C**ity of Seattle Request for Proposal #DIT 130067**

**PRISEM System – IT Research and Development Project for**

**Visualization and Analysis of Cyber Attack Traffic**

**Addendum One**

**05/13/13**

The following is additional information regarding Request for Proposal DIT 130067 released on May 1, 2013. This addendum includes both questions from prospective proposers and the City’s answers, and revisions, if any, to the RFP. This addendum is hereby made part of the RFP and therefore the information contained herein shall be taken into consideration when preparing and submitting a proposal.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Item # | Date Received | Date Answered | Vendor’s Question | City’s Answer | RFP Revisions |
| 1 | 5/10/13 | 5/13/13 | City of Seattle uses the word "Portal". Does City of Seattle mean the McAfee/Nitro ESM Console?  | Yes. |  |
| 2 | 5/10/13 | 5/13/13 | "Nitro Threat Center" is called out.  Please describe what this is?  | Nitro ThreatCenter (formerly known as Log Matrix CommandCenter) is the user interface portal for a security information and event management (SIEM) system. It processes real-time log events collected from numerous Log Matrix Collectors including data from security devices, network devices, identity stores, data stores, and business services from across the enterprise.The SEIM performs real-time event correlation and generates alerts which the ThreatCenter portal displays to the user. It also allows the user to create reports of both real time and recent historical data without writing complex SQL queries and trying to merge multiple device logs. Combined with LogCenter, the same reports can be run against longer term data for compliance reporting and forensic analysis.  |  |
| 3 | 5/10/13 | 5/13/13 | Please clarify the statement "Consultant must meet system requirements for command line capabilities within Nitro Portal and SOD Portal."  |  | Paragraph One of RFP Section 7.1 and Contract Section 3.1 are amended to read: “Develop and Implement Specialized Views: The Consultant shall research US-CERT requirements and current vulnerability trends applicable to log collection. For fifteen provisioned jurisdictions, the Consultant shall assist the City in developing new capabilities list for specialized views of log collection services. Log collection services must meet Nitro Collector specifications. The Consultant will implement the specialized views of the log collection services. The Consultant will research and document prior code development as well as all design and configuration changes. The Consultant shall activate Nitro Portal following established data model and project team requirements. Portal functional features will be the same in two ((~~Nitro Portal, SOD Portal, and any other~~)) portals as determined by the City. |
| 4 | 5/10/13 | 5/13/13 | The consultant shall "develop code and implement 2-way alerts for selected security traffic between PRISEM and US-CERT."  What code language does City of Seattle use?  | The choice of programming language is not material. This will be performed using the STIX/TAXII protocols developed by Mitre Corporation.    |  |
| 5 |  | 5/13/13 |  |  | Paragraph One of RFP Section 7.4 and Contract Section 3.4 are amended as follows:Integrate CIF and NetFlow Botnets Detection System: The Consultant shall develop and implement code within PRISEM that provides integration with CIF and NetFlow Botnets Detection system. This includes exporting alerts from the Nitro Threat Center into CIF, and enriching Threat Center alerts to include contextual historical data from within CIF. Consultant must meet system requirements for command line in two portals as determined by the City ((~~capabilities within Nitro Portal and SOD Portal~~)). |
| 6 |  | 5/13/13 |  |  | RFP Section 7.5(1) and Contract Section 3.5(1) are amended as follows:Five test alerts are successfully received by US-CERT Verification verifying that the protocol successfully integrated ((~~database consolidation is functional and operational~~)) |