Request for Proposals for Maritime Cyber Security
Proposals due April 25, 2016

BACKGROUND

The Maritime Security Center (MSC) supports DHS efforts to provide for the safe and secure use of our nation's maritime domain and a resilient Marine Transportation System (MTS), through advancement of the relevant sciences and the professional development of the current and future maritime security workforce. More information on MSC may be found on www.stevens.edu/msc.

In November 2015, MSC co-hosted the Maritime Risk Symposium in conjunction with the U.S. Coast Guard Research and Development Center. The theme of the Symposium was: "Risk in the Western Hemisphere and Southern Border Approaches." The event included discussions on transnational threats and maritime challenges to the MTS and U.S. national security over the next ten years, specifically focusing on: (1) Combating Networks; (2) Securing Borders; and (3) Safeguarding Commerce.

The Symposium served as a forum to inspire and generate areas of study and future research projects for the DHS S&T Center of Excellence researchers, students and academic partners. The two-day Symposium facilitated dialogue and an exchange of ideas between a diverse group of public and private maritime and homeland security practitioners. Outcomes from the Symposium included a number of research questions that are of particular interest to DHS and its component agencies that have missions related to the maritime domain and will be subject of an open call for White Papers and Proposals (via a Request for Proposals, Request for Information, etc.). Some of the questions are the subject of this RFP. This call is being issued to a wide audience involved in various maritime disciplines and will solicit proposals that will focus on interdisciplinary research, education and technology transition in maritime cyber security.

PROBLEM STATEMENT

"Cybersecurity represents the latest risk to this [marine transportation] system and is a growing concern for consumers, corporations, and law enforcement agencies. This concern is well founded. Computers and other cyber-dependent technologies are growing parts of our lives and businesses. These systems are potentially vulnerable to many types of risks, from deliberate attacks, to the unintended but damaging

introduction of malware, to simple technical failure. In most cases, cyber "accidents" are at least as likely as a targeted cyber attack. Regardless of the source or motivation of the threat, however, cyber vulnerabilities within the marine system could compromise vital safety, security, and environmental functions, or lead to widespread trade disruptions."

RADM Marshall B Lytle III, USCG and RADM Paul F. Thomas, USCG, USCG Proceedings, Winter 2014-2015, p. 4.

PROPOSAL TOPIC AREAS

This RFP aims to solicit answers to the following research questions:

1. 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?

2. What type of criteria should be utilized to develop an academically rigorous framework for Cyber Policy for the MTS?

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

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

5. What methodologies can be utilized or invented to develop a framework to analyze a point of Failure Detection Methodology?

6. What methodologies can be employed to conduct a quantitative analysis of maritime cyber deterrent strategy effectiveness?

Applicants should take into consideration the following documents as they prepare to respond:

U.S. Coast Guard Cyber Strategy

(http://www.uscg.mil/seniorleadership/DOCS/cyber.pdf)

U.S. Coast Guard Western Hemisphere Strategy

(http://www.uscg.mil/seniorleadership/docs/uscg_whem_2014.pdf)

Cybersecurity, USCG Proceedings, Winter 2014-2015

(http://www.uscg.mil/proceedings/archive/2014/Vol71_No4_Wint2014.pdf)

MRS conference presentations and rapporteur's report:
http://www.stevens.edu/research-entrepreneurship/research-centers-labs/maritime-security-center/maritime-risk-symposium

PROPOSAL FORMAT AND EVALUATION CRITERIA

Funding under this call will be for one (1) award. Funding for this award will be up to $350,000. The available funds will be used for the project that scores the highest against the evaluation criteria.

The performance period is two years and will begin on July 1, 2016.

Applicants will submit a 10 page proposal using the provided template (12 point font, double spaced, including figures and references) that addresses the following:

Given the complexity of challenges posed by the research questions above, we encourage and give preference to applications received for proposals that incorporate multi-disciplinary expertise as well as methodological approaches.

Technical

Research Question(s) being addressed
Research Description
- *Objective or Purpose*
- *Research Methodology*
- *Milestones*
- *Performance Metrics*
- *Stakeholder and Transition Approach*
- *Relevance to DHS*
- *Outcomes or Outputs*

Data Needs– outline the data you will use in this project and how you will obtain it (publicly available, available for purchase, federal data, etc.). If you are relying on federal data sources, please explain in detail how you plan to gain access to these, as their release is not a condition of the award.

Qualifications of PI (short paragraph, details provided in CV)

Cost/Supplementary Information (not included in 10 page limit)

Detailed Budget showing itemized direct costs as well as indirect costs
Budget Narrative/Justification
Copies of Current Indirect Rate/Fringe Rate Agreements
NSF-style CV (2 pages) for the PI

SUBMISSION INSTRUCTIONS

Proposals must be submitted in compiled PDF (electronic format) to MSC at the following email address: msc@stevens.edu by 8pm EST on April 25, 2016.

***Note that additional reference information or supporting documentation (in any format) may be requested following submission.**

REVIEW/SELECTION PROCESS

Reviewers from the academic/research community and DHS will evaluate the proposals.

A merit-based evaluation criteria will be used to determine the award: Scientific quality and relevance to DHS mission.

Scientific Quality Review. Reviewers will be asked to rate how the proposal addresses the following criteria, posed as questions. Reviewers will rate applications using numerical ratings of 1 to 5 (poor to excellent) and apply the percentage-weighting factor as indicated for an overall rating.

(1) Originality and/or Innovativeness (25%).

- Is it original, e.g., does the proposed effort challenge and seek to shift current research or paradigms by utilizing novel theoretical concepts, inter-disciplinary approaches or methodologies?

- Is it innovative, e.g., is the proposal a novel refinement, improvement, or new application of theoretical concepts, inter-disciplinary approaches or methodologies proposed?

- Does this research have the potential to generate influential publications in the scientific community or lead to new discoveries or areas of investigation?

(2) Proposed Approach/Methodology (25%).

- Are the research goals clear and based on sound theory?

- Are the methods proposed clearly stated and appropriate for testing the hypotheses?

- Are the data generation or collection approaches appropriate for the research methods?

- Is the approach or methodology technically sound, incorporate inter-disciplinary expertise when appropriate, including a demonstrated understanding of the critical technology or engineering challenges required for achieving the project goals?

(3) Influence and Cooperative Linkages (25%).

- Does the application show partnerships or cooperative initiatives with other institutions or organizations?

- Does the application demonstrate a viable plan for developing substantial and continuing linkages with the Homeland Security Enterprise?

(4) Qualifications of Personnel and Suitability of Facilities (15%).

- Does the investigative team have the breath of qualifications - credentials and experience - to conduct and complete the proposed research?

- Does the investigative team have prior experience in similar efforts and do they clearly demonstrate an ability to deliver products that meet the proposed technical performance within their proposed budget and schedule.

- Are the facilities suitable for the proposed research?

(5) Costs (10%).

- Is the proposed research (and education) costs appropriate and reasonable?

Relevancy Review. Reviewers will be asked to rate how the proposal addresses the following criteria, posed as questions. Reviewers will rate applications using numerical ratings of 1 to 5 (poor to excellent) and apply the percentage-weighting factor as indicated for an overall rating.

A. Mission Relevance (75%)

- Is the proposed research project relevant to and does it support DHS's mission and its stakeholders?

- Does the proposed project address one or more of the research questions?

- Does the proposed project complement - and not duplicate – existing research and development programs sponsored by DHS or others?

- Are the potential research outcomes and users of the research well described?

B. Communicating/Transitioning Results (25%). Does the applicant have a track record of effectively communicating or successfully transitioning research results to appropriate stakeholders, specifically:

- Will the research team be able to deploy a technology and/or solution(s) that can be transitioned effectively to the user community either through commercialization of the technology, open source distribution, or through other means?

- Does the proposal demonstrate the implementation of an appropriate knowledge transfer process (i.e. models from case studies to other areas, patents, etc) from academic to government end-users and other DHS customers?

AWARD PROCESS

Awardees will be notified by MSC when a determination is made. The anticipated award date is July 1, 2016.

Application submission period will be closed on April 25, 2016 at 8:00 PM EST.

FAQs
Q: When is this proposal due?
A: The proposal is due by 8pm EST on April 25, 2016

Q: When will awards be announced?

A: Awards will be announced in July 2016.

Q: Where will I submit my final proposal?
A: Proposals must be submitted to **msc@stevens.edu** - You will receive an email confirming your submission.

Q: What is the performance period for this award?
A: The performance period is for two years.

Q: Can the funds be awarded to independent contractors?
A: No, all applicants must be associated with an accredited college, university, or non-profit.

Q: Should I include IDC in my budget?
A: Yes. This RFP calls for standard, IDC costs. Please follow your institutional policy regarding cost basis used and cost elements when completing your budget.