

**IFB STPD 12-001-B**

**Statement of Work**

**FOR CALNET 3, CATEGORY 7**

**NETWORK BASED MANAGED SECURITY**

**TECHNICAL REQUIREMENTS**

**ADDENDUM 4**

November 26, 2013

Issued by:

**STATE OF CALIFORNIA**

California Department of Technology

Statewide Technology Procurement Division

PO Box 1810

Rancho Cordova, CA 95741

Disclaimer: The original PDF version and any subsequent addendums of the IFB released by the Procurement Official of this bid remain the official version. In the event of any inconsistency between the Bidder's versions, articles, attachments, specifications or provisions which constitute the Contract, the official State version of the IFB in its entirety shall take precedence.

**IFB STPD 12-001-B**  
**PART 2**  
**BIDDER RESPONSE**

---

**Statement of Work (SOW)**

**Category 7**

**Network Based Network Security  
Technical Requirements**

## TECHNICAL REQUIREMENTS

### CATEGORY 7—NETWORK BASED MANAGED SECURITY

#### TABLE OF CONTENTS

<b>TECHNICAL Requirements</b> .....	<b>1</b>
<b>CATEGORY 7—NETWORK BASED MANAGED SECURITY</b> .....	<b>1</b>
<b>7.1 OVERVIEW</b> .....	<b>1</b>
7.1.1 BIDDER RESPONSE REQUIREMENTS .....	1
7.1.2 DESIGNATION OF REQUIREMENTS .....	1
7.1.3 PACIFIC TIME ZONE .....	2
<b>7.2 NETWORK BASED MANAGED SECURITY SERVICES</b> .....	<b>2</b>
7.2.1 DDoS Detection and Mitigation Service.....	2
7.2.1.1 DDoS Initiation.....	3
7.2.1.2 DDoS Activities.....	3
7.2.1.3 DDoS Detection and Mitigation Web Portal and Reporting.....	5
7.2.1.4 DDoS Detection and Mitigation Features.....	6
7.2.2 Email Monitoring and Scanning Services .....	12
7.2.2.1 Email Monitoring and Scanning Service Functionality .....	13
7.2.2.1.1 Anti-Virus Protection .....	13
7.2.2.1.2 Anti-Spam Protection .....	14
7.2.2.1.3 Content Control.....	15
7.2.2.1.4 Isolation Area .....	16
7.2.2.2 Email Monitoring and Scanning Service Web Portal and Reporting	17
7.2.2.3 Email Monitoring and Scanning Service Features .....	17
7.2.3 Web Security and Filtering Service.....	22
7.2.3.1 Authorized User Administration and Reporting - Web Portal .....	23
7.2.3.2 Web Security and Filtering Service Features .....	24
7.2.4 Security Information and Event Management (SIEM) .....	24
7.2.4.1 SIEM Web Based Security Dashboard .....	34
7.2.4.2 SIEM Features.....	38
<b>7.3 SERVICE LEVEL AGREEMENT (sla)</b> .....	<b>41</b>
7.3.1 SERVICE LEVEL AGREEMENT FORMAT .....	41
7.3.2 TECHNICAL REQUIREMENTS VERSUS SLA OBJECTIVES .....	41
7.3.3 TWO METHODS OF OUTAGE REPORTING: CUSTOMER OR CONTRACTOR	42
7.3.4 BIDDER RESPONSE TO SERVICE LEVEL AGREEMENTS.....	42
7.3.5 CONTRACTOR SLA MANAGEMENT PLAN .....	42
7.3.6 TECHNICAL SLA GENERAL REQUIREMENTS .....	43
7.3.7 TROUBLE TICKET STOP CLOCK CONDITIONS .....	44
7.3.8 TECHNICAL SERVICE LEVEL AGREEMENTS .....	47
7.3.8.1 Availability (M-S).....	47
7.3.8.2 Catastrophic Outage 2 (CAT 2) (M-S).....	48
7.3.8.3 Catastrophic Outage 3 (CAT 3) (M-S).....	49
7.3.8.4 Email Monitoring and Scanning Services—Average Delivery Time (M-S).....	50
7.3.8.5 SIEM Event Notification (M-S).....	51
7.3.8.6 DDoS Customer Notification (M-S) .....	52
7.3.8.7 Excessive Outage (M-S) .....	53
7.3.8.8 DDoS Time to Mitigate (M-S) .....	54
7.3.8.9 Notification .....	55
7.3.8.10 Provisioning (M-S) .....	56

7.3.8.11	Time to Repair (TTR) (M-S).....	58
7.3.8.12	Unsolicited Service Enhancement SLAs .....	59
7.3.8.13	Proposed Unsolicited Offerings .....	59
7.3.8.14	Contract Amendment Service Enhancement SLAs.....	59

## TECHNICAL REQUIREMENTS

### CATEGORY 7—NETWORK BASED MANAGED SECURITY

#### 7.1 OVERVIEW

This Category 7 IFB provides the State's solicitation for best value solutions for Network Based Managed Security services.

The IFB will be awarded to Bidders that meet the award criteria as described in IFB Section 4. The CALNET 3 Contract(s) that result from the award of will be managed on a day-to-day basis by the CALNET 3 Contract Management and Oversight (CALNET 3 CMO).

#### 7.1.1 BIDDER RESPONSE REQUIREMENTS

Throughout this IFB, Bidders are required to acknowledge acceptance of the requirements described herein by responding to one (1) of the following:

Example A (for requirements that require confirmation that the Bidder understands and accepts the requirement):

*"Bidder understands the Requirement and shall meet or exceed it? Yes\_\_\_\_\_ No\_\_\_\_\_"*

Or,

Example B (for responses that require the Bidder to provide a description or written response to the requirement):

*"Bidder understands the requirements in Section xxx and shall meet or exceed them? Yes\_\_\_\_\_ No\_\_\_\_\_"*

*Description:"*

#### 7.1.2 DESIGNATION OF REQUIREMENTS

All Technical Requirements specified in this IFB Section are Mandatory and must be responded to as identified in IFB Section 3.4.2.5 by the Bidder. Additionally, some Mandatory requirements are "Mandatory-Scorable" and are designated as "(M S)". The State will have the option of whether or not to include each item in the Contract, based on the best interest of the State. Furthermore, Customers will have the option whether or not to order services or features included in the Contract. Service Requests for some CALNET 3 services or features may require CALNET 3 CMO approval.

Costs associated with services shall be included in the prices provided by the Bidder for the individual items included in the Cost Worksheets. Items not listed in the Cost Worksheets will not be billable by the Contractor. If additional unsolicited items include the features described in the IFB and are not included as billable in the Cost Worksheets, the cost associated with the features shall not be included in the unsolicited price.

Services and features included in the Cost Worksheets are those that the Bidder must provide. All Bidders must provide individual prices as indicated in the Cost Worksheets in the Bidder's Final Proposal. Items submitted with no price will be considered as offered at no cost.

### 7.1.3 PACIFIC TIME ZONE

Unless specific otherwise, all times stated herein are times in the Pacific Time Zone.

## 7.2 NETWORK BASED MANAGED SECURITY SERVICES

### 7.2.1 DDoS Detection and Mitigation Service

Contractor shall provide a network based Distributed Denial of Service (DDoS) detection and mitigation service. Detection and mitigation shall occur in the Contractor IP backbone before traffic reaches Customer edge router. Contractor shall establish normal traffic patterns and to minimize false positives during the detection/mitigation process and perform periodic “tuning” of normal traffic patterns established. The Contractor shall analyze, identify, report and alert on anomalies in Customer traffic and DDoS attacks. Upon detection of DDoS attack, Contractor shall reroute traffic to a network based mitigation center where DDoS attack packets are identified and dropped. Valid packets shall be routed to the Customer edge router. Upon Contractor determination that the DDoS attack has subsided, Contractor shall restore the normal routing of Customer traffic.

**Bidder shall describe its DDoS offering.**

*Bidder understands the requirements in Section 7.2.1 and shall meet or exceed them?*

Yes   Y   No       

*Description:*

***CenturyLink DDoS Mitigation Service is available to CenturyLink customers that want an additional level of protection on their CenturyLink Internet Ports. The service provides network-based detection and mitigation of Distributed Denial of Service (DDoS) attacks. The DDoS mitigation service is provisioned per Centurylink Internet port that is being protected.***

***CenturyLink DDoS Mitigation Service monitors and identifies threats, validates those threats with you the customer, and then takes action on validated threats to keep you connected. The attack mitigation takes place within the network-based mitigation infrastructure. The malicious traffic is filtered in the CenturyLink network before it reaches your network, while valid traffic is allowed to pass.***

***CenturyLink deploys multiple layers of defense for DDoS attack mitigation. We mitigate the DDOS attack up to capacity of our network and do not impose per customer limits.***

***We mitigate distributed attacks via the scrubbing platform. In addition to the scrubbing capacity, we can mitigate certain types of DDOS attacks by deploying filters via FlowSpec on our borders/edges/peering points that can drop significantly more traffic. For large size attacks FlowSpec based filters can be the first line of defense.***

*Also, we want to communicate a slight variation in how some of the competitors offer the service. We will mitigate the attacks up to our capacity in our network. As we upgrade our mitigation capacity, the customer will automatically benefit from that new capacity. Some of the competitors sell DDoS mitigation up to certain BW level that you purchase. For example, when you buy 2Gbps mitigation service from such a competitor, they will clean DDoS attacks up to 2Gbps. If the attack exceed that, they will drop that extra good and bad traffic. In our case, we would clean the attack up to our network capacity, that we upgrade as DDoS attack needs dictate.*

**CenturyLink DDoS Mitigation service benefits:**

- *Detects DDoS attacks*
- *Helps remove malicious traffic while allowing legitimate business traffic to pass through*
- *Mitigates malicious traffic in the CenturyLink network before it floods your private network*
- *Improves service availability of your business*

#### 7.2.1.1 DDoS Initiation

The Contractor shall support the initiation of DDoS mitigation described below:

1. Customer identifies the DDoS attack and initiates the mitigation; and,
2. Contractor identifies the DDoS attack and initiates the mitigation.

*Bidder understands the requirements in Section 7.2.1.1 and shall meet or exceed them?*

Yes   Y   No       

*Description:*

***DDoS Mitigation service is offered as a shared service.***

***CenturyLink identifies—Proactive Shared DDoS Mitigation service—CenturyLink continuously monitors for non-conforming traffic – when it is detected, your agency is alerted, and when your approval is given, CenturyLink begins rerouting the traffic for scrubbing.***

#### 7.2.1.2 DDoS Activities

The Contractor shall perform the following activities:

1. Monitoring of Customer traffic patterns;
2. Establishment of network traffic baselines;
3. Detection of Customer traffic anomalies;
4. Scrubbing of Customer traffic by dropping DDoS attack packets;

5. Perform detection and anomaly analysis;
6. Develop and provide access to a strategy for identifying and mitigating real time attacks;
7. Issuance of email alert and a verbal person-to-person telephone call to authorized users within 15 minutes when an anomaly or attack is detected;
8. Issuance of email alert and a verbal person-to-person telephone call to authorized users within 15 minutes of when mitigation services commence; and,
9. Analyze attack patterns throughout Contractor IP backbone and alerting authorized users of IP threats, provide authorized users the information via secure portal for addressing/mitigating IP threats and provide authorized users with links to patches, updates and workarounds for known and documented IP threats.

**Bidder shall describe its DDoS Activities offering.**

*Bidder understands the requirements in Section 7.2.1.2 and shall meet or exceed them?*

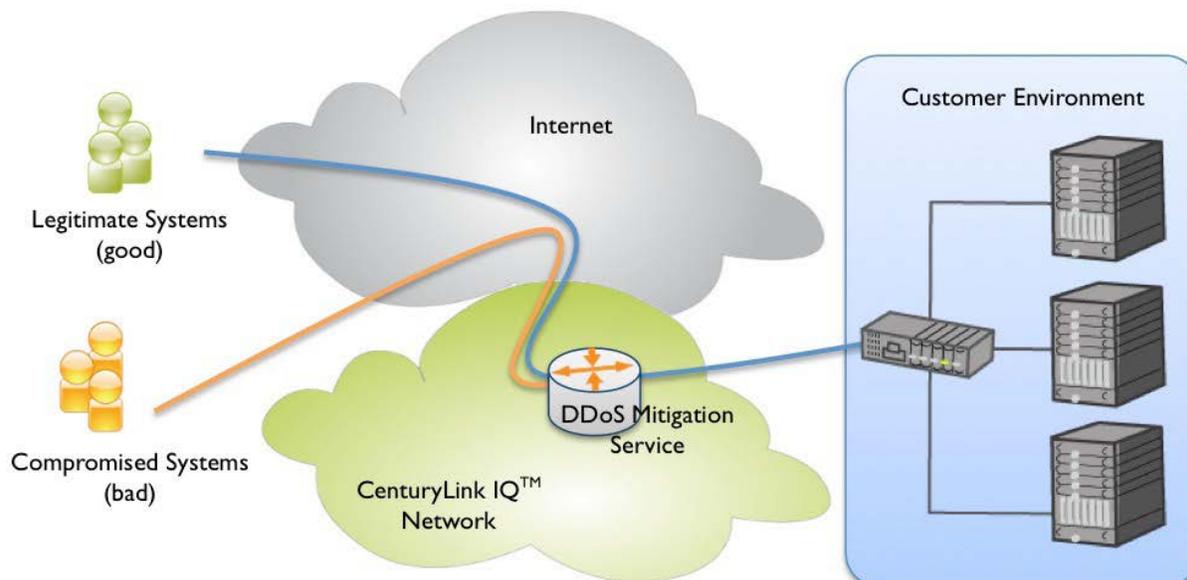
Yes   Y   No       

*Description:*

***The CenturyLink Proactive Shared DDoS Mitigation service constantly monitors your network traffic. CenturyLink uses baselines and thresholds derived from your data flow to do the following:***

- ***Monitoring of Customer traffic patterns***
- ***Establishment of network traffic baselines***
- ***Detection of Customer traffic anomalies***
- ***Scrubbing of Customer traffic by dropping DDoS attack packets***
- ***Perform detection and anomaly analysis***
- ***Develop and provide access to a strategy for identifying and mitigating real-time attacks***
- ***Issuance of email alert and a verbal person-to-person telephone call to authorized users within 15 minutes after an anomaly or attack is detected***
- ***Issuance of email alert and a verbal person-to-person telephone call to authorized users within 15 minutes of when mitigation services commence***
- ***Analyze attack patterns throughout CenturyLink IP backbone and alerting authorized users of IP threats, provide authorized users the information for addressing/mitigating IP threats via secure portal, and provide authorized users with links to patches, updates and workarounds for known and documented IP threats***

*These derived baselines are used to identify normal versus abnormal network behavior. When the DDoS Mitigation service detects a possible DDoS attack, CenturyLink operations center personnel contact your office to validate the attack. When the attack is validated and after you approve, network traffic is rerouted for scrubbing in the CenturyLink network to help eliminate the malicious traffic and pass along valid traffic.*



### 7.2.1.3 DDoS Detection and Mitigation Web Portal and Reporting

Contractor shall provide a secure web based portal for authorized users.

Contractor's portal shall provide authorized users:

1. A view of their traffic patterns;
2. A view of the real time attack and mitigation strategy;
3. IP threat alerts;
4. Information for addressing and mitigating IP threats; and,
5. Links to patches, updates, and workarounds for known and documented IP threats.

Contractor's portal shall provide authorized users access to the following anomaly report:

1. Traffic anomaly detection.

**Bidder shall describe its DDoS Detection and Mitigation Web Portal and Reporting offering.**

*Bidder understands the requirements in Section 7.2.1.3 and shall meet or exceed them?*  
Yes Y No

*Description:*

***CenturyLink has a robust secure web-based portal for authorized DDoS users. In addition to the State requirements to provide:***

- ***A view of their traffic patterns***
- ***A view of the real-time attack-and-mitigation strategy***
- ***IP threat alerts***
- ***Information for addressing and mitigating IP threats***
- ***Links to patches, updates, and workarounds for known and documented IP threats***

***CenturyLink provides Status Screen summary. Upon successful login, the customer is presented with a status summary view:***

- ***Navigating by means of the top menu bar***
- ***Portal customers can examine characteristics of their network traffic at any time***
- ***Independent of DDoS events and alerts – alerts can be examined through the menu bar, or from the Alerts panel in the Status page.***
- ***Traffic-into (top) and out-of (bottom) summary of current and recent DDoS alerts is presented***
- ***Peak-flow system displays a summary of the traffic broken down by application***
- ***Available graph types are: Stacked, (default), Pie, and Bar***
- ***TCP report for TCP traffic broken down by TCP port***
- ***UDP report for UDP traffic aggregated by UDP port***
- ***IP report for traffic by IP-level protocol***

#### 7.2.1.4 DDoS Detection and Mitigation Features

The Contractor shall offer the DDoS Detection and Mitigation features detailed in Table 7.2.1.4.a.

**Table 7.2.1.4.a DDoS Detection and Mitigation Features**

	Feature Name	Feature Description	Bidder Meet or Exceeds?		Bidder's Product Identifier
			Y	N	
1	<b>DDoS Detection and Mitigation, 1 – 2 GB</b>	DDoS Detection and Mitigation Service as described in Section 7.2.1 for 1-2 GB of traffic flow.	Y		<b>QNB60900</b>
Bidder's Product Description: <i>CenturyLink DDoS Detection and Mitigation Service for 1 to 2 GB of traffic flow includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack, notifies the customer, then initiates the mitigation process based on the customers pre approved thresholds.</i>					
2	<b>DDoS Detection and Mitigation, 3 – 4 GB</b>	DDoS Detection and Mitigation Service as described in Section 7.2.1 for 3-4 GB of traffic flow	Y		<b>QNB60901</b>
Bidder's Product Description: <i>CenturyLink DDoS Detection and Mitigation Service for 3 to 4 GB of traffic flow includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack, notifies the customer, then initiates the mitigation process based on the customers pre approved thresholds.</i>					
3	<b>DDoS Detection and Mitigation, 5 – 6 GB</b>	DDoS Detection and Mitigation Service as described in Section 7.2.1 for 5-6 GB of traffic flow	Y		<b>QNB60902</b>
Bidder's Product Description: <i>CenturyLink DDoS Detection and Mitigation Service for 5 to 6 GB of traffic flow includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack, notifies the customer, then initiates the mitigation process based on the customers pre approved thresholds.</i>					

The Contractor may offer Unsolicited DDoS Detection and Mitigation features in Table 7.2.1.4.b.

**Table 7.2.1.4.b Unsolicited DDoS Detection and Mitigation Features**

	Feature Name	Feature Description	Bidder's Product Identifier
1	<i>DDoS Detection and Mitigation, FastE - 10 MB</i>	<i>DDoS Detection and Mitigation Service as described in Section 7.2.1.3 or FastE 10 MB of traffic flow.</i>	<b>QNB60924</b>
Bidder's Product Description: <i>CenturyLink DDoS Detection and Mitigation Service for FastE 10 – MB of traffic flow includes our Proactive Shared DDoS Mitigation Service where CenturyLink</i>			

	Feature Name	Feature Description	Bidder's Product Identifier
	<i>identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
2	<i>DDoS Detection and Mitigation, FastE - 20 MB</i>	<i>DDoS Detection and Mitigation Service as described in Section 7.2.1.3 for FastE 20 MB of traffic flow.</i>	<i>QNB60925</i>
	Bidder's Product Description: <i>CenturyLink DDoS Detection and Mitigation Service for FastE 20 – MB of traffic flow includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
3	<i>DDoS Detection and Mitigation, FastE - 30 MB</i>	<i>DDoS Detection and Mitigation Service as described in Section 7.2.1.3 for FastE 30 MB of traffic flow.</i>	<i>QNB60926</i>
	Bidder's Product Description: <i>CenturyLink DDoS Detection and Mitigation Service for FastE 30 – MB of traffic flow includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
4	<i>DDoS Detection and Mitigation, FastE - 40 – 100 MB</i>	<i>DDoS Detection and Mitigation Service as described in Section 7.2.1.3 for FastE 40 to 100 MB of traffic flow.</i>	<i>QNB60927</i>
	Bidder's Product Description: <i>CenturyLink DDoS Detection and Mitigation Service for FastE 40 - 100 MB of traffic flow includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
5	<i>DDoS Detection and Mitigation, GigE 100 MB</i>	<i>DDoS Detection Mitigation Service as described in Section 7.2.1.3 for 100 MB of traffic flow</i>	<i>QNB60928</i>
	Bidder's Product Description: <i>CenturyLink DDoS Detection and Mitigation Service for GigE 100 MB of traffic flow includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
6	<i>DDoS Detection and Mitigation, GigE 200 MB</i>	<i>DDoS Detection Mitigation Service as described in Section 7.2.1.3 for 200 MB of traffic flow</i>	<i>QNB60929</i>
	Bidder's Product Description: <i>CenturyLink DDoS Detection and Mitigation Service for GigE 200 MB of traffic flow includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once</i>		

	<b>Feature Name</b>	<b>Feature Description</b>	<b>Bidder's Product Identifier</b>
	<i>the customer agrees to start the mitigation process.</i>		
7	<i>DDoS Detection and Mitigation, GigE 300 MB</i>	<i>DDoS Detection Mitigation Service as described in Section 7.2.1.3 for 300 MB of traffic flow</i>	<i>QNB60930</i>
	Bidder's Product Description: <i>CenturyLink DDoS Detection and Mitigation Service for GigE 300 MB of traffic flow includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
8	<i>DDoS Detection and Mitigation, GigE 400 – 1000 MB</i>	<i>DDoS Detection Mitigation Service as described in Section 7.2.1.3 for 400 – 1000 MB of traffic flow</i>	<i>QNB60931</i>
	Bidder's Product Description: <i>CenturyLink DDoS Detection and Mitigation Service for GigE 400 to 1000 MB of traffic flow includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
9	<i>DDoS Detection and Mitigation, 10 GigE - 1 GB</i>	<i>DDoS Mitigation Service as described in Section 7.2.1.3 for 1 GB of GigE traffic flow</i>	<i>QNB60932</i>
	Bidder's Product Description: <i>CenturyLink DDoS Mitigation Service for 1 GB of traffic flow includes our Reactive Shared DDoS Mitigation Service where the Customer identifies the DDoS attack and notifies CenturyLink, asking us to start the mitigation process.</i>		
10	<i>DDoS Detection and Mitigation, 10 GigE - 2 GB</i>	<i>DDoS Mitigation Service as described in Section 7.2.1.3 for 2 GB of GigE traffic flow</i>	<i>QNB60933</i>
	Bidder's Product Description: <i>CenturyLink DDoS Mitigation Service for 2 GB of traffic flow includes our Reactive Shared DDoS Mitigation Service where the Customer identifies the DDoS attack and notifies CenturyLink, asking us to start the mitigation process.</i>		
11	<i>DDoS Detection and Mitigation, 10 GigE - 3 GB</i>	<i>DDoS Mitigation Service as described in Section 7.2.1.3 for 3 GB of GigE traffic flow</i>	<i>QNB60934</i>
	Bidder's Product Description: <i>CenturyLink DDoS Mitigation Service for 3 GB of traffic flow includes our Reactive Shared DDoS Mitigation Service where the Customer identifies the DDoS attack and notifies CenturyLink, asking us to start the mitigation process.</i>		
	<i>DDoS Detection and Mitigation, 10</i>	<i>DDoS Mitigation Service as described in Section 7.2.1.3 for 4 to 10 GB of GigE traffic flow</i>	<i>QNB60935</i>

	Feature Name	Feature Description	Bidder's Product Identifier
12	<b><i>GigE 4 – 10 GB</i></b>		
	Bidder's Product Description: <i>CenturyLink DDoS Mitigation Service for 4 to 10 GB of traffic flow includes our Reactive Shared DDoS Mitigation Service where the Customer identifies the DDoS attack and notifies CenturyLink, asking us to start the mitigation process.</i>		
13	<b><i>DDoS Detection and Mitigation DS1 (1.5 Mbps)</i></b>	<b><i>DDoS Detection Mitigation Service as described in Section 7.2.1.3 for a DS1 of traffic flow.</i></b>	<b><i>QNB60936</i></b>
	Bidder's Product Description: <i>CenturyLink DDoS Mitigation Service for 1.54 Mbps of traffic flow includes our includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
14	<b><i>DDoS Detection and Mitigation 2xDS1 (3 Mbps)</i></b>	<b><i>DDoS Detection Mitigation Service as described in Section 7.2.1.3 for 2xDS1 of traffic flow.</i></b>	<b><i>QNB60937</i></b>
	Bidder's Product Description: <i>CenturyLink DDoS Mitigation Service for 3 Mbps of traffic flow includes our includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
15	<b><i>DDoS Detection and Mitigation 3xDS1 (4.5 Mbps)</i></b>	<b><i>DDoS Detection Mitigation Service as described in Section 7.2.1.3 for 4.5 Mbps of traffic flow.</i></b>	<b><i>QNB60938</i></b>
	Bidder's Product Description: <i>CenturyLink DDoS Mitigation Service for 4.5 Mbps of traffic flow includes our includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
16	<b><i>DDoS Detection and Mitigation 4xDS1 (6 Mbps)</i></b>	<b><i>DDoS Detection Mitigation Service as described in Section 7.2.1.3 for 6 Mbps of traffic flow.</i></b>	<b><i>QNB60939</i></b>
	Bidder's Product Description: <i>CenturyLink DDoS Mitigation Service for 6 Mbps of traffic flow includes our includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
17	<b><i>DDoS Detection and Mitigation 5xDS1 (7.5 Mbps)</i></b>	<b><i>DDoS Detection Mitigation Service as described in Section 7.2.1.3 for 7.5 Mbps of traffic flow.</i></b>	<b><i>QNB60940</i></b>
	Bidder's Product Description:		

	Feature Name	Feature Description	Bidder's Product Identifier
	<i>CenturyLink DDoS Mitigation Service for 7.5 Mbps of traffic flow includes our includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
	<i>DDoS Detection and Mitigation 6xDS1 (9 Mbps)</i>	<i>DDoS Detection Mitigation Service as described in Section 7.2.1.3 for 9 Mbps of traffic flow.</i>	<i>QNB60941</i>
18	Bidder's Product Description: <i>CenturyLink DDoS Mitigation Service for 9 Mbps of traffic flow includes our includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
	<i>DDoS Detection and Mitigation 7xDS1 (10.5 Mbps)</i>	<i>DDoS Detection Mitigation Service as described in Section 7.2.1.3 for 10.5 Mbps of traffic flow.</i>	<i>QNB60942</i>
19	Bidder's Product Description: <i>CenturyLink DDoS Mitigation Service for 10.5 Mbps of traffic flow includes our includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
	<i>DDoS Detection and Mitigation 8xDS1 (12 Mbps)</i>	<i>DDoS Detection Mitigation Service as described in Section 7.2.1.3 for 12 Mbps of traffic flow.</i>	<i>QNB60943</i>
20	Bidder's Product Description: <i>CenturyLink DDoS Mitigation Service for 12 Mbps of traffic flow includes our includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
	<i>DDoS Detection and Mitigation DS-3 (45 Mbps)</i>	<i>DDoS Detection Mitigation Service as described in Section 7.2.1.3 for 45 Mbps of traffic flow.</i>	<i>QNB60944</i>
21	Bidder's Product Description: <i>CenturyLink DDoS Mitigation Service for 45 Mbps of traffic flow includes our includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
	<i>DDoS Detection and Mitigation OC3</i>	<i>DDoS Detection Mitigation Service as described in Section 7.2.1.3 for OC3 traffic flow</i>	<i>QNB60945</i>
22	Bidder's Product Description: <i>CenturyLink DDoS Mitigation Service for OC3 traffic flow includes our includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer</i>		

	Feature Name	Feature Description	Bidder's Product Identifier
	<i>agrees to start the mitigation process.</i>		
23	<i>DDoS Detection and Mitigation OC12</i>	<i>DDoS Detection Mitigation Service as described in Section 7.2.1.3 for OC12 traffic flow</i>	<i>QNB60946</i>
	Bidder's Product Description: <i>CenturyLink DDoS Mitigation Service for OC12 traffic flow includes our includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		
24	<i>DDoS Detection and Mitigation OC48</i>	<i>DDoS Detection Mitigation Service as described in Section 7.2.1.3 for OC48 traffic flow</i>	<i>QNB60947</i>
	Bidder's Product Description: <i>CenturyLink DDoS Mitigation Service for OC48 traffic flow includes our includes our Proactive Shared DDoS Mitigation Service where CenturyLink identifies the DDoS attack notifies the customer, then initiates the mitigation once the customer agrees to start the mitigation process.</i>		

**7.2.2 Email Monitoring and Scanning Services**

Contractor shall provide a network based email monitoring and scanning service. All hardware/software necessary to provide service shall reside in the Contractors network and shall be maintained, monitored and supported by the Contractor. The service functions shall consist of anti-virus, anti-spam protection and content control. These monitoring and scanning functions shall be performed in the Contractor's network prior to email traffic reaching the Customers internal network. The service shall work with the Customers' existing email systems.

**Bidder shall describe its Email Monitoring and Scanning Services offering.**

*Bidder understands the requirements in Section 7.2.2 and shall meet or exceed them?*

Yes   Y   No       

*Description:*

*CenturyLink Email Defense is our answer for Anti-Virus Anti-Spam protection and provides a network-based managed security service that filters and cleans email from the Internet prior to reaching your network. The service can block inappropriate content and can prevent email worms from infiltrating your network. This service is ideal if you would like to move the burden of dealing with spam and viruses away from the end user to a single managed solution for all email users on your network.*

***How Email Defense works:***

- *Your mail exchange (MX) record is updated to the CenturyLink™ platform*
- *Email Defense filters and forwards messages to your email server based on the policies you set*
- *A secure web site allows your authorized administrators to define filtering policies, define quarantined message settings, create safe lists and black lists, view reports and statistics and perform forensic searches*
- *If your email server goes down, your email is automatically spooled and after your email server is restored, CenturyLink automatically delivers spooled email*
- *Using Email Defense, the new MX record conceals your mail servers and protects them from email DDoS attacks*
- *Each email will be sent to a redundant load-balanced infrastructure*
- *Each email is subject to multiple layers of defense*
- *Only emails deemed legitimate will reach customers*
- *Bayesian statistical filtering—statistical algorithms that quantify the possibility that an email message is spam based on how often elements in that email have appeared in identified spam messages*
- *Industry heuristics—thousands of successful industry-wide spam-fighting rules to recognize characteristics of spam*
- *Proprietary heuristics—thousands of proprietary rules to block spam including phishing attacks*
- *URL filtering—analyses embedded links in email messages for spam and threats*
- *Reputation analysis—CenturyLink constantly monitors inbound email to build a list of IP addresses and domain names that send spam and/or legitimate email*
- *Reputation-based RBL filtering—CenturyLink weighs the results of multiple lists to help gauge the likelihood of an email being sent by a known spammer*

#### 7.2.2.1 Email Monitoring and Scanning Service Functionality

The managed email monitoring and scanning service shall provide the following functionality:

##### 7.2.2.1.1 Anti-Virus Protection

The anti-virus function shall scan both inbound and outbound Customer E-mail for viruses. The Contractor shall provide automatic and timely updates of virus pattern and signature files as they become available. Detected viruses shall be removed from infected E-mail or otherwise the infected E-mail shall be deleted.

**Bidder shall describe its Anti-Virus Protection offering.**

*Bidder understands the requirements in Section 7.2.2.1.1 and shall meet or exceed them?* Yes   Y   No       

*Description:*

*CenturyLink Email Defense is our answer for Anti-Virus protection. Email Defense filters all your inbound email prior to it reaching your network. Email Defense can also filter the email leaving your network. All encountered viruses are quarantined on CenturyLink servers and can be managed by you 24/7/365.*

*Email Defense will help reduce the amount of your network usage and storage by blocking e-mail born viruses. We obtain virus updates multiple times a day and are constantly updating scanning techniques, always providing the latest in virus protection.*

*A secure custom web site allows authorized administrators access to the quarantined messages to define filtering preferences, create safe and black lists, view message reports, view statistics, and search the quarantine database. If your email server goes down, we'll automatically store your email until your email server is restored and then deliver your email.*

**Features**

- *Gateway-based email filtering*
- *Virus scanning and worm detection*
- *Web-based interface for monitoring and administration*
- *Email backup support*
- *Customized safe and black lists*
- *Customized threshold levels*
- *Quarantine reports*
- *Support 24/7/365*

**7.2.2.1.2 Anti-Spam Protection**

The anti-spam function shall isolate detected incoming spam E-mail. The Customer shall have the capability to review detected spam for appropriate handling.

**Bidder shall describe its Anti-Spam Protection offering.**

*Bidder understands the requirements in Section 7.2.2.1.2 and shall meet or exceed them?* Yes   Y   No

*Description:*

*CenturyLink Email Defense is our answer for Anti-Spam protection. Email Defense filters all your inbound prior to reaching your network. Email Defense can also filter the email leaving your network. All encountered spam and adult content quarantined on CenturyLink servers and can be managed by you 24/7/365.*

*It is estimated that 45% to 50% of all email is spam. Email Defense will help reduce the amount of your network usage and storage by blocking spam. We obtain updates multiple times a day and are constantly updating scanning techniques, always providing the latest in email spam protection.*

*A secure custom web site allows authorized administrators access to the quarantined messages to define filtering preferences, create safe and black lists, view message reports, view statistics and search the quarantine database. If your email server goes down, we'll automatically store your email until your email server is restored and then deliver your email.*

**Features**

- **Gateway-based email filtering**
- **Virus scanning and worm detection**
- **Web-based interface for monitoring and administration**
- **Email backup support**
- **Customized safe and black lists**
- **Customized threshold levels**
- **Quarantine reports**
- **Support 24/7/365**

7.2.2.1.3 Content Control

The content control function shall allow a Customer to apply an acceptable use policy on incoming/outgoing email automatically as emails are scanned.

**Bidder shall describe its Content Control offering.**

*Bidder understands the requirements in Section 7.2.2.1.3 and shall meet or exceed them? Yes   Y   No*

*Description:*

***A secure custom web site allows authorized administrators to set acceptable use policies and thresholds. In addition the administrators will have access to quarantined messages have the ability to create safe and black lists, view message reports, view statistics, and search the quarantine database.***

***If your email server goes down, we'll automatically store your email until your email server is restored and then deliver your email.***

#### 7.2.2.1.4 Isolation Area

The isolation area shall isolate and contain virus infected E-mail, spam E-mail and E-mail not conforming to the Customer acceptable use policy. The isolation area shall be accessible via a web based interface and Customer shall be able to configure different levels of access to isolation area E-mail.

**Bidder shall describe its Isolation Area offering.**

*Bidder understands the requirements in Section 7.2.2.1.4 and shall meet or exceed them? Yes   Y   No*

*Description:*

***The Isolation Area is a secure custom web site allows authorized administrators access to the quarantined messages to define filtering preferences, create safe and black lists, view message reports, view statistics and search the quarantine database. If your email server goes down, we'll automatically store your email until your email server is restored and then deliver your email.***

#### 7.2.2.1.5 Notification

Notification shall allow a Customer to be notified via E-mail when an anti-virus, anti-spam or content control function has been invoked.

**Bidder shall describe its Notification offering.**

*Bidder understands the requirements in Section 7.2.2.1.5 and shall meet or exceed them? Yes   Y   No*

*Description:*

***Within the CenturyLink Email Defense WEB tool all customers have access to set customized threshold levels for anti-virus, anti-spam and content control functions. Once those thresholds are set the customer can choose from a list of notification options including email.***

7.2.2.2 Email Monitoring and Scanning Service Web Portal and Reporting

The Contract shall provide the following reporting functionality via a secure web portal:

1. Traffic/mail statistics;
2. Infections detected;
3. Policy violations; and,
4. Event log of actions performed.

**Bidder shall describe its Email Monitoring and Scanning Service Web Portal and Reporting offering.**

*Bidder understands the requirements in Section 7.2.2.2 and shall meet or exceed them?*  
 Yes Y No       

*Description:*

*Within the CenturyLink Email Defense Web Tools, covering email monitoring and scanning services, customers have access to reports that support the State requirements for:*

- *Traffic/mail statistics*
- *Infections detected*
- *Policy violations*
- *Event log of actions performed*

*The CenturyLink Email Defense WEB tool is a public URL that will be provided to the customer. Once the user account is setup to the secured WEB tool, the user will receive a secure username/password for log-in, have access to 24/7/365 reporting and management, and will have phone and online support.*

7.2.2.3 Email Monitoring and Scanning Service Features

The Contractor shall offer the network based email monitoring and scanning service features detailed in Table 7.2.2.3.a.

**Table 7.2.2.3.a – Email Monitoring and Scanning Service Features**

	Feature Name	Feature Description	Bidder Meet or Exceeds?		Bidder's Product Identifier
			Y	N	
1	<b>Email Monitoring and Scanning Service, 1-49</b>	Email managed security services seat as described in Section 7.2.2.	Y		<b>QNB60903</b>
	Bidder's Product Description: <i>CenturyLink provides Email defense to support Email managed security services seat as described in Section 7.2.2</i>				

	Feature Name	Feature Description	Bidder Meet or Exceeds?		Bidder's Product Identifier
			Y	N	
2	<b>Email Monitoring and Scanning Service, 50-74</b>	Email managed security services seat as described in Section 7.2.2.	Y		<b>QNB60904</b>
Bidder's Product Description: <i>CenturyLink provides Email defense to support Email managed security services seat as described in Section 7.2.2</i>					
3	<b>Email Monitoring and Scanning Service, 75-99</b>	Email managed security services seat as described in Section 7.2.2.	Y		<b>QNB60905</b>
Bidder's Product Description: <i>CenturyLink provides Email defense to support Email managed security services seat as described in Section 7.2.2</i>					
4	<b>Email Monitoring and Scanning Service, 100-500</b>	Email managed security services seat as described in Section 7.2.2.	Y		<b>QNB60906</b>
Bidder's Product Description: <i>CenturyLink provides Email defense to support Email managed security services seat as described in Section 7.2.2</i>					
5	<b>Email Monitoring and Scanning Service, 501-1000</b>	Email managed security services seat as described in Section 7.2.2.	Y		<b>QNB60907</b>
Bidder's Product Description: <i>CenturyLink provides Email defense to support Email managed security services seat as described in Section 7.2.2</i>					
6	<b>Email Monitoring and Scanning Service, 1001 and above</b>	Email managed security services seat as described in Section 7.2.2.	Y		<b>QNB60908</b>
Bidder's Product Description: <i>CenturyLink provides Email defense to support Email managed security services seat as described in Section 7.2.2</i>					

The Contractor may offer Unsolicited Network Based Email Managed Security Service features in Table 7.2.2.3.b.

**Table 7.2.2.3.b Unsolicited Network Based Email Managed Security Service Features**

	Feature Name	Feature Description	Bidder's Product Identifier
1	<i>Email Encryption 1 – 400 Users</i>	<i>Email Encryption 1 to 400 users. (Optional feature requiring Email Defense)</i>	<b>QNB60940</b>

	Feature Name	Feature Description	Bidder's Product Identifier
		<p>Bidder's Product Description:</p> <p><i>The Centurylink Email Encryption enhancement is a "Security as a Service" SaaS network email encryption tool that safeguards your confidential data and enables you to maintain compliance with regulations requiring encryption of sensitive data. A cloud-based solution, Centurylink SaaS Email Encryption delivers unparalleled scalability, eliminates the burden of managing a solution, and empowers your mobile workforce to send and receive encrypted emails ubiquitously from any email client. And, with advanced pre-built data loss prevention (DLP) rules and advanced content scanning, establishing and enforcing policies are easier than ever before.</i></p> <p><i>All customer SaaS Email Encryption is sent to our secure servers and is run through our trusted and proven standards-based encryption technologies. It removes the difficulty of installing and managing current solutions and is easy to use.</i></p> <p><i>Encryption technologies used include: PKI, S/MIME, X.509 certificates (including the ability to enforce certificate authorities), 3DES, AES-256, and 1024-bit RSA keys (with MDS and SHA-1 encryption algorithms). The encrypted message web portal utilizes 128-bit secure sockets layer (SSL).</i></p> <p><i>As an administrator, use the unified web-based Centurylink SaaS Control Console to set, review, and customize your organization's privacy policies (policy-driven encryption), so that confidential content is automatically encrypted or acted on as required. Multiple policies may be customized and enforced for respective user groups, branch offices, and lines of businesses.</i></p> <p><i>As a sender, simply compose your email and send. The content is automatically scanned and encrypted if it matches the policy set by the administrator. This occurs transparently behind the scenes. Or, if the on-demand encryption option has been enabled, simply enter "[encrypt]" in either the subject line or the message body to force encryption. Regular expression technology may also be utilized to identify keywords and phrases.</i></p> <p><i>Your email recipients can retrieve the message from the web-based message pickup portal, or they can download a secure message reader, which enables viewing of the message directly through the recipients' email client. And, when they reply, the message can also be encrypted, providing bidirectional protection.</i></p> <p><i>Email Encryption enables customers to address the following business needs:</i></p> <ul style="list-style-type: none"> <li><i>• Regulatory compliance</i></li> <li><i>• Pre-built enterprise-class regulatory libraries and templates</i></li> <li><i>• Integrated reporting with support for audits</i></li> <li><i>• Secure, private email communications with business partners and customers</i></li> <li><i>• Encryption via policy enforcement or user initiated</i></li> <li><i>• Policy enforcement transparent to senders</i></li> <li><i>• Protect your business</i></li> <li><i>• Predictable monthly cost</i></li> </ul>	

	Feature Name	Feature Description	Bidder's Product Identifier
	<ul style="list-style-type: none"> <li>• <i>Easy administration</i></li> <li>• <i>Web-based policies, reports, statistics and management</i></li> <li>• <i>Key management free</i></li> <li>• <i>Cloud based high-availability enterprise-class encryption solution</i></li> <li>• <i>Requires no on-site hardware or software</i></li> </ul>		
2	<p><i>Email Encryption 401 – 2000 Users</i></p>	<p><i>Email Encryption 401 to 2000 users (Optional feature requiring Email Defense)</i></p> <p>Bidder's Product Description:  <i>The Centurylink Email Encryption enhancement is a "Security as a Service" SaaS network email encryption tool that safeguards your confidential data and enables you to maintain compliance with regulations requiring encryption of sensitive data. A cloud-based solution, Centurylink SaaS Email Encryption delivers unparalleled scalability, eliminates the burden of managing a solution, and empowers your mobile workforce to send and receive encrypted emails ubiquitously from any email client. And, with advanced pre-built data loss prevention (DLP) rules and advanced content scanning, establishing and enforcing policies are easier than ever before.</i></p> <p><i>All customer SaaS Email Encryption is sent to our secure servers and is run through our trusted and proven standards-based encryption technologies. It removes the difficulty of installing and managing current solutions and is easy to use.</i></p> <p><i>Encryption technologies used include: PKI, S/MIME, X.509 certificates (including the ability to enforce certificate authorities), 3DES, AES-256, and 1024-bit RSA keys (with MDS and SHA-1 encryption algorithms). The encrypted message web portal utilizes 128-bit secure sockets layer (SSL).</i></p> <p><i>As an administrator, use the unified web-based Centurylink SaaS Control Console to set, review, and customize your organization's privacy policies (policy-driven encryption), so that confidential content is automatically encrypted or acted on as required. Multiple policies may be customized and enforced for respective user groups, branch offices, and lines of businesses.</i></p> <p><i>As a sender, simply compose your email and send. The content is automatically scanned and encrypted if it matches the policy set by the administrator. This occurs transparently behind the scenes. Or, if the on-demand encryption option has been enabled, simply enter "[encrypt]" in either the subject line or the message body to force encryption. Regular expression technology may also be utilized to identify keywords and phrases.</i></p> <p><i>Your email recipients can retrieve the message from the web-based message pickup portal, or they can download a secure message reader, which enables viewing of the message directly through the recipients' email client. And, when they reply, the message can also be encrypted, providing bidirectional protection.</i></p> <p><i>Email Encryption enables customers to address the following business needs:</i></p> <ul style="list-style-type: none"> <li>• <i>Regulatory compliance</i></li> <li>• <i>Pre-built enterprise-class regulatory libraries and templates</i></li> </ul>	<p><i>QNB60941</i></p>

	Feature Name	Feature Description	Bidder's Product Identifier
	<ul style="list-style-type: none"> <li>• <i>Integrated reporting with support for audits</i></li> <li>• <i>Secure, private email communications with business partners and customers</i></li> <li>• <i>Encryption via policy enforcement or user initiated</i></li> <li>• <i>Policy enforcement transparent to senders</i></li> <li>• <i>Protect your business</i></li> <li>• <i>Predictable monthly cost</i></li> <li>• <i>Easy administration</i></li> <li>• <i>Web-based policies, reports, statistics and management</i></li> <li>• <i>Key management free</i></li> <li>• <i>Cloud based high-availability enterprise-class encryption solution</i></li> <li>• <i>Requires no on-site hardware or software</i></li> </ul>		
3	<p><i>Email Encryption 2001 – Plus Users</i></p>	<p><i>Email Encryption 2001 Plus users (Optional feature requiring Email Defense)</i></p> <p>Bidder's Product Description:  <i>The Centurylink Email Encryption enhancement is a "Security as a Service" SaaS network email encryption tool that safeguards your confidential data and enables you to maintain compliance with regulations requiring encryption of sensitive data. A cloud-based solution, Centurylink SaaS Email Encryption delivers unparalleled scalability, eliminates the burden of managing a solution, and empowers your mobile workforce to send and receive encrypted emails ubiquitously from any email client. And, with advanced pre-built data loss prevention (DLP) rules and advanced content scanning, establishing and enforcing policies are easier than ever before.</i></p> <p><i>All customer SaaS Email Encryption is sent to our secure servers and is run through our trusted and proven standards-based encryption technologies. It removes the difficulty of installing and managing current solutions and is easy to use.</i></p> <p><i>Encryption technologies used include: PKI, S/MIME, X.509 certificates (including the ability to enforce certificate authorities), 3DES, AES-256, and 1024-bit RSA keys (with MDS and SHA-1 encryption algorithms). The encrypted message web portal utilizes 128-bit secure sockets layer (SSL).</i></p> <p><i>As an administrator, use the unified web-based Centurylink SaaS Control Console to set, review, and customize your organization's privacy policies (policy-driven encryption), so that confidential content is automatically encrypted or acted on as required. Multiple policies may be customized and enforced for respective user groups, branch offices, and lines of businesses.</i></p> <p><i>As a sender, simply compose your email and send. The content is automatically scanned and encrypted if it matches the policy set by the administrator. This occurs transparently behind the scenes. Or, if the on-demand encryption option has been enabled, simply enter "[encrypt]" in either the subject line or the message body to force encryption. Regular expression technology may also be utilized to identify keywords and phrases.</i></p> <p><i>Your email recipients can retrieve the message from the web-based message</i></p>	<p><i>QNB60942</i></p>

	Feature Name	Feature Description	Bidder's Product Identifier
		<p><i>pickup portal, or they can download a secure message reader, which enables viewing of the message directly through the recipients' email client. And, when they reply, the message can also be encrypted, providing bidirectional protection.</i></p> <p><i>Email Encryption enables customers to address the following business needs:</i></p> <ul style="list-style-type: none"> <li>• <i>Regulatory compliance</i></li> <li>• <i>Pre-built enterprise-class regulatory libraries and templates</i></li> <li>• <i>Integrated reporting with support for audits</i></li> <li>• <i>Secure, private email communications with business partners and customers</i></li> <li>• <i>Encryption via policy enforcement or user initiated</i></li> <li>• <i>Policy enforcement transparent to senders</i></li> <li>• <i>Protect your business</i></li> <li>• <i>Predictable monthly cost</i></li> <li>• <i>Easy administration</i></li> <li>• <i>Web-based policies, reports, statistics and management</i></li> <li>• <i>Key management free</i></li> <li>• <i>Cloud based high-availability enterprise-class encryption solution</i></li> <li>• <i>Requires no on-site hardware or software</i></li> </ul>	

### 7.2.3 Web Security and Filtering Service

Contractor shall provide a network based web security and filtering service. All hardware/software necessary to provide service shall reside in the Contractors network and shall be maintained, monitored and supported by the Contractor. The service shall analyze and block web requests for malicious software (malware) and filter content that fails to meet the Customer acceptable use policy. The service shall provide protection against computer viruses, worms, Trojan horses, spyware and adware (malware). The Customer shall have the ability to configure both inbound and outbound content policy. The service shall:

1. Accept http and https requests;
2. Support Lightweight Directory Access Protocol (LDAP) integration; and,
3. Support mobile users at the same level as fixed users.

**Bidder shall describe its Web Security and Filtering Service offering.**

*Bidder understands the requirements in Section 7.2.3 and shall meet or exceed them?*

Yes   Y   No       

*Description:*

***The CenturyLink Web Defense service is an easy-to-use security solution that provides effective protection against spyware, viruses, and phishing attacks and blocks access to inappropriate Web sites.***

*Web Defense, powered by McAfee®, is an easy-to-use web security solution effectively blocks quickly-evolving web threats including spyware, viruses and phishing attacks and helps prevent access to inappropriate sites. Protects the network, including remote users Provides continuous updates to protect against the latest threats Delivers reliable 24/7/365 service and support Provides threat activity and Internet use reports.*

*Web Defense adds several necessary layers of protection for web email users:*

- *Enables administrators to enforce policies which prevent users from accessing popular web mail sites (e.g., Yahoo!, Hotmail, Gmail)*
- *Can limit access to fraudulent phishing sites*

*Web Defense is completely managed requiring no additional hardware or software. The service allows easy administration through an online administration portal. Your web traffic is routed through our web proxy server, which filters traffic according to policies you've determined. Threats are stopped at the network perimeter before they reach your computers or network.*

*The secure custom online portal allows authorized administrators to view and download real-time reports via an administrative console that provides insight into overall threat, individual threat, and web use activity.*

#### 7.2.3.1 Authorized User Administration and Reporting - Web Portal

The service shall include a web based portal allowing authorized users to configure content policy at the user, group and global levels for both inbound and outbound content policy.

The service shall include standard and custom reports accessible through the web based portal.

**Bidder shall describe its Authorized User Administration and Reporting - Web Portal offering.**

*Bidder understands the requirements in Section 7.2.3.1 and shall meet or exceed them?*

Yes   Y   No       

*Description:*

*Within the CenturyLink Email Defense WEB tool all authorized customers have access configure content policy at the user, group and global levels for both inbound and outbound content policy.*

*The CenturyLink Email Defense WEB tool is a public URL that will be provided to the customer. Once the user account is setup to the secured WEB tool, the user will receive a secure username/password for log-in, have access to 24/7/365 reporting and management, and will have phone and online support.*

### 7.2.3.2 Web Security and Filtering Service Features

The Contractor shall offer the Web Security and Filtering features detailed in Table 7.2.3.2.a.

**Table 7.2.3.2.a. Web Security and Filtering Service Features**

	Feature Name	Feature Description	Bidder Meet or Exceeds?		Bidder's Product Identifier
			Y	N	
1	<b>Web Security and Filtering Service</b>	Web Security and Filtering service as described in Section 7.2.3.	Y		<b>QNB60911</b>
<b>Bidder's Product Description:</b> <i>CenturyLink provides Web Security and Filtering service as described in Section 7.2.3.</i>					

The Contractor may offer Unsolicited Web Security and Filtering features in Table 7.2.3.2.b.

**Table 7.2.3.2.b Unsolicited Web Security and Filtering Service Features**

	Feature Name	Feature Description	Bidder's Product Identifier
1			
Bidder's Product Description:			
2			
Bidder's Product Description:			
3			
Bidder's Product Description:			

### 7.2.4 Security Information and Event Management (SIEM)

Contractor shall provide a networked based SIEM service. The service shall collect, analyze, assess and correlate security events from devices located on the Customer premise. All hardware/software necessary to provide service shall reside in the Contractors network and shall be maintained, monitored and supported by the Contractor, with the exception of equipment required to collect security events from devices located on the Customer premise. Supported devices shall include routers, network intrusion detection probes, server based firewalls, host intrusion detection management stations and unified threat management appliances. The service shall categorize and prioritize security events utilizing the Contractor's threat and risk management methodologies generated from Contractor and Customer defined

standards. Security events that represent a security incident or threat shall be escalated to the Customer in accordance with the SLA requirements of Section 7.3.8.5. Contractor escalations shall consist of a security incident report as defined in Section 7.2.4.1 below.

**Bidder shall describe its Security Information and Event Management offering.**

*Bidder understands the requirements in Section 7.2.4 and shall meet or exceed them?*

Yes Y No \_\_\_\_\_

*Description:*

*CenturyLink provides its customers with a suite of services that leverage the considerable strengths of our Security Operations Center (SOC) team, and our hosting, network and professional services capabilities. CenturyLink' legacy of delivering security services dates back to 1987, with the formation of our Common Criteria Test Lab.*

*Today, we offer one of the broadest portfolios of managed and professional security services, with teams dedicated to delivering services across the globe. CenturyLink Managed Security Services support for (SIEM) Security Information and Event Management is based on our Log Management Services.*

*The Log Management Service provides a robust log collection, alerting, and archival solution. Our Log Management Service provides you with a valuable tool to help you address your applicable compliance requirements. Historically, enterprise-class log management solutions have been extremely expensive and time-consuming to implement. However, our Log Management Service provides the functionality of an enterprise-class solution, without the significant up-front costs and implementation timelines.*

*Service highlights include:*

*Log Collection: The service supports a wide variety of security and network devices, operating systems, and applications. Logs are collected locally via a dedicated collection appliance, and then transmitted, fully-encrypted, to CenturyLink' redundant storage and reporting infrastructure.*

*Reporting and Alertin: The Log Management Service includes a standardized set of reports, including reports related to specific security standards. In addition, CenturyLink provides you with access to the dedicated logging appliance to run customizable reports and with guidance regarding how you can utilize the reporting interface to create customized reports.*

*With this service you also receive alerting based on standardized, pre-defined alert criteria, with up to 20 customized alert-rules available. The standardized alerts are responded 24/7 by the CenturyLink Security Operations Center (SOC), with a response time SLA that meets the State SLA for alerts.*

*Storage and Archival: CenturyLink has deployed a high-availability storage infrastructure, with daily backups, to support the service. For your further*

*protection, the Log Management Service Infrastructure runs ongoing integrity checks to verify that log data has not been altered.*

*Real-time logs are available online for 90 days, via our Log Management Service portal. In addition, older log data is retained in an off-site archive for up to 12 months, utilizing CenturyLink' Utility Backup and Vaulting Infrastructure. And restoration of log data greater than 90 days old will commence within six hours of your request.*

*Since the Log Management Service is a fully-managed service, you can rely on CenturyLink to:*

- Provision the log collection appliance and work with each customer to set up and configure the service.*
- Work with each customer to determine your logging rate--measured in messages per second--and also determine the appropriate size of the service offering to deploy.*
- Provide you with log source configuration guidelines for supported devices, for later use by your device administrator.*

*Centurylink has standardized our solution on the LogLogic edge devices to collect data at the customer site. Centurylink will collect 100% of the log 100% of the time.*

*Our Analytics Services will aggregate and archiving 100% of all network, system, application and security logs.*

- Any Syslog, SNMP trap and file-based logs can be supported without the requirement of agents. Supports both TCP and UDP Syslog.*

*Via the Centurylink Analytics Services we provide our customers the ability to retrieve application log files using SMB/CIFS, HTTP, HTTPS, SCP, SFTP, FTP and FTPS. The collection can be scheduled to occur periodically (delay or time)*

*Alternatively, customers can push log files to Analytic's appliance via HTTP upload.*

- The solution has intelligent auto-identification functionality allowing automatic identification of any Syslog messages sent to the appliances. This unique capability reduces the amount of time it takes for the administrators to configure the appliances by auto-discovering message types such as HP-UX servers, IBM AIX servers, RedHat Linux Servers, Cisco PIX, Cisco VPN 3000, Check Point firewalls, Juniper firewalls, and many others*
- Provides centralized collection via the Check Point LEA protocol Check Point firewalls. In addition, we can retrieve Check Point policies via CPML so logs and policies can be correlated.*

- *Includes connectors allowing retrieval of logs stored in MS-SQL, Oracle, DB2 or Sybase Databases without the need for an agent*
- *Includes NetFlow connectors*
- *Includes Real Time File Agent and Multi line delimiters*

### **Server Support**

*No agents are required for the collection of log data from servers, not even for the collection of log data from Windows servers. Log data from UNIX and Linux servers is collected through TCP or UDP Syslog. Customers have a choice between a centralized Windows event collection facility, an agent based solution or a combination of both.*

*Advantages of centralized Windows event collection:*

- *Capture events from a large number of Window servers at up to 1000 MPS*
- *Reliable transport using TCP so logs are never lost*
- *Log buffering when unable to connect to the Analytics appliance*
- *Reduced management overhead by eliminating the need for an agent on each server*

*Log data collection from servers is typically done in real-time. However, by utilizing TCP transport of log data, customers have the ability to apply traffic shaping algorithms to prioritize or de-prioritize log transport. This way customer can ensure that log data never impacts other product traffic on the network. During extreme circumstances log data can be buffered up to a full day at the remote collector and will be automatically transmitted only during those times that bandwidth is available. This automated method is much preferred over manually trying to estimate when might be the best time of day to transfer log data. The Windows Event Collector (Lasso or Universal Collector) enables you to convert Windows Event Logs into a Syslog stream that can be collected by the Analytics appliance. Lasso/UC can be configured to monitor multiple machines across your network from a single Windows host machine. There is no need for additional software to be installed on each machine to be monitored.*

*All messages are delivered to a through the SysLog-ng protocol (TCP). Syslog-ng enables you to specify the origination source IP Address, so the Analytics Appliance recognizes it as having come from the original source host, and not the collection host.*

### **Lasso:**

- *Monitors specified Windows hosts from a central Log Collection Server*
- *Collects all Event Log records and additional related data from specified Windows hosts*
- *Can monitor and collect from the following: System, Security, Application, DNS Server, AD Server, File Replication Service, and custom logs*
- *Generates complete and easy-to-read Event Log messages*

- *Sends Event Log messages to Log Management appliances*
- *Stores “high-water marks” of the last processed events for all monitored Event Logs in a file. Upon implicit restart (such as a system reboot or if Lasso goes down), Lasso restarts from the “high water marks” per monitored Event Log.*

*Centurylink services are designed to collect and forward log data using a number of built-in security, reliability and efficiency features:*

- *Accurate time stamp. The first thing any appliance does when receiving log data is apply an NTP synchronized timestamp to ensure that messages collected by different appliances across different time zones can be compared accurately.*
- *MD5 / SHA256 check sum. Upon receipt of the log data, the Centurylink services will append a MD5/SHA 256 check sum to every one minute of log data. This check sum is thereafter transported and stored separately from the log data to prove that log data was not altered during transport or storage.*
- *Analysis performed on a copy of the log data. The system can maintain two separate records of log data. Whereas the Storage appliance receives a complete unfiltered raw log record, the analytics appliance will normalize and summarize log data to facilitate advanced alerting and reporting.*
- *Encryption during transmission. All log transport between appliances can be secured through 128-bit encryption.*
- *Authentication during transmission. All log transport between appliances can be setup to be authenticated using public key.*
- *Compression during transmission. All log transport between appliances can be compressed for reduced bandwidth usage. Compression ratio is generally 12:1.*
- *TCP encapsulation during transmission. All appliances have the capability to receive a TCP Syslog (SysLog-ng compatible) log stream. For sources that cannot or do not transmit TCP Syslog, Centurylink services will encapsulate log data into a reliable TCP stream before transporting or forwarding.*
- *Buffering during network failure. The buffering capability allows logs to be queued in case there are network or system problems. The buffering size is user configurable up to a maximum of about 4 Giga Byte, which allows for at least 24 hours of log data buffering even while running the Centurylink services at maximum sustained data rates.*
- *Auto-detection of network failure. This feature enables Centurylink services to quickly detect any failure of sending log to remote host, and buffer the logs at the receiving appliance without any drops.*
- *Auto-recovery of network failure. Centurylink services solution will continue to monitor network connectivity and recover once it detects the network or remote host is back up. Logs will then be transferred to the remote host.*

*Encryption of data at rest. Centurylink services is compatible with third party solutions that encrypt log data at rest including NetApp Decru and others solutions*

#### ***Universal Device Support***

*The ability to handle ANY Syslog messages or Text Log File message is unique in the industry. Once the message is received, users can search and create alerts based on the content of the message.*

*In addition to supporting any device that produces logs in a Syslog and Text format, we can also retrieve log data directly from specific applications such as Oracle, Active Directory, SiteProtector, McAfee ePolicy Orchestrator and more.*

#### ***Auto-Discovery***

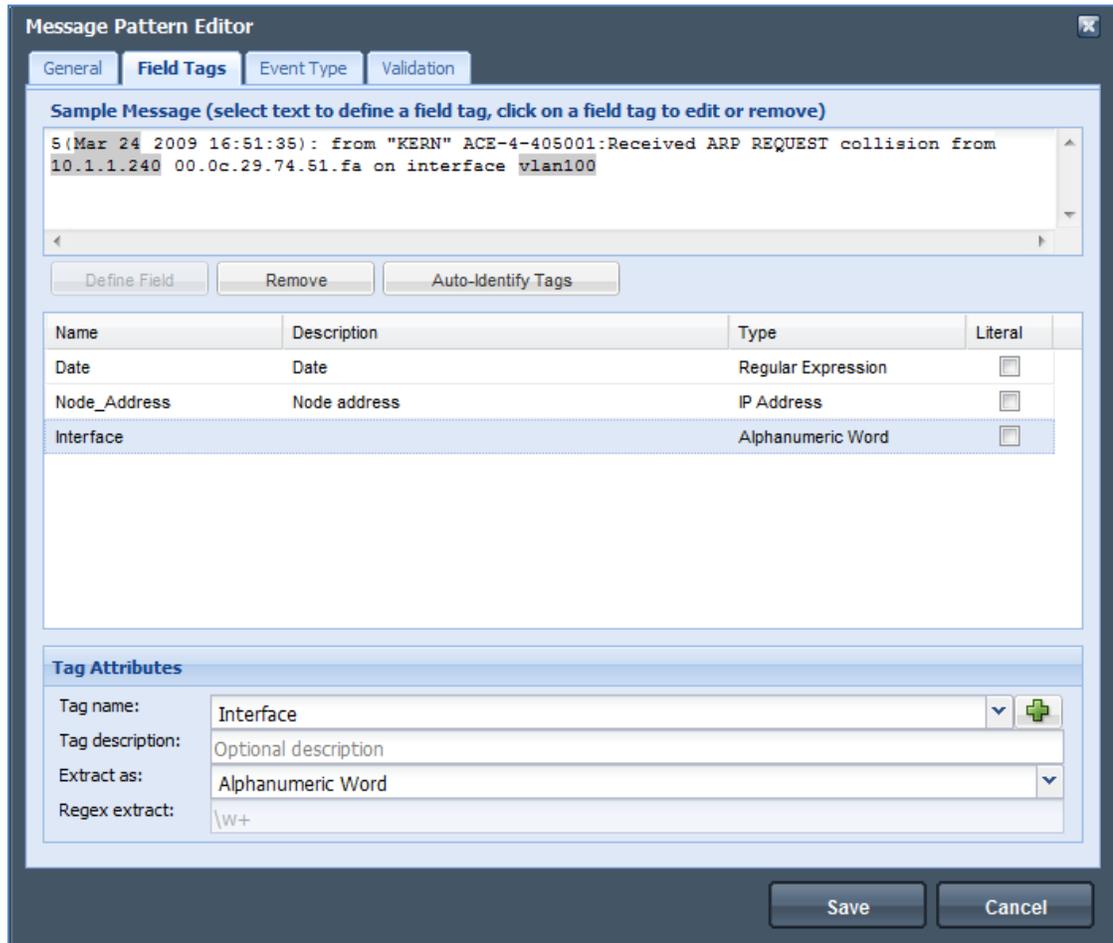
*The solution can intelligently identify any Syslog message sent to the appliances. This unique capability reduces the amount of time it takes for the administrators to configure the appliances by auto-discovering message types such as Cisco PIX, Cisco VPN 3000, NetScreen firewalls, and many others.*

#### ***Message Parsing***

*The solution can natively parse data from more than 120 devices allowing deep analysis and reporting based on field and type identification.*

*In addition to the parsed device included by default the solutions gives the administrator the ability to define device types as well as tag contents within the messages to create a parsed like report.*

*See example below:*



### **Ad-Hoc Search**

*The solution provides robust searching ability to investigate an incident quickly and easily.*

*Search Homepage – example*



### ***Fast Index Search***

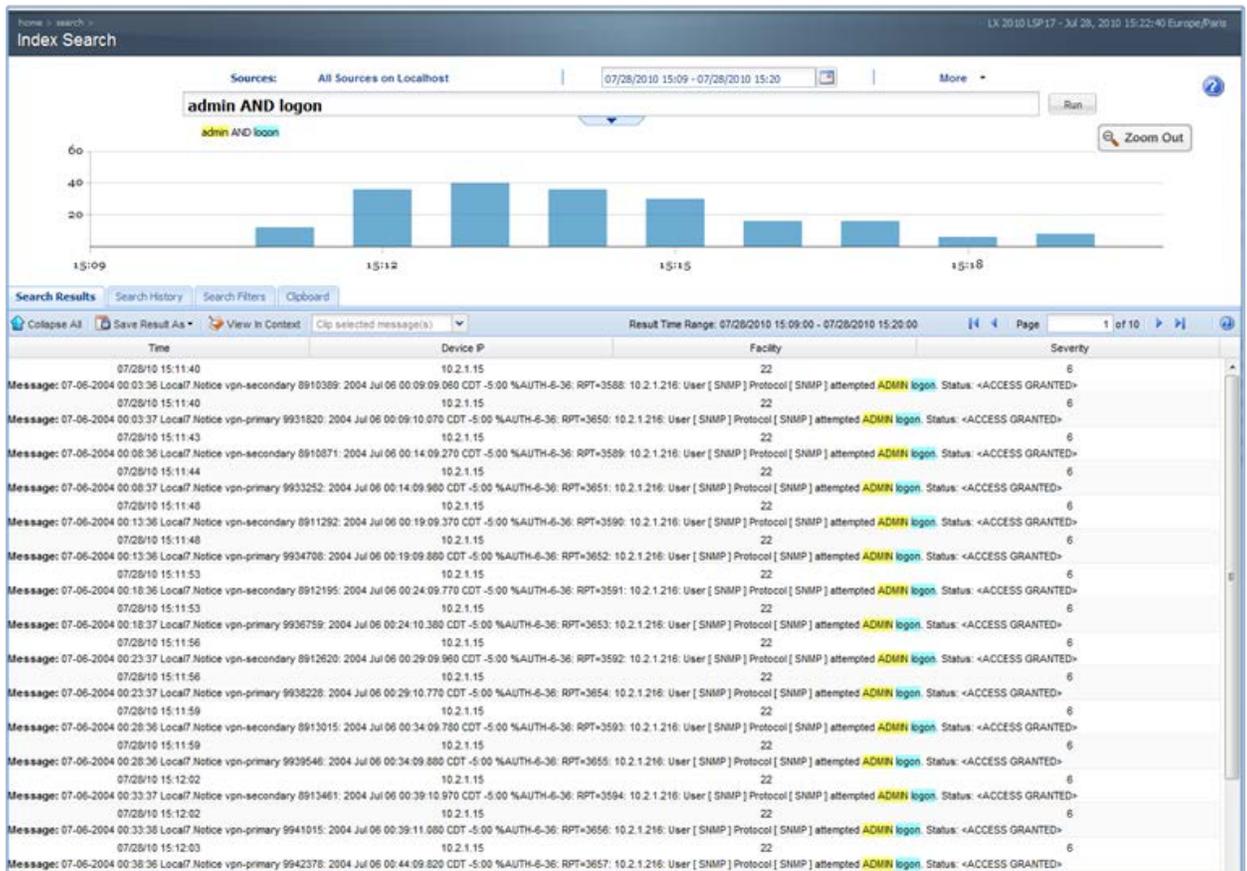
*The fast access to log data combines keyword search and data querying features into one overall search process. Keyword search features are designed to match the keyword search functionality of leading web search engines. The keyword search for log messages is facilitated via Boolean search: AND, OR, NOT are applied as logical operators to express constraints for the messages of interest. Data querying settings assure that all messages satisfying specified criteria (not just assumed to be most relevant) are delivered (and sorted by time). Note that unlike a web search, an index search delivers those and only those messages that fully satisfy the criteria specified via Boolean search expression.*

*The solution has taken log analysis one-step further by providing full-text indexed log data search capabilities. Users are always looking for the fastest way to retrieve relevant log data to perform root cause and forensic analysis. Utilities such as grep scripts are used often to accomplish such tasks. However, if the log data that the user is looking for is buried in a large volume of data, the grep process can take a long time to complete. In addition, for the search to filter log data based on several conditions, multiple grep commands would need to be chained together, resulting in further delay.*

*In addition to the real-time baseline provided in the Main Dashboard, a unique and very interesting feature is provided when performing searches and obtaining search results. In addition to the number of "hits" and the list of all of the relevant logs, a graphical representation of the baseline trend that shows the distribution of these "hits" in the corresponding time window.*

*Below is a screenshot of a search with the trending baseline, specifically showing all occurrences of yahoo.com across all devices these past 24 hours.*

### ***Index Search – example***



*These user-defined filters can be shared and saved as custom reports.*

### **Advanced Regular Expression Search**

*Regular Expression searches are extremely useful to locate targeted information either for troubleshooting, incident triage or forensic investigations.*

### Defining Advanced Search Filters – example

home > search >

## Regular Expression Search

RegEx Search Filter | Finished Searches | Pending Searches

Saved Custom Report:

Device Type:  Source Device:

Search Filter

Retrieve All

Pre-Defined:

Use Words:  AND

Use Exact Phrase:

Regular Expression:

Time Interval

The selected time interval spans from 07/28/10 14:30:15 to 07/28/10 15:30:15.

Hourly Periods:

Daily Periods:

Time Period

From: Date:  Time:   
mm/dd/yy hh:mm:ss

To: Date:  Time:   
mm/dd/yy hh:mm:ss

Schedule search to run immediately

Start Time:

Notify me when this search completes

Search Name:

Save Custom Report

#### 7.2.4.1 SIEM Web Based Security Dashboard

The service shall include a web based portal providing authorized users a security dashboard. The security dashboard shall provide 24x365 access to security reports.

The reports shall provide security information on devices and agents, individually and aggregated. Contractor's escalation security incident report shall contain (when applicable):

1. Identity of the affected device and its location;
2. Timestamp of the incident;
3. Source/Destination addresses;
4. Threat signature information; and,
5. Packet dump.

**Bidder shall describe its SIEM Web Based Security Dashboard offering.**

*Bidder understands the requirements in Section 7.2.4.1 and shall meet or exceed them?*

Yes   Y   No       

*Description:*

*The Centurylink service provides a web based portal for authorized users including a security dashboard that is available 24x365 to access log data and security reports.*

*The protal will provide customer access to:*

- *Identity of the affected device and its location*
- *Timestamp of the incident*
- *Source/Destination addresses*
- *Threat signature information*
- *Packet dump*

*Centurylink High-performance reporting*

*The solution process high message rates while maintaining nearly instantaneous reporting speed (several seconds) for ad-hoc reports, searches, and drill-downs functions. The unique metalog Creation Engine, Parallel Processing Architecture and Domain Virtualization technology enable search results to be returned in seconds, instead of minutes or hours, so that network incidents can be investigated and addressed rapidly.*

*The solution provides the fastest response time in the log management space.*

*Dynamic Reporting*

*Dynamic Reporting capability offers numerous advantages including customizable reports, real-time reports, scheduled executive reports, and ad-hoc searches, allowing administrators to slice, dice and examine all the device and application logs quickly and effectively. In addition, reports can be produced, e-mailed, and exported to PDF or CSV files on demand.*

*These reports, in addition to the unique searching capability, enable users to quickly identify and detect network/system/security problems.*

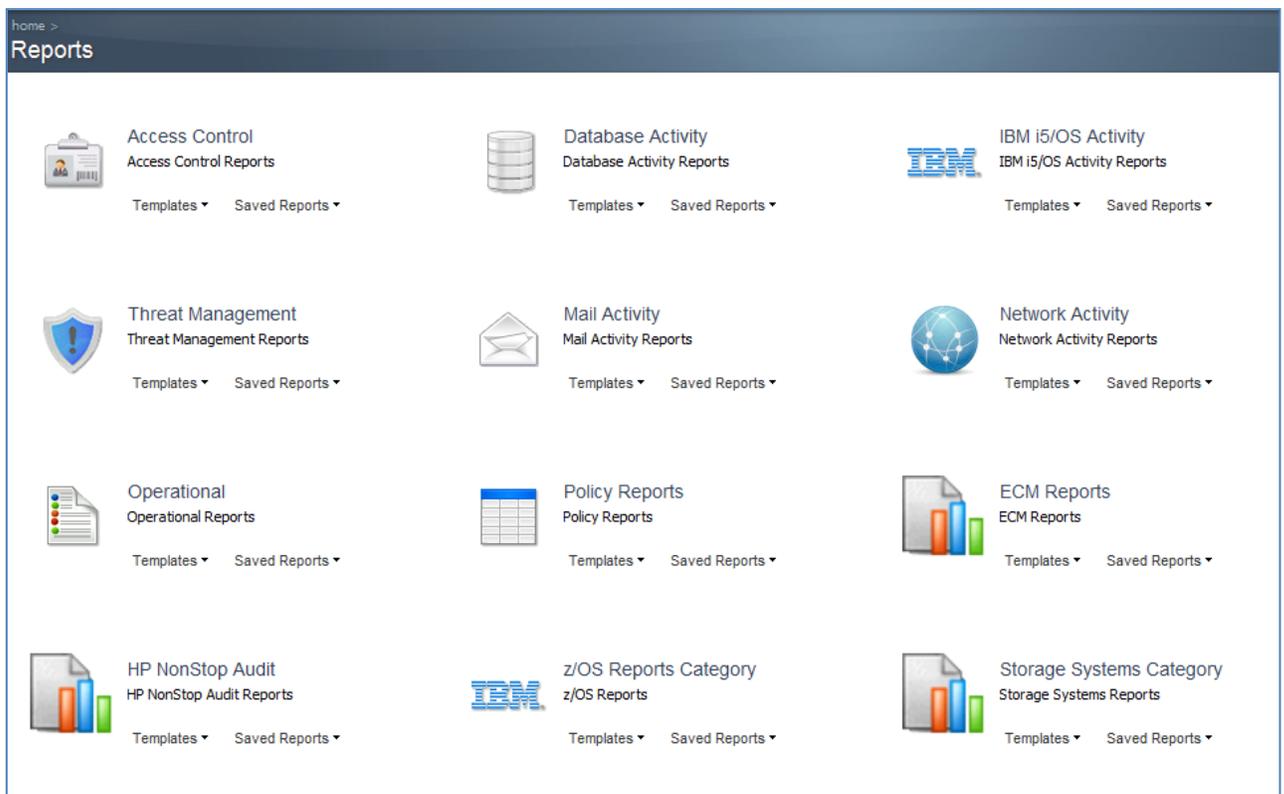
*Report generation does not affect other capabilities of the system, such as collecting, analyzing or alerting. Parallel and distributed architecture allows the whole system to easily scale up.*

**Detailed and Summarized Reports on Parsed Data**

*The solution ships with built-in intelligence and best practice reports such as access control, user accounting, network connectivity, system activity and web surfing activity. Network activity is monitored in real time, increasing IT's visibility and allowing for the creation of timely, accurate reports. Such reports are necessary for complying with HIPAA, SOX and other standards and regulations.*

*Most of the results on parsed data presented in the User Interface are clickable so as to provide drill-down capabilities and can be used dynamically as filters*

**Reports Homepage - example**



**Drill down Cisco ASA - Example :**

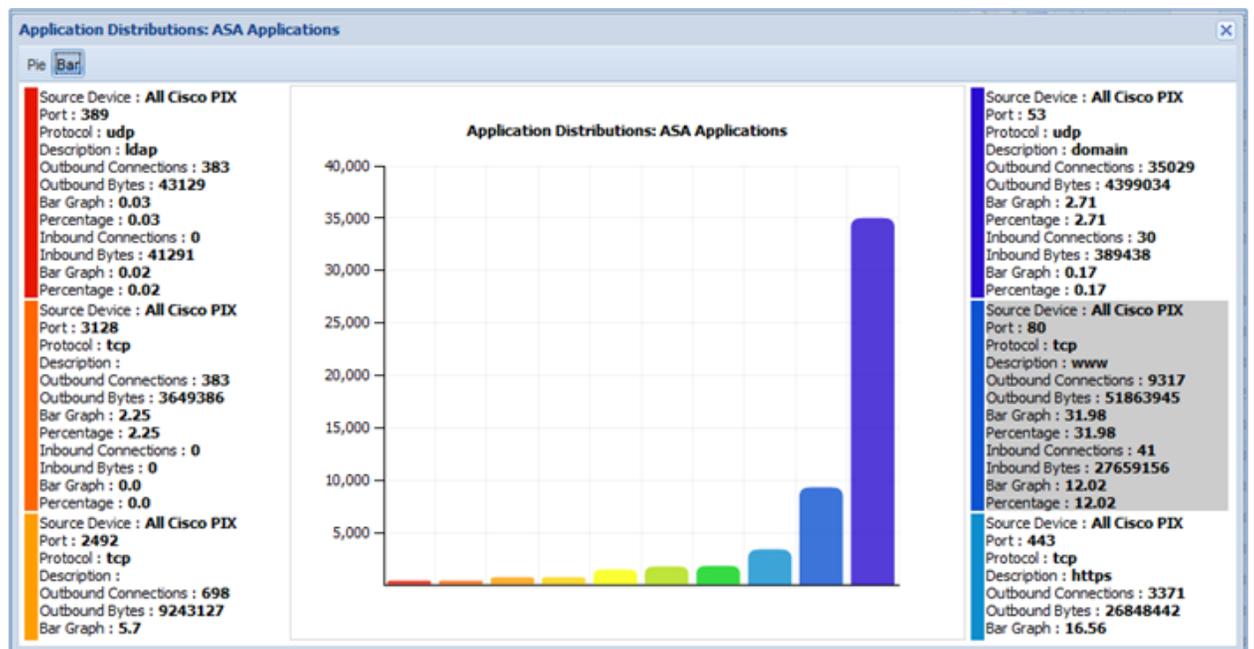
home > reports > network activity > application distribution > Application Distributions: ASA Applications LX 2010 LSP:17 - Jul 28, 2010 16:15:29 Europe/Paris

Sources: 0 Rules & 1 Log Source | No Filters | Display Chart | Edit Settings

28 Jul 2010 15:10:00 to 28 Jul 2010 16:10:00 Page 1 of 538

#	Source Device	Port	Protocol	Description	Outbound Connects	Outbound Bytes	Bar Graph	Percentage	Inbound Connector	Inbound Bytes	Bar Graph	Percentage
1	All Cisco PIX	80	tcp	www	9317	51863945		31.98	41	27659156		12.02
2	All Cisco PIX	7618	tcp		13	27148313		16.74	0	0		0.0
3	All Cisco PIX	443	tcp	https	3371	26848442		16.56	732	67709125		29.42
4	All Cisco PIX	110	tcp	pop3	1806	10190345		6.28	0	2827392		1.23
5	All Cisco PIX	2492	tcp		698	9243127		5.7	52	14530123		6.31
6	All Cisco PIX	13282	tcp		1	8033710		4.95	0	0		0.0
7	All Cisco PIX	22	tcp	ssh	177	5891488		3.63	26	25050029		10.89
8	All Cisco PIX	53	udp	domain	35029	4399034		2.71	30	389438		0.17
9	All Cisco PIX	515	tcp	printer	2	3742999		2.31	0	0		0.0
10	All Cisco PIX	3128	tcp		383	3649386		2.25	0	0		0.0
11	All Cisco PIX	993	tcp	imaps	69	2756838		1.7	0	5927641		2.58
12	All Cisco PIX	1443	tcp		43	2278649		1.41	0	0		0.0
13	All Cisco PIX	9100	tcp		42	705691		0.44	0	0		0.0
14	All Cisco PIX	5190	udp	aol	14	447323		0.28	0	50052		0.02
15	All Cisco PIX	5190	tcp	aol	200	436344		0.27	0	1023863		0.44
16	All Cisco PIX	3851	udp		229	318688		0.2	0	0		0.0
17	All Cisco PIX	554	tcp	rtsp	4	275577		0.17	0	0		0.0
18	All Cisco PIX	10550	udp		28	257344		0.16	0	0		0.0
19	All Cisco PIX	22947	udp		1	216911		0.13	0	0		0.0
20	All Cisco PIX	1863	tcp		100	177336		0.11	0	0		0.0

The report below describes the most popular applications passing inside Cisco ASA firewall, this report is called “application distribution”, and can be used to fine-tune the firewall policy table by putting on top the items for the most popular applications: Application Distribution – Tabular View



## ***Application Distribution – Chart View***

### ***Index Reports***

***Centurylink Analytics for open log management allows generation of reports on all data, including custom log sources. Each user-defined or predefined index search can be used to generate a custom report. These custom reports are based on single or multiple selection of index search filters.***

### ***Scheduled Reports***

***Centurylink Analytics provides additional capability of allowing summary reports to be sent to anyone, including CIOs and CSOs. Summary reports are sent via e-mail in PDF, HTML or CSV format. Scheduled reports allow CIOs and CSOs to quickly get an overview of their infrastructure each day, week or month.***

### ***Exporting Reports***

***To provide administrators the flexibility of viewing reports in different ways, Centurylink Analytics can export reports in PDF or CSV. PDF reports can be used as executive wqreports for CIOs and CSOs. CSV reports can be loaded into other tools such as Microsoft® Excel® to perform further analysis if needed.***

### ***Ratio-Based Detection***

***Unique ratio-based anomaly detection can be used to perform data analysis in real time and alert users when anomalous events are detected. Rate-based anomalies can be monitored on the basis of individual (groups of) devices and specific event types.***

### ***Policy-Based Detection***

***Proprietary policy validation engine allows customers to define a corporate business policy that is separate from the firewall or router's technical policy. By having a separate business policy, you can validate traffic logs to ensure there are no false positives or false rejections***

### ***Log Volume Detection***

***One of the most effective uses of log management is to ensure devices and applications are up and performing as designed. This rule has the capability of monitoring and alerting administrators when a device or application has stopped sending log data. This capability helps identify failed devices or applications, allow administrators to quickly recover from potential disasters and drill down to identify the root causes.***

### ***Baseline Alert***

***A built-in Artificial Intelligence Engine is available in the appliances. It builds a baseline of typical behavior over the span of a week. This baseline is built the first 2 weeks and continuously refined over the lifespan of the solution so as to accommodate for long-term behavioral modifications. It has knowledge and intelligence about each specific device individually, as well as about the whole infrastructure.***

### System Alert

*All Appliances include several system alerts that are preconfigured and enabled. These system alerts provide basic alerting on the Appliance itself*

### Alerting

*The solution supports SMTP and SNMP alerting. Users can customize alert priority, threshold level and keyword/regular expression matches, as well as device type or event type for individual SMTP/SNMP alert recipients.*

*The solution has a built-in alert viewing capability. Any problems detected and alerted by the can be viewed in the alert viewer. They can then be acknowledged by the appropriate personnel. The solution can also run reports on all alerts to identify any previously undetected anomalies.*

*To minimize the number of alerts being sent at one time, you can customize both the time span as well as the reset time of the alerts.*

### 7.2.4.2 SIEM Features

The Contractor shall offer the Web Security and Filtering features detailed in Table 7.2.4.2.a.

#### 1. Additional Devices Ordered Above Tier Maximum

The Contractor shall utilize the pricing structure identified below that allows for an initial installation and supplemental augmentation of the initial installation. This allows for the addition of devices beyond the number installed without requiring the Customer to be charged for the next feature/pricing install tier.

#### 2. Additional Devices Ordered Below Tier Maximum

If the initial order of devices is less than the maximum number allowed within the tier, no additional charges shall apply for additional devices up to the maximum number allowed by the tier.

**Table 7.2.4.2.a SIEM Features**

	Feature Name	Feature Description	Bidder Meet or Exceeds?		Bidder's Product Identifier
			Y	N	
1	<b>SIEM, 1 – 15 Devices</b>	SIEM service as described in Section 7.2.4.	Y		<b>QNB60912</b>
	Bidder's Product Description: <i>Log Management up to 50 devices using Tibco / LogLogic LX825. Includes services described in SOW, Install of site equipment, maintenance and management</i>				
2	<b>Each additional</b>	Each additional device above 15.	Y		<b>QNB60913</b>
	Bidder's Product Description: <i>Log Management up to 50 devices using Tibco / LogLogic LX825. Includes services described in SOW, Install of site equipment, maintenance and</i>				

	Feature Name	Feature Description	Bidder Meet or Exceeds?		Bidder's Product Identifier
			Y	N	
	<i>management</i>				
3	16-40 Devices	SIEM service as described in Section 7.2.4.	Y		QNB60914
	Bidder's Product Description: <i>Log Management up to 50 devices using Tibco / LogLogic LX825. Includes services described in SOW, Install of site equipment, maintenance and management</i>				
4	Each additional	Each additional device above 40.	Y		QNB60915
	Bidder's Product Description: <i>Log Management up to 50 devices using Tibco / LogLogic LX825. Includes services described in SOW, Install of site equipment, maintenance and management</i>				
5	41-100 Devices	SIEM service as described in Section 7.2.4.	Y		QNB60916
	Bidder's Product Description: <i>Log Management up to 250 devices using Tibco / LogLogic LX825. Includes services described in SOW, Install of site equipment, maintenance and management</i>				
6	Each additional	Each additional device above 100.	Y		QNB60917
	Bidder's Product Description: <i>Log Management up to 250 devices using Tibco / LogLogic LX825. Includes services described in SOW, Install of site equipment, maintenance and management</i>				
7	101-250 Devices	SIEM service as described in Section 7.2.4.	Y		QNB60918
	Bidder's Product Description: <i>Log Management up to 1000 devices using Tibco / LogLogic LX1025. Includes services described in SOW, Install of site equipment, maintenance and management.</i>				
8	Each additional	Each additional device above 250.	Y		QNB60919
	Bidder's Product Description: <i>Log Management up to 1000 devices using Tibco / LogLogic LX1025. Includes services described in SOW, Install of site equipment, maintenance and management.</i>				
9	251-1000 Devices	SIEM service as described in Section 7.2.4	Y		QNB60920

	Feature Name	Feature Description	Bidder Meet or Exceeds?		Bidder's Product Identifier
			Y	N	
	Bidder's Product Description: <i>Log Management up to 2500 devices using Tibco / LogLogic LX4025. Includes services described in SOW, Install of site equipment, maintenance and management.</i>				
10	Each additional	Each additional device above 1000.	Y		QNB60921
	Bidder's Product Description: <i>Log Management up to 2500 devices using Tibco / LogLogic LX4025. Includes services described in SOW, Install of site equipment, maintenance and management.</i>				
11	1001-2500 Devices	SIEM service as described in Section 7.2.4.	Y		QNB60922
	Bidder's Product Description: <i>Log Management up to 2500 devices using Tibco / LogLogic LX4025. Includes services described in SOW, Install of site equipment, maintenance and management.</i>				
	Each additional	Each additional device above 2500.	Y		QNB60923
12	Bidder's Product Description: <i>Log Management up to 2500 devices using Tibco / LogLogic LX4025. Includes services described in SOW, Install of site equipment, maintenance and management.</i>				

The Contractor may offer Unsolicited SIEM features in Table 7.2.4.2.b.

**Table 7.2.4.2.b Unsolicited SIEM Features**

	Feature Name	Feature Description	Bidder's Product Identifier
1	Bidder's Product Description:		
2	Bidder's Product Description:		
3	Bidder's Product Description:		

## 7.3 SERVICE LEVEL AGREEMENT (SLA)

The Contractor shall provide Service Level Agreements (SLAs) as defined below. The intent of this section is to provide Customers, CALNET 3 CMO and the Contractor with requirements that define and assist in the management of the SLAs. This section includes the SLA formats, general requirements, stop clock conditions and the Technical SLAs for the services identified in this solicitation.

### 7.3.1 SERVICE LEVEL AGREEMENT FORMAT

The Contractor shall adhere to the following format and include the content as described below for each Technical SLA added by the Contractor throughout the Term of the Contract:

1. SLA Name - Each SLA Name must be unique;
2. Definition - Describes what performance metric will be measured;
3. Measurements Process - Provides instructions how the Contractor will continuously monitor and measure SLA performance to ensure compliance. The Contractor shall provide details describing how and what will be measured. Details shall include source of data and define the points of measurement within the system, application, or network;
4. Service(s) - All applicable Categories or Subcategories will be listed in each SLA;
5. Objective(s) – Defines the SLA performance goal/parameters; and,
6. Rights and Remedies
  - a. Per Occurrence: Rights and remedies are paid on a per event basis during the bill cycle; and,
  - b. Monthly Aggregated Measurements: Rights and remedies are paid once during the bill cycle based on an aggregate of events over a defined period of time.

The Contractor shall proactively apply an invoice credit or refund when an SLA objective is not met. CALNET SLA Rights and Remedies do not require the Customer to submit a request for credit or refund.

*Bidder understands the Requirement and shall meet or exceed it? Yes Y No*

### 7.3.2 TECHNICAL REQUIREMENTS VERSUS SLA OBJECTIVES

Section 7.2 (Network Based Managed Security Services) defines the technical requirements for each service. These requirements are the minimum parameters each Bidder must meet in order to qualify for Contract award. Upon Contract award the committed technical requirements will be maintained throughout the remainder of the Contract.

Committed SLA objectives are minimum parameters which the Contractor shall be held accountable for all rights and remedies throughout Contract Term.

*Bidder understands the Requirement and shall meet or exceed it? Yes Y No*

### 7.3.3 TWO METHODS OF OUTAGE REPORTING: CUSTOMER OR CONTRACTOR

There are two (2) methods in which CALNET 3 service failures or quality of service issues may be reported and Contractor trouble tickets opened: Customer reported or Contractor reported.

The first method of outage reporting results from a Customer reporting service trouble to the Contractor's Customer Service Center via phone call or opening of a trouble ticket using the on-line Trouble Ticket Reporting Tool (IFB STPD 12-001-B Business Requirements Section B.9.4).

The second method of outage reporting occurs when the Contractor opens a trouble ticket as a result of network/system alarm or other method of service failure identification. In each instance the Contractor shall open a trouble ticket using the Trouble Ticket Reporting Tool (IFB STPD 12-001-B Business Requirements Section B.9.4) and monitor and report to Customer until service is restored.

*Bidder understands the Requirement and shall meet or exceed it? Yes Y No*

### 7.3.4 BIDDER RESPONSE TO SERVICE LEVEL AGREEMENTS

Many of the Service Level Agreements described below include multiple objective levels – Basic, Standard and Premier. Bidders shall indicate one (1) specific objective level they are committing to for each service in space provided in the “Objective” section of each SLA description.

*Bidder understands the Requirement and shall meet or exceed it? Yes Y No*

### 7.3.5 CONTRACTOR SLA MANAGEMENT PLAN

Within 90 calendar days of Contract award, the Contractor shall provide CALNET 3 CMO with a detailed SLA Management Plan that describes how the Contractor will manage the Technical SLAs for services in this IFB. The SLA Management plan shall provide processes and procedures to be implemented by the Contractor. The SLA Management Plan shall define the following:

1. Contractor SLA Manager and supporting staff responsibilities;
2. Contractor's process for measuring objectives for each SLA. The process shall explain how the Contractor will continuously monitor and measure SLA performance to ensure compliance. The Contractor shall provide details describing how and what will be measured. Details should include source of data and define the points of measurement within the system, application, or network;
3. Creation and delivery of SLA Reports (IFB STPD 12-001-B Business Requirements Section B.9.5). The Contractor shall include a sample report in accordance with IFB-B Business Requirements Section B.9.5 (SLA Reports) for the following: SLA Service Performance Report (IFB STPD 12-001-B Business Requirements Section B.9.5.1), SLA Provisioning Report (IFB STPD 12-001-B Business Requirements Section B.9.5.2), and SLA Catastrophic Outage Reports (IFB STPD 12-001-B Business Requirements Section B.9.5.3). The Contractor shall commit to a monthly due date. The reports shall be provided to the CALNET 3

CMO via the Private Oversight Website (IFB STPD 12-001-B Business Requirements Section B.9.2);

4. SLA invoicing credit and refund process;
5. Contractor SLA problem resolution process for SLA management and SLA reporting. The Contractor shall provide a separate process for Customers and CALNET 3 CMO; and,
6. Contractor SLA Manager to manage all SLA compliance and reporting. The Contractor shall include SLA Manager contact information for SLA inquiries and issue resolution for Customer and CALNET 3 CMO.

*Bidder understands the Requirement and shall meet or exceed it? Yes Y No \_\_\_\_\_*

### 7.3.6 TECHNICAL SLA GENERAL REQUIREMENTS

The Contractor shall adhere to the following general requirements which apply to all CALNET 3 Technical SLAs (Section 7.3.8):

1. With the exception of the Provisioning SLA, the total SLA rights and remedies for any given month shall not exceed the sum of 100 percent of the Total Monthly Recurring Charges (TMRC). Services with usage charges shall apply the Average Daily Usage Charge (ADUC) in addition to any applicable TMRC rights and remedies;
2. If a circuit or service fails to meet one (1) or more of the performance objectives, only the SLA with the largest monthly Rights and Remedies will be credited to the Customer, per event;
3. The Contractor shall apply CALNET 3 SLAs and remedies for services provided by Subcontractors and/or Affiliates;
4. The Definition, Measurement Process, Objectives, and Rights and Remedies shall apply to all services identified in each SLA. If a Category or Subcategory is listed in the SLA, then all services under that Category or Subcategory are covered under the SLA. Exceptions must be otherwise stated in the SLA;
5. TMRC rights and remedies shall include the service, option(s), and feature(s) charges;
6. The Contractor shall proactively and continuously monitor and measure all Technical SLA objectives;
7. The Contractor shall proactively credit all rights and remedies to the Customer within 60 calendar days of the trouble resolution date on the trouble ticket or within 60 calendar days of the Due Date on the Service Request for the Provisioning SLA;
8. To the extent that Contractor offers additional SLAs, or SLAs with more advantageous rights and/or remedies for same or similar services offered through tariffs, online service guides, or other government contracts (Federal, State, County, City), the State will be entitled to the same rights and/or remedies therein. The Contractor shall present the SLAs to CALNET 3 CMO for possible inclusion via amendments;

9. The Contractor shall apply CALNET 3 SLAs and remedies to services provided in geographic areas which the Contractor has committed to provide service;
10. The election by CALNET 3 CMO of any SLA remedy covered by this Contract shall not exclude or limit CALNET 3 CMO's or any Customer's rights and remedies otherwise available within the Contract or at law or equity;
11. The Contractor shall apply rights and remedies when a service fails to meet the SLA objective even when backup or protected services provide Customer with continuation of services;
12. The Contractor shall act as the single point of contact in coordinating all entities to meet the State's needs for provisioning, maintenance, restoration and resolution of service issues or that of their Subcontractors, Affiliates or resellers under this Contract;
13. The Customer Escalation Process (IFB STPD 12-001-B Business Requirements Section B.3.4.2) and/or the CALNET 3 CMO Escalation Process (IFB STPD 12-001-B Business Requirements Section B.3.4.1) shall be considered an additional right and remedy if the Contractor fails to resolve service issues within the SLA objective(s);
14. Trouble reporting and restoration shall be provided 24x365 for CALNET 3 services;
15. SLAs apply 24x365 unless SLA specifies an exception;
16. Contractor invoices shall clearly cross reference the SLA credit to the service Circuit ID in accordance with IFB STPD 12-001-B Business Requirements Section B.5.1 (Billing and Invoicing Requirements, #14);
17. The Contractor shall provide a CALNET 3 SLA Manager responsible for CALNET 3 SLA compliance. The SLA Manager shall attend regular meetings and be available upon request to address CALNET 3 CMO SLA oversight, report issues, and problem resolution concerns. The CALNET 3 SLA Manager shall also coordinate SLA support for Customer SLA inquiries and issue resolution;
18. The Contractor shall provide Customer and CALNET 3 CMO support for SLA inquiries and issue resolution; and,
19. Any SLAs and remedies negotiated between Contractor and third party service provider in territories closed to competition shall be passed through to the CALNET 3 Customer.

*Bidder understands the Requirement and shall meet or exceed it?* Yes Y No     

### **7.3.7 TROUBLE TICKET STOP CLOCK CONDITIONS**

The following conditions shall be allowed to stop the trouble ticket Outage Duration for CALNET 3 Contractor trouble tickets. The Contractor shall document the trouble ticket Outage Duration using the Stop Clock Condition (SCC) listed in Table 7.3.7 and include start and stop time stamps in the Contractor's Trouble Ticket Reporting Tool (IFB STPD 12-001-B Business Requirements Section B.9.4) for each application of a SCC.

Note: The Glossary (SOW Appendix A) defines term “End-User” as the “individual within an Entity that is utilizing the feature or service provided under the Contract.”

Stop Clock Conditions are limited to the conditions listed in Table 7.3.7.

**Table 7.3.7 – Stop Clock Conditions (SCC)**

#	Stop Clock Condition (SCC)	SCC Definition
1	<b>END-USER REQUEST</b>	Periods when a restoration or testing effort is delayed at the specific request of the End-User. The SCC shall exist during the period the Contractor was delayed, provided that the End-User’s request is documented and time stamped in the Contractor’s trouble ticket or Service Request system and shows efforts are made to contact the End-User during the applicable Stop Clock period.
2	<b>OBSERVATION</b>	Time after a service has been restored but End-User request ticket is kept open for observation. If the service is later determined by the End-User to not have been restored, the Stop Clock shall continue until the time the End-User notifies the Contractor that the Service has not been restored.
3	<b>END-USER NOT AVAILABLE</b>	Time after a service has been restored but End-User is not available to verify that the Service is working. If the service is later determined by the End-User to not have been restored, the Stop Clock shall apply only for the time period between Contractor’s reasonable attempt to notify the End-User that Contractor believes the service has been restored and the time the End-User notifies the Contractor that the Service has not been restored.
4	<b>WIRING</b>	Restoration cannot be achieved because the problem has been isolated to wiring that is not maintained by Contractor or any of its Subcontractors or Affiliates. If it is later determined the wiring is not the cause of failure, the SCC shall not apply.
5	<b>POWER</b>	Trouble caused by a power problem outside of the responsibility of the Contractor.
6	<b>FACILITIES</b>	Lack of building entrance Facilities or conduit structure that are the End-User’s responsibility to provide.
7	<b>ACCESS</b>	<p>Limited access or contact with End-User provided the Contractor documents in the trouble ticket several efforts to contact End-User for the following:</p> <ul style="list-style-type: none"> <li>a. Access necessary to correct the problem is not available because access has not been arranged by site contact or End-User representative;</li> <li>b. Site contact refuses access to technician who displays proper identification;</li> <li>c. Customer provides incorrect site contact information which prevents access, provided that Contractor takes reasonable steps to notify End-User of the improper contact information and takes steps to obtain the correct information ; or,</li> <li>d. Site has limited hours of business that directly impacts the Contractor’s ability to resolve the problem.</li> </ul> <p>If it is determined later that the cause of the problem was not at the</p>

#	Stop Clock Condition (SCC)	SCC Definition
		site in question, then the Access SCC shall not apply.
8	<b>STAFF</b>	Any problem or delay to the extent caused by End-User's staff that prevents or delays Contractor's resolution of the problem. In such event, Contractor shall make a timely request to End-User staff to correct the problem or delay and document in trouble ticket.
9	<b>APPLICATION</b>	End-User software applications that interfere with repair of the trouble.
10	<b>CPE</b>	Repair/replacement of Customer Premise Equipment (CPE) not provided by Contractor if the problem has been isolated to the CPE. If determined later that the CPE was not the cause of the service outage, the CPE SCC will not apply.
11	<b>NO RESPONSE</b>	Failure of the trouble ticket originator or responsible End-User to return a call from Contractor's technician for on-line close-out of trouble tickets after the Service has been restored as long as Contractor can provide documentation in the trouble ticket substantiating the communication from Contractor's technician.
12	<b>MAINTENANCE</b>	An outage directly related to any properly performed scheduled maintenance or upgrade scheduled for CALNET 3 service. Any such stop clock condition shall not extend beyond the scheduled period of the maintenance or upgrade. SLAs shall apply for any maintenance caused outage beyond the scheduled maintenance period. Outages occurring during a scheduled maintenance or upgrade period and not caused by the scheduled maintenance shall not be subject to the Maintenance SCC.
13	<b>THIRD PARTY</b>	Any problem or delay caused by a third party not under the control of Contractor, not preventable by Contractor, including, at a minimum, cable cuts not caused by the Contractor. Contractor's Subcontractors and Affiliates shall be deemed to be under the control of Contractor with respect to the equipment, services, or Facilities to be provided under this Contract.
14	<b>FORCE MAJEURE</b>	Force Majeure events, as defined in the PMAC General Provisions - Telecommunications, Section 28 (Force Majeure).

Bidder understands the Requirement and shall meet or exceed it? Yes Y No

### 7.3.8 TECHNICAL SERVICE LEVEL AGREEMENTS

The Contractor shall provide and manage the following Technical SLAs.

#### 7.3.8.1 Availability (M-S)

<b>SLA Name:</b> Availability					
<b>Definition:</b> The percentage of time a CALNET 3 service is fully functional and available for use each calendar month.					
<b>Measurement Process:</b> The monthly Availability Percentage shall be based on the accumulative total of all Unavailable Time derived from all trouble tickets closed, for the affected service (includes Contractor provided web portal, dashboard and reports), and feature per calendar month. The monthly Availability Percentage equals the Scheduled Uptime per month less Unavailable Time per month divided by Scheduled Uptime per month multiplied by 100. Scheduled Uptime is 24 x number of days in the month. All Unavailable Time applied to other SLAs, which results in a remedy, will be excluded from the monthly accumulated total.					
<b>Service(s):</b>					
DDoS Detection and Mitigation Service		Email Monitoring and Scanning Service			
Web Security and Filtering Service		Security Information and Event Management (SIEM)			
<b>Objective(s):</b>					
		Basic (B)	Standard (S)	Premier (P)	Bidder's Objective Commitment (B, S or P)
	DDoS Detection and Mitigation Service	≥ 99.9%	≥ 99.95%	≥ 99.99%	<b>S</b>
	Email Monitoring and Scanning Service	≥ 99.9%	≥ 99.95%	≥ 99.99%	<b>P</b>
	Web Security and Filtering Service	≥ 99.9%	≥ 99.95%	≥ 99.99%	<b>P</b>
	SIEM	≥ 99.9%	≥ 99.95%	≥ 99.99%	<b>P</b>
<b>Rights and Remedies</b>	<b>Per Occurrence:</b> N/A				
	<b>Monthly Aggregated Measurements:</b> First month the service fails to meet the committed SLA objective shall result in a 15 percent rebate of the TMRC. The second consecutive month the service fails to meet the committed SLA objective shall result in a 30 percent rebate of TMRC. Each additional consecutive month the service fails to meet the committed SLA objective shall result in a 50 percent rebate of the TMRC.				

Bidder understands the Requirement and shall meet or exceed it? Yes Y No

7.3.8.2 Catastrophic Outage 2 (CAT 2) (M-S)

<b>SLA Name:</b> Catastrophic Outage 2 (CAT 2)					
<b>Definition:</b> Failure of any part of the Network Based Managed Security Services architecture components (hardware, software, and interconnection of components) based on a common cause that results in a total failure of a service for two (2) or more CALNET 3 Customers.					
<b>Measurement Process:</b> The Outage Duration begins when a network alarm is received by the Contractor from an outage-causing event or the opening of a trouble ticket by the Customer or Contractor, whichever occurs first. Upon notification from the Customer or network alarm, the Contractor shall compile a list for each End-User service and feature affected by a common cause for tracking and reporting of the SLA rights and remedies. Outage Duration shall be measured on a per-End-User service basis from information recorded from the network equipment/system or Customer reported trouble ticket. Each End-User service is deemed out of service from the first notification until the Contractor determines the End-User service is restored. Any End-User service reported by the End-User/Customer as not having been restored shall have the outage time adjusted to the actual restoration time.					
<b>Service(s):</b>					
DDoS Detection and Mitigation Service		Email Monitoring and Scanning Service			
Web Security and Filtering Service		Security Information and Event Management (SIEM)			
<b>Objective(s):</b>					
The objective restoral time shall be:					
		Basic (B)	Standard (S)	Premier (P)	Bidder's Objective Commitment (B, S or P)
	DDoS Detection and Mitigation Service	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	<b>S</b>
	Email Monitoring and Scanning Service	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	<b>P</b>
	Web Security and Filtering Service	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	<b>P</b>
	SIEM	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	<b>B</b>
<b>Rights and Remedies</b>	<b>Per Occurrence:</b> 100 percent of the TMRC for each End-User service not meeting the committed objective for each CAT 2 fault				
	<b>Monthly Aggregated Measurements:</b> N/A				

Bidder understands the Requirement and shall meet or exceed it? Yes Y No

7.8.3.3 Catastrophic Outage 3 (CAT 3) (M-S)

<b>SLA Name:</b> Catastrophic Outage 3 (CAT 3)					
<b>Definition:</b> The total loss of one (1) or more CALNET 3 Network Based Managed Security services on a system wide basis.					
<b>Measurement Process:</b> The Outage Duration begins when a network alarm is received by the Contractor from an outage-causing event or the opening of a trouble ticket by the Customer or Contractor, whichever occurs first. Upon notification from the Customer or network alarm, the Contractor shall compile a list for each End-User service and feature affected by a common cause. Outage Duration shall be measured on a per-End-User service basis from information recorded from the network equipment/system or trouble ticket. Each End-User service is deemed out of service from the first notification until the Contractor determines the End-User service is restored. Any End-User service reported by the End-User/Customer as not having been restored shall have the outage time adjusted to the actual restoration time.					
<b>Service(s):</b>					
DDoS Detection and Mitigation Service		Email Monitoring and Scanning Service			
Web Security and Filtering Service		Security Information and Event Management (SIEM)			
<b>Objective(s):</b>					
The objective restoral time shall be:					
		Basic (B)	Standard (S)	Premier (P)	Bidder's Objective Commitment (B, S or P)
	DDoS Detection and Mitigation Service	≤ 30 minutes	N/A	≤ 15 minutes	<b>B</b>
	Email Monitoring and Scanning Service	≤ 30 minutes	N/A	≤ 15 minutes	<b>P</b>
	Web Security and Filtering Service	≤ 30 minutes	N/A	≤ 15 minutes	<b>P</b>
	SIEM	≤ 30 minutes	N/A	≤ 15 minutes	<b>B</b>
<b>Rights and Remedies</b>	<b>Per Occurrence:</b> 100 percent of the TMRC for each End-User service not meeting the committed objective for each CAT 3 fault.				
	<b>Monthly Aggregated Measurements:</b> N/A				

Bidder understands the Requirement and shall meet or exceed it? Yes Y No



7.3.8.5 SIEM Event Notification (M-S)

<b>SLA Name:</b> SIEM Critical Event Notification				
<b>Definition:</b> The Contractor shall notify the Customer via a verbal person-to-person telephone call to authorized users when a critical security event that represents a security incident or threat to the Customer, within the objective timeframe.				
<b>Measurement Process:</b> The amount of time between the identification of a critical security event and the notification (or when the Contractor initially attempts to notify) of the customer.				
<b>Service(s):</b>				
SIEM				
<b>Objective(s):</b>				
				Bidder's Objective Commitment (B, S or P)
Service	Basic (B)	Standard (S)	Premier (P)	
SIEM	≤ 45 minutes	≤ 30 minutes	≤ 15 minutes	<b>B</b>
<b>Rights and Remedies</b>	<b>Per Occurrence:</b> Customer will receive a credit equal to 25 percent of the SIEM Service TMRC for each event in which a Customer is not notified within the committed objective.			
	<b>Monthly Aggregated Measurements:</b> N/A			

Bidder understands the Requirement and shall meet or exceed it? Yes Y No

7.3.8.6 DDoS Customer Notification (M-S)

<b>SLA Name:</b> DDoS Customer Notification				
<b>Definition:</b> The Contractor shall notify the Customer via an e-mail and a verbal person-to-person telephone call to authorized users when an anomaly or attack is detected, within the objective timeframe.				
<b>Measurement Process:</b> The amount of time between the identification of an anomaly or attack, and the notification (or when the Contractor initially attempts to notify) of the customer.				
<b>Service(s):</b>				
DDoS Detection and Mitigation				
<b>Objective(s):</b>				
				Bidder's Objective Commitment (B, S or P)
Service	Basic (B)	Standard (S)	Premier (P)	
DDoS Detection and Mitigation	≤ 45 minutes	≤ 30 minutes	≤ 15 minutes	<i>P</i>
<b>Rights and Remedies</b>	<b>Per Occurrence:</b> Customer will receive a credit equal to 25 percent of the DDoS Detection and Mitigation Service TMRC for each event in which a Customer is not notified within the committed objective.			
	<b>Monthly Aggregated Measurements:</b> N/A			

Bidder understands the Requirement and shall meet or exceed it? Yes Y No



7.3.8.8 DDoS Time to Mitigate (M-S)

<b>SLA Name:</b> DDoS Time to Mitigate				
<b>Definition:</b> The time to initiate DDoS mitigation upon the identification of an attack.				
<b>Measurement Process:</b> The amount of time between the detection via Customer or Contractor identification of an anomaly or attack, and the initiation of the mitigation process.				
<b>Service(s):</b>				
DDoS Detection and Mitigation				
<b>Objective(s):</b>				
Mitigation shall begin within:				
	Basic (B)	Standard (S)	Premier (P)	Bidder's Objective Commitment (B or S)
DDoS Detection and Mitigation	45 minutes	30 minutes	15 minutes	<b>P</b>
<b>Rights and Remedies</b>	<b>Per Occurrence:</b>			
	Basic Time to Mitigate Minutes	Standard Time to Mitigate Minutes	Premier Time to Mitigate Minutes	Percentage of TMRC per event
	46 - 75	31 -60	16 - 45	25%
	76 - 135	61- 120	46- 105	50%
	136 and over	121 and over	106 and over	100%
<b>Monthly Aggregated Measurements:</b> N/A				

Bidder understands the Requirement and shall meet or exceed it? Yes Y No

7.3.8.9 Notification

<b>SLA Name:</b> Notification	
<b>Definition:</b> The Contractor notification to CALNET 3 CMO and designated stakeholders in the event of a CAT 2 or CAT 3 failure, Contractor, Subcontractor or Affiliate network event, terrorist activity, threat of natural disaster, or actual natural disaster which results in a significant loss of telecommunication services to CALNET 3 End-Users or has the potential to impact services in a general or statewide area. The State understands initial information regarding the nature of the outage may be limited.	
<b>Measurement Process:</b> The Contractor shall adhere to the Network Outage Response requirements (IFB STPD 12-001-B Business Requirements Section B.3.3) and notify the CALNET 3 CMO and designated stakeholders for all CAT 2 and CAT 3 Outages or for network outages resulting in a significant loss of service. Notification objectives will be based on the start time of the outage failure determined by the opening of a trouble ticket or network alarm, whichever occurs first. For events based on information such as terrorist activity or natural disaster, the Contractor shall notify CALNET 3 CMO and designated stakeholder when information is available.	
<b>Service(s):</b> All services	
<b>Objective(s):</b> Within 60 minutes of the above mentioned failures' start time, the Contractor shall notify CALNET 3 CMO and designated stakeholders using a method defined in IFB STPD 12-001-B Business Requirements Section B.3.3 (Network Outage Response). At 60 minute intervals, updates shall be given on the above mentioned failures via the method defined in IFB STPD 12-001-B Business Requirements Section B.3.3 (Network Outage Response). This objective is the same for Basic, Standard and Premier commitments.	
<b>Rights and Remedies</b>	<b>Per Occurrence:</b> Senior Management Escalation
	<b>Monthly Aggregated Measurements:</b> N/A

Bidder understands the Requirement and shall meet or exceed it? Yes Y No

7.3.8.10 Provisioning (M-S)

<b>SLA Name:</b> Provisioning				
<p><b>Definition:</b> Provisioning shall include new services, moves, adds and changes completed by the Contractor on or before the due dates. The Provisioning SLA shall be based on committed installation intervals established in this SLA or due dates negotiated between Customer and Contractor documented on the Contractor’s order confirmation notification or Contracted Service Project Work SOW in accordance with IFB STPD 12-001-B Business Requirements Section B.2.5.4 #7 (Provisioning and Implementation). The Contractor shall meet the committed interval dates or due date negotiated with the Customer. If the Customer agrees to a negotiated due date, the negotiated due date supersedes the committed interval. At the Customer’s discretion, if the scope of the Service Request(s) meets the Coordinated or Managed Project criteria, negotiated due dates will be established and documented in the Project Schedule per IFB STPD 12-001-B Business Requirements Section B.6 (Contracted Service Project Work).</p> <p>Provisioning SLAs have two (2) objectives:                  Objective 1: Individual Service Request; and                  Objective 2: Successful Install Monthly Percentage by Service Type.</p> <p>Note: Provisioning timelines include extended demarcation wiring, when appropriate.</p>				
<b>Measurement Process:</b>				
<p><b>Objective 1: Individual Service Request:</b> Install intervals are based on the committed installation intervals established in this SLA or due dates negotiated between Customer and Contractor documented on the Service Request. This objective requires the Contractor to meet the due date for each individual Service Request.</p> <p><b>Objective 2: Successful Install Monthly Percentage per service Type:</b> The Contractor shall sum all individual Service Requests per service, as listed below, meeting the objective in the measurement period (per month) and divide by the sum of all individual Service Requests due per service in the measurement period and multiply by 100 to equal the percentage of Service Requests installed on time. The Contractor must meet or exceed the objective below in order to avoid the rights and remedies.</p>				
<b>Service (Features must be installed in conjunction with the service except when listed below)</b>		<b>Committed Interval Calendar Days</b>	<b>Coordinated/Managed Project</b>	
DDoS Detection and Mitigation Service		N/A	Coordinated/Managed Project	
Email Monitoring and Scanning Service		N/A	Coordinated/Managed Project	
Web Security and Filtering Service		N/A	Coordinated/Managed Project	
SIEM		N/A	Coordinated/Managed Project	
<b>Objective(s):</b>				
<p>Objective 1: Individual Service Request: Service installed on or before the Committed Interval or negotiated due date.</p> <p>Objective 2: Successful Install Monthly Percentage per Service:</p>				
Service	Basic (B)	Standard (S)	Premier (P)	Bidder’s Objective Commitment (B, S or P)
DDoS Detection and Mitigation Service	N/A	≥ 90%	≥ 95%	<b>P</b>

	Email Monitoring and Scanning Service	N/A	≥ 90%	≥ 95%	P	
	Web Security and Filtering Service	N/A	≥ 90%	≥ 95%	P	
	SIEM	N/A	≥ 90%	≥ 95%	S	
<b>Rights and Remedies</b>	<b>Per Occurrence:</b> Objective 1: Individual Service Requests: 50 percent of installation fee credited to Customer for any missed committed objective.					
	<b>Monthly Aggregated Measurements:</b> Objective 2: 100 percent of the installation fee credited to Customer for all Service Requests (per service type) that did not complete on time during the month if the Successful Install Monthly Percentage is below the committed objective.					

Bidder understands the Requirement and shall meet or exceed it? Yes Y No



7.3.8.12 Unsolicited Service Enhancement SLAs

All unsolicited service enhancements shall be considered a feature of the service, and therefore shall be included as such under the SLAs as defined in this Section.

*Bidder understands the Requirement and shall meet or exceed it?* Yes Y No       

7.3.8.13 Proposed Unsolicited Offerings

The Contractor shall provide SLAs as defined in SLA Section 7.3. for each unsolicited offering determined by the CALNET 3 CMO not to be a feature of a service or a component of an unbundled service identified in the technical requirements. SLA tables shall be amended after Contract award to include all new unsolicited services. Bidder understands the Requirement and shall meet or exceed it?

*Bidder understands the Requirement and shall meet or exceed it?* Yes Y No       

7.3.8.14 Contract Amendment Service Enhancement SLAs

All Contract amendment service enhancements shall be considered a feature of the service, therefore included as such under the SLAs as defined in this Section 7.3.8.

*Bidder understands the Requirement and shall meet or exceed it?* Yes Y No