Request for Proposal

Introduction

Impact Washington is requesting proposals from qualified contractors to assist in conducting programmatic elements of initial cybersecurity & DFARs assessment and consulting for members of the Defense supply chain in Washington State to fulfill a related grant's requirements.

Key Dates

Deadline for submission of RFP responses: Friday, September 25, 2020

Work completion date: Monday, May 31, 2021

Table of Contents

Background

Impact Washington (IW) is a non-profit organization that provides competitive, value-driven services to enhance growth, improve productivity, reduce costs, and expand manufacturing capacity in Washington State. We are an affiliate of the National Institute of Standards and Technology's Manufacturing Extension Program (NIST MEP), and our solutions, consulting, and educational opportunities focus on the small & medium-sized manufacturers located throughout the state.

IW has been awarded a cybersecurity grant by the Department of Defense (DoD) Office of Economic Adjustment through the Washington State Department of Commerce, with the broad intent of strengthening Washington State Defense's cyber-security posture supply chain. Work performed under the grant will focus on two core elements – Cyber Independence and Cyber Resiliency.

The intent of Cyber Independence is to provide outreach to all known Defense suppliers in Washington to create awareness of DoD cybersecurity requirements and provide more in-depth training with at least 10% of that population.

Cyber Resiliency will focus on conducting broad and tactical asset-value based cyber assessments for 1% of the known Defense suppliers (19 companies), evaluating results, and providing recommendations for correction.

Further work under the grant will provide one-on-one support engagements with the 1% of the companies that have participated in the cyber resiliency element to move their negative resiliency responses to cybersecurity compliance.

Scope of Work

Nineteen (19) private companies will receive one-on-one support, as outlined in the introduction above. It is intended that the work will be divided between 3 – 5 contractors to build regional capacity and expertise in engaging the private market to benefit those companies involved in these initial engagements and establishing options to support the broader Defense supply chain in the future. Accordingly, each selected Contractor will receive contracts to work with 4 – 7 companies. IW has contracted a third party, Ignyte Institute (Ignyte), to provide self-paced, e-learning, and an assurance management platform for reporting and tracking client progress - the Ignyte Certification and Accreditation Platform (Platform).

The Platform manages compliance, vendor risk, business continuity, threat management, and learning management through a single interface for Small to Medium-sized Businesses (SMBs). Platform technology fully integrates with current standard SMB operational security toolsets such as Qualys, Tenable, KnowBe4, and other operational toolsets to ensure compliance. Included within the connector eco-system is full integration with DoD level tools such as SAM and Enterprise Mission Assurance Support Service (eMASS). This technology for the SMB will help accelerate compliance & cybersecurity processes end to end. The Platform is expected to be used by the bidder's analyst to complete SMB cyber tasks. Team members from Ignyte will provide training & on-boarding.

Impact Washington (IW) Engagement Methodology

Contractors must follow IW prescribed methodology in managing and leading the engagement.

- At the start of the engagement, IW will provide proper scoping information.
- The Contractor must identify themselves to IW as potential future "CMMC Auditor" and/or "Registered Consultant."
- IW is to lead as the primary Contractor and provide back-end support for managing contractual obligations with the selected private company.
- IW will provide all contract documentation to support cyber activities for the target SMB.
- Leverage the use of the Platform. Platform training and usage will be provided directly to the assigned security analyst.
- A single license of the Platform will be assigned to the organization.
- Project reporting, performance tracking, and work-products deliverables are the be captured within the Platform.
- Report & debrief IW assigned project manager on tasks & work completed.
- Complete a brief project plan per organization provided by IW team before engagement starts.

Initial Cybersecurity & DFARs Assessment Scope of Work

Each engagement must quickly capture and assess the following within each private organization leveraging the Platform:

- Organization chart
- Organization departments
- Organization locations
- Current IT and/or security policies (if any)
- Current known Security Classification Guides as provided by DoD (if any)
- A complete Asset Inventory, including the following elements:
    - Hardware (Servers, network devices, end-user devices)
    - Critical Business Software
        - SaaS Services, ERP systems, etc...
- The following critical asset inventory attributes must be identified:
    - CUI and CUI Type (a list of CUI and CUI type will be provided)
    - Sensitive business information according to a standardized classification scheme within the Platform
    - Relate all assets with organizational departments & locations
    - Determine the qualitative impact of business systems
        - Determine the cyber impact of business systems based on C, I, A values
    - Capture other attributes such as RTOs & RPOs per asset as optional attributes
    - Capture additional optional asset attributes such as known vulnerabilities, EOL, etc... (optional attributes for assets containing aggregated CUI). Please see the intrusive technology section on determining vulnerabilities.
    - A complete asset record is desired; however, assets that contain CUI shall be the focus of the assessment.
- Policy & Documentation records per organization:
    - Place all documents collected within a structured folder system within the Platform
        - Policies, Procedures, Guidelines, Evidence, CUI Contract Documents

- Promote the training provided by Impact Washington to reduce the cost of training for the assigned SMB.
- Capture training records from the Ignyte LMS and place it within the compliance area, specifically the "Awareness & Training" domain of CMMC and/or NIST 800-171.
- Conduct an Initial Draft CMMC framework assessment based on level 3. An initial evaluation must include the following:
    - Review of each requirement by the assigned security analyst.
    - Provide an expert opinion summary response per requirement based on discussion with the private company.
    - Capture each requirement's current status according to the CMMC draft framework (Performed, Documented, Managed, Reviewed, Optimized).
    - Attachments of any documentation provided by the organization to each NIST 800-171 requirement. Documentation should be uploaded to structured folders as well as provided within the Platform.
- Any NIST 800-171 requirement with the current status of “Performed” a POA&M will be automatically generated.
- A recommendation on how to "document" the requirement shall be provided within the POA&M summary section. A recommendation must include the following:
    - Recommended policy & procedure name for gap closure and a brief description of the policy and/or missing procedure.
    - Optional automation technologies can be recommended within the control/practice statement and/or within the POA&M. However, if an organization is missing critical documentation, it must be identified within the automatically generated POA&M.
- Company SSP and POA&M will be automatically generated by the Platform based on structured work completed for the SMB.
- A client level, analyst level, and multi-level per company dashboard will be automatically generated based on the work completed.
- The estimated level of effort per requirement range shall be provided to IW for determining the competitiveness of your offer and understanding of your draft CMMC requirements.

Usage of Impact Washington Resources Provided

One of this grant's fundamental goals is to help SMBs by leveraging resources provided under the grant. The Contractor shall leverage these resources as part of the engagement as cost reduction efforts include the following. Over time, IW will release additional resources to benefit the IW community:

- CMMC self-paced, e-learning courses
- CMMC pre-assessment tool kit (if required)
- Ignyte pre-certification Platform to create a system of record
- Provided project plan (if required)
- Provided scoping worksheet
- Policies and procedures templates (as developed over time)
- Outline or IW Team members (account manager, project managers & collaborative cyber partners)

Intrusive Technology Usage limitations and Basic Rules of Engagement

IW has determined that the highest need is to help SMBs prepare for winning future defense contracts while helping retain current agreements is to ensure robust DoD contract activity and a healthy local State of Washington economy.

This goal is achieved by assisting SMBs to prepare for executive risk management & cyber assurance activities primarily and technical security operational tasks as secondary items.

IW also has determined that it does not desire to engage in high-profile attacks, threat modeling, defense and offensive security exercises, web-application attacks, and external inspection scoring systems targeted at small businesses.

This preparation includes leveraging a basic rating system to inspect the small business website, SSL certificates checks, external corporate traffic, etc.… that may not contain any sensitive information, including CUI. It also includes conducting & interpreting vulnerability tests that could lead to the exploitation of a small business network. The essence and intent of this sort of activity is captured within the asset-value based portion of the Initial Cybersecurity & DFARs Assessment Scope of Work.

Determination of location CUI, aggregation of CUI, assets cyber impact, business impact, and asset value to the organization will set the potential scope of technical surveillance, continuous monitoring, penetration testing, vulnerability testing, threat modeling, and similar operational security work in the near future. Engagement should be focused on management level cyber risk & assurance management coaching to increase local manufacturing leaders' technical literacy before engaging in highly specialized activities that lead to minimal value without management support.

Expected Work-Products and Deliverables

To be delivered & organized within the Platform

- Summary response per DFARs and/or Draft CMMC Requirement (estimated 130 requirements for Level 3)
- POA&M responses & corrective recommendations within POA&M (where applicable)
- Critical Asset inventory with up to 20 crucial attributes per asset
- Current documentation (policies, procedures, screenshots, evidence of meeting requirements) from the organization.
- Reference of relevant documents to each requirement

Work Location and Execution

IW recognizes the impact of COVID-19 and envisions that this entire engagement could be delivered remotely, with assessments conducted via teleconference calls. However, agreement with IW, Contractor, and on-site client work can be done assuming State-mandated safety measures are in place and observed.

Pricing and Level of Effort

IW goal is to build a regional capacity of expertise for both current and future partner work through Impact Washington to help grow the state's defense industrial base. Your proposal should reflect pricing based on the level of effort and required analyst skillset. The price should be provided as a range per company based on the target market that IW traditionally serves and scope described within the Initial Cybersecurity & DFARs Assessment Scope of Work paragraph.

IW Target Market

IW serves constituents with the following characteristics:

- Typical organization size of 10 – 200 employees
- Typically led by a non-technical business leader with a strong manufacturing background
- Small IT staff (1-3 people) and /or completely outsourced IT staff
- 1 to 50 Critical Assets that may contain CUI and/or sensitive business information

Questions

We invite didders to submit written questions and requests for clarifications regarding the RFP. IW assumes no responsibility for verbal representations made by its officers or employees unless such representations are confirmed in writing and incorporated into the RFP. Any ambiguity regarding this RFP must be addressed through this question and answer process. Bidders are not permitted to include assumptions in their bid proposals. Please direct all your questions to IW via email at Geoff Lawrence glawrence@impactwashington.org

Rejection of Bid Proposals

IW reserves the right to reject any or all bid proposals, in whole and part, and cancel this RFP at any time prior to executing a written contract. Issuance of this RFP in no way constitutes a commitment by the IW to award a contract.

Disqualification

IW reserves the right to reject outright and not evaluate proposals for any one of the following reasons:

- The bidder states that a service requirement cannot be met.
- The bidder fails to deliver the bid proposal by the due date and time.
- The bidder fails to deliver the detailed cost section.
- The bidder's response materially changes a service requirement.
- The bidder’s response limits the rights of the IW
- The bidder initiates unauthorized contact regarding the RFP with IW partners and employees.
- The bidder provides misleading or inaccurate responses.

Reference Checks

IW reserves the right to contact any reference to assist in evaluating the bid proposal, verify the information contained in the bid proposal, and discuss the bidder's qualifications and the qualifications of any subcontractor identified in the bid proposal.

Information from Other Sources

IW reserves the right to obtain and consider information from other sources concerning a bidder, such as a bidder's capability and performance under different contracts.

NDA Signature Required

Bidder must sign an NDA with IW, private companies, and IW partners to protect IW resources, company sensitive information, and partner resources provided to contractors to fulfill this grant's requirements.

Contractor Conflict of Interest

The bidder shall submit any Conflict of Interest information to IW regarding IW ability to partner with other cybersecurity teams. For this contract's purposes, the conflict of interest definition includes direct or indirect relationships, including, but not limited to, the Contractor and its parent company, subsidiaries, affiliates, subcontractors, clients, and principals.

Proposal Submission Instructions and Due Date

The bidder's proposals must be sent via email by close of business **Friday, September 25, 2020** to:

Impact Washington
Geoff Lawrence
glawrence@impactwashington.org

The bidder's proposal must include the following areas:

1. Title page
2. Overview of your our work experience in cybersecurity and your organization's experience
    a. Expected goal to become a consulting organization and audit organization (C3PAO)
3. Scope of work with all the sub-sections addressed.
4. Expected Deliverables
5. Estimated timelines & cost per company assessment

Evaluation Criteria

The Impact Washington Panel Review will evaluate each proposal individually against the following criteria, listed below in order of importance, and not against competing bids. Please use the below criteria as a reference but do not structure your proposal according to the sub-sections.

1. Cost-effectiveness & best value for small businesses.

IW strongly encourages bidders to demonstrate project cost-effectiveness in their approach, including examples of leveraging IW institutional and other resources. However, cost-sharing or other examples of leveraging other resources are not needed. The inclusion of cost-sharing in the budget does not result in additional points awarded during the review process. Budgets should have low and reasonable overhead

and administration costs, and applicants should provide clear explanations and justifications for these costs concerning the work involved. All budget assessment items need to be explained and justified to demonstrate necessity, appropriateness, and connection to the project objectives.

2. Technical approach

IW encourages bidders to demonstrate their technical approach per the Scope of Work Expected Work-products & Deliverables. A substantial bidder will include a clear articulation of how the assigned analyst will complete the desired activities to contribute to the overall IW cybersecurity project objectives as part of a single seamless team working with up to 5 small businesses.