Port of Port Angeles IT Continuity of Operations Plan Questions and Answers

In the statement of work section regarding cyber incident response, we saw this as a different deliverable then the business continuity plan (BCP). We see the BCP as a documented set of procedures and protocol to follow in the event of disastrous event such as database corruption, sprinkler pipe break in the data center, earthquake, etc. When we saw the cyber incident response section, it mentions a "cyber incident response plan" which we see as another document of procedures and protocol to follow should there be a security breach such as a virus infection, hacking attack, ransom-ware attack, and other attacks from various threat agents. Are we reading this correctly or does the Port want the BCP to cover procedures and protocol to recover from a cybersecurity event as one of the possible scenarios?

Yes – we would like the IT continuity of operations plan to cover all scenarios – from sprinkler pipes to cyber-attacks. The intent of the grant funding we are using is to improve our ability to recover from any type of event that would disrupt operations at our Port.

For the information systems business impact analysis (BIA), the statement talks of "The plan…" and then the second sentence states, "The report should identify vulnerabilities, threats, and risks to the Port information systems." This seems like two different deliverables – the BIA (which identifies critical functions and systems for recovery prioritization) and a risk assessment report that identifies vulnerabilities, threats, and risks to the Port information systems. Is this correct OR does the Port want us to integrate the risk assessment piece into the BIA?

Yes – these could be considered two different deliverables. An assessment that identifies risks, and a plan that outlines how to deal with those risks in the event they occur.

What if we find based on the BIA that the Port does not have the infrastructure/systems available to support the recovery time objectives (RTOs) and recovery point objectives (RPOs) as specified by the business units that depend on the systems? For example, finance and accounting requires an RTO of 8 hours; however, the Port's actual recovery time capability is more like 24-48 hours after a disaster. Is it expected that we would develop the BCP based on the existing infrastructure or with a different, planned solution (e.g., alternate DR site) that the Port would need to implement?

We would expect a plan based on our existing infrastructure along with suggestions of how we could improve.

Do we need TWIC card in order to perform this work at the Port? I ask because other Port work we've done have mentioned the TWIC card as a possible requirement.

No, I do not anticipate TWIC cards being needed. We have little to no IT infrastructure within our TWIC secured areas.

Under the minimum qualifications section, it states "The firm selected by POPA…..must meet all requirements of firms qualified to receive federal grant funds, including debarment qualifications." Could you please clarify this requirement a bit more and give examples of firms that would fit this criteria?

The debarment issue is the primary consideration. Any firm that is currently debarred or has been debarred from receiving federal funds in the past 3 years would not be eligible for this federal grant funded project.

Under the Proposed Job Arrangement Letter section, it states "The proposal must include examples of the job arrangement letters your firm would require covering this engagement….." I am unclear on what is meant by "job arrangement letters." Is this an engagement letter? Could you provide further clarity or examples?

Yes – an example of an engagement letter would cover this requirement

Are you able to provide any details about the technology environment at the Port that would be in scope of the engagement?

- Number of connected sites **6**
- Number of servers **3**
- Percentage of servers that are virtualized **100%**
- Server operating system platform in use **MS Windows Server 2012 R2 Std**
- Type of storage platform in use **All server based hard drives**
- Does the Port utilize cloud-based service providers for any critical applications? **No**
- Number of critical business applications – **Not sure, part of the goal of this project is to figure what our critical application are**
- Number of IT staff and their roles **0 – IT support is outsourced to a local vendor**
- Number of end users **+/- 40**

1. What is the size or your organization? We generate approximately $10 million per year in revenue spread over multiple business lines including marinas, airports, and industrial property rentals. Further information can be found on our website www.PortofPA.com.
    a. Number of locations? We have 5 locations that have access to our IT system.
    b. Location proximity - if multiple locations? All within a 20 mile area.
    c. Number of Employees? 40-50 depending on the season and business activity

2. Does your organization have a single / common set of information security policies and procedures? If no, please explain. No we do not, this is another project being undertaken at the same time.

3. Do you have any internal or external deadlines that you are trying to manage to? This project is funded under a federal Port Security grant and we have 3 years to complete it. We expect this specific project to be completed much sooner than 3 years.

4. What type of sensitive data does you store, process, or transmit (ePHI, PII, PCI, other business sensitive information)? Employee HR data (banking and social security numbers), customer data (tax ID numbers and banking data), and other business related items.

5. What compliance framework(s) do you follow or are looking to follow (HIPAA, EI3PA, SOX, COBIT, PCI, NIST, ISO, other)? NIST is the framework as specified by the US Coast Guard.

6. Does your organization utilize Cloud services and, if so, how? No we do not.

7. How many servers are in use? 3 primary network servers and 3 site specific servers.

8. What percent of IT operations is in a virtualized environment (VMware, Hyper-V, other)? The 3 primary servers are all Hyper-V.

9. How many databases support the in-scope applications? The primary data base is Microsoft Dynamics SL2015, plus a few other small applications.

10. What are the operating systems for the servers (MS, UNIX, Linux, AS400, etc.)? Microsoft Windows Server 2012 R2 Std

11. What is the primary OS platform (MS, Linux, other)? Microsoft.

12. Does segmentation exist within your organization's networking environment? If so, how is it achieved (VLAN, Firewall, etc)? No

13. Is any part of the networking environment outsourced? No

14. Are there third parties, outsourcers, or business partners connecting to the network? Yes – our general IT support is outsourced to a local vendor and there are a couple other software support vendors that connect remotely as well.

15. Has your organization completed the following within the last year? If so, please provide approximate complete date.

    a. Internal Network Vulnerability Scan and Penetration Test No – planned soon.

    b. External Network Vulnerability Scan and Penetration Test No – planned soon.

1. Is this work completely focused on the Information Systems function? Yes
   If so, in order to prioritize recovery among critical functions and systems, it will be helpful to have available the results of POPA's most recent business impact analysis (BIA), to understand the business's requirements for IT resources, applications and services. Will that BIA data be made available to the contractor? A BIA has not been completed, and our expectation was that this engagement would include a BIA to the extent needed to plan our cyber COOP.

2. Is the report that identifies vulnerabilities, threats, and risk to Port information systems to be an "environmental" risk assessment or also a "cyber risk assessment"? How "deep a dive" does the Port perceive that this cyber risk assessment need to go (e.g. high level risk assessment, deep pen tests/scans, black/white hat tests, etc.?) No – we are just starting a separate cyber risk assessment and the intent of this project is to develop appropriate recovery plans if we were to experience an adverse IT event.

3. Is the Port open to developing the cyber incident response plan as a cloud-hosted website hosted outside POPA's firewall for optimal access under disruptive events? Most likely not, based on our geographical location we would expect a prolonged connectivity loss to the internet in the event of a natural disaster.

4. Is the "Job Arrangement Letter" mentioned in Section 2. D. referring to the "letter of engagement" that defines the contractor's relationship with POPA and the scope of work, timetable and fees? Yes

1. On the State of Washington WEBS system, POPA's solicitation posting lists $30,000 as the Estimated Value (see below). Is this the Not-To-Exceed (NTE) budget for the project, or is there another amount that is relevant? This was our initial estimate and there are no other relevant amounts.

2. On page 2, the RFP states that POPA will begin a "3-6 month relationship." Can you elaborate on this timing, please? We ask since this is a wide span of time and we are wondering if this is because of other priorities of POPA staff in that they may not always be available for interviews and facilitated sessions. Do you envision the successful vendor performing continuous work in the 3-6 month window you state? Yes – we expect a continuous engagement once the project is started. The timeframe could be less but that is not a requirement for this project.

3. Under the section *Proposal Submission Guidelines* (page 4), we believe there may be a typo. We believe POPA meant the proposal deadline to be December 18, 2015 @ 5:00 p.m. Please confirm this. That is correct.

4. In the section *Questionnaire and Written Responses*, *Item D* (page 5), can you please elaborate what is meant by "job arrangement letters"? In our experience working with our government clients, we work under a written contract, and part of that contract is a *Statement of Work* (SOW). The SOW documents what work will be performed, what the responsibilities are between the vendor and client, what deliverables are expected and (usually) what payment milestones are defined. Is this what POPA means when it refers to a job arrangement letter? If not, please explain. Yes, a SOW and or engagement letter was the intent.

5. Is the funding for this project through a grant or similar mechanism? If yes, can you identify the grantor and if there are any terms or conditions (including milestone dates) that might be relevant to the successful vendor and the work to be performed? This project is 75% funded by a Port Security Grant from FEMA / Homeland Security. We have 3 years to complete the project and we are not allowed to use any vendors that have been excluded from federally funded projects.

6. How many POPA staff members do you expect to be part of the project team? If different, how many staff members would you consider to be subject matter experts that should be interviewed? I will be the primary POPA staff member with relevant information coming from our Finance Manager, Accounting Manager, CEO, and our outsourced IT support vendor (Albright networks).

7. If POPA has documented its business processes, can these be shared prior to the proposal due date? How many processes are there (documented and/or undocumented)? This has not happened.

8. Is there an existing Business Continuity Plan or similar asset that has been developed in the past? If yes, when was it finalized? No – there is no BCP yet.

1. Does the scope of the RFP anticipate the inclusion of a Vulnerability Assessment and Penetration Test? No – prior to this engagement there will be a specific risk analysis to identify risks and opportunities

2. For the Cyber Incident Response portion of the RFP, does POPA have a prescribed computer security incident response capability (CSIRC) methodology in mind? (e.g. NIST Computer Security Incident Handling Guide or American Institute of Certified Public Accountants Incident Response Plan). NIST

3. What is the budgeted amount that POPA has earmarked for this Information Systems Business Continuity Plan (ISBCP) project? $30,000

4. Has POPA contemplated outsourcing the Security Operations for Incident Response as an alternative to developing their own Cyber Incident Response process? Contemplated? Yes, but concerned about geographical isolation issues and ability to connect to distant backup sites.

5. How many Business Functions and sub departments will be included in the BIA? Purchasing, HR, Payroll, Accounting, ??

6. For the "Information systems backup and recovery - The resulting plan should formulate methods to ensure that systems and critical functions can be brought back online in the event of a disruption.": Is this a request for a backup and recovery strategy and later implementation or is this a request for a DR Plan now? DR plan now

7. Can you provide the following information about your environment today?

Application environment high level questions:

- No of applications that need protecting, with a brief description of each General Domain, MS Dynamics SL2015, Access/Gate control software (Topaz), camera control and recording (Milestone)
- Are the applications Internet facing, or are they accessed only via a private network? 95% via private network – one online credit card access point from internet
- Is your environment virtualized? If so what is the percentage of virtualization? 100% virtual
- If you are currently employing virtualization technology, what hypervisor do you use? (ESX, Hyper-V, KVM, or Xen) Hyper - V
- Are there any applications that can't be virtualized? No
- Are you under regulatory compliance (eg. FISMA/Fedramp, PCI, HIPAA), and would the DR facility need to comply with such regulations as well? Following NIST framework for FEMA/Homeland Security/Coast Guard
- Describe your AD environment Single domain, multiple domain controllers at 2 locations

Server Information:

- Do you have a detail CMDB? No
- Server details
    - Make/model of server HP Proliant DL380
    - number cores 8
    - amount of MEM 64GB
    - amount of internal disk space 4TB
    - amount of external disk (if any) 0
    - number and type of adapters std 1GB NIC
    - OS release / version 2012 Std R2

Data Bases:

- Type(s) of Data bases and Version (i.e. Oracle Standard or Enterprise and the version) SQL 2015
- What is the current replication strategy between primary and secondary sites (i.e. data guard, data log transfer, mirroring, etc) mirroring
- How often is the data replicated? Real time
- Storage Size of the data base? Less than 100 GB
- Who currently manages the databases? i.e. 3rd party or in-house 3rd party out-source
- How do you manage the change process between Primary and Secondary site? N/A

Production SAN storage information (this will be used to size Target SAN storage)

- How is your storage presented to systems? (fiber, iSCSI, NFS)? NA
- What is the make/model of the SAN storage? NA

- We will need high level disk config info (storage capacity, size & speed of drives, amount of cache, # of ports, etc) NA
- What is the replication method currently being used? NA
- Amount of data to be protected? NA
- Volatility (rate of change) of the data to be protected? NA
- Estimate yearly rate of growth? NA
- Is any storage virtualization being done? No
- Who currently manages the storage? i.e. 3rd party or in-house NA
- Do you have the same storage set up in both the primary and secondary sites? NA

Network:

- Are you using any load balancing today? No
- Will data encryption be needed across the WAN (replication circuit) yes
- Estimated bandwidth for data replication (if unknown we will estimate from data provided above) unknown
- For user access how much internet bandwidth is required 100 MB
- Will VPN access be required Yes

Security:

- How will you be accessing your DR site? VPN over internet? MPLS? MPLS (private VLAN on local network)
- Will edge firewalling / IDS/IPS / Web application firewalling / Threat mgmt. services be needed in your DR? yes
- Data encryption required at the server level? yes
- Does your DR need to be PCI compliant? No
- What method of authentication is required? 2 factor, single sign-on? 2 factor

1. Does POPA have an internal resilience team or crisis management team? No we do not.
2. Does POPA have any documented policies/practices in place related to Resilience or Business Continuity? None.
3. Are there any existing incident response plans for recovery of business processes? If so, will these be shared upon award? None
4. What is the approximate total number of systems/functions within POPA that need to be evaluated? Approximately 6 – Accounting, HR, Payroll, Purchasing, Access Control, Camera Control
5. Are there any vendor/externally hosted systems? No
6. What is the expected budget for this initiative? $30,000
7. Has a steering committee been established to support this initiative? No