Coastal Virginia

5115 Hampton Boulevard
Norfolk, Virginia 23529

COVA CCI Request for Proposals: Cybersecurity Research and Innovation FY 2022

RFP #: COVACCI-21-02

Project Title: A Real-Time Dependency Network Approach to Quantifying Risks and Ripple Effects from Cyberattacks in Shipbuilding and Repair Supply Networks

Project Abstract (no more than 250 words):

The evolution of defense shipbuilding supply networks toward digital environments increases operational complexity and requires reliable communication and coordination to regulate information exchange. As workers and suppliers transition to digital platforms, interconnection, information transparency, and decentralized decisions become prevalent. The appearance and extensive use of these digital platforms inexorably increase their exposure to cyberattacks. Unfortunately, the effects of a systematic cyberattack on one or more nodes belonging to the shipbuilding supply network (e.g., Colonial Pipeline) are unknown. This collectively may represent a substantial source of disruption. Cybersecurity protection of these networks requires a systemic approach to evaluate their vulnerability and understand ripple effects. However, current evaluation technologies and techniques are primarily applied to individual nodes or firms (if they are applied at all) and commonly lack systemic perspectives that consider overlapping risks and tiered hierarchies.

To overcome these limitations, we propose developing a cybersecurity supply network Artificial Intelligence (A.I.) framework that enables characterizing and monitoring shipbuilding supply networks and determining ripple effects from disruptions caused by cyberattacks. By representing and replicating the collective behavior of relevant shipbuilding supply network nodes, shipbuilders can monitor and measure the impact of cybersecurity disruptions and test the reconfiguration options that minimize the detrimental effects on the supply network. This framework extends a novel risk management framework developed by Diaz and Smith (2021) and Smith and Diaz (2021) that considers complex tiered networks and systemic hypervulnerabilities (COVA CCI - 2021ODU-06.005) and is currently tested in the port security cyber-physical setting.

Total Requested Amount: $150,000

Project Investigators:

PI Name	Institution	Department	Phone Number	Email
Rafael Diaz	ODU	VMASC	(757)9173045	rdiaz@odu.edu
H. Shen	UVA	Computer Science	(434)9248271	hs6ms@virginia.edu

1.1. Overview

As we advance into 2021, the ongoing COVID-19 public health crisis demands regions of the country attempt to organize an economic recovery under pandemic conditions. During this challenging economic recovery, the fact that suppliers serving the military-industrial base are still facing risks within the life cycle of the current pandemic and various cybersecurity threats creates a real possibility for disastrous consequences that may have far-reaching implications for our nation's readiness.

Achievement of growth in the naval fleet under ship acquisition plans and the National Defense Authorization Act requires new vessel construction and service life extensions at a level that necessitates the maritime industrial base to perform near-maximum capacity [1]. However, with current delays and the current public health crisis, global and domestic industrial capacity has been weakened [2, 3]. Although many shipyards and several suppliers have benefited from the COVID-19 economic recovery [4], any additional supply disruptions (e.g., cyberattacks) will only exacerbate backlogs and scheduling delays further. These threats extend into the future.

Cybersecurity is a significant concern to the U.S. Department of Defense [1, 5, 6]. Shipbuilders and suppliers handling any U.S. Government technical information must comply with DFARS cyber-security requirements cited in the Defense Federal Acquisition Regulation System (DFARS 252.204.7012 and 252.204-7020). However, this compliance only relates to 20-30% of materials used in a shipyard. The remaining 70-80% of the material and supplies used in shipbuilding originate in the commercial sector, which does not require compliance. Accordingly, Fairlead Inc., a Hampton Roads shipyard that supports this application, asserts that the impact of a cyber-attack on firms providing commercial supplies to shipyards is of significant interest to the industry. S.S.I. Inc., a digital shipbuilding firm that serves the U.S. National Shipbuilding and Research Program (NSRP), estimates a one-week delay caused by a disruption to a project’s critical path due to a late or incorrect component has an approximate cost impact of $50,000 per ship.

Cybersecurity threats to supply chains and industrial systems are growing exponentially due to the rapid rise in computing power [7]. As the incidence of remote working becomes predominant in new digital environments, workers, suppliers, and manufacturers become increasingly exposed to cyberattacks [8, 9]. Cyberattacks may further slow or halt shipbuilding and repair activities, generating shortages in labor and sparking cascading disruptions through supply chains [1]. Cyberattacks on critical industrial sectors related to shipbuilding suppliers are on the rise [10]. A cyberattack on the 5,500-mile pipeline system that carries about 45% of the fuel used on the East Coast (Colonial Pipeline) was perpetrated on May 7, 2021 [11]. This, and other disruptions, affect shipbuilders and suppliers differently, suggesting the necessity of an approach that rigorously quantifies the impact of cybersecurity breaches on shipbuilding supply networks. Ripple and bullwhip effects propagate backward and forward simultaneously throughout supply networks [12], negatively impacting suppliers as distortions become amplified [13]. These fluctuations are especially harmful to small and medium-sized businesses, constituting roughly 62% of active suppliers to the shipbuilding and repair sector (Newport News Shipbuilding [14]).

The evolution of shipbuilding supply networks toward digital environments increases operational complexity and requires reliable communication and coordination to regulate information exchange. As workers and suppliers transition to digital platforms, interconnection, information transparency, and decentralized decisions become prevalent [3, 15]. The appearance and extensive use of these digital platforms inexorably increase their exposure to cyberattacks. Unfortunately, the effects of a systematic cyberattack on one or more nodes belonging to the shipbuilding supply network (e.g., Colonial Pipeline [11]) are unknown. This collectively may represent a substantial source of disruption [16]. Cybersecurity protection of these networks requires a systemic approach to evaluate their vulnerability and understand ripple effects [12, 17, 18]. However, current evaluation technologies and techniques are primarily applied to individual nodes or firms (if they are applied at all) and commonly lack systemic perspectives [14] that consider overlapping risks and tiered hierarchies [19], as presented in Figure 1.

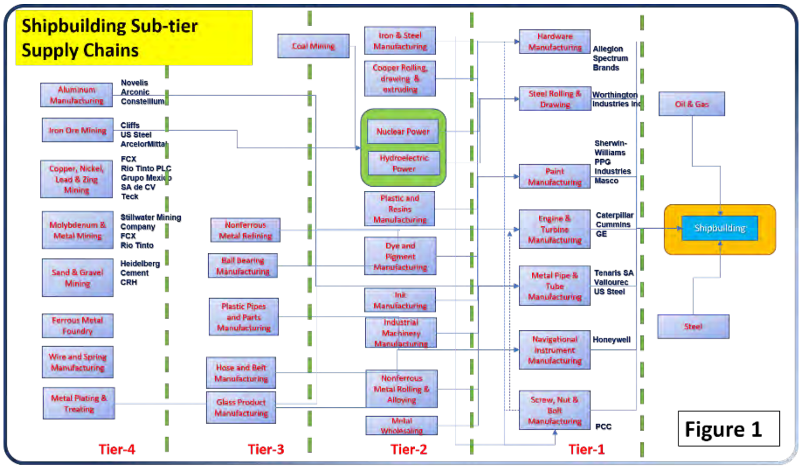

Shipbuilding Sub-tier Supply Chains
Aluminum Manufacturing
Novelis
Arconic
Constellium
Iron Ore Mining
Cliffs
US Steel
ArcelorMittal
Copper, Nickel, Lead & Zing Mining
FCX
Rio Tinto PLC
Grupo Mexico
SA de CV
Teck
Molybdenum & Metal Mining
Stillwater Mining Company
FCX
Rio Tinto
Sand & Gravel Mining
Heidelberg Cement
CRH
Ferrous Metal Foundry
Wire and Spring Manufacturing
Metal Plating & Treating
Nonferrous Metal Refining
Ball Bearing Manufacturing
Plastic Pipes and Parts Manufacturing
Hose and Belt Manufacturing
Glass Product Manufacturing
Coal Mining
Iron & Steel Manufacturing
Cooper Rolling, drawing & extruding
Nuclear Power
Hydroelectric Power
Plastic and Resins Manufacturing
Dye and Pigment Manufacturing
Ink Manufacturing
Industrial Machinery Manufacturing
Nonferrous Metal Rolling & Alloying
Metal Wholesaling
Hardware Manufacturing
Allegion
Spectrum Brands
Steel Rolling & Drawing
Worthington Industries Inc
Paint Manufacturing
Sherwin-Williams
PPG Industries
Masco
Engine & Turbine Manufacturing
Caterpillar
Cummins
GE
Metal Pipe & Tube Manufacturing
Tenaris SA
Vallourec
US Steel
Navigational Instrument Manufacturing
Honeywell
Screw, Nut & Bolt Manufacturing
PCC
Oil & Gas
Shipbuilding
Steel
Tier-4
Tier-3
Tier-2
Tier-1

Figure 1

Current tools fail to quantify ripple effects and subsequent delays in the defense shipbuilding sector [18]. We argue that without that knowledge is not possible to develop a timely understanding of the impacts of cybersecurity disruptions on schedules, adjust a response (e.g., reconfigure operations), and prevent significant losses. As trends in cyber-attacks suggest using intelligent actors to learn from systems vulnerabilities [20], short-term cyber-attacks on network supply chains may conceal more dire plans to disrupt long-term operational effectiveness, including supplying goods during periods of critical need [5].

To overcome these limitations, we propose developing a cybersecurity supply network Artificial Intelligence (A.I.) framework that enables characterizing shipbuilding supply networks and determining ripple effects from disruptions caused by cyberattacks to the supply network. By representing and replicating the collective behavior of relevant shipbuilding supply network nodes, shipbuilders can monitor and measure the effects of cybersecurity disruptions and test the reconfiguration options that minimize the detrimental impact on the supply network. It also enables the study of individual and simultaneous failure of one or more nodes and propagation effects across the network as a whole. This framework extends a novel risk management framework developed by Diaz and Smith [18] and Smith, Diaz [21] that considers complex tiered networks and systemic hypervulnerabilities (COVA CCI - 2021ODU-06.005) and is currently tested in the port security cyber-physical setting.

1.2. Broader Impacts

Shipbuilding and repair activities are essential at both local and national economic scales as the U.S. Navy expansion and growth are expected to continue. These activities coincide with a host of cybersecurity-related issues, one of which is the collective and systematic assessment of potential vulnerabilities and alternative recovery plans from cyberattacks. Since military shipbuilders share supply chains with other DoD branches, it is not surprising that its activities may impact broader defense and homeland security industrial bases. Although there has traditionally been an increased focus on introducing innovative technologies while producing and repairing ships, there has been less focus on supply chain risk resilience.

1.3. Objectives and Research Questions

This proposal is well-poised to contribute to the challenges posed in the R.F.P. In particular, this approach emphasizes potential risks resulting from the degradation of shipbuilding supply networks and answers the question, "how should shipbuilding supply networks be protected from the effects of cyberattacks?". Throughout this process, the approach recognizes that there remain feasibility and technical knowledge gaps. Thus, the research questions addressed are:

- How do cyberattacks become a hurdle creating delays that may frustrate the active acquisition of parts, components, and services schedules?
- How can planners explore and determine potential interventions (policies and practices) that may increase agility (e.g., portfolio reconfigurations) in aligning manufacturing and suppliers with forecasted schedules in the presence of a supply network cyberattack?
- How can artificial intelligence be used to build a data-driven decision support system that considers real-time, big data, and relevant dynamics of the shipbuilding and repair process?

1.4. Intellectual Merit

This research approach leverages knowledge from a multi-disciplinary and cross-trained team with a robust intellectual grounding in the areas of system engineering, computer science, cybersecurity, artificial intelligence, modeling & simulation, risk management, and supply chain networks. The results from this project will contribute to the body of knowledge in several domains, including systems engineering, cybersecurity, supply chain risk management, digital shipbuilding, homeland security, U.S. defense shipbuilding, and U.S. strategic studies. Results will enable identifying potential reconfiguration of shipbuilding schedules that reduce costs and delays in addition to discovering new bottlenecks that may inform shifts on critical paths to project management.

The research approach makes both theoretical and methodological contributions. On the theoretical side, our current understanding suggests vulnerable suppliers, including sub-tier suppliers, are subject to cyberattacks, and therefore must be protected. However, as suppliers embrace digital transformations, a myriad of additional systemic cyber-vulnerabilities and hyper-vulnerabilities may emerge. The effects of cyberattacks in the supply network may not be evident and require a network approach that detects vulnerable spaces while enabling actions that harden interconnected suppliers in place. On the methodological side, our approach advances the design and validation of capable cybersecurity frameworks that integrate data that encompass big data and real-time monitoring of different industrial sectors in the shipbuilding supply chain ecosystem. This investigation will extend current funded research in port cybersecurity (COVA CCI - 2021ODU-06.005) to the U.S. defense shipbuilding domain.

1.5. Technical Background

The definition of the intrinsic vulnerabilities of the systems entails undermining their security [22]. We employ a systemic perspective based on extensions to the Functional Dependency Network Analysis (FDNA) that considers: cyber threats [23], [24]; systems vulnerabilities [25],[26]; the risks associated with the cyber-attacks; security risks related to the loss of confidentiality, integrity, or availability (C.I.A. triad) of information [27]; and the countermeasures to deal with cybersecurity issues [26]. The cybersecurity evaluation framework proposed in this work seeks to extend Diaz, Smith, et al (2021) by examining emergent behavior and vulnerabilities to enable assessment of effects of cybersecurity breaches on suppliers. The new method, Adaptive Risk Network Dependency Analysis (ARNDA), is an extension of the so-called Systems Operational Dependency Analysis (SODA) [28], which improves FDNA [29, 30] by enabling partial dependency analyses, progressive absorption, tiered structures, and embedding risk profiles. Both FDNA and SODA fail to consider hierarchies such as those observed in the shipbuilding multi-tier supply network and the simultaneous propagation effects that may lead to hyper-vulnerability. Hierarchical structures and hyper-vulnerable dependencies [31] are two critical components prevalent in supply networks [17, 18]. Figure 2 presents a hypothetical supply network for a watertight door on a naval vessel. Figures 2(a)-(d) show a high-level modeling process in which nodes (suppliers) are identified, connected, analyzed, and scored.

Our method allows for combining a probabilistic, graphical, real-time Bayesian Network, with functional dependencies leading to lower computational costs and integration of parameters with intuitive meaning to tiered

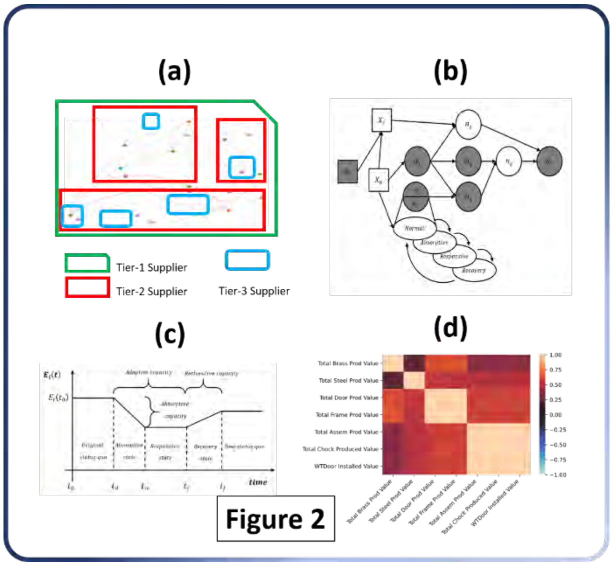


Figure 2

suppliers [32]. The extension will model risk events, embed node risk profiles, interdependencies, and determine ripple effects. Thus, stakeholders can prioritize investments [17] and analyze supplier reconfigurations that minimize the cyberattack disruptions via optimization.

2. RESEARCH PLAN

2.1. Premise

The premise of the investments in the defense shipbuilding and repair supply networks towards supply chain digitalization will increase efficiencies and agility and create positive operational and environmental impacts. Although highly fragmented, collectively, these investments are significant, and the premise of resilience while maintaining the integrity of the supply network should be assessed in real-time by a systematic tool.

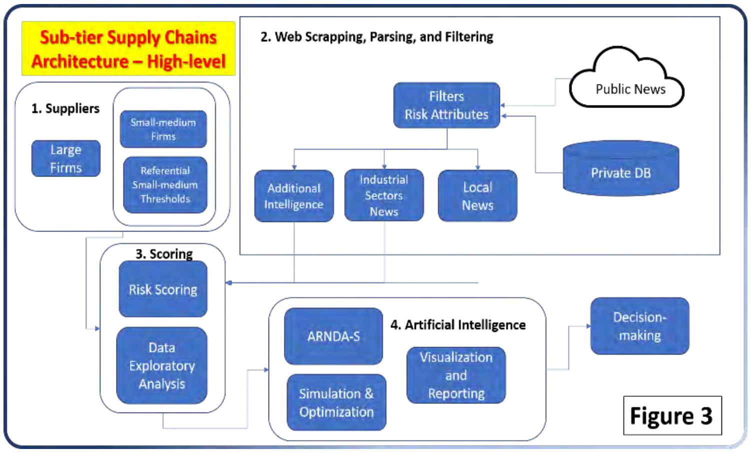

Sub-tier Supply Chains Architecture – High-level
2. Web Scrapping, Parsing, and Filtering
Public News
Filters
Risk Attributes
Private DB
Additional Intelligence
Industrial Sectors News
Local News
1. Suppliers
Large Firms
Small-medium Firms
Referential Small-medium Thresholds
3. Scoring
Risk Scoring
Data Exploratory Analysis
4. Artificial Intelligence
ARNDA-S
Visualization and Reporting
Simulation & Optimization
Decision-making

Figure 3

This proposal aims at extending and applying a new risk management framework (ARNDA) and build a testable prototype to perform a cybersecurity assessment of the supply network connected to the defense shipbuilding supply chain (ARNDA-S). The framework considers the systematic examination of strategic sectors of the defense shipbuilding industry to monitor disruptions in real-time, determine ripple effects and enhance the ability of the supply portfolio to recover from node failures in the presence of a cyberattack. The framework will identify hypervulnerable nodes, determine propagation effects, generate data to predict potential supply failures, suggest portfolio reconfigurations, and confirm the adequacy of such measures after implementation [33]. Figure 3 presents the high-level architecture of the framework.

2.2. Framework Development

A four-phase "Framework Development and Testing Process" (FD&TP) methodology is designed and followed to model and assess the shipbuilding supply network ecosystem (Figure 4).

I. Data & Outreach

In the first phase, relevant use cases in the shipbuilding ecosystem data are elicited. Model scenarios and related environments are characterized, as well.

<u>Goal 1.1</u> *Supply network mapping.* Critical suppliers and sub-tier suppliers are identified guided by Fairlead. Supply network mapping is performed by identifying and connecting firms to relevant processes and eliciting attributes to predict performance.

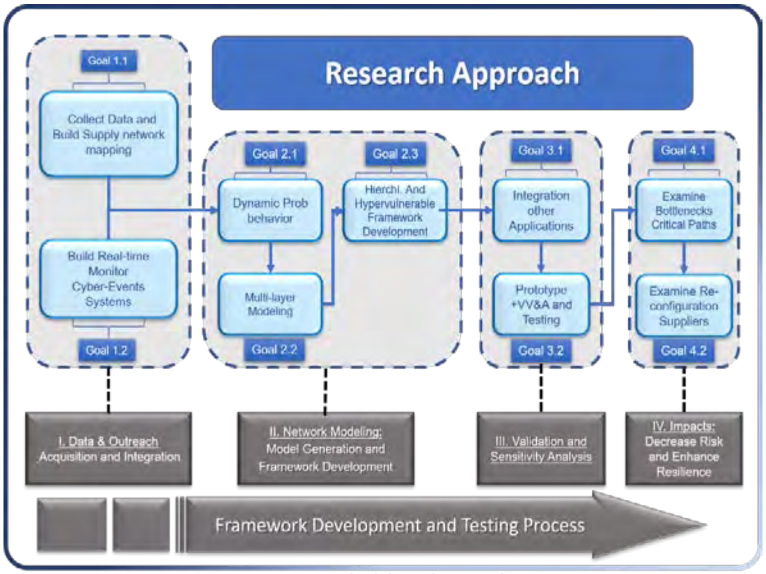

Research Approach
Goal 1.1
Collect Data and Build Supply network mapping
Build Real-time Monitor Cyber-Events Systems
Goal 1.2
Goal 2.1
Goal 2.3
Dynamic Prob behavior
Hierchl. And Hypervulnerable Framework Development
Multi-layer Modeling
Goal 2.2
Goal 3.1
Integration other Applications
Prototype +VV&A and Testing
Goal 3.2
Goal 4.1
Examine Bottlenecks Critical Paths
Examine Re-configuration Suppliers
Goal 4.2
I. Data & Outreach Acquisition and Integration
II. Network Modeling: Model Generation and Framework Development
III. Validation and Sensitivity Analysis
IV. Impacts: Decrease Risk and Enhance Resilience
Framework Development and Testing Process

Figure 4 – Methodological approach

<u>Goal 1.2.</u> *Monitor supply network Cybersecurity*. We use Natural Language Processing (N.L.P.) and webscraping to monitor and extract information by a parser relative to key events (e.g., cybersecurity breaches) that affect industrial sectors and suppliers. Relationships and hierarchies among suppliers and sub-tier suppliers are confirmed and organized as a graph that scores stochastic elicited information dynamically.

II. *Model Generation*

In this modeling environment, the ARNDA framework is extended to ARNDA-S.

Goal 2.1. *Dynamics Probabilistic Behavior*. The risk space will be defined along with the model network and methods for learning model parameters.

Goal 2.2. *Multilayer Modeling*. Methodology for defining the network as a group of network layers developed assigning properties to nodes, and equations for network propagation are developed.

Goal 2.3. V&V *Model Hierarchies and Hyper-vulnerabilities*. The hierarchical network and the risk dimensions will be brought together by defining the dependent relationships between entities in the risk space, i.e., risks and nodes in the hierarchical network.

III. Assessment

The goal of this stage is to replicate the ARNDA-S framework to examine graph disruptions. It includes performing sensitivity analyses for model verification and validation (V&V). This stage aims to assess the new real-time data-driven prototype.

Goal 3.1 *Integration.* Using a composite scheme that combines information of suppliers' cybersecurity delays/disruption risks to integrate and process data flows with scheduling.

Goal 3.2 *Testing*. Execute ARNDA-S model and stress it to test cybersecurity disruptions and identify security deficiencies. Since the model is connected to shipbuilding schedules, variations in suppliers' performance are quantified as they propagate through the suppliers' network. Impacts are further evaluated in terms of degradation of production rate, increasing maintenance efforts, and delays in fulfilling demand. Short and long-term impacts are assessed using [5].

IV. Impacts

The impact of ARNDA-S is evaluated with programs used for capacity planning and execution to enhance resource assignment and visibility.

Goal 4.1 *Examine expected bottlenecks and shifting critical paths.* Opportunities for mitigative actions and optimization of suppliers' portfolios are identified.

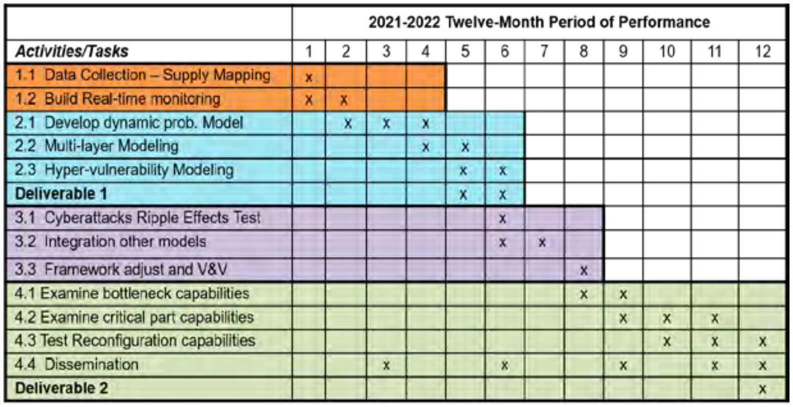
Goal 4.2 *Explore the collective impact and reconfigurations.* These tasks consider model refinement by deploying: 1) Conceptual Modeling, 2) Solution (countermeasures) elicitation and testing. 3) Results, analysis, and sensitivity analysis. 4) Model generalization.

2.3. Dissemination and Deliverables

The data analysis and reporting will be delivered to State policymakers, port planners, and the regional planning agencies through scheduled meetings (Section 2.4). Group sessions are planned to receive and incorporate feedback before full release. The draft of at least one peer-reviewed journal article will be made within the project's performance period. Deliverables are 1. Conceptual real-time cyber-risk monitoring supply network ripple effects model (ARNDA-S) 2. Model V&V performed ARNDA supply chain reconfiguration capabilities to cyber-attacks.

2.4. Tasks and Timeline

The project's research, deliverables, and dissemination activities are organized into four general sections of FD&TP, as illustrated in Figure 5. The project begins with supply mapping and monitoring (1). followed by network modeling, parameter design, prototyping, and hyper-vulnerability modeling (2). V&V activities and extensive testing are then performed (3). The final phase is reconfiguration as a response to cybersecurity breaches in the supply network.



	2021-2022 Twelve-Month Period of Performance											
Activities/Tasks	1	2	3	4	5	6	7	8	9	10	11	12
1.1 Data Collection – Supply Mapping	x											
1.2 Build Real-time monitoring	x	x										
2.1 Develop dynamic prob. Model		x	x	x								
2.2 Multi-layer Modeling				x	x							
2.3 Hyper-vulnerability Modeling					x	x						
Deliverable 1					x	x						
3.1 Cyberattacks Ripple Effects Test						x						
3.2 Integration other models						x	x					
3.3 Framework adjust and V&V								x				
4.1 Examine bottleneck capabilities								x	x			
4.2 Examine critical part capabilities									x	x	x	
4.3 Test Reconfiguration capabilities										x	x	x
4.4 Dissemination			x			x			x		x	x
Deliverable 2												x

Figure 5 – Timeline and Deliverables

2.5. Project Team

Expertise is drawn from computer engineering, mathematics, artificial intelligence, and modeling and simulation. The team has a track record of collaboration in data gathering, building and validating frameworks, and designing scaled prototypes to test and assess cyber-intrusions. Dr. Diaz (M&S Engineering) is an expert in supply chain risk simulation, neural networks, systems modeling; Dr. Shen (Computer Engineering) is an expert in cybersecurity design and testing; Dr. Behr (VMASC) is an expert in social sciences; Katie Smith (Mathematics) is an expert in network modeling and System-of-Systems methodologies.

3. IMPACT ON THE COMMONWEALTH

The cases discussed in [10] and the recent cyber-attack to Colonial Pipeline[11] demonstrate that beyond attacks to a component or individual system, there is a need to understand the systemic perspective of the cybersecurity layer of shipbuilding supply networks.

The anticipated benefits from State and U.S. Defense sector investments are characterized as general in support of sustainability and resiliency goals. Since the nature of shipbuilding supply networks and data flow are heterogeneous with many dynamic interactions, they often move through supply chain ecosystems, each with its own level of exposure as the entire industry moves towards supply chain digitalization. We seek to model these processes, quantify the expected system's vulnerability, and create a testbed that allows examination and optimization of response to a cyberattack that jeopardizes shipbuilding and repair schedules.

3.1. Workforce Development in the Commonwealth

Old Dominion University has been recognized as the first University to offer cybersecurity instruction at both undergraduate and graduate levels [34]. The developed framework will be employed for O.D.U. activities for Graduate Certificate students in ENMA 625, Introduction to Homeland Security [35], and Graduate and undergraduate Cybersecurity students [36]. Likewise, it will be used for a graduate course, "CS 6501: Cloud Computing" and undergraduate Capstone course in the Computer Science Department at the University of Virginia (UVA). Through student training, this project will develop a workforce able to undertake cybersecurity issues in this sector.

3.2. Commercialization and Economic Development

This proposal has been endorsed by Fairlead Inc, S.S.I., and MIBE (attached). A cybersecurity evaluation framework focusing on supply network disruptions and agility is unique. The need for such a platform is apparent in nearly every shipbuilding community throughout the United States. Further, the additional functionality of the platform to allow reconfiguration of assets after a cyberattack is also unique. As these communities pursue the concept and practice of building resilience, the need to stand up a cybersecurity platform is attractive.

One of the applicants of this proposal has been conducting an N.S.F. Partnerships for Innovation (PFI) project for research product commercialization in collaboration with I.B.M., Microsoft, and Brain of Things Caspar company (which provides AI-IoT service). During the project, we will partner with our industry collaborators, identify technologies with greater market potential, and try to bridge the funding gap to commercialization. We will work with the Licensing & Ventures Group (L.V.G.) at UVA and O.D.U.

4. PLAN FOR COLLABORATION

We seek to provide a much-needed systemic framework that produces recommendations to our State and Defense sectors that may assist in managing cybersecurity issues, crafting a robust cybersecurity strategy and support of executive decisions relative to cybersecurity systems.

The applicants plan to leverage the research stated in this proposal to seek additional supporting funds to N.S.F., O.N.R., and D.O.D. Applications of this framework will be tested in shipbuilding environments. Research from the development of this novel system framework will be published in top journals. Inter-institutional coursework domains will be explored.

References

1. DoD, U., *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States. Report to President Donald J. Trump by the Interagency Task in Fulfillment of Executive Order 13806. Office of the Under Secretary of Defense for Acquisition and Sustainment, Office of the Deputy Assistant Secretary of Defense for Industrial Policy, September 2018*. 2018.

2. Wu, D. and T. Mochizuki. *Why Shortages of a $1 Chip Sparked Crisis in Global Economy*. Bloomberg 2021 [cited 2021 5/5/2021]; Available from: https://www.msn.com/en-us/money/other/why-shortages-of-a-1-chip-sparked-crisis-in-global-economy/ar-BB1fkxEy?ocid=entnewsntp.

3. Hermann, M., T. Pentek, and B. Otto. *Design principles for industrie 4.0 scenarios*. in *2016 49th Hawaii international conference on system sciences (HICSS)*. 2016. IEEE.

4. Eckstein, M. *Austal USA Expanding to Make Steel Ships*. 2021 [cited 5/1/2021; Available from: https://news.usni.org/2021/03/29/austal-usa-expanding-to-make-steel-ships-yard-looks-to-bid-on-coast-guard-offshore-patrol-cutter-navy-light-amphib-programs.

5. Lamberty, J.M., *Short Term Cyber Attacks with Long Term Effects and Degradation of Supply Chain Capability*. 2016, Naval Postgraduate School Monterey United States.

6. Officer, O.o.t.D.C.I., *DOD INSTRUCTION 5000.82 - ACQUISITION OF INFORMATION TECHNOLOGY (IT)*. 2020.

7. McGrath, J. *Protecting supply chains and industrial control systems from cyber attacks* 2021 14-04-2021]; Available from: https://www.intelligentinsurer.com/contributed-article/protecting-supply-chains-and-industrial-control-systems-from-cyber-attacks.

8. Truran, C. *Remote Working: The New Security Perimeter*. 2021 [cited 2021 5/5/2021]; Available from: https://www.infosecurity-magazine.com/opinions/remote-working-new-security/.

9. Jones, A. *Surge in cyber attacks leads to 'massive cost' for manufacturers – report*. 2021 [cited 2021 5/5/2021]; Available from: https://uk.news.yahoo.com/surge-cyber-attacks-leads-massive-230100033.html.

10. Khan, S. and A. Perez, *Eventwatch - Annual report.* 2019 p. 10.

11. Watson, B. and B. Penistone. *Ransomware shuts US pipeline*. 2021 [cited 2021 5/10/2021]; Available from: https://www.defenseone.com/threats/2021/05/the-d-brief-may-10-2021/173905/.

12. Li, Y., et al., *Ripple effect in the supply chain network: Forward and backward disruption propagation, network health and firm vulnerability.* European Journal of Operational Research, 2021. **291**(3): p. 1117-1131.

13. Stevenson, W.J., *Operations management*. Eleventh ed. 2012: McGraw-Hill / Irwin

14. Humphrey, K. and Q. Williams. *Strategic Sourcing Supplier Development - Forward Grow The Business Base*. 2018 [cited 2021 6/5/2021]; Available from: https://supplier.huntingtoningalls.com/sourcing/docs/Supplier_Training/Supplier_conference_SD_and_STAV.pdf.

15. Bücker, I., et al. *Towards a methodology for Industrie 4.0 transformation*. in *International conference on business information systems*. 2016. Springer.

16. Diaz, R., et al., *Developing an Artificial Intelligence Framework to Assess Shipbuilding and Repair Sub-Tier Supply Chains Risk* in *International Conference on Industry 4.0 and Smart Manufacturing*. 2020.

17. Diaz, R., et al., *Developing an Artificial Intelligence Framework to Assess Shipbuilding and Repair Sub-Tier Supply Chains Risk.* Procedia Computer Science, 2021. **180**: p. 996-1002.

18. Diaz, R. and K. Smith, *An Artificial Intelligence Approach to Assess Shipbuilding and Repair Supply Networks*, in *Production and Operations Management, Annual Conference 2021*. 2021.

19. Cook, D., *US INDUSTRY (NAICS) REPORT 33661a - Ship Building in the US*. 2020, IBIS Wolrd.

20. Blum, W. and M.D.R. Team. *Applying reinforcement learning to security*. 2021; Available from: https://www.microsoft.com/security/blog/2021/04/08/gamifying-machine-learning-for-stronger-security-and-ai-models/.

21. Smith, K., et al., *Conceptual Development of a Probabilistic Graphical Framework for Assessing Port Resilience* in *23rd International Conference on Harbor, Maritime and Multimodal Logistic Modeling & Simulation*. 2021: Poland.

22. Lezzi, M., M. Lazoi, and A. Corallo, *Cybersecurity for Industry 4.0 in the current literature: A reference framework.* Computers in Industry, 2018. **103**: p. 97-110.

23. Khalid, A., et al., *Security framework for industrial collaborative robotic cyber-physical systems.* Computers in Industry, 2018. **97**: p. 132-145.

24. Flatt, H., et al. *Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements*. in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*. 2016. IEEE.

25. Jansen, C. and S. Jeschke, *Mitigating risks of digitalization through managed industrial security services.* AI & SOCIETY, 2018. **33**(2): p. 163-173.

26. Kissel, R., *Glossary of key information security terms*. 2011: Diane Publishing.

27. Jansen, C., *Stabilizing the industrial system: Managed security services' contribution to cyber-peace.* IFAC-PapersOnLine, 2017. **50**(1): p. 5155-5160.

28. Guariniello, C. and D. DeLaurentis, *Supporting design via the system operational dependency analysis methodology.* Research in Engineering Design, 2017. **28**(1): p. 53-69.

29. Garvey, P.R. and C.A. Pinto. *Introduction to functional dependency network analysis*. in *The MITRE Corporation and Old Dominion, Second International Symposium on Engineering Systems, MIT, Cambridge, Massachusetts*. 2009.

30. Servi, L. and P.R. Garvey, *Deriving global criticality conditions from local dependencies using Functional Dependency Network Analysis (FDNA).* Systems Engineering, 2017. **20**(4): p. 297-306.

31. Wang, Y.I., J. Li, and R. Anupindi, *Risky suppliers or risky supply chains? An empirical analysis of sub-tier supply network structure on firm performance in the high-tech sector.* 2015.

32. Guariniello, C. and D. DeLaurentis, *Supporting design via the System Operational Dependency Analysis methodology.* Research in Engineering Design, 2017. **28**: p. 53-69.

33. Elder, R., *Defending and operating in a contested cyber domain,".* Air Force Scientific Advisory Board, Winter Plenary, 2008.

34. Wavy. *ODU to open School of Cybersecurity, first of its kind in the nation* 2020 10-1-2020]; Available from: https://www.wavy.com/news/local-news/norfolk/odu-school-of-cybersecurity-to-open-october-1/.

35. ODU. *Homeland Security Online*. 2020; Available from: https://online.odu.edu/programs/homeland-security-certificate.

36. ODU. *Cyber Systems Security Online*. 2020 10-1-2020]; Available from: https://online.odu.edu/programs/cyber-systems-security-advanced-certificate.

Project Budget Worksheet

I. Proposal Information

a. Sponsor Name:	COVA CCI/ODU
b. RFP Name:	Cybersecurity Research and Innovation Funding FY 2022
RFP Number:	COVACCI-21-02
c. Sponsor Deadline:	05/15/2021
d. Project Name:	A Real-Time Dependency Network Approach to Quantifying Risks and Ripple Effects from Cyberattacks in Shipbuildling and Repair Sup
e. Overall PI Name/Institution:	Dr. Rafael Diaz, ODU
f. Institutional PI/Co-PI Name/Institution:	Ms. Katie Smith, ODU; Dr. Joshua Behr, ODU; Dr. Haiying Shen, UVA
g. Project Start Date:	07/01/2021
h. Project End Date:	06/30/2022
i. Total Project Budget: Auto calculates from costs identified below.	150000

II. Labor Costs

a. Faculty: List total cost for all faculty supporting the project by academic institution. Include salary based on level of effort for each faculty.

Institution	Total Salary
ODU	9975
UVA	8472
Total	$ 18447

b. Support Staff / Post-Docs / Research Scientists / Lab Managers / Hourly

List total cost for all support staff, etc., supporting the project by academic institution. Include salary and fringe benefit based on level of effort for each faculty. Each institution has their own fringe rate and this rate will be used in calculating total fringe.

Institution	Total Salary
ODU	60000
UVA	0
Total	$ 60000

c. Graduate Research Assistants (GRAs)

List total cost for graduate research assistances by institution.

Institution	Total
ODU	0
UVA	17246
Total	$ 17246

Include tuition in budget? (Select Yes or No) [✓ Yes] No

d. Fringe Benefits: Include fringe benefit based on level of effort for each faculty and staff. Each institution has their own fringe rate and this rate will be used in calculating total fringe. ODU Fringe rate for CCI funded projects is 23.25% + 12,000

Calculations: Annual Salary x Fringe Rate (.2325 + 12000) x % of effort = Total Fringe

Institution	Total
ODU	30025
UVA	2347
Total	$ 32372

III. Other Direct Costs

Use the table below to plan other expenses are needed to accomplish the project. Include institution receiving funding in the description along with a brief description of the item requested.

Category/Description	**Total Budget**
a. **Equipment**	
	0
b. **Materials & Supplies**	
UVA	1365
c. **Travel**	
UVA	4500
d. **Subcontract & Consultant**	
	0
e. **Other Expenses**	
UVA - GRA tuition, health subsidy; publications; CS Dept facility fee	16070
Total Other Direct Costs	$ 21935

IV. Subcontractors / Consultants

If you will need any subcontractors or consultants for your project, please provide the following information.

Company Name:	Contact Name/e-mail:

V. Budget Summary

Include a budget summary showing total costs by category as calculated above. All cells in this table will auto calculate.

Category	**Amount**
II. Labor Costs	
a. Faculty	$ 18447
b. Support Staff	$ 60000
c. Graduate Research Assistants	$ 17246
d. Fringe Benefits	$ 32372
Total Labor Costs	**$** 128065
III. Other Direct Costs	
a. Equipment	$ 0
b. Materials & Supplies	$ 1365
c. Travel	$ 4500
d. Subcontract/Consultant	$ 0
e. Other Expenses	$ 16070
Total Other Direct Costs	**$** 21935
Total Budget	**$** 150000

VI. Indirect Costs or Facilities & Administrative (F&A) Costs

CCI funds CAN NOT be used for indirect costs or facilities and administration costs. Nodes may offer unrecovered F&A as the basis for matching funds, separately calculated for each of the four broad categories: Research, Regional Innovation Ecosystem, Talent Pipeline, and Operations .

Indirect costs or F&A costs are real expenses that cannot be readily identified with certain activities. Examples include library costs, utility costs, costs to operate and maintain buildings and grounds, and costs of administering sponsored projects. Indirect costs are determined by each institution and these rates will be used to calculate total IDC for the project. The IDC rate is applied to the total direct costs of the budget minus individual equipment costing $5,000 or more; subcontract costs in excess of $25,000; graduate student tuition; rental costs; and participant support costs.

Current IDC rate for Norfolk State
Current IDC rate for Old Dominion University
Current IDC rate for William & Mary

VII. Matching Funds/Cost Sharing

Does the RFP or solicitation require matching [✓ YES]
NO

Include indirect costs as part of the Matching Funds/Cost Sharing.
Identify Funding Source for match.

Category/Funding Source	Amount
Cash Match	
IDC/F&A costs	113353
Faculty Release Time	
Federal Grant	36647
Other	
Other	
Other	
Total	**$** 150000

IX. Contact Information

Send this form to jcostanz@odu.edu

Old Dominion University Research Foundation
BUDGET JUSTIFICATION OF COST DETAIL

SALARIES & WAGES

Principal Investigator

Faculty salary for the Principal Investigator, Dr. Rafael Diaz, is based on a 12-month performance period. Amounts charged are calculated as follows: salary/12 = rate per month. Rate per month x number of months in semester x percent effort in semester = charge per period. Dr. Diaz's salary at the start of this project will be $147,000, and the PI will devote approximately 0.4 month of effort to this project.

Co-Principal Investigators

Faculty salary for the Co-Principal Investigator, Ms. Katie Smith, is based on a 12-month performance period. Amounts charged are calculated as follows: salary/12 = rate per month. Rate per month x number of months in semester x percent effort in semester = charge per period. Ms. Smith's salary at the start of this project will be $102,743, and the Co-PI will devote approximately 0.55 month of effort to this project.

Faculty salary for the Co-Principal Investigator, Dr. Joshua Behr, is based on a 12-month performance period. Amounts charged are calculated as follows: salary/12 = rate per month. Rate per month x number of months in semester x percent effort in semester = charge per period. Dr. Behr's salary at the start of this project will be $169,373, and the Co-PI will devote approximately 0.03 month of effort to this project.

Project Scientist

We are requesting funding for 12 months of effort for a Project Scientist based on a 12-month performance period. Amounts charged per project period were calculated as follows: salary/12 = rate per month. Rate per month x number of months in period x percent effort in period = charge per period. The Project Scientist's salary is budgeted at $60,000.

FRINGE BENEFITS (ONR negotiated rate dated June 30, 2020)

Principal Investigator and Co-Principal Investigators

The fringe benefit rate applicable to university faculty salaries is 40.3% of the salary attributable to this project. This rate includes the university's contribution to the Virginia Supplemental Retirement System, FICA, health, life and disability insurance premiums, worker's compensation, unemployment insurance premiums, annual leave, and sick leave.

Project Scientist

FICA (6.2% & 1.45%), unemployment insurance (1% of 1st $8,000 of calendar year), worker's compensation (0.435%), health (actual), dental (actual), life (0.233%) and disability insurance premiums (0.43%), and annual (6%) and sick leave (2%) premiums have been budgeted for this position in accordance with current Old Dominion University Research Foundation policies. Benefits for Annual Leave (6%), Sick leave (2%), and tuition reimbursement (.5%) are also included.

OTHER DIRECT COSTS

Subcontract

We have requested funding in the amount of $50,000 to enter into a contractual agreement with University of Virginia to develop a system for identifying disruptions in real-time based on identified attributes. Specifically, UVA will build a machine learning model that takes the identified attributes as inputs and outputs the disruptions. The machine learning model will be trained using the datasets collected in this project. UVA will conduct trace-driven experiments for the disruption identification and evaluate the performance of the system in terms of identifying accuracy, real-time performance and so on.

INDIRECT COSTS

Our ONR negotiated rate dated May 8, 2018 authorizes an on-campus indirect cost rate of 55% of modified total direct costs (MTDC) effective July 1, 2018 through June 30, 2021. Cognizant Contact: Linda B. Shipp, 703-696-8559, linda.shipp@navy.mil. However, per CCI policies, IDC has been waived for this project.

COST SHARE

SALARIES & WAGES

Principal Investigator

Faculty salary for the Principal Investigator, Dr. Rafael Diaz, is based on a 12-month performance period. Amounts charged are calculated as follows: salary/12 = rate per month. Rate per month x number of months in semester x percent effort in semester = charge per period. Dr. Diaz's salary at the start of this project will be $147,000, and the PI will contribute approximately 0.66 month of effort to this project.

FRINGE BENEFITS (ONR negotiated rate dated June 30, 2020)

Principal Investigator

The fringe benefit rate applicable to university faculty salaries is 40.3% of the salary attributable to this project. This rate includes the university's contribution to the Virginia Supplemental Retirement System, FICA, health, life and disability insurance premiums, worker's compensation, unemployment insurance premiums, annual leave, and sick leave.

UNRECOVERABLE INDIRECT COSTS

Our ONR negotiated rate dated May 8, 2018 authorizes an on-campus indirect cost rate of 55% of modified total direct costs (MTDC) effective July 1, 2018 through June 30, 2021. Cognizant Contact: Linda B. Shipp, 703-696-8559, linda.shipp@navy.mil.

CCI DIRECT COSTS = $150,000
MTDC = $150,000
CCI INDIRECT COSTS = $0
TOTAL CCI COSTS = $150,000

MATCHING DIRECT COSTS ODU = $11,290
MATCHING DIRECT COSTS UVA = $25,357
UNRECOVERABLE IDC ODU = $88,710
UNRECOVERABLE IDC UVA = $24,643
TOTAL MATCHING FUNDS = $150,000

Budget Justification - UVA

Personnel - Dr. Haiying “Helen” Shen, PI, (CY@$197,400 plus increases) will contribute 0.50 calendar months during this twelve month project.

Graduate Research Assistants (GRAs) and Undergraduate Research Assistants (URAs) - Costs are estimated based on the minimum and maximum payments for the academic year established by the University Office of the Vice-President and Provost. All compensation in SEAS proposals are within these guidelines. Per UVa policy, GRAs and URAs are limited in the number of hours they can work while taking classes, therefore to calculate hourly rates conversions are made by applying 1056 (GRA) and 840 (URA) hours per calendar year. The support provided for GRAs also includes tuition and health insurance shown below as Other costs. Salary is requested for part time GRA, (CY@$33,488 plus increases) to devote 6.0 calendar months over the course of this twelve month period of performance.

Salary Increases - Salary increases of 3% per year (calculated effective July 1st) are from the University's Multi-Year Financial Plan used by the Board of Visitors and administration to guide the University of Virginia in long-term financial planning. The plan is also submitted to the State of Virginia. The projected rate for salary increases is based on available competitive salary surveys with other institutions.

Fringe Benefits - The University of Virginia's fringe benefits rates as they apply to sponsored programs are as follows: 27.7% for faculty, research staff, postdoctoral fellows, 37.4% for classified staff, university staff and professional staff, 6.5% for hourly staff, temporary employees and wage employees. Fringe Benefits can include: FICA/Medicare, Retirement, Disability Insurance, Life Insurance, TIAA/CREF, Workers’ Compensation, Unemployment Insurance and Health Insurance.

Travel - Trips to related technical conferences, workshops, seminars, etc. Trips to sponsor for technical discussions and presentation of results. $4,500 has been budgeted.

Materials and Supplies - Laboratory supplies for specific use in the research project Laboratory supplies for specific use in the research project including networking equipment components, hard disk, updating software, books, AWS credits for conducting experiments and etc. Does not include office or other general purpose supplies. $1,365 has been budgeted.

Departmental Computer Facilities Fees - Departmental Computer Facilities Fees - Departmental Computer Service Fees: the Computer Science department operates an extensive computing facility in support of its research activities. There are ~200 multicore compute servers, with ~3200 total cores. Approximately half of the servers contain from 1 to 8 GPU accelerators. These servers are available through infrastructure-as-a-service and software-as-a-service interfaces. Research software (e.g., R, SAS, SPSS, MATLAB, Simics) is available for interactive use on research workstations and for high-throughput use on load balanced clusters. Research storage provides ~1PB of RAID total storage with offsite backup. Departmental computing is connected via switched gigabit or 10 gigabit Ethernet, with some Infiniband connectivity within clusters. The facility also provides permanent staff to support specialized programming, specialized database and web services, use of local and remote high-performance computing facilities, and setup/maintenance for custom hardware/OS/network/software infrastructure for sponsored research. Rates are established annually by the managing unit and approved by the University Office of the Comptroller in compliance with OMB rules governing cost-recovery centers. Rate calculations consist of personnel, equipment depreciation, supplies and materials, and profit/(loss). The current computing service rate for faculty and staff is $2.60 per hour (173.33 hrs. per month x $2.60/hr. = $450/month) and for Graduate Students it is $225/month (86.67 hrs. per month x $2.60/hr.). Rates are applied equally to all users of the Research Facility. For Dr. Shen this equates to $2.60/hr. x 86.67 hours = $225; GRA = $225/month x 6 months = $1,350.

Publications - $3,000 has been budgeted toward publications and page charges in related technical journals.

Other –

a. Tuition Remission - Effective September 1, 1990, it is the policy of the University of Virginia to provide tuition for graduate research assistants as partial compensation for services. Year one = $9,930.

b. Graduate Research Assistant Health Insurance – Effective July 1, 2005, it is the policy of the University of Virginia to provide health insurance for graduate research assistants as partial compensation for services. Health insurance is increased 5% each year to cover future rate increases. Year one = $1,565.

Facilities and Administrative (F&A) (Indirect/Overhead) Costs - The University of Virginia's negotiated (Modified Total Direct Costs (MTDC) F&A rates with DHHS, per agreement of January 29, 2021, is 61.5% "on campus", 26% "off-campus", and 38% for Other Sponsored Activities. (Note: The MTDC base consists of total direct costs less equipment, capital expenditures, charges for patient care, rental costs, tuition remission, scholarships and fellowships, participant support costs and the portion of each subaward in excess of $25,000. Includes F&A on the first $25,000 of subcontracts. **Indirect costs (IDC) are NOT eligible costs in the proposals submitted in response to this RFP, unrecovered IDC can be used to fulfill this contribution requirement.**

https://sponsoredprograms.virginia.edu/sites/sponsoredprograms.virginia.edu/files/UVA.RA.FY2022.pdf

The University defines Fiscal Year as July 1 through June 30.

NAME: : Rafael Diaz

POSITION TITLE & INSTITUTION: Associate Research Professor, Old Dominion University

A. PROFESSIONAL PREPARATION
(see PAPPG Chapter II.C.2.f.(i)(a))

INSTITUTION	LOCATION	MAJOR/AREA OF STUDY	DEGREE (if applicable)	YEAR (YYYY)
Jose Ma Vargas Univ.	Caracas	Management	BSIE	1994
Old Dominion Univ.	Norfolk	Finance and IT	MBA	2002
Old Dominion Univ.	Norfolk	Modeling and Simulation	PhD	2007

B. APPOINTMENTS
(see PAPPG Chapter II.C.2.f.(i)(b))

From - To	Position Title, Organization and Location
2019-Present	Associate Research Professor, Virginia Modeling, Analysis and Simulation Center, Old Dominion University (ODU), Suffolk, VA
2019-Present	Co-Director, Advanced Analytics Laboratory (AAL), Virginia Modeling, Analysis, and Simulation Center, Old Dominion University, Suffolk, VA
2015-2020	Research Affiliated, Massachusetts Institute of Technology (MIT), MIT Center for Transportation & Logistics, Cambridge, MA
2015-2020	Professor Supply Chain, ZLC/CTL, MIT – International Logistics Program, Zaragoza, Spain
2013-2015	Associate Research Professor, Virginia Modeling, Analysis and Simulation Center, Old Dominion University (ODU), Suffolk, VA
2013-2015	Director, Advanced Analytics Laboratory (AAL), Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA
2008-2013	Assistant Research Professor, Virginia Modeling, Analysis and Simulation Center, Old Dominion University (ODU), Suffolk, VA

C. PRODUCTS

(see PAPPG Chapter II.C.2.f.(i)(c))

Products Most Closely Related to the Proposed Project

1. Diaz R. and Behr J. G. (2020) "Supply Chain Modeling in the Aftermath of a Disaster." IEEE Transactions on Engineering Management: Print ISSN: 0018-9391 Online ISSN: 1558-0040 Digital Object Identifier: 10.1109/TEM.2019.2950047
2. Diaz R., Behr J. G., Kumar S. (2015) Modeling Labor Dynamics of a Supply Chain after a Natural Disaster. International Journal of Disaster Risk Reduction. 12: 154-162.
3. Behr J. G. and Diaz R. (2013). Disparate health implications stemming from the propensity of elderly and medically fragile populations to shelter in place during severe storm events. Journal of Public Health Management and Practice on Dynamics of Preparedness. 2013 Sep-Oct; 19 Suppl 2:S55
4. Behr J. G., Diaz R. and Mitchell M. (2016) Building Resiliency in Response to Sea Level Rise and Recurrent Flooding: Comprehensive Planning in Hampton Roads. Virginia Newsletter. Vol. 92 No. 1 January.
5. Behr, Joshua G., and Carol Considine. (2019) "Parcel Buyout and Greenspace Acquisition as Adaptation Policy in Response to Storm Risk and Recurrent Flooding in a Coastal Port City." Coastal Management: Joining forces to shape our future coasts. ICE Publishing. 517-533

Other Significant Products, Whether or Not Related to the Proposed Project

1. Behr, J. G., Diaz R., and Giles B. City of Portsmouth. (2015) Adaption Response to Recurrent Flooding: Portsmouth Comprehensive Planning Support, Report 1 (aka Adaptive Capacity Report and Community Vulnerability Report).
2. Behr, J. G. et. al. Hampton Roads Regional Catastrophic Planning Team (HRRCPT) and VA Department of Emergency Management (VDEM) (2013): 1. Behavioral Study Report; 2. Refuge of Last Resort, Identification and Capacity Study; 3. Sheltering, Identification and Capacity Study; 4. Housing Report. J. Behr, R. Diaz, and B. Giles
3. Behr J. G. and Diaz R. (2014). Hurricane Preparedness: Community Vulnerability and Medically Fragile Populations. Virginian Newsletter. Vol. 90 No. 2 February
4. Kumar, Sameer, Rafael Diaz, Joshua G. Behr, and Ange-Lionel Toba. "Modeling the effects of labor on housing

D. SYNERGISTIC ACTIVITIES

(see PAPPG Chapter II.C.2.f.(i)(d))

1. NSF CONVERGE. (May-June 2020) Evacuation and Sheltering of Vulnerable Populations in a Hurricane-Pandemic: Vulnerable Populations & Planning Considerations for the 2020 Hurricane Season, Six-report Series.
2. VA Go grant (2019-Present) – Building Digital Shipbuilding Research – Supply Chain Analytics
3. Healthcare Erasmus+(2017-2019). Structured and delivered healthcare management programs at Masters and PhD level for the European Community in partnerships with Universities in Finland, Estonia, Belgium, Netherlands, and Germany
4. Ng M., Behr J. G., Diaz R.. (2013). Unraveling the Evacuation Behavior of the Medically Fragile Population: Findings from Hurricane Irene. Transportation Research Part A: Policy and Practice.

NSF BIOGRAPHICAL SKETCH

NAME: Joshua G. Behr

POSITION TITLE & INSTITUTION: Associate Research Professor, Old Dominion University

A. PROFESSIONAL PREPARATION

INSTITUTION	LOCATION	MAJOR/AREA OF STUDY	DEGREE	YEAR
California State Univ.	Fullerton	Political Science	A.B.	1989
California State Univ.	Fullerton	Political Science	M.A.	1992
Univ. of New Orleans	New Orleans	Political Science	Ph.D.	2001

B. APPOINTMENTS

From - To	Position Title, Organization and Location
2019-Present	Associate Vice President for Strategic Initiatives, Old Dominion Univ., Norfolk, VA
2019-Present	City of Norfolk Resilience Fellow, Norfolk, VA
2018-Present	Bruce and Lilly Bradley Distinguished Research Fellow in Coastal Resilience, Old Dominion University, Norfolk, VA
2017-Present	Program Manager Institute Coastal Adaptation and Resilience (ICAR), Social Science & Policy, Old Dominion University, Norfolk, VA
2015-2018	Director, Advanced Analytics Laboratory (AAL), Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Norfolk, VA
2014-2020	Governor's Appointee, State's representative to the Scientific and Technical Advisory Committee (STAC), EPA-funded Chesapeake Bay Program
2009-Present	Adjunct Professor, Eastern Virginia Medical School, School of Community Health Professionals, Norfolk, VA
2008-Present	Associate Research Professor, Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA
2008-Present	Board Member, Access Partnership, Chesapeake, VA
2007-2009	Associate Professor, Political Science, Old Dominion University, Norfolk, VA
2001-2007	Assistant Professor, Political Science, Southwestern Oklahoma State University
2000-2001	Assistant Professor, Political Science, Old Dominion University, Norfolk, VA
1999-2000	Adjunct Instructor, Political Science, University of New Orleans, LA
1999	Adjunct Instructor, Political Science, Metropolitan College, University of New Orleans, LA
1997	Adjunct Instructor, Political Science, Delgado College, New Orleans, LA
1995-1999	Instructor of Record, Political Science, University of New Orleans, LA

C. PRODUCTS

Products Most Closely Related to the Proposed Project

1. Diaz R. and Behr J. G. (2020) "Supply Chain Modeling in the Aftermath of a Disaster." IEEE Transactions on Engineering Management: Print ISSN: 0018-9391 Online ISSN: 1558-0040 Digital Object Identifier: 10.1109/TEM.2019.2950047

2. Diaz R., Behr J. G., Kumar S. (2015) Modeling Labor Dynamics of a Supply Chain after a Natural Disaster. International Journal of Disaster Risk Reduction. 12: 154-162.

3. Behr J. G. and Diaz R. (2013). Disparate health implications stemming from the propensity of elderly and medically fragile populations to shelter in place during severe storm events. Journal of Public Health Management and Practice on Dynamics of Preparedness. 2013 Sep-Oct; 19 Suppl 2:S55

4. Behr J. G., Diaz R. and Mitchell M. (2016) Building Resiliency in Response to Sea Level Rise and Recurrent Flooding: Comprehensive Planning in Hampton Roads. Virginia Newsletter. Vol. 92 No. 1 January.

5. Behr, Joshua G., and Carol Considine. (2019) "Parcel Buyout and Greenspace Acquisition as Adaptation Policy in Response to Storm Risk and Recurrent Flooding in a Coastal Port City." Coastal Management: Joining forces to shape our future coasts. ICE Publishing. 517-533

Other Significant Products, Weather of Not Related to the Proposed Project

1. Behr, J. G., Diaz R., and Giles B. City of Portsmouth. (2015) Adaption Response to Recurrent Flooding: Portsmouth Comprehensive Planning Support, Report 1 (aka Adaptive Capacity Report and Community Vulnerability Report).

2. Behr, J. G. et. al. Hampton Roads Regional Catastrophic Planning Team (HRRCPT) and VA Department of Emergency Management (VDEM) (2013): 1. Behavioral Study Report; 2. Refuge of Last Resort, Identification and Capacity Study; 3. Sheltering, Identification and Capacity Study; 4. Housing Report. J. Behr, R. Diaz, and B. Giles

3. Behr J. G. and Diaz R. (2014). Hurricane Preparedness: Community Vulnerability and Medically Fragile Populations. Virginian Newsletter. Vol. 90 No. 2 February

4. Kumar, Sameer, Rafael Diaz, Joshua G. Behr, and Ange-Lionel Toba. "Modeling the effects of labor on housing reconstruction: A system perspective." International Journal of Disaster Risk Reduction 12 (2015): 154-162

5. McLeod, George M., Thomas R. Allen, and Joshua G. Behr. "Geospatial Risk Assessment of Marine Terminal Infrastructure to Storm Surge Inundation and Sea Level Rise." Transportation Research Record (2018): 0361198118774234.

D. SYNERGISTIC ACTIVITIES

1. NSF CONVERGE. (May-June 2020) Evacuation and Sheltering of Vulnerable Populations in a Hurricane-Pandemic: Vulnerable Populations & Planning Considerations for the 2020 Hurricane Season, Six-report Series. Leads: J Behr and W. Yusuf.

2. Unsolicited. (2018) The 'New Normal' of Flooding in Portsmouth, Virginia: Perspectives, Experiences, and Adaptive Responses of Residents and Business Owners in Low to Moderate-Income Communities. Council, D., M. Covi, W. Yusuf, J. Behr and M. Brown.

3. NIH Chair, ZRG1 HDM W (58): Systems Science and Health in the Behavioral and Social Sciences

4. NIH Chair, ZRG1 HDM W (55): Modeling Social Behavior

5. Ng M., Behr J. G., Diaz R.. (2013). Unraveling the Evacuation Behavior of the Medically Fragile Population: Findings from Hurricane Irene. Transportation Research Part A: Policy and Practice.

NAME: Haiying "Helen" Shen

POSITION TITLE & INSTITUTION: Associate Professor; The Rector and Visitors of the University of Virginia

A. PROFESSIONAL PREPARATION
(see PAPPG Chapter II.C.2.f.(i)(a))

INSTITUTION	LOCATION	MAJOR/AREA OF STUDY	DEGREE (if applicable)	YEAR (YYYY)
Tongji University	Shanghai, China	Computer Science and Engineering	B.S.	2000
Wayne State University	Detroit, MI	Computer Engineering	M.S.	2004
Wayne State University	Detroit, MI	Computer Engineering	Ph.D.	2006

B. APPOINTMENTS
(see PAPPG Chapter II.C.2.f.(i)(b))

From - To	Position Title, Organization and Location
2016-present	Associate Professor, Computer Science Dept., Systems & Information Engineering Dept. and Electrical & Computer Engineering Dept., University of Virginia, Charlottesville, VA
2013-2016	Associate Professor, Dept. of Electrical and Computer Engineering, Clemson University, Clemson, SC
2009-2013	Assistant Professor, Dept. of Electrical and Computer Engineering, Clemson University, Clemson, SC
2006-2009	Assistant Professor, Dept. of Computer Science and Computer Engineering, University of Arkansas, Fayetteville, AR

C. PRODUCTS

(see PAPPG Chapter II.C.2.f.(i)(c))

Products Most Closely Related to the Proposed Project

1. Ankur Sarker, Haiying Shen, Tanmoy Sen, and Hua Uehara, An Advanced Back-Box Adversarial Attack for Deep Driving Maneuver Classification Models. Proceedings of 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), December 10-13, 2020, Delhi NCR, India
2. L. Kang and H. Shen, Preventing Battery Attacks on Electrical Vehicles based on Data-Driven Behavior Modeling, Proc. of International Conference on Cyber-Physical Systems (ICCPS), April 16-18, 2019, Montreal, Canada
3. A. Sarker and H. Shen, Data-Driven Misbehavior Detection System For Connected Autonomous Vehicles, Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT), vol. 2(4), 2018
4. A. Sarker, H. Shen, M. Rahman, M. Chowdhury, K. Dey, F. Li, Y. Wang, and H. Narman. A review of intelligent controller, sensing and communication, and human factors aspects for information-aware connected autonomous vehicles. IEEE transaction on Intelligent Transportation Systems (ITS), 2018
5. K. C. Dey, L. Yan, X. Wang, Y. Wang, H. Shen, M. Chowdhury, L. Yu, C. Qiu, and V. Soundararaj, A Review of Communication, Driver Characteristics and Controls Aspects of Cooperative Adaptive Cruise Control (CACC), IEEE transaction on Intelligent Transportation Systems (ITS), Vol. 17, no. 2, pp. 491--509, 2016

Other Significant Products, Whether or Not Related to the Proposed Project

6. C. Qiu, H. Shen, A. Sarker, V. Soundararaj, M. Devine, and E. Ford, Towards Green Transportation: Fast Vehicle Velocity Optimization for Fuel Efficiency, Proc. of CloudCom, 2016, Luxembourg [best paper award]
7. A. Sarker, C. Qiu, and H. Shen, Quick and Autonomous Platoon Maintenance in Vehicle Dynamics For Distributed Vehicle Platoon Networks, Short paper, Proc. of ACM/IEEE IoTDI, 2017, Pittsburgh, USA
8. L. Kang, H. Shen and A. Sarker, Velocity Optimization of Pure Electric Vehicles With Traffic Dynamics and Driving Safety Considerations, short paper, Short paper, Proc. of ICDCS, 2017, Atlanta
9. A. Sarker, C. Qiu and H. Shen, A Decentralized Network with Fast and Lightweight Autonomous Channel Selection in Vehicle Platoons for Collision Avoidance, Proc. of MASS, 2016, Brasília, Brazil

D. SYNERGISTIC ACTIVITIES

(see PAPPG Chapter II.C.2.f.(i)(d))

- Microsoft Research Faculty Fellow, 2010 (only seven awardees)
- IEEE Technical Committee on Scalable Computing (TCSC) Award for Excellence, 2015
- Associate Editor for the IEEE/ACM Transactions on Networking (TON), the International Journal of Parallel, Emergent and Distributes Systems (IJPEDS), the IEEE Networking Letters (NL) and the Journal of Information Science and Engineering
- General Co-Chair of the 6th ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI), 2021 and of the IEEE International Conference on Fog and Edge Computing (ICFEC), 2020
- Program Co-Chair of the IEEE Mobile Ad hoc and Smart Systems (MASS), 2019, the IEEE International Conference on Fog and Edge Computing (ICFEC), 2018 and 2019

Revised 05/01/2020 **NSF BIOGRAPHICAL SKETCH** **OMB-3145-0058**

NAME**:** Katherine Leigh Smith

POSITION TITLE & INSTITUTION: Research Associate, Old Dominion University

A. PROFESSIONAL PREPARATION

(see PAPPG Chapter II.C.2.f.(i)(a))

INSTITUTION	LOCATION	MAJOR/AREA OF STUDY	DEGREE (if applicable)	YEAR (YYYY)
	Norfolk, VA	Applied Mathematics	BS	2008
Old Dominion UniversityOld Dominion University	Norfolk, VA	Mechanical Engineering	BS	2008
Old Dominion University	Norfolk, VA	Applied and Computational Mathematics	MS	2009
Old Dominion University	Norfolk, VA	Modeling and Simulation	Certificate	2009
Old Dominion University	Norfolk, VA	Modeling and Simulation	PhD	2021 (anticipated)

B. APPOINTMENTS

(see PAPPG Chapter II.C.2.f.(i)(b))

From - To	Position Title, Organization and Location
2019-Present	Research Associate, Digital Shipbuilding, Virginia Modeling, Analysis, and Simulation Center, Old Dominion University, Suffolk, VA
2017-2019	Senior Lecturer, Department of Mathematics and Statistics, Old Dominion University, Norfolk, VA
2011-2017	Lecturer, Department of Mathematics and Statistics, Old Dominion University, Norfolk, VA
2011	Adjunct Instructor, Department of Mathematics and Statistics, Old Dominion University, Norfolk, VA
2009-2011	Aerospace Engineer, NASA Langley Research Center, Hampton, VA

C. PRODUCTS

(see PAPPG Chapter II.C.2.f.(i)(c))

Products Most Closely Related to the Proposed Project

Diaz, R., Smith, K., Landaeta, R., Padovano, A. “Shipbuilding Supply Chain Framework and Digital Transformation: A Project Portfolios Risk Evaluation.” Procedia Manufacturing 42 (2020): 173-180. doi: https://doi.org/10.1016/j.promfg.2020.02.067

Smith, K., Shen, Y., Dean, A. “Software Design Considerations for Mathematics in Mobile Games.” in Game Design and Intelligent Interaction. Deliyannis, I. (Ed.) IntechOpen (2019). ISBN: 978-1-83880-010-9.

Shen Y., Zhu, Z., Lin, C., Ren, S., Smith, K., Dean A. "Design of A Virtual Laboratory for Automation Control." Proceedings of the 2018 ASEE Annual Conference & Exposition. Salt Lake City, UT, June 24-27, 2018.

Smith, K., Shull, J., Shen, Y., Dean, A., and Michaeli, J. “Overcoming Challenges in Educational STEM Game Design and Development.” Proceedings of the 2017 Winter Simulation Conference. Las Vegas, NV, December 3-6, 2017.

Smith, K., Shull, J., Dean, A., Shen, Y., and Michaeli, J. “SiGMA: A software framework for integrating advanced mathematical capabilities in serious game development.” Advances in Engineering Software 100 (2016): 319-325. doi: 10.1016/j.advengsoft.2016.08.007

Other Significant Products, Whether or Not Related to the Proposed Project

Smith, K., Shen, Y., and Dean, A. “Incorporating Diegetic Elements to Increase Engagement in Games for Engineering Education.” Proceedings of the 2018 ASEE Annual Conference & Exposition. Salt Lake City, UT, June 24-27, 2017.

Smith K., Shull J., P. Heaney, Shen Y., Dean A., Michaeli J. “Overview of Game and Content Design for a Mobile Game that will Prepare Students in Calculus and Physics Prerequisites to the Engineering Curriculum.” Proceedings of the 2017 ASEE Annual Conference & Exposition. Columbus, OH, June 25-28, 2017.

Heaney P., Smith K., Shull J., Eller B., Dean A., Shen Y., Michaeli J. “Stern2STEM: Implementation of a Feed Forward Model for Educational Game Development.” Proceedings of ASNE Day Technology, Systems, & Ships. Arlington, VA, February 14-16, 2017.

D. SYNERGISTIC ACTIVITIES

(see PAPPG Chapter II.C.2.f.(i)(d))

Led the development of a system of systems model for naval computing systems.

Engaged in educational game development and deployment, content design, and website maintenance and development for Stern2STEM, a project assisting military veterans pursuing STEM degrees.

Festival Organizer/Director (2018-present) for the annual Julia Robinson Mathematics Festival for elementary and middle school students held at ODU. This outreach event is a free, non-competitive celebration of great ideas and problems in mathematics that hosted approximately 360 3rd through 8th grade students and 130 volunteers at the February 2020 event.

Member of the organizing committee for the Second International Conference on Mathematics of Data Science

HAMPTON ROADS
MARITIME INDUSTRIAL BASE
ECOSYSTEM
Moving Maritime Forward Together

May 11, 2020

Coastal Virginia Center for Cyber Innovation (COVA CCI),

I am writing to provide our support for the scope of work within the proposal submitted by Drs. Rafael Diaz and Haiying Shen from the Old Dominion University and University of Virginia (ODU-UVA) Team titled, "A Real-Time Dependency Network Approach to Quantifying Risks and Ripple Effects from Cybersecurity attacks in Shipbuilding and Repair Supply Networks" in response to the COVA CCI Request for Proposals: CCI Cybersecurity Research Collaboration Funding (COVACCI-21-02).

The Hampton Roads Maritime Industrial Base Ecosystem (MIBE) works tirelessly to drive the Digital Transformation technologies that can enhance our shipbuilding and ship repair industries. Critical to that evolution and growth is providing cyber protection to the shipbuilding supply chains that enable these industries. The proposed project recognizes the need for the adoption and use of System of Systems Engineering (SoSE) tools and advances the application of Artificial Intelligence to support the monitoring of supply networks, and the significantly enhances the ability to react to cyberattacks quickly.

MIBE supports the ODU-UVA team because the ODU-UVA team leading this project has a recognized record of research on cybersecurity and cyber physical systems (CPS), as demonstrated through their performance at ODU's Virginia Modeling, Analysis, and Simulation Center.

In support of this project, MIBE will support the ODU-UVA team through participation at technical meetings, assist them in connecting with shipbuilding and repair suppliers, and evaluate the technologies developed during this project for potential applications to other maritime industry stakeholders. Should COVACCI-21-02 fund this proposal, my office is committed to supporting this vital work. If there is anything further I can add in support of this proposal, please feel free to contact me directly at the number and email provided below.

Most Sincerely,

Brad Williamson
Executive Director
Hampton Roads Maritime Industrial Base Ecosystem
1030 University Blvd
Suffolk, VA 23435
757-814-0865
B7willia@odu.edu

SSI

Autodesk® based Shipbuilding & Offshore Solutions

ShipConstructor Software USA, Inc.
775 University Blvd. N., Suite 140. Mobile, AL, 36608, USA
Toll free: +1-888-554-0557 Tel: +1-251-340-6200 Fax: +1-251-343-4715
SSIUSA@SSI-corporate.com www.SSI-corporate.com

12 May 2021

Old Dominion University Research Foundation (ODURF)
Virginia Modeling Analysis and Simulation Center (VMASC)
1030 University Blvd
Suffolk, VA 23435

Subj: Letter of Support

Dear Dr. Diaz:

We are writing this letter of commitment and support for the Old Dominion University Research Foundation (ODURF) / Virginia Modeling Analysis and Simulation Center (VMASC) project: A Real-Time Dependency Network Approach to Quantifying Risks and Ripple Effects from Cyberattacks in Defense Shipbuilding and Repair Supply Networks.

The application of digital shipbuilding technologies to improve the informational flow of shipbuilding and ship repair processes is critical to shipbuilders as it enhances communication, speed, and coordination among different stakeholders. In addition, it opens opportunities to the development of Artificial Intelligence applications to improve planning and execution practices, including prospects to become agile when experiencing potential delays. Cybersecurity is a critical issue in these environments that can disrupt supply networks that serve the defense shipbuilding industry. This project acknowledges the need to explore the application of Artificial Intelligence to support resiliency management when facing a cyberattack at the supply network layer. The project explores opportunities to extends digital shipbuilding applications in planning and scheduling.

ShipConstructor Software, USA Inc. (SSIUSA) supports Old Dominion University Research Foundation (ODURF) in COVA CCI Program COVACCI-21-02. In support of this project, SSIUSA will provide ODURF with guidance and help to evaluate the methodologies developed during this project. Please feel welcome to share this letter of support with COVA CCI as our expression of support for the proposal.

For questions regarding this Letter of Support, please contact me at (251) 340-6200, ext. 400 (Office) or (251) 510-3860 (Cell).

Sincerely,

Patrick Roberts
Vice President of Sales & Operations
ShipConstructor Software USA, Inc. (SSIUSA)

FAIRLEAD

10 May 2021

Old Dominion University
Virginia Modeling, Analysis, and Simulation Center (VMASC)
1030 University Blvd, Suffolk, VA 23435

Attention: Rafael Diaz, PhD, Research Associate Professor,
Advanced Analytics Research Lab Director

Subject: Letter of Support – *"A Real-Time Dependency Network Approach to Quantifying Risks and Ripple Effects from Cyberattacks in Shipbuilding and Repair Supply Networks"*

Dear Dr. Diaz:

On behalf of Fairlead Boatworks Inc. and its affiliate Fairlead Integrated. LLC (Fairlead), I am pleased to provide this letter of support, formalizing Fairlead's commitment to the Old Dominion University Research Foundation (ODURF)/Virginia Modeling Analysis and Simulation Center (VMASC) for their proposal to COVACCI-21-02, *"A Real-Time Dependency Network Approach to Quantifying Risks and Ripple Effects from Cyberttacks in Shipbuilding and Repair Supply Networks."* As an active project support resource, Fairlead will participate at ODURF technical meetings, evaluate the project developed technologies for possible use by Fairlead, and assist with case study development and model testing, validation, and demonstrations.

Emerging technologies and innovation drive evolution and growth throughout the United States' shipbuilding and ship repair industries. It is critical that companies identify and understand the business impacts from cybersecurity breaches occurring in their supply network that disrupt the flow of material and supplies. This project recognizes the need to adopt and use advanced Artificial Intelligence to support executing complex risk monitoring and assessment activities that may positively affect ongoing operations. Fairlead would benefit greatly from determining the specific effects on our inbound delivery schedules, and being afforded the opportunity to proactively respond, reconfiguring operations, adjusting production schedules, and minimizing or avoiding costly delays.

Please feel free to share Fairlead's letter of support with COVA CCI and appropriate agencies, expressing our commitment to this proposal and the future project. Should you or others require additional information or wish to speak with me further about this commitment, I can be reached by phone at 757- 606-2034 (office) or email at dwood@fairleadint.com.

Sincerely

Daniel S. Wood
Vice President, Contract & Procurement