32nd Space Symposium, Technical Track, Colorado Springs, Colorado, United States of America
Presented on April 12-14, 2016

Developing an Adaptive OPIR Exploitation Framework

Beth Clark, Katherine Luce, Ken Onorato, Ben Tarr, Tom Walker
Lockheed Martin and Northrop Grumman SBIRS Team

1 Abstract

The OPIR community is face-to-face with the challenge of supporting a rapidly changing Battlespace Awareness (BA) mission landscape. Increasing data accuracy and timely data feeds are providing critical real time information and as a result, OPIR-based sensor data exploitation has become even more critical to the warfighter. While steeped in the Missile Warning culture that demands perfection, the OPIR community must establish adaptive processes for innovating in a rapidly changing world that requires accelerated capability deployment. This paper proposes a modular, layered framework and processes to support the multi-mission, multi-sensor OPIR Battlespace Awareness Center (OBAC).

2 Introduction

Within the Air Force Open Approaches Way Ahead briefing, industry assistance is requested in several areas. These included: growing the USAF Open Systems Architecture (OSA) business model; defining and refining open architectures; increasing the penetration of OSA into USAF legacy platforms; energizing industry partners for more resilient and innovative capabilities, subsystems, and components; and creating agile, affordable, resilient USAF systems of the future (Priddy).

The Department of Defense (DoD) Overhead Persistent Infrared (OPIR) community has been the premier provider of Missile Warning for more than 40 years. This was achieved through development and deployment of enterprise-scale overhead sensor constellations and ground data processing systems. These systems provide timely and accurate data regarding ballistic missile launch detection, identification, and predicted impact-point location. Missile Warning demands a high level of perfection from system providers and operators. The result is intentionally stringent processes and certifications ensuring "no-fail" Missile Warning mission requirements.

Over the last decade, advances in sensor accuracy and computing power enabled improvements in data accuracy and data access. These improvements deliver real-time sensor information to the warfighter, as well as non-Missile Warning users. As a result, the Missile Warning-based ground processing systems and architectures now face challenges supporting a risk tolerant, rapidly and continuously changing Battlespace Awareness (BA) mission.

The expanding demand for OPIR data and the BA mission's dynamic nature are driving significant changes in evaluating legacy ground processing systems. These Missile Warning focused architectures required the United States Government (USG) to rely on a limited numbers of vendors and proprietary point solutions. As a result, the mission focused, mission assurance architectures were expensive to develop and sustain over system lifecycles. In order to fully leverage OPIR data and support new missions, including civil applications, the USG must enable accelerated data processing application development and operational deployment. For context, Figure 1 provides a high level depiction of the Missile Warning and Evolving Mission Domains such as BA that OPIR supports.

Figure 1: The Expanding OPIR Mission Domain

To meet increasing warfighter BA demands, the Air Force established the OPIR Battlespace Awareness Center (OBAC). This paper outlines a recommended architectural framework to achieve the goal of creating agile, affordable, and resilient OPIR ground systems.

3 An Open Systems Approach

Recommendations for moving forward on an agile, affordable, resilient OBAC are based on the DoD implementation approach for open systems known as *Open Systems Architecture* (OSA). This approach espouses using commercially available, widely accepted interface standards to integrate commercial products from multiple vendors. OSA is mandated by Better Buying Power and DoDI 5000.2 and brings a new way of thinking about system acquisition and engineering ("Better Buying Power," "Operation of the Defense Acquisition System"). To quote the Defense Acquisition Guidebook, OSA "enhances system interoperability and the ability to integrate new capabilities without redesign of entire systems or large portions of the enterprise." ("DAG Systems Engineering").

Better Buying Power also acknowledges a key open architecture enabler is adopting an open business model. This model requires doing business transparently to leverage collaborative innovation of numerous participants across the enterprise. The combination of open architecture and an open business model permits OSA acquisitions yielding modular, interoperable systems.

3.1 Traditional vs. Open Systems Approaches

In the traditional approach to system development, unique interfaces were defined between components, then components were developed and integrated, and then the system was used and sustained. With OSA, standard interfaces are adopted and components are acquired rather than developed. A key OSA benefit is creating more evolvable systems. Components can be added, modified, replaced, removed, or supported by different vendors throughout the system lifecycle. This affords opportunities for enhanced competition and innovation.

Legacy OPIR ground systems were built via the traditional approach and focused on stringent Missile Warning requirements. Missile Warning systems are purposely structured to allow technology insertion only after extensive and time consuming operational testing. While these systems have proven invaluable in their ability to meet strict Missile Warning demands, they have often been criticized for a lack of rapid adaptability to emerging missions.

By employing OSA in the OPIR ground processing domain, the USG can achieve the affordability and efficiencies needed to extract maximum value from overhead assets. This includes providing capabilities necessary for emerging missions such as BA. At the same time, this can be accomplished without hindering the critical Missile Warning system. Successful OSA concept implementation will be proven after demonstrating qualified third parties can add, modify, replace, remove, or support OPIR data exploitation components based on open standards and published interfaces.

From an engineering perspective, several key practices (identified in Figure 2) are necessary to achieve the goal of an OSA-based OPIR ground system. The Air Force Space Command (AFSPC) Enterprise Ground Services (EGS) Ground Reference Architecture (GRA) provides a framework for common space ground systems and will be the foundation for an enterprise command and control approach. The EGS GRA is an OSA that will specify technical standards the USG will use to procure and sustain capabilities and services. Organized around MILSTD 881-C, the OSA defined mission functions, including mission data processing and analysis, are applicable to the OPIR ground processing domain ("Department of Defense Standard Practice - MIL-STD-881C"). The OSA specifies hardware, middleware, and software layers, as well as tools and simulators that can be seamlessly changed and

modernized without impacting other components. Any data processing framework going forward should be held to the practices and standards outlined by OSA and the EGS GRA respectively.

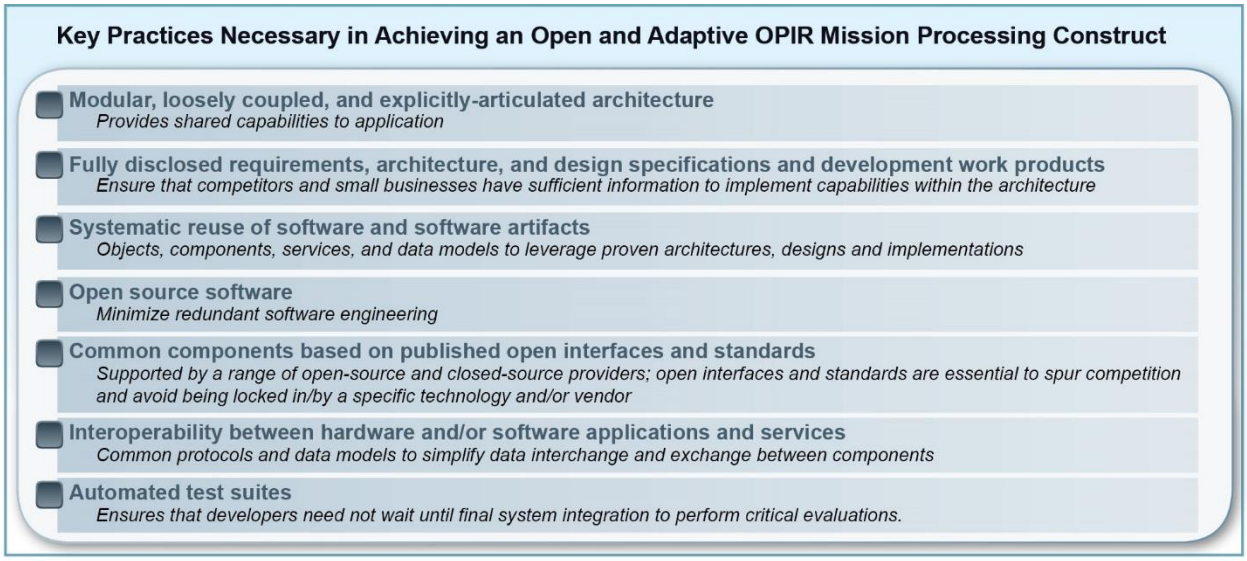

Figure 2: Key OSA Practices

3.2 Frameworks and Open Source Overview

Well-developed frameworks inherently make it easier to develop a component (service or application). Frameworks are layered structures that define common interfaces (usually via Application Programmer Interfaces (APIs)), provide data transport and handling (Middleware), and often include tools that ease application integration (Software Development Kits). The traditional large industry providers, should leverage their expertise in OPIR ground systems to enable frameworks based on OSA and EGS constructs to create development and integration efficiencies for application developers.

Advances in commercial computing technologies, especially in *Open Source Software* (OSS), allow for affordable implementation of required framework constructs. One example of OSS adoption comes from the field of real-time business intelligence. In this example, real-time streaming data from business sources/sensors is analyzed and rapidly turned into actionable information. These stream processing solutions are designed to handle high volumes of data in real-time with scalable, highly available, and fault tolerant architectures. Existing OSS stream processing solutions solve various challenges that were traditionally thought to be unique to the ground data processing domain.

Another valuable OSS solution that is common across multiple platforms is *application orchestration* ("Orchestration (computing)"). Orchestration applies at numerous levels of an architecture but in the context of a data processing framework is the process of dynamically integrating two or more components together to automate a process, or synchronize data. In legacy systems, point-to-point integration resulted in a complex tangle of application dependencies that was very hard to manage, monitor, and maintain. OSS-based application orchestration provides a way to centrally manage and monitor application integration. Commonality and overlap between OSS solutions and satellite ground processing needs provides significant value while aligning with OSA principles.

While the traditional DoD ground system development approach has often resisted OSS, the DoD has detailed OSS policy that makes it clear that OSS must be considered. Additionally, as OSA, EGS, and future open processing frameworks are developed, USG labs can be used to ensure compliance to DoD OSS and cyber security requirements. Two such labs have recently been stood up to promote this approach in support of EGS and OBAC. The Air Force Space Command (AFSPC) EGS System Integration Lab (SIL) and Space and Missile Systems Center's (SMC) Tools, Applications, and Processing (TAP) Room were designed to provide R&D environments where adherence to standards and integration efficiency can be enforced.

Beyond OSS within framework implementations, it is recommended AFSPC leverage overall ownership of framework source code to offer solutions as *Government Open Source Software* (GOSS). Major advantages to using the GOSS model include framework solutions that can be maintained by the broader OPIR community and enabling

participation by smaller businesses that have limited resources. Reuse and collaborative OSS and GOSS software development are in the best interest of the OPIR community, as it reduces costs by eliminating duplicative efforts and can increase quality through community-wide peer review.

3.2.1 Framework Architectural Tenets

In addition to commercially accepted concepts such as OSS there are primary architectural tenets that adaptive OPIR frameworks should embrace. Figure 3 illustrates the primary architectural constructs recommended for OBAC and future ground processing environments. These tenets are meant to convey the primary support mechanisms that drive the efficiencies required for emerging missions such as BA. These tenets also provide implementation concepts for many of the OSA practices defined earlier in Figure 3.

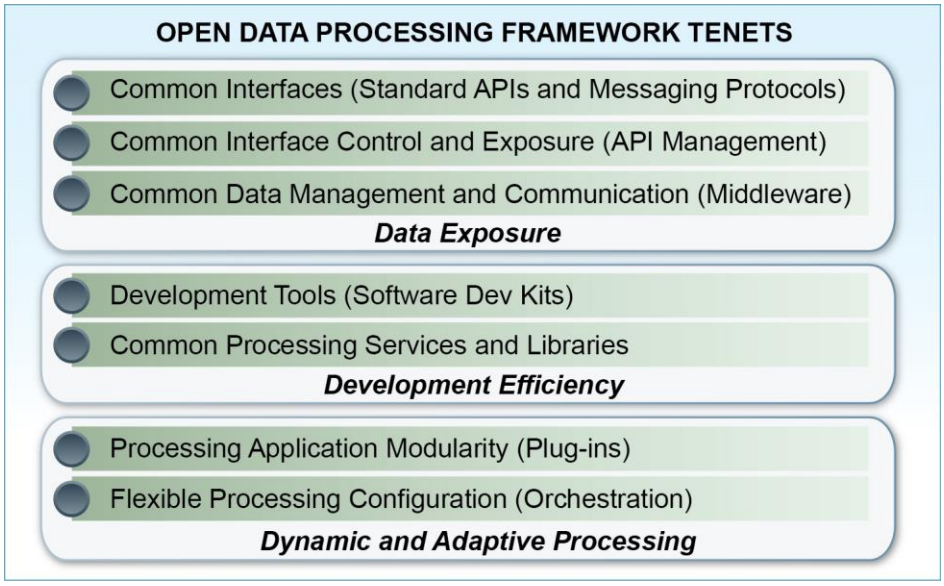

Figure 3: Primary Architectural Tenets to Ensure Scalability and Flexibility

The recommended tenets are grouped into three primary categories, data exposure, development efficiency, and dynamic and adaptive processing.

From a data exposure perspective, standard practice is the use of APIs based on widely accepted standards. Included in the API construct is the management of the established APIs to ensure configuration management and exposure to developers. Within a framework, APIs are built upon middleware that should again be based on widely accepted standards (many OSS implementations exist).

The development efficiency category is driven by concepts such as software development kits (SDK) and common services and libraries. Ultimately, efficiency is created by allowing application developers to focus on their capability development without having to re-create commonly required functions. These common functions are provided via the framework services, libraries, and SDK.

Lastly is the ability to create new processing threads or workflows dynamically. This category is enabled by orchestration technologies and proper design of applications to leverage plug-ins. Processing orchestration allows developers and users to integrate processing chains constructed of various applications to explore support to emerging mission needs without specifying an end-to-end solution. Plug-ins (much like common services) allow for application developers to swap specific portions of their applications without re-writing the entire application. Over time, a library of plug-ins becomes available as part of the common library that drives development efficiency.

When examining the path forward for developing an OBAC exploitation framework, these tenets should be at the root of everything the community builds. Adherence to these simple tenets (validation discipline through R&D labs is key) ensures an efficient exploitation environment as well as solutions that fit into larger architectural visions such as EGS.

3.3 Development and Deployment Concepts

In addition to the framework itself, achieving the level of rapid response and adaptability desired by the OBAC requires innovative software development and deployment concepts that focus on greater BA mission effectiveness. Key elements to realizing these goals include community embracement of agile software development (ASD), Development Operations (DevOps) practices, and cloud computing.

Agile software development (ASD) is a set of software development principles in which requirements and solutions evolve through collaborating self-organizing, cross-functional teams. ASD promotes adaptive planning, evolutionary development, early delivery, and continuous improvement while encouraging rapid and flexible response to change. ASD also aligns well with the transparency outlined in Better Buying Power.

DevOps emphasizes software developer collaboration and automating the process of software delivery and infrastructure changes. DevOps establishes a culture and environment where building, testing, and releasing software can happen rapidly, frequently, and more reliably. These attributes clearly support the idea of an adaptive OPIR environment.

Cloud computing provides opportunities to maximize utility and minimize waste by leveraging inherent service models. The cloud environment, where the OPIR Enterprise resides, should include *Infrastructure as a Service* (IaaS) for provisioning of computing hardware, *Platform as a Service* (PaaS) for development environments, and *Software as a Service* (SaaS) for software licensing and efficient application delivery. This path enables the OPIR software community to access existing services and build a valid business model across enterprise-wide application software licensing.

These concepts working together will move the USG towards an innovative OBAC environment that readily takes advantage of common framework and services.

4 Recognized Constraints

The current Missile Warning dominated OPIR sensor data environment is driven by assured delivery of real time products. As is shown in Figure 4, this environment is typically constrained by compliance testing, user training, and system reliability. These factors ensure each community-wide product is consistent, accurate and, completely reliable. Cyber Security and data source security classification will equally constrain environments. These constraints must be addressed holistically ensuring successful integration of multiple intelligence channels and industry layers into the OPIR data processing chain.

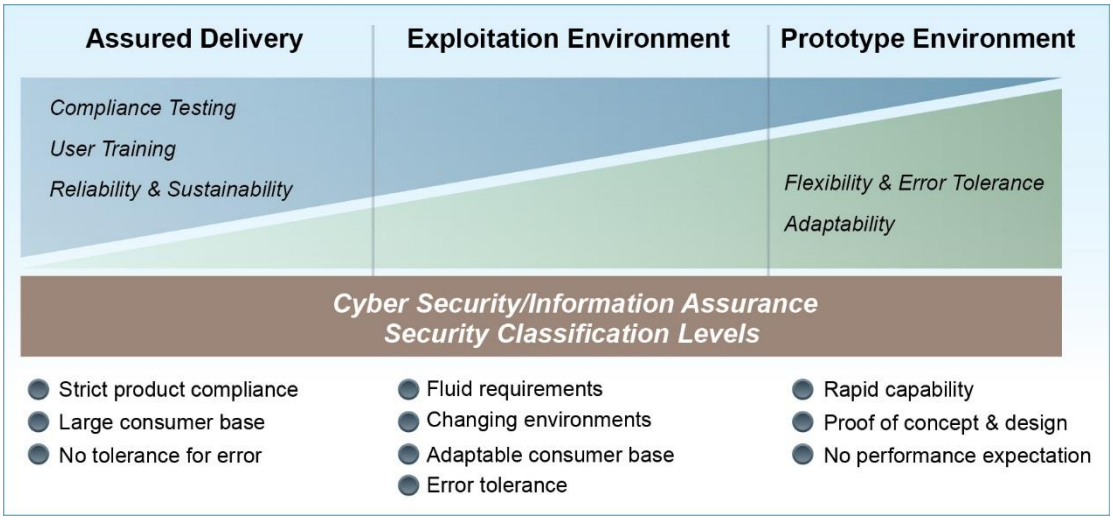

Figure 4: Recognized Environment Constraint Variations

4.1 Unique Environment Constraint Factors

There are four constraint factors that must be carefully planned to ensure products in all environments meet operational need: compliance testing, user training, reliability/sustainability, and cyber security.

Compliance testing demonstrates system-level performance will meet mission parameters. In the assured delivery component, this is a critical activity that spans a great period of time and has multiple levels of validation. Compliance testing ensures the system will support operators in mission execution and will produce the high quality alerts/warning expected of the OPIR community. For exploitation environments, compliance testing requirements can be relaxed thereby allowing more rapid product integration. Compliance testing constraints often increase as community expectations and reliance grow.

User training ensures operational consistency and repeatable performance over long periods of time. Details and requirements significantly impact capabilities deployment. Completing up-front user training requirements and performance expectations allow new capabilities to smoothly transition from prototype applications through assured delivery. Operational expectations of product performance must be tightly coupled with expected training capability and personnel turnover. For exploitation environments, training can be adapted to expect more dynamic influx of capability and greater flexibility to change. This is achieved through greater visibility into product development by operational users via concepts such as agile software development. Such visibility allows developers to address user needs during development vs. training for complex user interface designs post deployment.

Reliability and sustainability determine cost and support structures required to integrate new capabilities from the prototype environment through the exploitation environment and into the assured delivery component. Quickly adding capabilities into infrastructure supports quick discovery and injects new capabilities. Ensuring consistency and product availability determines support levels and infrastructure required to ensure products are available to support. For exploitation environments, leveraging deployment concepts such as DevOps enables the commonality between all environments thereby reducing integration cost and schedule.

Cyber Security is a vital component of any operational system. As shown in Figure 4, security constraints are equally stringent across operational environments. Security must be accounted for, whether developing prototype BA capabilities or maintaining a Missile Warning system. Each environment must ensure adequate user controls are in place and system integrity is tightly controlled. Each system and integration level must be accredited under the Risk Management Framework ("Risk Management Framework Overview"). This accreditation will drive schedule and implementation. Focus on application level integration will drive additional system constraints and force a strict security evaluation of development standards and code delivery. Security concerns must be well understood and passed to development teams ensuring innovation in prototype and exploitation environments are not hindered through deployment. Security constraints must be addressed from initial coding through final deployment.

Additionally, security classification levels of data, applications, and services will be key constraints on OPIR processing systems. The ability to share data and system capabilities at the lowest levels while maintaining OPSEC and need-to-know constraints are common system constraints that must be planned into development and services infrastructure. Without adequate controls, the vision of integrated multiple intelligence platforms and incorporating academic institutions, and small companies to facilitate innovation will not be possible. Strict user identification and control, with built-in auditing and monitoring, will be required to protect the system from intrusion and malicious attacks.

The constraints of our mission domains are well understood. It has become increasingly clear that development and deployment methods and technologies adapted from commercial practices offer new paradigms that can effectively address many of these constraints. Adapting these practices in the OPIR domain ensures the USG's ability to meet the needs of environments such as the OBAC and determine viability for traditional Missile Warning domains.

5 Way Forward

5.1 Migrating to an Open Framework

Adapting the current Missile Warning architectures to allow for greater effectiveness for missions such as BA, requires community focus on an implementation of the various OSA constructs described throughout this whitepaper. The common data processing framework is of primary importance amongst these constructs. Further analysis

of the framework architectural tenets identified in Figure 3 highlight that the tenets differ from one another when examined under the auspice of implementation complexity versus exploitation value.

As acquisitions and development organizations weigh each development activity against budget and schedule constraints, priority decisions must be made. Figure 5 depicts the recommended approach for framework development with areas such as Common Middleware and Common APIs of highest priority. As the figure shows, these tenets are relatively easy to implement and provide the greatest value to emerging missions such as BA.

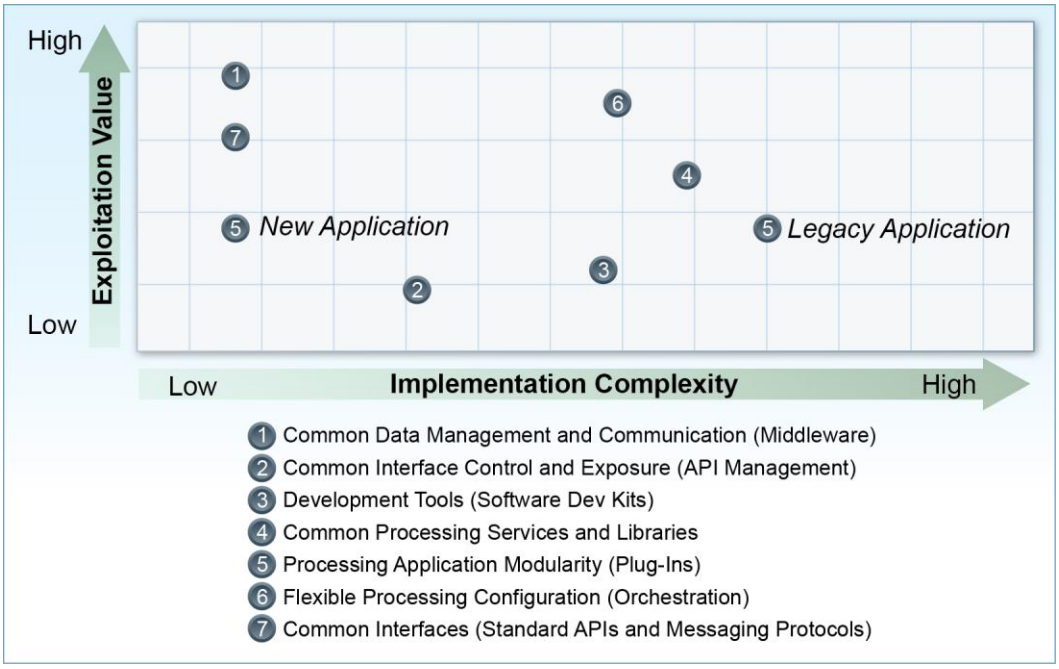

Figure 5: Architectural Tenets - Value vs. Complexity

Adoption of existing processing frameworks that meet the illustrated constructs (in whole or in part) allows the Air Force to leverage validation being done by Federally Funded Research and Development Center (FFRDC) counterparts and development being funded by numerous other organizations. While open systems-based command and control frameworks have been a major focus of efforts such as EGS, considerable effort is starting to coalesce around common frameworks for mission data processing. Leveraging this effort strengthens near-term OBAC processes while also providing ties into long term efforts such as EGS.

To create the efficiencies needed for OBAC (and future missions) success, the processing framework must be available at all R&D and Operational facilities. R&D labs provide an excellent environment for application developers to validate their processing techniques against recorded and live data sets. Additionally, R&D labs provide an optimal setting for rapid development demonstrations allowing users to provide feedback on applications as they develop versus waiting for the final product based on a specification. Once validated, having the same processing framework at Operational facilities ensures a seamless deployment. More importantly, having the same framework at multiple Operational facilities drives a larger user base for the applications being developed and in turn a larger community of developers addressing BA needs.

Another important step in transitioning is the migration of legacy applications that play a vital role in various users mission data processing needs. While the BA domain will drive many new applications, there are many existing and proven applications that may contribute to the mission. As value added legacy applications are identified, investment into decoupling from their legacy designs to allow integration into the common processing framework should be examined.

Perhaps the most important transitional step required is the movement of this open framework and data sets into a more accessible and scalable environment. Beyond even the R&D labs, the Air Force needs to ensure that it properly supports the common framework software, documentation, and any processing applications in repositories that are reachable by a larger audience of developers than the traditional models allow. That needs to be followed up with acquisitions that specify required usage of these common repositories and validation of compliance.

5.2 Ensuring a Common Security Posture

To accomplish the ability to leverage the open framework model and pull from multiple applications and developers the community must provide an executable security framework. Traditional development has dictated security standards through contract deliverable products and multiple software design reviews and test cycles. Third party applications added onto the deliveries were validated through organizations such as National Information Assurance Partnerships (NIAP). Vendors would test and achieve NIAP certification and would be acceptable for integration into multiple Government Information systems. These types of certifications are not feasible for application developers in the open framework model described in this whitepaper. Obtaining NIAP certifications is a very costly and time consuming effort.

In the open framework model, security requirements for applications should be driven by the Application Security and Development Security Technical Implementation Guide (STIG). Framework integration by application developers would require developers to validate they meet the Application Security STIG requirements for delivery into an accredited security enclave. This in turn requires a very flexible security plan to realize the expected gains of an open framework while maintaining a strong security posture under the risk management framework.

5.3 A Services Environment

In concert with the open processing framework and applications, providing an environment to fully support processing capabilities spread through multiple operational structures requires key capabilities for cost effective insertions. These capabilities include a robust infrastructure for capability delivery and information assurance wrapped and controlled by a common management infrastructure as depicted in Figure 6.

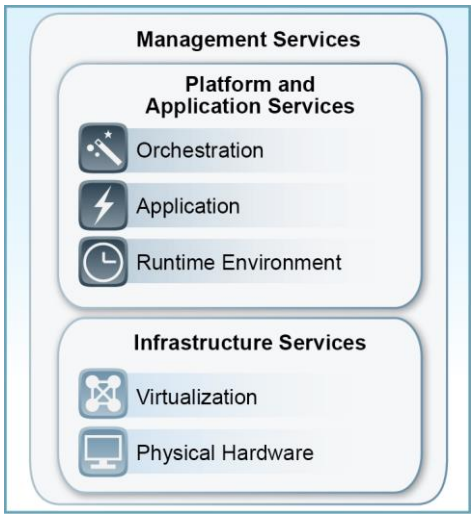

Figure 6: Recommended Services Levels

Separation of hardware infrastructure from application delivery is a critical component in developing a more adaptable processing system. The ability to reduce cost related to processing/storage/networking infrastructure will be realized by separating underlying hardware infrastructure and provide those capabilities as a service rather than as part of each independent solution. This capability is readily available in industry (in private and public cloud systems) as Infrastructure as a Service (IaaS).

Residing on the IaaS, platform and/or application services provide a consistent run time environment that includes the operating system and select services to maintain required security posture. Operating system deployments along with auditing and access control services are centralized, configuration managed, and pushed to applications developers. This ensures environments that are consistent with security approved controls and interfaces. Controlled data distribution, messaging, data base management, and unique OPIR processing services all reside within this service layer as well. This layer is traditionally where the processing framework described throughout this whitepaper is prescribed. These services allow application developers to test to a common services layer and limit system testing constraints. Isolating applications to service interfaces (APIs), allows traditional test and delivery of widely consumed industry products while allowing innovative capability insertions in the exploitation and prototype environments.

Numerous items need to be addressed to fully realize a more agile, affordable, and resilient ground system. The OBAC and ultimately future Missile Warning environments can adapt through sustainment to the provided way forward suggestions. As these concepts are adapted, the USG will enable the quick integration and application approval into operating environments that is desired.

6 Summary

The establishment of the OPIR Battlespace Awareness Cell (OBAC) is a concrete example of the desire to leverage OPIR data beyond its intended Missile Warning origins. The value in transitioning our current OPIR ground processing environments to support domains such as the OBAC will be measured by the positive impact on warfighter needs. Based on concepts in this paper, the ability to efficiently deliver new capabilities supporting emerging missions will yield:

- **Quicker responsiveness to expressed needs.** *Providing efficient deployment and data access environments will allow the community to quickly determine if OPIR can answer a warfighter need.*
- **Effective and efficient transition from R&D to Operations.** *If assessed capabilities show promise, transition to operational usage is seamless and realizable. This has historically been an issue across all of the DoD. Creating common infrastructure and services allows us to ensure a seamless transition path for R&D capabilities that meet a warfighter need.*
- **Better usage of resources to address emerging missions.** *The community needs environments that allow acquisitions and contractors to succeed and fail quickly. In new missions, experimentation is vitally important in driving advanced capabilities. These environments can effectively shift focus from legacy infrastructure issues and onto development of solutions for the emerging missions.*
- **Enhanced Missile Warning and Missile Defense.** *In addition to addressing emerging missions such as BA, improved capabilities for traditional missions are provided the opportunity for more efficient development and deployment.*

The community has only scratched the surface of OPIR data exploitation. As new sensors continue to come online, significant opportunity exists in emerging missions and enhancements to legacy missions. The OSA framework will allow integration of new applications through standards and open systems based designs and also serve as platforms for exploitation pathfinders and prototyping initiatives. This approach leverages open architectures and advances the environment to seamlessly accept third party applications while supporting transition from Research and Development to Operations. The ability to combine information technology maturity and acquisition flexibility will greatly advance the value of OPIR data for the warfighters and all users.

7 References

"Better Buying Power." Department of Defense Better Buying Power Acquisition, Technology, and Logistics. 2010. Web. 01 March 2016. <http://bbp.dau.mil/>.

"DAG Systems Engineering." Defense Acquisitions Guidebook. DAU. Web. 01 March 2016. <https://dag.dau.mil/Pages/Default.aspx>.

"Department of Defense Standard Practice - MIL-STD-881C." DAU. 2011. Web. 01 March 2016. <https://acc.dau.mil/adl/en-US/482538/file/61223/MIL-STD%20881C%203%20Oct%2011.pdf>.

"DODI 5000.02, Operation of the Defense Acquisition System." DoD Issuances. 2015. Web. 01 March 2016. <http://www.dtic.mil/whs/directives/corres/ins1.html>.

"Orchestration (computing)." Wikipedia. 2016. Web. 01 March 2016. <https://en.wikipedia.org/wiki/Orchestration_%28computing%29>.

Priddy, Kevin. USAF Open Approaches Way Ahead. United States Air Force Air Force Life Cycle Management Center. 2015. Web. 01 March 2016. <https://www.google.com/search?q=US+Air+Force+Open+Approaches+Way+Ahead&ie=utf-8&oe=utf-8>.

"Risk Management Framework Overview." Computer Security Resource Center. NIST. 2014. Web. 01 March 2016. <http://csrc.nist.gov/groups/SMA/fisma/framework.html>.