The Agile Defense Ecosystem: A Strategic Framework for Next-Generation Supply Chain Resilience and Global Partnerships

I. Executive Summary and Strategic Mandate

A. The Modern Defense Industrial Challenge and the Victoria Model

The contemporary defense industrial base (DIB) faces an operational environment characterized by unprecedented speed, complexity, and unpredictability, placing resilience and agility at the forefront of military sustainment requirements. Traditional supply chain models, which often rely on proprietary, vertically integrated systems, are inherently brittle against rapidly evolving threats, obsolescence cycles, and global geopolitical instability. The U.S. Department of Defense (DoD) has mandated a fundamental shift away from these stovepiped architectures toward competitive, open frameworks to maintain a technological and operational advantage. This paradigm shift requires integrating technical expertise, robust financial risk modeling, and advanced regulatory compliance into a unified strategic approach.

The strategic role of the Manager of Supply Chain Strategy and Proposals—held by Victoria, operating remotely from Seattle, WA, and serving the Melbourne, FL, Network and Imaging division of Leonardo DRS—is uniquely positioned to navigate this transition. The successful execution of this role demands a fusion of disciplines: a foundational understanding of software architecture and engineering (B.S. in Computer Science and Software Engineering), rigorous economic analysis and risk assessment (B.S. in Economics), executive leadership capacity (managing complex legal and hospitality operations), and specialized legal/linguistic mastery for international engagement (interpreter experience and fluency in USA English, Polish, Russian Federation Language, and Belorussian). This interdisciplinary "Victoria Model" addresses the integrated demands of next-generation defense acquisition, including rapid technology insertion, aggressive cost avoidance, and mitigation of high-stakes geopolitical supply chain risks.

B. Strategic Mandate: Transitioning the MFoCS Ecosystem and Embracing MOSA

Defense Contractors currently holds a critical position as the sole-source provider of mission command computing and display systems for the U.S. Army through the Mounted Family of Computer Systems program. This system, which provides crucial Situational Awareness (SA), Command and Control (C2), and tactical logistics capabilities, represents the culmination of nearly two decades of combat experience. However, the strategic landscape is changing. The government is signaling a clear intent to modernize MFoCS by transitioning to

Block III systems, specifically requesting industry information on All-In-One (AIO) solutions, reduced size, weight, power, and cost (SWaP-C), and—most critically—innovative strategies for long-term obsolescence mitigation and cost reduction.
This procurement shift directly aligns with the DoD's legislative mandate to adopt a Modular Open Systems Approach (MOSA). MOSA is the DoD's preferred method for acquisition and is explicitly required by Title 10 U.S.C. 4401(b) for all major defense acquisition programs (MDAP). The primary objective of MOSA is to foster a system architecture that employs modular interfaces between major components, allowing these components to be incrementally added, removed, or replaced throughout the system's life cycle. This framework achieves several critical benefits, including significant cost savings or avoidance, schedule reduction, rapid deployment of new technology, and enhanced competition. The implementation of MOSA within the Network and Imaging domain is manifested through adherence to the CMOSS (C5ISR/EW Modular Open Suite of Standards) and SOSA (Sensor Open Systems Architecture) standards, which define the standardized, vendor-agnostic technical requirements necessary for true plug-and-play capability. Defense Contractors must strategically pivot its proposal methodology from defending a sole-source, proprietary position to aggressively embracing the role of a master system integrator and orchestrator of a resilient, open ecosystem.

C. The Three Grandiosa Ideas (Dissertation Pillars)

To capitalize on the shift to MOSA and transform strategic proposals into executable competitive advantages, three strategic pillars are proposed, forming the core of an advanced supply chain strategy dissertation:

1. **The Open Compute Ecosystem Consortium (OCEC):** A formal, legal partnership mechanism structured using Other Transaction Authorities (OTAs) designed to rapidly integrate Non-Traditional Defense Contractors (NTDCs) and Commercial Off-the-Shelf (COTS) technologies that are compliant with CMOSS/SOSA standards, thereby proactively mitigating single-source obsolescence risks.
2. **Quantified Cyber-Physical Resilience (QCPR):** An integrated risk management framework that mandates the use of Cybersecurity Risk Quantification (CRQ) and Software Bill of Materials (SBOM) documentation to provide financially measurable, data-driven security profiles for all supply chain components, justifying investment in resilience within acquisition proposals.
3. **The Geo-Linguistic Risk Assessment and Partnership Desk (GLRAPD):** A specialized strategic function leveraging multilingual and legal expertise to rigorously vet international supply chain partners, mitigate geopolitical risks (particularly concerning Eastern European provenance), and enhance Foreign Military Sales (FMS) and Direct Commercial Sales (DCS) outcomes through precise contractual negotiation and localized sustainment support.

II. The Strategic Imperative: Navigating the Defense Industrial Base (DIB) in the Digital Age

A. The Dual Challenge: Sole-Source Transition and Obsolescence Mitigation

The defense supply chain inherently contends with severe operational challenges, including massive complexity, vulnerability to geopolitical factors, and increasing exposure to sophisticated cybersecurity threats. For incumbent providers like Defense Contractors, the reliance on proprietary systems under a sole-source contract model presents a critical strategic vulnerability. While the sole-source arrangement for MFoCS II ensures steady revenue , it often results in the long-term logistical burden of diminishing manufacturing sources and material shortages (DMSMS) and parts obsolescence. When systems age, they frequently require parts that are at their end of life and unavailable, forcing organizations to incur significant costs to source components on the secondary market or restart production lines for old components. Furthermore, the lack of inherent competition in sole-source scenarios has drawn legislative scrutiny, with stakeholders alleging that defense firms have overcharged the U.S. government for equipment, potentially costing billions of dollars. This public and congressional scrutiny provides significant impetus for the DoD's mandate to move toward open, competitive architectures. The specific requests embedded in the MFoCS Block III Request for Information—demanding innovative ways to reduce cost, mitigate obsolescence, and implement a strategic refresh schedule while maintaining backward compatibility —confirm that the government is actively seeking to leverage market competition to drive down life cycle costs.

B. The DoD Mandate: Modular Open Systems Approach (MOSA) as a Competitive Driver

The DoD's acquisition strategy is now fundamentally anchored in MOSA, which constitutes both a technical and business strategy for designing affordable and adaptable systems. Technically, MOSA requires the use of modular, loosely coupled systems with interfaces conforming to accepted, consensus-based open standards. Legally, 10 U.S.C. 4401(b) mandates that MDAPs must comply with specific requirements, including the use of modular interfaces and a system architecture that explicitly permits the incremental addition, removal, or replacement of major system components throughout the life cycle. This design philosophy ensures opportunities for enhanced competition and innovation.

The benefits derived from strict MOSA implementation are profound: cost savings, rapid schedule reduction for new technology deployment, and enhanced technical upgrades and refresh opportunities. By enabling system components to be severable and replaceable, the DoD directly addresses the high costs associated with proprietary systems and obsolescence risk.

C. CMOSS/SOSA Implementation in Network and Imaging

The Network and Imaging domain must focus on the technical implementation of MOSA through the CMOSS and SOSA standards. CMOSS is a direct implementation of MOSA principles designed to reduce Size, Weight, Power, and Cost (SWaP-C) for Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C5ISR) and Electronic Warfare (EW) systems. SOSA, or Sensor Open Systems Architecture, focuses on joint-service interoperability within this modular framework.

Adherence to these standards dictates specific, non-proprietary hardware requirements. For example, SOSA demands consistency in power, limiting the power output for power supply units (PSUs) typically to 12V, with some 3.3V auxiliary power. Furthermore, the system must employ an Intelligent Platform Management Controller (IPMC) to communicate with the chassis

manager. Modern SOSA-aligned boards also require higher backplane speeds, such as PCIe Gen4 (16 Gbaud/s) and 100GbE, necessitating specialized components like high-grade PCB material and advanced cooling solutions.
For Leonardo DRS, the MFoCS Block III transition requires acceptance that backwards compatibility with fielded MFoCS Block I/II installation kits is the absolute minimum threshold for compliance. The strategic advantage lies in demonstrating how the new system, built on CMOSS/SOSA, transforms component acquisition. By facilitating open interfaces and vendor-agnostic solutions, Leonardo DRS shifts its business value proposition from supplying proprietary hardware to mastering the orchestration and integration of a vast ecosystem of diverse, competitive, and compliant suppliers. This strategic pivot is necessary to ensure long-term cost avoidance and enhanced supply chain resilience by continuously integrating new, high-performance standardized technology from competitive sources, resolving the fundamental problem of proprietary system obsolescence.

III. Pillar 1: Strategic Proposals for Technology-Driven Partnership and MOSA Alignment (The OCEC)

A. Grandiosa Idea 1: Establishing the ‘Open Compute Ecosystem Consortium (OCEC)’

The OCEC is proposed as a structural solution to the limitations of traditional procurement processes, facilitating the rapid adoption of MOSA-compliant components for programs like MFoCS Block III. The establishment of this formal enterprise partnership must leverage the flexibility of Other Transaction Authorities (OTAs). OTAs are contractual instruments distinct from standard procurement contracts, grants, or cooperative agreements. They provide the government with a flexible mechanism to acquire research and development (R&D) activities and prototypes, crucially allowing access to cutting-edge solutions from Non-Traditional Defense Contractors (NTDCs).
Utilizing OTAs for the OCEC bypasses standard procurement barriers, such as complex Cost Accounting Standards (CAS) compliance requirements, making it significantly easier for smaller, innovative technology firms to engage with the defense sector. This model directly aligns with the DoD’s acquisition transformation strategy, which aims to maximize the use of commercial standards and remove policy barriers for NTDCs. The strategic function of the OCEC is to create a pre-vetted, managed competition pool of suppliers who demonstrate strict adherence to CMOSS, SOSA, and VICTORY standards.

B. Consortium Membership, Vetting, and Technical Standards

OCEC membership must be selective, focusing on suppliers capable of delivering components essential for high-performance mounted computing. These components include high-speed backplane providers, advanced cooling solution manufacturers, and firms specializing in complex RF/optical interfaces necessary for modern C5ISR functionality. The vetting process must ensure potential partners meet stringent compliance standards, including explicit certification of ITAR and DFARS adherence, limiting access to sensitive information to authorized personnel, and maintaining up-to-date security patches.
The OCEC serves as a risk mitigation tool by transforming hundreds of NTDCs from potential

single-point supply chain risks into regulated, competing suppliers. By continually validating compliance with open standards, the consortium institutionalizes rapid technology insertion. This proactive approach ensures that when a component reaches its end-of-life status (DMSMS), an established, competitively-priced alternative component that is fully interoperable within the SOSA-aligned chassis can be swiftly procured, achieving the long-term cost avoidance benefit promised by MOSA.

The foundational requirement for any OCEC member is adherence to data transparency and technical interchange standards.

Table 3: OCEC Partnership Onboarding Checklist (Pillar 1)

Phase	Action Item	Strategic Justification
Prequalification	ITAR/DFARS Compliance Certification	Mandatory for controlling technical data export and securing sensitive systems.
Technical Vetting	SOSA/CMOSS Alignment Verification (IPMC, 12V power)	Ensures physical and electrical interoperability and plug-and-play capability.
Digital Security	Submission of Software Bill of Materials (SBOM) and VEX	Foundation for supply chain software transparency and vulnerability assessment.
Contract Mechanism	Utilization of Prototype or Research OTAs	Reduces time-to-market and lowers regulatory barriers for Non-Traditional Defense Contractors.
Sustainment Clause	Negotiated Technical Data Package (TDP) and IP Rights	Grants the government and prime contractor the necessary rights for sustainment, modification, and obsolescence mitigation.

C. Strategy for Data Rights and Intellectual Property (IP) in MOSA Contracts

While MOSA mandates open standards and interfaces, the successful long-term sustainment of complex systems requires a rigorous strategy for managing Intellectual Property (IP) and technical data rights. The OCEC's contracting framework must reflect the modern approach seen in programs like NorthStar, which mandates a government-designed and -owned architecture at the center of the capability. This mandates that all future OCEC partners deliver the necessary software-defined interface syntax, properties, and documentation in a machine-readable format to ensure that any new vendor can enter the program without intellectual property barriers hindering capability upgrades.

Contractual terms must be strategically drafted to grant the Army the necessary technical rights to maintain and update the system independently. This includes clauses addressing software availability, patch automation, and technical data packages (TDPs). Leverage of legal expertise in contract management is vital for negotiating precise terms, such as surge purchase rights for software licenses at fixed prices or the right to build replacement parts based on technical standards. Furthermore, the negotiation strategy should capitalize on opportunities to obtain targeted IP when an Original Equipment Manufacturer (OEM) or component supplier demonstrates a diminished business case or "waning interest" in supporting older technology.

This proactive IP management is a key differentiator between simple compliance and strategic sustainment mastery in the MOSA environment.

D. Partnerships for AI, COTS, and Predictive Logistics

The Network and Imaging strategy must extend beyond hardware to encompass software dominance, emphasizing a commercial-first approach to technology adoption. The OCEC should actively court partnerships that provide advanced Commercial-Off-the-Shelf (COTS) software solutions, such as proven C4ISR suites, to enable seamless integration across allies, domains, and echelons.

A particularly crucial area for partnership is Artificial Intelligence (AI) and Machine Learning (ML). Predictive analytics driven by AI/ML is revolutionizing military sustainment by transitioning logistics from reactive to proactive readiness. Strategic OCEC partners should deliver tools capable of analyzing historical data, current trends, and operational plans to forecast component demand, monitor equipment health, and optimize inventory positioning—what is known as predictive logistics. This capability is critical for ensuring the right resources are available at the right time in contested, complex operational environments. Furthermore, the DoD is accelerating the adoption of frontier AI, using partnerships with leading U.S.-based companies to develop agentic AI workflows. The OCEC must integrate these cutting-edge AI capabilities into the MFoCS ecosystem to enhance battlefield management, intelligence, and enterprise information systems.

IV. Pillar 2: Building Resilient and Secure Supply Chains (C-SCRM)

A. Grandiosa Idea 2: Quantified Cyber-Physical Resilience (QCPR) in Proposals

To address the growing cybersecurity threat landscape—which adversaries increasingly target in military supply chains —the Quantified Cyber-Physical Resilience (QCPR) framework is necessary. QCPR integrates rigorous financial risk modeling into every stage of component procurement, supply chain management, and proposal development. Cybersecurity is no longer merely an IT compliance concern; it is a measurable, mission-critical supply chain risk.

The QCPR framework utilizes Cybersecurity Risk Quantification (CRQ) methodologies to transform vague, subjective risk assessments (e.g., red/yellow/green ratings) into concrete financial terms. The methodology involves using frameworks such as those detailed in NISTIR 8286A to establish scope, context, and criteria; identify specific cybersecurity-related risks; and calculate the likelihood and estimated financial impact of successful exploitation. The process requires identifying key assets—including proprietary systems, intellectual property (IP), and crucial data—and estimating the dollar figure associated with potential attack effects, such as recovery costs, lost IP, and reputational damage.

By translating cybersecurity posture into dollars and cents, proposals can justify strategic investments in secure hardware and software. For instance, QCPR can rigorously demonstrate why a $50,000 investment in advanced cybersecurity hardware is warranted by proving it mitigates an estimated $1.5 million risk of data breach or system compromise. This approach enables data-driven budget justifications, improves corporate board conversations regarding

enterprise risk, and guides smarter insurance and procurement decisions. Procurement specifications from suppliers with high vulnerability scores can then rigorously require better cybersecurity implementation as a condition of contract award.

B. Mandating Software Bill of Materials (SBOM) and VEX for Digital Trust

A foundational element of QCPR and effective cyber supply chain risk management (C-SCRM) is complete transparency into the software components embedded in defense systems. The Software Bill of Materials (SBOM) has emerged as a key requirement for enhancing understanding and security across the software supply chain. An SBOM provides a standardized, nested inventory—a "list of ingredients"—that makes up software components. Mandatory SBOM submission for all OCEC partners is vital for securing the software supply chain at the component level.

Coupled with the SBOM is the requirement for a Vulnerability Exploitability eXchange (VEX) document. A VEX document is a security advisory that attests whether a product or products are affected by specific known vulnerabilities. The combination of SBOM and VEX allows Leonardo DRS acquisition specialists to evaluate the influence of a supplier’s cybersecurity practices on attack risk by calculating vulnerability and recoverability scores. This enables procurement specialists to proactively demand enhanced cybersecurity or select an alternative vendor if a vulnerable supplier demonstrates poor security practices. This transparency mechanism is critical for meeting the security mandates established by numerous Executive Orders (EOs) requiring federal agencies to address risks associated with Information and Communications Technology (ICT) supply chains.

C. Mitigating Hardware Obsolescence and Single-Source Vulnerability

QCPR provides a mechanism to unify digital and physical resilience. C-SCRM strategies must integrate policies for Diminishing Manufacturing Sources and Material Shortages (DMSMS) and counterfeit prevention. The financial modeling of QCPR should extend to quantifying the expected cost of obsolescence avoidance.

The strategy necessitates embedding long-term obsolescence planning and contractual sustainment terms upfront in all procurement agreements. This includes requiring clear refresh schedules and ensuring that contractual terms—beyond overly relying on OEMs for software and hardware rights—call for minimally acceptable performance capabilities. Proactive measures include pricing line items for technical data packages, data escrow accounts, and securing full software licenses and warranties, thus guaranteeing the capability to execute surge purchases or build replacement parts based on technical standards in the face of supply disruption. This combined approach—where QCPR defines the financial consequences of both cyber risk and material shortage—ensures that proposals are defended not just on initial cost, but on long-term risk-adjusted life cycle value.

V. Pillar 3: Global Competitive Advantage through Strategic Multilingual Negotiation and Compliance

A. Grandiosa Idea 3: The Geo-Linguistic Risk Assessment and

Partnership Desk (GLRAPD)

As Leonardo DRS expands its global footprint and engages in increasingly complex international defense trade, a strategic function dedicated to managing foreign partners, geopolitical risk, and legal compliance is paramount. The GLRAPD formalizes the leverage of specialized linguistic and legal expertise—particularly the mastery of USA English, Polish, Russian Federation Language, and Belorussian, coupled with experience in court interpreting and law firm management—to achieve competitive advantage and rigorous compliance. International contracts, whether Foreign Military Sales (FMS) or Direct Commercial Sales (DCS), are inherently challenging. FMS systems acquisition often involves foreign partners who may be unfamiliar with the myriad of DoD acquisition policies and require substantial assistance in articulating their requirements. While Direct Commercial Sales (DCS) allow international partners more direct involvement in contract negotiation, this necessitates absolute clarity on complex technical and legal terms. The expertise provided by the GLRAPD ensures that technical and compliance specifications (e.g., ITAR, DFARS) are translated and negotiated by an authoritative subject matter expert, guaranteeing semantic accuracy and mitigating the risk of misinterpretation, which is a major factor in international contract disputes. Although English is often the lingua franca of international business, drafting the contract in both English and the official language of the foreign country remains a best practice to ensure legal clarity and enforceability.

B. Geopolitical Risk Modeling and Partnership Diversification

The specialized linguistic proficiency of the GLRAPD is directly applicable to managing acute geopolitical supply chain risks, particularly in Eastern Europe. The current environment is marked by ongoing military partnership and coordination between the Russian Federation and Belarus. Any component sourcing that may originate from or transit high-risk areas associated with these nations must be subjected to immediate, heightened scrutiny under the QCPR framework to prevent exposure to sanctions, espionage, or technology dependence risks. Conversely, the GLRAPD facilitates strategic diversification within key NATO allies. European nations are increasingly focused on improving supply chain resilience and reducing technological dependence on certain US weapons systems, driven by concerns over potential software "kill switches" or restricted updates. Strategic partnerships with suppliers in countries like Poland, a NATO ally, can enhance resilience and interoperability. The GLRAPD provides essential linguistic and legal support to proactively vet these partners, ensuring they meet rigorous U.S. export control obligations, including proper registration and adherence to compliance programs tailored to the defense trade business. This strategy positions of Defense Contractors as a reliable, compliant partner committed to mutual resilience.

Table 4: Geo-Linguistic Risk Matrix for Eastern European Sourcing (Pillar 3)

Region/Country	**Language Relevance**	**Supply Chain Risk Type**	**Mitigation Strategy (GLRAPD Role)**
NATO Allies (e.g., Poland)	Polish (Native)	Diversification, Compliance, and Integration risk	Direct support for ITAR/DFARS compliance onboarding, precise negotiation of localized contracts, and fostering

Region/Country	Language Relevance	Supply Chain Risk Type	Mitigation Strategy (GLRAPD Role)
			integrated supply chain resilience.
Russia/Belarus	Russian/Belorussian (Native)	Geopolitical risk, Sanctions, Espionage, Data Vulnerability	Aggressive, quantified vetting (via QCPR) of all commercial software and hardware with potential regional provenance; strict adherence to prohibited destinations screening.
Global DCS Partners (e.g., Thailand)	N/A (Focus: Contract Law)	Sustainment dependence and unauthorized technology transfer risk	Negotiating robust, localized sustainment contracts (Chaiseri model) and ensuring local partners comply with ITAR limitations on technical data access.

C. Enhancing FMS/DCS through Localized Sustainment

The success of Deefense Contractors' partnership with Chaiseri Defense Systems in supporting the Royal Thai Army's Stryker units provides a definitive model for future international strategy. This partnership demonstrates that providing localized support—system installation, operator training, and through-life sustainment—is critical for securing long-term FMS/DCS contracts. The GLRAPD plays a vital compliance role within this model. Since the provision of defense services and technical data is strictly controlled by the ITAR, international partners must be compliant. The desk ensures that as local partners take on sustainment roles, they establish and maintain robust ITAR compliance programs, limit access to sensitive information, and understand the requirements for obtaining necessary licenses and approvals prior to engaging in export activities. This rigorous control over technical data rights and security is essential for mitigating the risk of unauthorized technology transfer and safeguarding the sensitive components of systems like MFoCS II and the new Battle Management System (BMS) provided to allies. By guaranteeing both strategic linguistic negotiation and legal compliance oversight, the GLRAPD converts geopolitical complexity into a core competitive strength.

VI. The Victoria Model: Operationalizing the Remote Strategy Manager

A. Integrating Cross-Functional Expertise into the Proposal Lifecycle

The role of Manager of Supply Chain Strategy and Proposals requires executive-level control and cross-functional fluency, a capability synthesized by the unique background of the incumbent. The shift to a MOSA environment demands that the procurement manager understand not just logistics, but the fundamental structure of the systems (Computer Science/Software Engineering) and the financial consequences of risk exposure (Economics).

The experience gained managing a law firm and interpreting for federal and circuit courts underscores a sophisticated mastery of compliance, contract drafting, and high-stakes negotiation, skills that are now non-negotiable in the highly regulated defense industry.
This strategic convergence means that the proposal lifecycle is managed end-to-end based on a risk-adjusted, technical understanding:

1. **Requirement Definition:** Using computer science expertise to ensure technical requirements mapped in Requests for Proposal (RFP) align precisely with MOSA/CMOSS/SOSA standards.
2. **Vendor Selection (OCEC):** Applying executive management principles to rapidly vet NTDCs and negotiate complex OTAs, securing the necessary IP and data rights.
3. **Proposal Pricing (QCPR):** Leveraging economic and analytical training to integrate CRQ data, translating supply chain resilience investments into measurable cost avoidance for the government, thereby ensuring competitive and compliant pricing.
4. **Global Negotiation (GLRAPD):** Utilizing legal and linguistic expertise to finalize international contracts (FMS/DCS), mitigating geopolitical and compliance risks upfront.

B. Optimizing the Remote Management Structure (Seattle/Melbourne)

Operating remotely from Seattle requires an intentional and high-leverage allocation of time and resources for the four dedicated annual visits to the Melbourne, FL, office. The remote operational structure allows for focused, data-intensive, strategic work, while in-person visits are reserved for tasks requiring executive presence and direct collaboration.
Remote Operations Focus (Seattle, WA): The majority of the work must be concentrated on strategic data analysis and orchestration:

- **QCPR Management:** Daily oversight and refinement of CRQ metrics, review of incoming SBOM/VEX data, and prioritization of supply chain cybersecurity mitigation efforts.
- **OCEC Pipeline:** Managing the virtual vetting, onboarding, and competitive sourcing pipeline for CMOSS-compliant NTDCs via the OTA consortia.
- **GLRAPD Leadership:** Conducting virtual international negotiation preparation, risk modeling (especially for Eastern European provenance), and managing ITAR compliance documentation across global partners.

High-Leverage Travel (Melbourne, FL): The four annual visits must be strictly dedicated to:

- **Executive Proposal Review:** Final approval and sign-off on major MFoCS Block III proposals, ensuring QCPR data and MOSA compliance strategies are fully integrated.
- **Strategic Partnership Initiation:** In-person negotiation and finalization of major OCEC partnership agreements with high-value NTDCs or international partners.
- **Mandated Compliance Training:** Leading high-level, in-person training sessions on critical export control policies, ITAR compliance best practices, and sophisticated social engineering/phishing awareness for authorized personnel.

This structure ensures that the manager's time is maximized for strategic oversight and complex analysis, leveraging the cross-functional expertise to drive innovation and resilience across the Network and Imaging supply chain.

VII. Conclusion and Future Research Directions

A. Summary of Strategic Impact

The traditional defense supply chain model is structurally incompatible with the DoD's urgent need for agility, affordability, and resilience. The mandated shift to MOSA, embodied by CMOSS and SOSA, transforms the competitive landscape for Defense Contractors, necessitating a pivot from proprietary component supplier to master ecosystem integrator.

The three strategic proposals—the **Open Compute Ecosystem Consortium (OCEC)**, the **Quantified Cyber-Physical Resilience (QCPR)** framework, and the **Geo-Linguistic Risk Assessment and Partnership Desk (GLRAPD)**—collectively address this imperative. The OCEC provides the technical mechanism for rapid, competitive technology refresh and obsolescence mitigation by integrating NTDCs via OTAs. QCPR transforms the acquisition justification process by providing financially measurable cyber and physical supply chain risk assessments (CRQ and SBOM/VEX), making resilience an economic necessity. Finally, the GLRAPD leverages highly specialized legal and linguistic skills to expertly navigate and mitigate the geopolitical risks inherent in FMS/DCS, securing global partnerships through meticulous compliance and contract negotiation. These pillars ensure that Defense Contractors can deliver MFoCS Block III proposals that are not merely compliant, but strategically superior in terms of cost, schedule, and mission readiness.

B. Future Research

The implementation of the proposed framework provides fertile ground for advanced quantitative analysis, suitable for doctoral-level research. A critical future research direction is the quantitative study utilizing the QCPR framework to model the projected Return on Investment (ROI) of MOSA compliance versus the risk exposure of proprietary sole-source systems.

This research would specifically focus on quantifying the financial impact of expedited technology refresh and obsolescence avoidance made possible by open architectures. The study would compare the total life cycle cost (TLCC) of a proprietary Block II system (factoring in escalating DMSMS mitigation costs and proprietary software update dependence) against a MOSA-compliant Block III system sourced through the OCEC (factoring in the initial investment in QCPR assessment but quantifying the cost avoidance from competitive sourcing and scheduled refresh cycles). The outcome would be a robust, data-driven methodology that proves the superior long-term financial viability of MOSA, providing definitive proof points for future defense acquisition policy beyond the Network and Imaging domain.

C. Dissertation Scope Finalization

The final scope of the dissertation centers on the strategic implementation of a structured hardware procurement policy aligned with software refresh cycles (lifecycle procurement) across the OCEC ecosystem. This involves establishing standardized guidelines for how hardware components, integrated from NTDCs, should be purchased, defining approval workflows, and setting policies for vendor selection and budget allocation. By ensuring that the OCEC procurement strategy is aligned with continuous software upgrades and maintenance requirements, the system maximizes COTS advantages while maintaining strict compliance adherence, achieving seamless sustainment that supports the resilient and agile sustainment strategies demanded by the future operational environment.

Works cited

1. Resilience And Agility: Supply Chain Requirements In Military Operations, https://tdhj.org/blog/post/resilience-agility-military-supply-chain-2/ 2. Supply Chain Management in the Defence Industry, https://www.defence-industries.com/articles/supply-chain-management-in-the-defence-industry 3. CMOSS: Building-block architecture brings speed, cost benefits, https://militaryembedded.com/comms/communications/cmoss-building-block-architecture-brings-speed-cost-benefits 4. Mounted Family of Computer Systems https://sam.gov/what-we-do/products-and-services/mounted-family-of-computer-systems-mfocs/ 5. Request for Information (RFI) Title: Mounted Mission Command (MMC) Mounted Family of Computer Systems (MFoCS) Block III Market Research Questionnaire for Industry Comment - SAM.gov, https://sam.gov/opp/017266cb4a97453e8f03683008fe53bb/view 6. Modular Open Systems Approach (MOSA) - Defense Standardization Program, https://www.dsp.dla.mil/Programs/MOSA/ 7. Modular Open Systems Approach (MOSA) | www.dau.edu, https://www.dau.edu/acquipedia-article/modular-open-systems-approach-mosa 8. MOSA & CMOSS | SOSA Aligned - Safran Federal Systems, https://www.safranfederalsystems.com/mosa-and-cmoss 9. Integrated CMOSS Systems - Pacific Defense, https://www.pacific-defense.com/integrated-cmoss-systems 10. The U.S. Defense Industrial Base: Background and Issues for Congress, https://www.congress.gov/crs-product/R47751 11. MOSA | NAVAIR, https://www.navair.navy.mil/MOSA 12. Understanding SOSA - everything RF, https://cdn.everythingrf.com/live/SOSA_ebook_Final_1_638575831347426778_2_3_638761395097370396.pdf 13. Other Transaction Agreements (OTA) - ATI | Advanced Technology International, https://www.ati.org/ota/ 14. Other Transactions | Adaptive Acquisition Framework, https://aaf.dau.edu/aaf/contracting-cone/ot/ 15. Acquisition Transformation Strategy - DoD, https://media.defense.gov/2025/Nov/10/2003819441/-1/-1/1/ACQUISITION-TRANSFORMATION-STRATEGY.PDF 16. ITAR and DFARS: What Electronics Procurement and Manufacturing Needs to Know, https://resources.altium.com/p/itar-and-dfars-for-electronics-procurement-and-manufacturing 17. Getting and Staying in Compliance with the ITAR - DDTC, https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=4f06583fdb78d300d0a370131f961913 18. The Right Balance: Ensuring the right balance in negotiating intellectual property in Army contracting | Article - Army.mil, https://www.army.mil/article/285512/the_right_balance_ensuring_the_right_balance_in_negotiating_intellectual_property_in_army_contracting 19. Tactical Sustainment Risk Management for the Future Fight | Article | The United States Army, https://www.army.mil/article/261649/tactical_sustainment_risk_management_for_the_future_fight 20. Intellectual Property: A Critical Product Support Enabler for Readiness | www.dau.edu, https://www.dau.edu/library/damag/january-february2024/intellectual-property-critical-product-su 21. CDAO Announces Partnerships with Frontier AI Companies to Address National Security Mission Areas - Chief Digital and Artificial Intelligence Office, https://www.ai.mil/latest/news-press/pr-view/article/4242822/cdao-announces-partnerships-with-frontier-ai-companies-to-address-national-secu/ 22. Defence Software | Command and Control | Interoperability, https://systematic.com/int/industries/defence/ 23. How AI is Revolutionizing Defense Sustainment and Readiness - PTC, https://www.ptc.com/en/blogs/service/ai-revolutioning-defense-readiness 24. Predictive Logistics is the Way of the Future | Article | The United States Army, https://www.army.mil/article/282488/predictive_logistics_is_the_way_of_the_future 25. Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management - NIST Technical

Series Publications, https://nvlpubs.nist.gov/nistpubs/ir/2021/nist.ir.8286a.pdf 26. Cybersecurity Risk Quantification: How to Estimate the True Cost of a Breach, https://centricconsulting.com/blog/quantifying-cybersecurity-risk-true-cost-of-a-breach_cyber/ 27. Towards a New Supply Chain Cybersecurity Risk Analysis Technique - Sandia National Laboratories, https://www.sandia.gov/app/uploads/sites/273/2024/01/Towards-a-New-Supply-Chain-Cybersecurity-Risk-Analysis-Technique.pdf 28. Software Bill of Materials (SBOM) - CISA, https://www.cisa.gov/sbom 29. Software Bill of Materials Guidance for Government Contractors | Insights, https://www.gtlaw.com/en/insights/2025/10/software-bill-of-materials-guidance-for-government-contractors 30. Cybersecurity Supply Chain Risk Management (C-SCRM) Acquisition Guide - GSA, https://www.gsa.gov/system/files/C-SCRM%20Acquisition%20Guide%20April%202025%20508reviewed.pdf 31. Supply Chain Risk Management Framework - OUSD A&S, https://www.acq.osd.mil/asds/log/docs/DoD_SCRM_Framework_Report_Phase_I.pdf 32. Foreign Military Sales (FMS) Systems Acquisition Job Support Tool (JST) - DAU, https://www.dau.edu/sites/default/files/Migrated/ToolAttachments/JST-05%20FMS%20Sys%20Acq%20JST%20Guidebook%2008-01-22.pdf 33. Foreign Military Sales FAQ | Defense Security Cooperation Agency, https://www.dsca.mil/Resources/Foreign-Military-Sales-FAQ 34. Top 10 Tips in Drafting and Negotiating International Contracts | Thomson Reuters, https://legal.thomsonreuters.com/en/insights/articles/top-10-tips-in-drafting-and-negotiating-international-contracts 35. Negotiating an Agreement with a Foreign Representative, https://www.trade.gov/negotiating-agreement-foreign-representative 36. Russia, Belarus FMs vow to strengthen ties amid Eurasian security talks - Xinhua, https://english.news.cn/europe/20251029/2486132a918741509b0385cf6f536a52/c.html 37. Belarus and Russia have approved a military partnership program until 2030 - Belsat, https://en.belsat.eu/89499061/belarus-and-russia-have-approved-a-military-partnership-program-until-2030 38. Europe's dependence on US foreign military sales and what to do about it - Bruegel, https://www.bruegel.org/policy-brief/europes-dependence-us-foreign-military-sales-and-what-do-about-it 39. Capability Vignette: Increased Focus on Supply Chains and Critical Raw Materials, https://www.iiss.org/publications/strategic-dossiers/progress-and-shortfalls-in-europes-defence-an-assessment/capability-vignette-increased-focus-on-supply-chains-and-critical-raw-materials/ 40. Leonardo DRS and Chaiseri Defense Strengthen Partnership with New Battle Management System Contract to Support Royal Thai Army | Morningstar, https://www.morningstar.com/news/business-wire/20251113433063/leonardo-drs-and-chaiseri-defense-strengthen-partnership-with-new-battle-management-system-contract-to-support-royal-thai-army 41. Leonardo DRS (DRS) Wins Contract to Enhance Thai Army's Stryker Units - GuruFocus, https://www.gurufocus.com/news/3207943/leonardo-drs-drs-wins-contract-to-enhance-thai-army s-stryker-units 42. What is a Freight Management System (FMS): A Complete Guide | GoRamp, https://www.goramp.com/blog/what-is-a-freight-management-system 43. IT Hardware Procurement: Definition, Process, And Best Practices - InvGate's Blog, https://blog.invgate.com/hardware-procurement 44. Hardware Procurement 2024: Key Strategies - RedBeam, https://redbeam.com/blog/resources/hardware-procurement