Maritime Cyber Security

Work Plan Draft

August 8, 2016
INTRODUCTION

On July 27, 2016, the American Bureau of Shipping (ABS) received notification of award of the Maritime Cyber Security project for the Maritime Security Center (MSC) Center of Excellence at the Stevens Institute of Technology. The project has a two year period of performance. The purpose of this task order is to perform research on six separate topics related to maritime cyber security.

RESEARCH TEAM

ABS’s Certified Cybersecurity Specialists have extensive experience with industrial control systems for ships, offshore installations, and facilities and are uniquely qualified to deliver a comprehensive security assessment. Our personnel have been selected for this assignment based on their previous experience in maritime cyber security, control systems, the maritime industry, and federal regulatory analysis. Our Team has experience in the analysis, review, and documentation of vulnerabilities of both commercial IT and process automation systems. We have analyzed cyber and physical security threats, risks, and vulnerabilities, and conducted site analyses for a wide array of operations and systems. The research will be performed by the following team.

Principal Investigator

Cris DeWitt leads our Software and Control Systems group, providing a range of cyber safety and security services for the maritime industry. Mr. DeWitt and his team conduct technology assessments for cybersecurity with control systems used in drill ships, ultra-deep water drilling rigs, LNG vessels, and other complex automation assets. He has also published on cyber security and its impact on offshore assets.

Risk Lead

Mr. Mowrer, the Director of Homeland Security Risk Management Technologies at ABSG Consulting Inc., has been working in the management consulting, risk management, data analytics, and information technology fields for the past 18 years. He has managed numerous projects for USCG, including cybersecurity assessments for the U.S. maritime industry; 10 annual phases of the MSRAM; the 2006, 2009, and 2011 National Maritime Strategic Risk Assessments; and the Ports, Waterways, Coastal Security (PWCS) Risk-Based Performance

Research Analysts

Mr. Rick Scott is a Registered Professional Engineer (#64544, TX) with over 40 years of experience ranging from engineer to senior executive in the high-technology manufacturing and offshore drilling industries. His specialties include: software services management, software product development, and software systems integration. He has witnessed testing and certified offshore drilling control software for ABS and developed the ABS certification process for software systems assessment and certification.

Other research analysts will be brought in over the course of the project to support task execution.
TECHNICAL APPROACH FOR RESEARCH QUESTIONS

The following sections describe our technical approach for each of the research questions included in the RFP.

1. RISK-BASED PERFORMANCE STANDARDS

**Question:** What risk-based performance standards can be developed for cyber risk management of the Marine Transportation System (MTS)? How would performance standards inter-relate with other infrastructure sectors and their performance standards? How would performance standards inter-relate with existing safety and security management systems?

TECHNICAL APPROACH

The following outlines the key tasks in our technical approach to answer research question #1. *Note: the results of Steps 2-5 provide a foundational structure that will support the analysis and communication of results for several of the research questions.*

1. **Doctrine Review.** We will review key maritime cyber risk management doctrine, strategies and policies (USCG Cyber Strategy, USCG Western Hemisphere Strategy, paper from Maritime Security Center Maritime Risk Symposium) to inform our research related to this questions. We will meet with select USCG, DHS, DoD, and select industry experts to gather their insight on risk-based performance standards.

2. **Performance Standards Review.** We will perform an in-depth literature review of recognized cyber risk management performance standards that could be applicable to MTS, including, but not limited to:
   - NIST Framework for Improving Critical Infrastructure Cybersecurity
   - NIST SP 800-82 Revision 2, Guide to Industrial Control Systems Security
   - ISO 27001: Information Security Management Standard
   - Department of Homeland Security’s (DHS’s) and Department of Energy’s (DOE’s) Cybersecurity Capability Maturity Model (C2M2)
   - International Society for Automation (ISA) Industrial Network and System Security (ISA 62443)
   - DoD Instruction 8500.01, Cybersecurity

3. **Asset Inventories.** We will inventory the range of asset types (e.g., ferry terminals, container ships, bridges, petroleum refineries) and infrastructure sectors that commonly operate within the U.S. MTS.

4. **Asset Class Taxonomy.** We will develop a standard taxonomy for classifying these maritime assets, classes, and infrastructure sectors.

5. **System Inventories.** We will inventory information technology (IT) and operational technology (OT) systems that are commonly found on the assets and map them to the asset taxonomy.

6. **Safety/Security Management System Review.** We will perform a literature review of governing regulations and standards for safety and security management systems applicable to each asset types. Due to the complexity of the MTS, there are a wide variety of assets that operate within the U.S. domain falling under many different safety/security requirements, including: USCG, DHS, OSHA, EPA, BSEE, DOT, IMO/BIMCO, Classification Societies, state/local agencies, and PHMSA. We will review existing requirements for safety/security management systems under each regime and clearly identify those
which cover, or could be expanded to cover cyber issues. We will then map each regime to their applicable asset classes.

7. **Performance Standards Crosswalk.** Based on (1) applicable performance standards, (2) IT/OT systems and (3) the associated safety/security management systems for each asset class, we will develop a crosswalk identifying which performance standard elements are currently being addressed by various safety/security management systems and where gaps exist.

8. **Conclusions & Recommendations.** Based on the results of the previous steps, we will summarize our conclusions comparing standards requirements across infrastructure sectors and provide recommendations on which performance standards could/should be applied to each asset type and infrastructure sector.

### 2. FRAMEWORK FOR CYBER POLICY

*Question:* What type of criteria should be utilized to develop an academically rigorous framework for Cyber Policy for the MTS?

**TECHNICAL APPROACH**

The following outlines the key tasks in our technical approach to answer research question #2.

1. **Literature Review.** We will perform an in-depth review of cyber frameworks, focusing on the NIST Framework for Improving Critical Infrastructure Cybersecurity and ISO 27001: Information Security Management Standard, to identify the criteria they included.

2. **Scope Definition.** We will first define the scope of the cyber policy for the MTS. The scope should address a number of factors, including, but not limited to: asset classes, IT/OT systems, threat types, and whether the policy covers both cyber safety and cyber security concerns. We will then define the goals and objectives for cyber security in the MTS. The scope and goals will be developed based on the results of the literature review and guidance from USCG, DHS, and DoD experts.

3. **Affected Party Identification.** Based on the scope, we will then research and identify parties effected by the policy, such as federal, state, and local government agencies, maritime facility owner/operators, vessel owner/operators, industry groups, ports, international organizations, and classification societies.

4. **Affected Process Identification.** We will identify and describe processes and decisions impacted by policy for each affected party. Processes such as cyber security assessments, audits, security plan development, security plan review, and vessel surveys are likely to be effected by policy changes.

5. **Criteria Identification.** We will recommend all of the relevant criteria that should be included in a cyber framework, spanning the phase of detection, identification, protection, response, and recovery.

### 3. CRITICAL POINTS OF FAILURE

*Question:* Based on a multi-node analysis, what are the critical Points of Failure within the cyber system supporting the MTS?

**TECHNICAL APPROACH**

The following outlines the key tasks in our technical approach to answer research question #3.
1. **Doctrine Review.** We will leverage the review of key maritime cyber risk management doctrine (Question 1, Step 1) to identify scenarios of concern and the associated definitions to develop an understanding of criticality thresholds. We will then meet with USCG, DHS, and DoD decision makers to clearly define “critical points of failure” and identify “criticality thresholds”. These definitions should address aspects of system vulnerability of and potential consequences of system exploitation (e.g., physical consequences).

2. **Asset Class Screening.** We will identify the subset of asset classes with cyber scenario consequence potential exceeding the criticality threshold.

3. **General Architecture Development.** We will develop general architecture profiles for each of the asset class based on the common systems identified in Question 1, Task 5. These will address both IT and OT systems and integration.

4. **Corruption Vector and Penetration Point Taxonomy.** We will develop a hierarchical taxonomy of corruption vectors and their associated penetration points. We will then map the potential corruption vectors and penetration points for each general architecture.

5. **Scenario Development.** For each general architecture/asset class combinations, we will identify specific scenarios that could result in consequences above the criticality threshold.

6. **Risk Assessment.** We will perform a high level risk assessment considering threat, vulnerability, and consequence factors. Due to the general nature of the assessment, we will choose a qualitative or simple quantitative risk methodology to assess the risk. Methods may include bow tie, event tree/fault tree, or preliminary risk analysis.

7. **Results Documentation.** We will document the results of the risk assessment process, identifying critical points of failure and articulating them as a function of asset classes, systems, corruption vectors, and penetration points.

### 4. REQUIREMENTS FOR MARITIME CYBER RANGE

**Question:** What are the critical requirements that should be considered when developing an academically rigorous and multi-use Maritime Cyber Range?

#### TECHNICAL APPROACH

The following outlines the key tasks in our technical approach to answer research question #4.

1. **Use Case Development.** We will first investigate known cyber range models (e.g., U.S. Marine Corps, ABS) to determine their relevance and applicability to this project. We will interview representatives from the most relevant ranges to discuss lessons learned and best practices. If needed, we will host a workshop with maritime government representatives to discuss findings and define cyber range objectives for this project. Based on workshop guidance and scenarios of interest identified in task 3, we will document methods for developing use cases.

2. **System Behavior Definition.** We will document methods for developing expected system behavior definitions (including integration among systems) for systems of interest.

3. **Test Boundary Development.** We will document methods for developing test boundaries for select architectures.

4. **Test Requirements.** We will document methods for defining test requirements.

5. **Equipment and Software Requirements.** We will document methods for developing test equipment and software requirements.
6. **Test Documentation.** We will document methods for recording and interpreting test results.

7. **Develop Training Requirements.** We will document competencies that users of the range require to conduct experiments. Competencies will address all phases of the experiment, including, but not limited to: initial range configuration, conduct of the experiment, results documentation, and procedure for returning range to baseline state.

---

**5. FRAMEWORK FOR POINT OF FAILURE DETECTION METHODOLOGY**

**Question:** What methodologies can be utilized or invented to develop a framework to analyze a point of Failure Detection Methodology?

---

**TECHNICAL APPROACH**

The following outlines the key tasks in our technical approach to answer research question #5.

1. **Scope Definition.** We will first define the analytical scope of the failure detection methodology. The scope will be informed by the outputs of tasks from questions 1 and 3. Specifically, the in relation to general architectures and scenarios of concern. We will document how other industries and government agencies detect points of failure and which performance standards and frameworks they use.

2. **Decision Definition.** We will first define key decision makers (e.g., government leaders, asset owners). For each decision maker type, we will identify the decisions to be supported by results of methodology. This will include the options available to the decision maker.

3. **Information Requirements.** We will identify the types and quality of information that is required to support each decision. There can be a wide variety of information needed, such as listing of specific critical vulnerabilities, ranking of the overall integrity/vulnerability of an asset, qualitative/quantitative risk score for an asset (TVC). We will define the requirements for the appropriate level of information.

4. **Methodology Identification.** We will then identify relevant methodologies capable of generating the required information. We will describe each methodology, list strengths and weaknesses, and compare across methodologies.

5. **Conclusions and Recommendations.** We will recommend any identified enhancements to the relevant methodologies.

---

**6. MARITIME CYBER DETERRENT STRATEGY EFFECTIVENESS**

**Question:** What methodologies can be employed to conduct a quantitative analysis of maritime cyber deterrent strategy effectiveness?

---

**TECHNICAL APPROACH**

The following outlines the key tasks in our technical approach to answer research question #6.

1. **Define Current Cyber Deterrent Strategy.** We will meet with government representatives to capture the elements of their current cyber strategy and means they use to develop strategy and measure effectiveness. We will document the multi-layer strategy in a comprehensive framework, likely using bow-tie methodology.
2. **Decision Definition.** We will then define key decision makers (e.g., government leaders, asset owners) who will use the cyber deterrent strategy effectiveness measurement model. For each decision maker type, we will identify the decisions to be supported by results of methodology. This will include the options available to the decision maker.

3. **Information Requirements.** We will identify the types and quality of information that is required to support each decision.

4. **Methodology Identification/Development.** We will identify relevant methodologies capable of generating the required information. We will describe each methodology, list strengths and weaknesses, and compare across methodologies. If needed, we will develop or tailor methodologies to meet the information requirements.

5. **Recommendations.** We will recommend any identified enhancements to the relevant methodologies.

**MILESTONES AND OUTPUTS**

Table 1 lists our planned outputs, timing, and associated research questions. While the period of performance is for two years, the research team proposes delivery of all required milestones with 16 months of the contract award.

<table>
<thead>
<tr>
<th>Output</th>
<th>Time</th>
<th>Associated Research Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Cyber Policy Framework Document</td>
<td>4 months from award</td>
<td>2</td>
</tr>
<tr>
<td>2 Points of Failure Analysis Report</td>
<td>7 months from award</td>
<td>3</td>
</tr>
<tr>
<td>3 Points of Failure Detection Report</td>
<td>7 months from award</td>
<td>5</td>
</tr>
<tr>
<td>4 Risk-Based Performance Standards</td>
<td>6 months from award</td>
<td>1</td>
</tr>
<tr>
<td>Recommendation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Comparative Analysis of Performance Standards to Existing Safety &amp; Security Measures</td>
<td>8 months from award</td>
<td>1</td>
</tr>
<tr>
<td>6 Comparative Analysis of Performance Standards to Other Infrastructure Results</td>
<td>12 months from award</td>
<td>1</td>
</tr>
<tr>
<td>7 Cyber Range Requirements Report</td>
<td>16 months from award</td>
<td>4</td>
</tr>
<tr>
<td>8 Cyber Deterrence Effectiveness Model</td>
<td>15 months from award</td>
<td>6</td>
</tr>
<tr>
<td>9 Cyber Deterrence Effectiveness Model Analysis Results Report</td>
<td>16 months from award</td>
<td>6</td>
</tr>
<tr>
<td>10 Delivery and socialization of outputs</td>
<td>1 month from completion of each output</td>
<td>all</td>
</tr>
</tbody>
</table>

The Gantt chart in describes our overall timeline for this project and execution of the tasks described in the technical approach for each of the six research questions. This notional project schedule is based on our understanding of the research objectives and our ability to complete the project within the required period of performance. It is based upon sound project management principles and resource allocations that will ensure we
complete the outputs listed in Table 1 within the required timetable. The delivery dates for the outputs are shown as black triangles in the figure. Note: this schedule assumes an August 2016 award. If award is delayed, the schedule will be updated accordingly.
PROJECT MANAGEMENT

We maintain a tailored system of organization, project controls and standardized processes, to ensure that MSC receives high-quality deliverables that meet or exceed the stated requirements. Through our 152-year history supporting nearly all aspects of maritime industry, we developed a project management methodology that is not only grounded in quality and integrity but also based upon the principles described in the Project Management Institute’s (PMI) “A Guide to the Project Management Body of Knowledge (PMBOK®) - Fifth Edition.” Our program management philosophy includes (1) providing an experienced project manager (PM) with appropriate decision-making authority, (2) following structured repeatable processes, and (3) utilizing our Oracle-based Global Enterprise Management System (GEMS) management system to provide real time tracking/oversight of all task activities. Table 9 provides an overview of our project management processes.

Table 2. Project Management Processes & Metrics

<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initiating</strong></td>
</tr>
<tr>
<td>Our financial/contract management system establishes cost code identification numbers for performance tracking of individual projects and tasks.</td>
</tr>
<tr>
<td><strong>Planning</strong></td>
</tr>
<tr>
<td>Our PM establishes budget, schedule and definition of deliverables for the call order. We will use MS Project for planning and monitoring progress throughout project execution.</td>
</tr>
<tr>
<td><strong>Execution</strong></td>
</tr>
<tr>
<td>The execution phase of the task involves conducting, monitoring, and managing all aspects of meeting the call order requirements. In general, we conduct bi-weekly meetings across the task team at which time the PM reviews schedule, percent completion on deliverables, budget percent complete, variance between project and budget status, and plans to correct any problems/deficiencies identified.</td>
</tr>
<tr>
<td><strong>Controlling &amp; Monitoring</strong></td>
</tr>
<tr>
<td>Our GEMS system provides real-time project detail reports (weekly or more often if desired). The reports provide key metrics that allow the PM to determine if a task is progressing as planned or requires corrective actions. GEMS automatically sends email alerts to the PM when defined task milestones are surpassed.</td>
</tr>
<tr>
<td><strong>Closing</strong></td>
</tr>
<tr>
<td>The PM initiates project closure as soon as all contract deliverables and all charges are made and the final invoice is approved. A required after-task review is performed to identify ideas/methods/processes for performance improvement on future call orders.</td>
</tr>
</tbody>
</table>

Our PM will provide bimonthly status reports to MSC representatives which:

- Summarizes progress made during the period
- Outlines work anticipated for the next period
- Highlights any key issues requiring MSC attention
- Provides key performance metrics
  - Percent completion on deliverables
  - Budget percent complete
  - Variance between project and budget status
- Invoices sent during the period
DHS STAKEHOLDER ENGAGEMENT

In addition to working with DHS Science and Technology (S&T), we will engage the following stakeholders for Technical Reviews and comments as well as Cyber Deterrence Effectiveness Model input:

- USCG Assistant Commandant for Prevention Policy (CG-5P)
- USCG Office of Port & Facility Compliance (CG-FAC)
- USCG Domestic Port Security Evaluation Division (CG-PSA-2)
- USCG Office of Standards Evaluation & Development (CG-REG)
- USCG Cyber Command (CGCYBERCOM)
- USCG Research & Development Center (CG-RDC)

BENEFITS TO DHS STAKEHOLDERS

- Awareness of critical failure points in the MTS
- Enhanced communication and information sharing between stakeholders
- Informed policy-making