the link between the recorder hardware and the analysis software.

- **Vendor Neutrality:** Because the metadata is plain JSON, any tool can parse it. It is not obfuscated by binary headers or encryption. A recording made by an Ettus USRP can be analyzed by a DeepSig classifier or a custom Python script without any conversion steps.

- **Machine Readability:** JSON is natively readable by modern data science tools (Python, Pandas, Jupyter), facilitating the integration of AI/ML workflows.[13] This contrasts sharply with binary formats that require specialized C++ parsers.
- **Extensibility:** SigMF supports "namespaces," allowing users to add custom metadata fields (e.g., "mission_id", "classification_level") without breaking the core standard. This flexibility is essential for accommodating the diverse and specific needs of different DoD programs.[14]

By mandating SigDrive, and by extension, SigMF, as the repository standard, a Program Manager ensures that data collected by a Lockheed Martin sensor today can be analyzed by a Booz Allen Hamilton algorithm tomorrow. This capability fulfills the "interoperability" and "competition" goals of MOSA, ensuring that the government is never locked into a single vendor's ecosystem for the lifecycle of the data.[4]

5. Operationalizing Compliance: DoD Strategies and AI Readiness

SigDrive does not exist in a vacuum; it is a critical enabler for several high-priority DoD strategies, specifically those related to Artificial Intelligence and Joint All-Domain Operations.

5.1 Project Linchpin and AI Data Readiness

Project Linchpin is the US Army's premier initiative to build a trusted AI/ML pipeline for sensor data.[6] The primary bottleneck for military AI is not the sophistication of the algorithms, but the "**data readiness**", the availability of curated, labeled, and standardized datasets.[1] Without clean, labeled data, AI models cannot be trained.

Dr. Neil Lawrence's concept of **Data Readiness Levels (DRLs)** has been adapted by the DoD to assess the maturity of data for AI.[34]

- **Level C (Hearsay Data):** Data is purported to exist but is inaccessible, unindexed, or lost in "sneakernet" logistics.
- **Level B (Accessible):** Data is loaded into a system but lacks context, formatting, or consistent metadata (e.g., missing sample rates or frequencies).
- **Level A (Contextual/Ready):** Data is standardized, labeled, annotated, and ready for training.

SigDrive effectively elevates RF data from Level C/B to Level A. Its **Canonical Schema** provides the necessary standardization and context. Furthermore, its **Region of Interest (ROI) Annotation** features allow analysts to label specific signals directly in the web browser (e.g., drawing a box around a radar pulse on the spectrogram).[1] These annotations are exported in SigMF format, creating the "ground truth" training data required for Cognitive EW algorithms.[36] In this capacity, SigDrive acts as the "Feature Store" for Project Linchpin, solving the data gravity and curation problem that currently stalls AI development.[37]

5.2 JADC2 and the Data Fabric

Joint All-Domain Command and Control (JADC2) envisions a unified network where data flows seamlessly between all branches of the military, from a Space Force satellite to a Navy ship to an Army battery.[1] This requires a "Data Fabric" that is agnostic to the underlying transport or storage mechanism.

SigDrive's support for **Federated Search** (a key part of its roadmap) aligns perfectly with this vision. By allowing a user at the Pentagon to query metadata on a forward-deployed SigDrive node (e.g., on a carrier group) without moving the massive 5TB binary file, the system respects the bandwidth constraints of the tactical edge while maintaining global visibility.[1] The use of open APIs and standard metadata (SigMF) ensures that SigDrive can plug into the broader JADC2 architecture, feeding metadata catalogs and mission planning tools.[24]

5.3 VAULTIS Compliance

The DoD Data Strategy outlines the **VAULTIS** goals: Visible, Accessible, Understandable, Linked, Trustworthy, Interoperable, and Secure.[24] SigDrive is engineered to meet each of these criteria:

VAULTIS Goal	SigDrive Implementation Details
Visible	Centralized indexing makes petabytes of formerly opaque binary data searchable via metadata and geospatial queries.
Accessible	Web-based UI and REST APIs provide immediate access; S3 backend allows for scalable, low-cost storage.
Understandable	Canonical Schema (SigMF) provides consistent, human-readable context (freq, gain, location) for every file.
Linked	Data lineage tracking connects raw recordings to derived datasets, annotations, and analysis results.
Trustworthy	Immutable audit logs and SHA-256 checksums ensure data integrity and provenance tracking.
Interoperable	Open standards (SigMF) and pluggable extractors break proprietary silos, allowing data to move between tools.
Secure	Air-gap ready design, RBAC, and support for classified deployment environments ensure data protection.

Table 3: SigDrive Compliance with VAULTIS

6. Business & Acquisition Strategy

Adopting a MOSA-compliant data system is not just a technical decision; it is a financial strategy designed to reduce lifecycle costs and streamline acquisition.

6.1 Avoiding the "Sustainment Death Spiral"

Legacy systems trap the DoD in a "**sustainment death spiral**" where costs rise exponentially over time due to monopoly pricing on proprietary parts and software.[5] The DoD estimates that software sustainment costs will exceed **$15 billion** over five years.[17] A significant portion of this is due to vendor lock-in, where the government pays premium rates for "updates" that are essentially maintenance of proprietary code.

By using SigDrive to decouple the *data* from the *analysis tools*, the government creates a competitive market. If Vendor A raises the price of their analysis software, the government can switch to Vendor B's tool because the underlying data is stored in the open SigDrive/SigMF repository, not in Vendor A's proprietary format. This leverage is estimated to save millions in licensing fees and avoid the costly "re-architecture" of legacy systems.[41]

6.2 The "Trojan Horse" Acquisition Model

To navigate the complex DoD acquisition cycle, the business plan proposes a "Trojan Horse" strategy.[1]

1. **Seed the Labs:** Provide SigDrive to University Affiliated Research Centers (UARCs) and government labs (e.g., GTRI, APL, Lincoln Labs) at a low cost. These entities act as trusted technical advisors to the DoD.
2. **Define the Standard:** As researchers adopt SigDrive for their analysis, they will begin to write SigDrive-compatibility and SigMF requirements into the Request for Proposals (RFPs) for major Programs of Record.
3. **Scale to Enterprise:** Once the standard is written into the requirements, the Program Offices must procure the enterprise-grade solution to remain compliant.

Leveraging **SBIR/STTR** (Small Business Innovation Research) grants provides a "sole-source justification" pathway. Once a company wins a Phase I or II SBIR, any federal agency can award a follow-on Phase III contract without a new competitive bidding process.[1] This mechanism significantly shortens the sales cycle and allows agile software to reach the warfighter faster.

7. Future-Proofing Defense Spectrum Operations

The roadmap for SigDrive demonstrates a commitment to evolving with the MOSA landscape and anticipating future requirements.

7.1 SOSA Alignment

Future development tasks include the implementation of a **SOSA-compliant schema export**.[1] As the **Sensor Open Systems Architecture (SOSA)** becomes the *de facto* standard for hardware modularity in C4ISR systems, ensuring that SigDrive can ingest and export data that fully aligns with SOSA Technical Standard 1.0/2.0 will be critical.[44] This includes validating metadata against SOSA profiles and potentially integrating with VITA 49 streams for real-time ingestion, bridging the gap between "data-in-motion" and "data-at-rest."

7.2 Federation and the Cloud Edge

The concept of **"SigDrive Mesh"** or federation addresses the distributed nature of modern warfare. Future iterations will allow dispersed SigDrive nodes (e.g., on a ship, a drone, and a ground station) to synchronize metadata catalogues.[1] This enables a "virtual data lake" that spans the globe, allowing a commander to "see" spectrum data collected at the tactical edge without incurring the latency and bandwidth cost of moving terabytes of binary files. This capability is the essence of JADC2, data availability at the speed of relevance.

Conclusion

The Department of Defense stands at a critical juncture. The exponential growth of RF data, combined with the increasing sophistication of peer adversaries, demands a radical departure from the proprietary, hardware-centric architectures of the past. **MOSA is not just a guideline; it is the law**, and open standards are the weapon of choice in the fight against obsolescence and cost overrun.

SigDrive represents the materialization of this doctrine. By combining a robust, air-gap-ready infrastructure with the flexibility of the SigMF open standard, it solves the immediate technical problems of data gravity and interoperability while addressing the long-term strategic need for data ownership and AI readiness. It transforms RF data from a perishable byproduct of testing into a permanent, searchable, and actionable intelligence asset.

For Program Managers, adopting SigDrive is not merely an IT upgrade; it is a strategic maneuver to secure data sovereignty, ensure statutory compliance with Title 10 U.S.C. 2446a, and build the foundational data architecture required for the AI-enabled conflicts of the future. The era of the "Black Box" is over; the era of the Open Data Lake has arrived.

References

1. Internal documentation, available on request
2. The Weakest Link: How To Avoid Aerospace And Tech Vendor Lock-In - Forbes, https://www.forbes.com/councils/forbestechcouncil/2024/01/18/the-weakest-link-how-to-avoid-aerospace-and-tech-vendor-lock-in/
3. 10 U.S.C. 2446a - Requirement for modular open system approach in major defense acquisition programs; definitions - Content Details - USCODE-2016-title10-subtitleA-partIV-chap144B-subchapI-sec2446a - GovInfo, https://www.govinfo.gov/app/details/USCODE-2016-title10/USCODE-2016-title10-subtitleA-partIV-chap144B-subchapI-sec2446a
4. Implementing a Modular Open Systems Approach in Department of Defense Programs - USD(R&E), https://www.cto.mil/wp-content/uploads/2025/03/MOSA-Implementation-Guidebook-27Feb2025-Cleared.pdf
5. GAO-25-107468, WEAPON SYSTEM SUSTAINMENT: DOD Can Improve Planning and Management of Data Rights [Reissued with revisions on Sep, https://www.gao.gov/assets/gao-25-107468.pdf
6. Project Linchpin | CSIAC, https://csiac.dtic.mil/wp-content/uploads/2024/04/Project-Linchpin-GEN_Overview-CSIAC-final.pdf
7. PEO IEW&S Artificial Intelligence and Software At Pace (AIS@P) Industry Day, https://peoiews.army.mil/wp-content/uploads/2025/01/AIS@P-MATOC_Industry-Day-1.7.25.pdf
8. Modular Open Systems Approach (MOSA), https://www.cto.mil/wp-content/uploads/2025/03/MOSA-Info-Sheet-Cleared-20250314.pdf
9. 10 U.S.C. § 2446a (2020) - Requirement for modular open system approach in major defense acquisition programs; definitions - Justia Law, https://law.justia.com/codes/us/2020/title-10/subtitle-a/part-iv/chapter-144b/subchapter-i/sec-2446a/
10. SUBCOMMITTEE ON CYBER, INFORMATION TECHNOLOGIES, AND INNOVATION - House Armed Services Committee, https://armedservices.house.gov/uploadedfiles/fy26_ndaa_citi_print.pdf
11. Let's Be Open and Modular: MOSA Implementation Guidebook - DAU, https://www.dau.edu/sites/default/files/2025-04/Speaker%20Slides__%20MOSA%20Implementation%20Guidebook__29%20April%202025.pdf
12. Air Force Data Rights Guidebook - DAU, https://www.dau.edu/sites/default/files/Migrated/ToolAttachments/Air-Force-Data-Rights-Guidebook.pdf
13. Genesys-SigMF/sigmf-spec.md at master · kunalsankhe/Genesys-SigMF - GitHub, https://github.com/kunalsankhe/Genesys-SigMF/blob/master/sigmf-spec.md
14. SigMF, https://sigmf.org/
15. Open System Architecture (OSA) Contract Guidebook for Program Managers June 13.pdf - AcqNotes,

https://www.acqnotes.com/Attachments/Open%20System%20Architecture%20%28OSA%29%20Contract%20Guidebook%20for%20Program%20Managers%20June%2013.pdf
16. (PDF) Implications of Artificial Intelligence-Driven Deepfakes for Cybersecurity and Regulation in Nigeria: Theorising for Cyberfakes and Cyberviolence - ResearchGate, https://www.researchgate.net/publication/360306375_Implications_of_Artificial_Intelligence-Driven_Deepfakes_for_Cybersecurity_and_Regulation_in_Nigeria_Theorising_for_Cyberfakes_and_Cyberviolence
17. GAO-19-173, WEAPON SYSTEM SUSTAINMENT: DOD Needs to Better Capture and Report Software Sustainment Costs - Government Accountability Office (GAO), https://www.gao.gov/assets/gao-19-173.pdf
18. F-35 Lightning II: Background and Issues for Congress, https://www.congress.gov/crs-product/R48304
19. Weapon System Sustainment: DOD Needs a Strategy for Re-Designing the F-35's Central Logistics System - GAO.gov, https://www.gao.gov/products/gao-20-316
20. THE RIGHT BALANCE - USAASC, https://asc.army.mil/web/the-right-balance/
21. Improving Acquisition to Support the Space Enterprise Vision: Supplemental Appendixes on Acquisition Concepts - RAND, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2600/RR2626/RAND_RR2626z1.appendixes.pdf
22. Overview of Law, Regulations, and Policy for Licensing Technical Data (TD) and Computer Software (CS) to DoD - DAU, https://www.dau.edu/sites/default/files/Migrated/CopDocuments/Fact%20Sheet%20Overview%20of%20Licensing%20Technical%20Data%20and%20Computer%20Software%20to%20DoD%20%287%20Dec%202015%29.pdf
23. Architecting Data for the AI Era - FRC - Federal Resources Corporation, https://fedresources.com/architecting-data-for-the-ai-era/
24. DOD Data Strategy, https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF
25. DOD Issues New Data Strategy - Department of War, https://www.war.gov/News/Releases/Release/Article/2376629/dod-issues-new-data-strategy/
26. Keysight M8085A MIPI C-PHY Receiver Test Software User Guide, https://www.keysight.com/cd/en/assets/9018-50005/user-manuals/9018-50005.pdf
27. Midas BLUE File Format Specification - Studylib, https://studylib.net/doc/8173203/midas-blue-file-format
28. SigMF: The Signal Metadata Format - Proceedings of the GNU Radio Conference, https://pubs.gnuradio.org/index.php/grcon/article/download/52/38/
29. Modular Open Systems Approaches: Empowering DoD's Intellectual Property Cadre to Evaluate Department of Defense Programs - American Bar Association, https://www.americanbar.org/groups/public_contract_law/resources/journal/202

4-fall/modular-open-systems-dod-programs/
30. sigmf/SigMF: The Signal Metadata Format Specification - GitHub, https://github.com/sigmf/SigMF
31. (PDF) The VITA 49 analog RF-digital interface - ResearchGate, https://www.researchgate.net/publication/234591876_The_VITA_49_analog_RF-digital_interface
32. GAO-25-107468, WEAPON SYSTEM SUSTAINMENT: DOD Can Improve Planning and Management of Data Rights, https://files.gao.gov/reports/GAO-25-107468/index.html
33. Artificial Intelligence: Resources | www.dau.edu, https://www.dau.edu/artificial-intelligence/resources
34. Rethinking Technological Readiness in the Era of AI Uncertainty - arXiv, https://arxiv.org/html/2506.11001v1
35. How to Talk Data Readiness - NT Concepts, https://www.ntconcepts.com/how-to-talk-data-readiness/
36. CSRD2025: A Large-Scale Synthetic Radio Dataset for Spectrum Sensing in Wireless Communications - arXiv, https://arxiv.org/html/2508.19552
37. IQTLabs/rfml - GitHub, https://github.com/IQTLabs/rfml
38. The Role of Open Standards in Future Force Protection ECM - L3Harris, https://www.l3harris.com/sites/default/files/2021-07/The-role-of-Open-Standards-in-Force-Protection-ECM-sas.pdf
39. Accelerating Readiness - International Cost Estimating and Analysis Association, https://www.iceaaonline.com/wp-content/uploads/2025/06/MTC01-Bonich-Accelerating-Readiness-paper.pdf
40. Weapon System Sustainment: DOD Needs to Better Capture and Report Software Sustainment Costs - Government Accountability Office (GAO), https://www.gao.gov/products/gao-19-173
41. GAO-25-107604, 2025 Annual Report: Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve an Additional One, https://www.gao.gov/assets/gao-25-107604.pdf
42. The High Cost of License Locked Software in DOD Procurement - Raft, https://teamraft.com/wp-content/uploads/The-High-Cost-of-License-Locked-Software-in-DOD-Procurement.pdf
43. DOD Releases Intellectual Property Guidebook: Key Insights for Defense Contractors, Part 1 | PilieroMazza, Law Firm, Government Contracts Attorney, https://www.pilieromazza.com/dod-releases-intellectual-property-guidebook-key-insights-for-defense-contractors-part-1/
44. Sensor Open Systems Architecture (SOSA) - Curtiss-Wright Defense Solutions, https://defense-solutions.curtisswright.com/capabilities/open-architectures/mosa/sensor-open-systems-architecture
45. GNU Radio Conference 2022 (26-30 September 2022), https://events.gnuradio.org/event/18/timetable/?view=standard_numbered