July 10, 2024

Request for Proposal

Assessment of Cyber Incident Response Plans (IRP)

The Northern Virginia Emergency Response System (NVERS) is seeking contract support on behalf of the Northern Virginia Chief Information Security Officers (CISO) to study, and analyze established, or in-process, local cyber IRP models and produce data driven reports for regional cybersecurity personnels' utilization. The purpose of this request for proposal is to enter into a firm fix-priced contract with a qualified organization or individual to conduct an assessment of local cyber IRPs. The assessment and resulting detailed reports should include best practices, strengths, concerns, risks, deficiencies, recommendations, and frequency of IRP training.

Background/Overview

The prevalence of cybersecurity threats and incidents has increased drastically over the past decade. Since 2020, cyberattacks have more than doubled globally.[1] Federal, state, local, and private organizations have all fallen victim to cyber-attacks with varying degrees of success. The current cyber threat landscape makes it imperative that organizations, private and public, have a well thought out cyber IRP in place. The Federal Government[2] has established guidelines for cyber IRPs in an effort to bolster organizations' cyber incident capabilities and resilience.

In this everchanging and complicated environment, cyber professionals are expected to protect their organizations and constituents from cyber threats. A well planned and trained IRP is a significant step towards cybersecurity preparedness and mitigation of cyber threats.

This request for proposal is seeking contract support to assess Northern Virginia localities' cyber IRPs and produce documents outlining the findings of the assessment. The final documents will include a summary regional report and jurisdictional annexes with specific findings and recommendations to be confidentially shared with the individual jurisdictions. The assessment will be conducted to ensure alignment and traceability with commonly accepted practices and plans, and applicable local, state, and federal guidance and laws.

[1] https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability#:~:text=Cyberattacks%20have%20more%20than%20doubled,experienced%20a%20much%20heavier%20toll.

[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf ; https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf

Contract support shall identify and document strengths, concerns, risks, and deficiencies based on assessments of locality plans. Additionally, contract support shall identify specific recommendations to aid localities in the improvement of their cyber IRPs. The documents shall also include information on how often the cyber IRPs are exercised, any challenges or inhibitors that may prevent testing, and recommendations on how to overcome potential challenges to testing. The documents shall include both applicable recommendations for the region and locality specific recommendations, shared confidentially with the relevant jurisdiction, of how to improve cyber IRPs. The documents should include all the above identified criteria and will be shared with the participating Northern Viriginia localities at the end of the project to ensure the findings can be utilized.

NVERS' subject matter experts will be utilized to validate the cyber IRP assessment outputs and ensure milestones and deliverables are being appropriately met.

Scope of Work and Technical Requirements

1. **Recurring project planning meetings.**
    a. Meet bi-weekly with project planning team members assigned by the Northern Virginia Cybersecurity Working Group to discuss project progress, needs, and direction.
    b. Collaborate with NVERS' regional partners to obtain regional cyber IRPs and related information.
    c. In coordination with the project planning team, validate project findings and direction prior to finalization of final documentation.
    d. Ensure tracking and timely follow up of action items for NVERS or planning team members arising from project planning meetings.

2. **Review and analyze Northern Virginia localities cyber IRP source material.**
    a. Analyze local Northern Virginia cyber IRPs and other relevant documentation to collect data on the strengths, concerns, risks, deficiencies, and federal, state, and local guidance adherence.

3. **Prepare written, cyber IRP assessment documents that identify cyber IRP best practices, potential gaps, limitations, strengths, and recommendations.**
    a. Contract support will coordinate with the project planning team to validate the written documents.
    b. The documents will address the cyber IRPs' best practices, potential gaps, limitations, strengths, and recommendations.

i. The documents will assess jurisdictional IRPs' adherence to the National Institute of Standards and Technology (NIST) SP 800-61 standards and practices.
    1. Additional standards such as the Cybersecurity and Infrastructure Security Agency (CISA) best practices and others identified by the project planning team should also be considered.
ii. Regarding training, the documents will note the frequency, deficiencies, strengths, and recommendations.

c. The documents will include recommendations for IRP improvement for the region as a whole, but also recommendations based on specific locality IRPs.
    i. A broad summary document will be produced for NVERS and the participating jurisdictions.
    ii. The locality specific recommendations annexes will be shared with the localities confidentially.

4. **Provide final cyber IRP assessment documents for utilization by participating Northern Virginia localities.**
    a. Contract support will provide final documents that identify the strengths, gaps, limitations, best practices, training standards, recommendations, and compliance with state, local, and federal guidelines of Northern Virginia cyber IRPs.

Access to References

For purposes of preparing a well-informed proposal to NVERS, prospective offerors may refer to NIST and CISA standards and practices previously referenced. Any additional questions can be directed to Jordan Meservy (Jordan.Meservy@nvers.org). If access to NVERS' subject matter experts or documentation is necessary, the offeror will be required to sign a non-disclosure agreement.

Project Timeline

This contract will begin on or around September 15, 2024 and terminate on April 30, 2025. Grant funding from the United States Department of Homeland Security (DHS) and Federal Emergency Management Agency (FEMA) will be used to support this effort.

Minimum Proposal Elements

1. Offeror's name, address, contact information, and subcontractor companies (if applicable).
2. A detailed timeline to complete the project, and any observed obstacles to completing the work.

3. A preliminary work plan that describes the phases or segments into which the proposed project can logically be divided and performed.
    a. This section should also contain a discussion of any changes proposed by the offeror that substantially differs from the project scope.
    b. This section should include detailed descriptions of activities that are to occur, significant milestones, and anticipated deliverables.
4. A statement of qualifications (i.e., organizational and staff experience, references, and personnel assigned to work on this project – including subcontractors).
5. A firm fixed-price cost proposal to complete all milestones and deliverables.

Proposal Evaluation

Responsive proposals will be scored and competitively evaluated to the maximum extent practical. The contract for this project will be awarded to the responsible offeror whose proposal is most advantageous to the project, in alignment with the weighted evaluation criteria listed below.

1. Cost – 10%
2. Demonstrated understanding of the project goals and deliverables – 20%
3. Offeror qualifications and experience with similar projects – 30%
4. Proposed methodology – 20%
5. Proposed key personnel – 10%
6. Comfort with the overall proposal – 10%

Billing Requirements and Product Ownership

The successful offeror will be required to furnish all necessary data elements that compose their periodic invoices in accordance with federal reimbursement guidelines. All created products associated with this project will be the property of NVERS and the contractor may not use any deliverables in the future without the expressed written consent of NVERS. Additionally, the successful offeror will be required to sign a Non-disclosure Agreement (NDA) prior to beginning work on the project.

Proposal Submission

An electronic copy of the proposal must be sent to Jordan Meservy (Jordan.Meservy@nvers.org), no later than Wednesday, August 14, 2024. Offerors may direct questions to the above-listed email address during the application period.