Verizon

IFB STPD 12-001-B, C3-B-13-02-TS-08
Amendment #10, Rev. March 28, 2018

CALNET 3, Category 7: Network Based Managed Security

Volume 2 – Response to Unique Subcategory Requirements

SOW Technical Requirements Response

© 2013 Verizon. All Rights Reserved.
The Verizon and Verizon Business names and logos and all other names, logos, and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States or other countries. All other trademarks and service marks are the property of their respective owners.

A PROPOSAL TO

State of California

California Department of Technology
Statewide Technology Procurement Division

for

Best and Final Offer Resubmission

Volume 2 – Category 7 – Network Based Managed Security

INVITATION FOR BID - IFB STPD 12-001-B

March 17, 2014

Presented by:

Ross Shapiro
Managing Partner

11080 White Rock Rd., Suite 200
Rancho Cordova, CA 95670
916 508-4704
ross.shapiro@verizon.com

© 2013 Verizon. All Rights Reserved.
The Verizon and Verizon Business names and logos and all other names, logos, and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States or other countries. All other trademarks and service marks are the property of their respective owners.

Contents

Required IFB Exhibits

Volume 2 should contain all information that is unique to each Category or Subcategory being bid, with each Category or Subcategory separated into its own binder (or binders). Each Category or Subcategory binder should contain the following items:

1. Required IFB Exhibits unique to each Category or Subcategory, in the following order:

b. Exhibit 12: GSPD 05-105, Bidder Declaration

Verizon Response

The required exhibit is provided in the following pages, and as an embedded document in the electronic version of this submission.

To Open File:

- *Double Click "icon"*

  Or

- *Right Click over "icon", then select "Object", then select "Open"*

Exhibit 12_Bidder Declarations_Cat 7.pd

Response to SOW Technical Requirements

TECHNICAL REQUIREMENTS

CATEGORY 7 – NETWORK BASED MANAGED SECURITY

7.7.1 OVERVIEW

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

This 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 this IFB 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 X No_____

Description:

Verizon will provide a network based Distributed Denial of Service (DDoS) detection and mitigation service. Detection and mitigation shall occur in the Verizon IP backbone before traffic reaches the Customer edge router. Verizon will collect samples of Customer IP packets from Customer edge router to establish normal traffic patterns and to minimize false positives during the detection/mitigation process and perform periodic "tuning" of normal traffic patterns established. Verizon will sample Customer traffic on an ongoing basis and route the samples to a network based DDoS function for analysis, identification, reporting and alerting of anomalies in Customer traffic and DDoS attacks. Upon detection of DDoS attack, Verizon will 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 via a secure tunnel. Upon Verizon determination that the DDoS attack has subsided, Verizon will restore the normal routing of Customer traffic.

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 X No_____

Description:

Verizon will support the initiation of DDoS mitigation described below:

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

2. Verizon identifies the DDoS attack and initiates the mitigation.

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 X No_____

Description:

Verizon will 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.

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 X No_____

Description:

Verizon will provide a secure web based portal for authorized users and it will include:

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.

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 Meets or Exceeds? Y	N	Bidder's Product Identifier
1	**DDoS Detection and Mitigation, 1 – 2 GB**	DDoS Detection and Mitigation Service as described in Section 7.2.1 for 1-2 GB of traffic flow.	Y		DDSO1002
	Bidder's Product Description: Verizon will provide DDoS Detection and Mitigation Service as described in Section 7.2.1 for 1-2 GB of traffic flow.				
2	**DDoS Detection and Mitigation, 3 – 4 GB**	DDoS Detection and Mitigation Service as described in Section 7.2.1 for 3-4 GB of traffic flow	Y		DDOS3004
	Bidder's Product Description: Verizon will provide DDoS Detection and Mitigation Service as described in Section 7.2.1 for 3-4 GB of traffic flow.				
3	**DDoS Detection and Mitigation, 5 – 6 GB**	DDoS Detection and Mitigation Service as described in Section 7.2.1 for 5-6 GB of traffic flow	Y		DDOS5006
	Bidder's Product Description: Verizon will provide DDoS Detection and Mitigation Service as described in Section 7.2.1 for 5-6 GB of traffic flow.				

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	**Bidder's Product Description:**		
2	**Bidder's Product Description:**		
3	**Bidder's Product Description:**		

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 X No_____

Description:

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

Verizon Managed Email Content service acts as a customer's first line of defense against viruses, spam, and unwanted e-mail content. By scanning e-mail at the network level, Managed Email Content can eliminate security threats before they reach their intended destination. Because Managed Email Content requires no additional hardware or software, it ensures virus protection without the need for upgrades or patches.

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 X No_____

Description:

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

The Verizon Anti-Virus solution uses artificial intelligence and learning from an ever-expanding KnowledgeBase of e-mail security threats to identify new viruses, both known and unknown. From its unique position, operating at the Internet level rather than server or desktop level, the Verizon Anti-Virus service can identify techniques or characteristics which are indicative of an e-mail virus before it reaches the customer enterprise.

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 X No_____

Description:

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

The heuristic scanning entails scoring each e-mail against extensive rule sets. The rule sets analyze both header and text of each individual e-mail to determine the probability of identifying spamming techniques used within the e-mail.

Verizon's Anti-spam enlists the use of the Bayesian theory. This method assists heuristics in accuracy of identifying "true" spam. The Bayesian theorem develops a statistical model to determine what messages are spam and which are non-spam. If an e-mail in question scores a specified value, the e-mail is immediately identified as spam and the alerting mechanism automatically goes into action.

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 X No_____

Description:

Verizon will provide content control function that will allow a Customer to apply an acceptable use policy on incoming/outgoing email automatically as emails are scanned.

Operating at the Internet level, Verizon Content Control intercepts inappropriate content sent and received by our customers' end-users by scanning the subject, body, and attachments of user e-mail. Verizon Content Control monitors for key words and phrases. Inappropriate content can include malicious as well as confidential content.

Verizon Content Control is a multi-layered solution that can be configured to meet each customer's needs by controlling the number, type, and size of e-mail and attachments by individual user or groups of users, as defined by the customer administrator. The administrator may also control these features by time of day and allows for the prioritization of e-mail based on the customer's e-mail policy.

- Uses advanced technology designed to detect confidential, malicious and inappropriate content.
- Monitors usage of specified key words and phrases and protects from email abuse.
- Uses block and approved lists to stop certain users or domains from sending/receiving e-mails to/from certain organizations.
- Determines what e-mail is and is not allowed to be sent in or out of an organization.
- Handles e-mails of high/low priority according to the organization’s email policy.

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 X No_____

Description:

Verizon will provide the isolation area that 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.

Administration is performed on a web based management portal. A single administrative logon can be used to manage multiple services.

When a virus or malware is detected in an email, the infected email is placed into a holding pen, where it is stored. This quarantine period means that the malicious email is isolated and cannot infect the intended recipient's computer. Each quarantined email is given a unique identifier. This identifier is provided in the alerts that can be issued to administrators and users when an email containing a suspect virus is received.

The e-mail detected as spam will not reach the end-user or network, but will be re-directed to spam Quarantine. The spam Quarantine has an end-user interface. End-users are able to view, release, and delete spam.

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 X No_____

Description:

Verizon will provide Notification that allows a Customer to be notified via E-mail when an anti-virus, anti-spam or content control function has been invoked.

E-mail notifications are sent to the user and administrator when a rule has been invoked. Messages can be customized for specific violations if desired.

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 X No_____

Description:

Verizon will 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.

Dashboard, summary, detailed, and scheduled reporting options are included and configurable.

The key statistics dashboard provides a quick view of the current service performance levels and notable activities such as virus blocks or emails that have triggered a policy.

Report requests provide a way to get more in-depth reporting, allowing you to customize what metrics and time periods are included. Reports can be executed as a one-off or scheduled to run at regular intervals, with options to deliver via portal or straight to your inbox.

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 Meets or Exceeds? Y	N	Bidder's Product Identifier
1	**Email Monitoring and Scanning Service, 1-49**	Email managed security services seat as described in Section 7.2.2.	Y		EMLM0049
	Bidder's Product Description: Verizon will provide Email managed security services seat as described in Section 7.2.2.				
2	**Email Monitoring and Scanning Service, 50-74**	Email managed security services seat as described in Section 7.2.2.	Y		EMLM0074
	Bidder's Product Description: Verizon will provide Email managed security services seat as described in Section 7.2.2.				

	Feature Name	Feature Description	Bidder Meets or Exceeds? Y	N	Bidder's Product Identifier
3	**Email Monitoring and Scanning Service, 75-99**	Email managed security services seat as described in Section 7.2.2.	Y		EMLM0099
	Bidder's Product Description: Verizon will provide Email managed security services seat as described in Section 7.2.2.				
4	**Email Monitoring and Scanning Service, 100-500**	Email managed security services seat as described in Section 7.2.2.	Y		EMLM0500
	Bidder's Product Description: Verizon will provide Email managed security services seat as described in Section 7.2.2.				
5	**Email Monitoring and Scanning Service, 501-1000**	Email managed security services seat as described in Section 7.2.2.	Y		EMLM1000
	Bidder's Product Description: Verizon will provide Email managed security services seat as described in Section 7.2.2.				
6	**Email Monitoring and Scanning Service, 1001 and above**	Email managed security services seat as described in Section 7.2.2.	Y		EMLM1001
	Bidder's Product Description: Verizon will provide Email managed security services seat as described in Section 7.2.2.				

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

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 X No_____

Description:

Verizon will provide a network based web security and filtering service. All hardware/software necessary to provide service shall reside in the Verizon network and will be maintained, monitored and supported by Verizon. The service will 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 will:

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.

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 X No_____

Description:

Verizon will provide a service that will 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 will include standard and custom reports accessible through the web based portal.

Summary reports provide status updates and metrics in a convenient PDF format. The summary report contains graphs, tables, and key statistics on Web volume, user activity, blocked threats and blocked Web page requests which violated the organization's policy. These reports can be customized to reflect a fixed or custom date range, and data for these reports is available from the previous day to the last 12 months of the use of the service.

Audit reports provide detailed information on individual users and are provided in a PDF format. Audit reports include the same customization filters that are available with the detailed reporting option; however it is also possible to specify additional report criteria for more granular data, such as filtering activity by specific URL categories, Policy rules triggered, or destination website URLs.

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 Meets or Exceeds? Y	N	Bidder's Product Identifier
1	**Web Security and Filtering Service**	Web Security and Filtering service as described in Section 7.2.3.	Y		WSFS0000
	Bidder's Product Description: Verizon will provide Web Security and Filtering service as described in Section 7.2.3.				

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

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 X No_____

Description:

Verizon will provide a networked based SIEM service. The service will collect, analyze, assess and correlate security events from devices located on the Customer premise. All hardware/software necessary to provide service will reside in the Verizon network and will be maintained, monitored and supported by Verizon, 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 Verizon 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. Verizon escalations will consist of a security incident report as defined in Section 7.2.4.1 below.

The Verizon network based SIEM service provides threat analysis by interpretation, analysis, and correlation of logs and alarms produced by the security devices located on the customer premise. Verizon's network based SIEM specializes in correlating threat data (Risk Based Correlation) with information about the protected devices and the assets they protect (vulnerability information, technical asset information and asset profile information) with security intelligence, and network intelligence to determine the risk to the customer's environment.

Deeper investigation and escalation of security incidents is provided by Verizon security analysts who specialize in root cause analysis and who can provide recommendations for remediation. The aim is to provide information critical to risk management, risk mitigation, and risk acceptance decisions. Security analysts assist with escalation of 'harmful attack' incidents, implementing emergency rule-set changes to block attacks and providing incident reports.

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 X No_____

Description:

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

The reports will provide security information on devices and agents, individually and aggregated. Verizon'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.

The Verizon Security Dashboard is a secure website or portal under control of Verizon that provides statistics, lifecycle management functions, audit trail and reports on customer services device(s). From the Security Dashboard customers can manage security threats and risks by investigating intrusion attempts and threats by reviewing security incidents, events and logs. Customers will have a near real time view on the events being processed customer can view their (virtual) security devices grouped by location or business unit.

Threat signature information is presented per event after it has gone through the Verizon proprietary SIEM and a risk based correlation process. Depending on signatures created in security devices, packet dumps per event can also be viewed through the security dashboard.

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 Meets or Exceeds? Y	N	Bidder's Product Identifier
1	**SIEM, 1 – 15 Devices**	SIEM service as described in Section 7.2.4.	Y		SIEM0015
	Bidder's Product Description: Verizon will provide SIEM service as described in Section 7.2.4.				
2	**Each additional**	Each additional device above 15.	Y		SIEA0015
	Bidder's Product Description: Verizon will provide Each additional device above 15.				

	Feature Name	Feature Description	Bidder Meets or Exceeds? Y	N	Bidder's Product Identifier
3	**16-40 Devices**	SIEM service as described in Section 7.2.4.	Y		SIEM0040
	Bidder's Product Description: Verizon will provide SIEM service as described in Section 7.2.4.				
4	**Each additional**	Each additional device above 40.	Y		SIEA0040
	Bidder's Product Description: Verizon will provide Each additional device above 40.				
5	**41-100 Devices**	SIEM service as described in Section 7.2.4.	Y		SIEM0100
	Bidder's Product Description: Verizon will provide SIEM service as described in Section 7.2.4.				
6	**Each additional**	Each additional device above 100.	Y		SIEA0100
	Bidder's Product Description: Verizon will provide Each additional device above 100.				
7	**101-250 Devices**	SIEM service as described in Section 7.2.4.	Y		SIEM0250
	Bidder's Product Description: Verizon will provide SIEM service as described in Section 7.2.4.				
8	**Each additional**	Each additional device above 250.	Y		SIEA0250
	Bidder's Product Description: Verizon will provide Each additional device above 250.				
9	**251-1000 Devices**	SIEM service as described in Section 7.2.4.	Y		SIEM1000
	Bidder's Product Description: Verizon will provide SIEM service as described in Section 7.2.4.				
10	**Each additional**	Each additional device above 1000.	Y		SIEA1000
	Bidder's Product Description: Verizon will provide Each additional device above 1000.				
11	**1001-2500 Devices**	SIEM service as described in Section 7.2.4.	Y		SIEM2500
	Bidder's Product Description: Verizon will provide SIEM service as described in Section 7.2.4.				
12	**Each additional**	Each additional device above 2500.	Y		SIEA2500
	Bidder's Product Description: Verizon will provide Each additional device above 2500.				

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

Table 7.2.4.2.b Unsolicited SIEM Features

Verizon Vulnerability Management (VVM) Service is a solution that automates network auditing and vulnerability management across an organization, including network discovery and mapping, asset management, vulnerability reporting and remediation tracking. Driven by our comprehensive KnowledgeBase of known vulnerabilities, VVM Service enables cost-effective protection against vulnerabilities with one scanner appliance deployed in the customer environment. The Verizon's Cloud Platform core scanning technology is inference-based. It begins by creating an accurate inventory of the operating system, protocols, ports and services with an IP Address in the customer environment. This IP Address inventory is then used to developed vulnerability expert system specific to the IP Address, which chooses the appropriate set of vulnerabilities to test based on the IP Address profile. The result is a customized scan of each target. Customer does not need to have an understanding of the systems on the network or obtain specific credentials to perform vulnerability scanning. An example is VVM will only launch applicable modules and specific vulnerability checks on listening applications (i.e. Microsoft 10 will have only Microsoft 10 vulnerability checks attempted, Apache will have only Apache vulnerabilities checks, etc.). Web Application Scanning is an additional layered on service feature outside this base VVM service.

During a Scan, VVM performs a user configurable TCP, UDP, and RPC port scan followed by a set of modules called Service Discovery. Service Discovery takes each port that is identified as open or filtered as part of the port scan modules and intelligently determines the application type, vendor, and version through a combination of banner detection and intelligent active packet/service testing. VVM Cloud Platform is able to more accurately determine IP address inventory of what "service" is actually running on a given port.

Another feature of VVM service is Verizon Payment Card Industry Compliance (PCI) which is included at no additional charge. PCI Compliance (PCI) module provides organizations storing cardholder data a cost-effective and highly automated solution to verify and document compliance with PCI Data Security Standards. The reports PCI Compliance scan produces to the customer provides the tools necessary to support their PCI compliant environment. This provides the customer the ability to use these reports available with the Verizon PCI scanning service to stay current to identify PCI scanning compliance (e.g. PCI Data Security Standards quarterly reviews). Verizon PCI Compliance service is an authorized PCI DSS scanning vendor which can document false positives and provide official quarterly scanning reports. The PCI module supports simple PCI work flow to identify gaps in compliance and allow customers to focus on areas to remediate.

The VVM Cloud Platform has standard template-driven reporting engine enables customers to easily mine scan results in a similar way that a SQL report writer queries a SQL database. Customer has the option for standard reporting or customized reports based on the customer needs and limits of vulnerability scan information collected available on the web based portal interface. Roles based access are available, controlled by the customer, for the flexibility of the access levels required to get reporting information to appropriate personal at no additional charge.

Customer must provide Internet Access for scanner appliance collection and reporting via the web based portal. Verizon will provide unlimited scanning on the number of IP's in the customer's service with this service. Scans are scheduled via the Verizon Portal on demand or recurring scheduled. Ad-hoc scans are also apart of good business practice to follow-up on vulnerable areas discovered to confirm progress and remediation of issues found. The customer will choose the amount of IP Addresses to have the vulnerability scan service. The customer would need to order additional quantities, should they require more IP Address to be scanned. Verizon will pre-configure the scanner appliance based on the customer service. Customer may also purchase add-on cloud scanner for use in Amazon or Microsoft cloud environments. Customer is responsible for the installation of the scanner appliance on their network. Additional customer installation instructions are available at https://www.qualys.com/docs/qualys-scanner-appliance-user-guide.pdf?_ga=1.158192435.887113033.1420830694. Verizon provides on-line training via instructor-led lead net-conferencing for tool and setup of the service. Customer is responsible for all remediation to include: discovering and categorizing assets for VVM, schedule scanning of systems to detect vulnerabilities, Prioritizing assets by business risk, Remediating vulnerabilities through patching software or other methods, Informing the security team, auditors, and management with reports, and continuously repeating these steps for ongoing security.

VVM Customer Care provides the option to obtain support services from Verizon that enable the Customer to optimize their existing VVM service investment and ensure a high level of vulnerability protection.

The Verizon VVM Customer Care package includes:

- Set-up Assistance. Assist in set-up activities for VVM service after customer has provided the necessary information about their current environment such as:
  - Names, responsibilities and contact info of relevant stakeholders
  - Approximate number of IP addresses to be scanned
  - Internal and/or external IP addresses
  - URLs to be scanned
  - List of Application/s to be scanned

In Set-up Assistance, Verizon will, upon request and upon behalf of the customer, set up the VVM service. This activity is essential to providing the basis of providing Vulnerability Reporting for the customer environment.

- Operational Assistance. Verizon will perform duties and responsibilities typically performed by the Customer including:
  - Vulnerability Scanning. Verizon will proactively scan targets for our comprehensive KnowledgeBase of known vulnerabilities in the Customer's environment. Per Customer request, Verizon will review and analyze scan results prior to delivery to Customer. Verizon will regularly perform four distinct types of scanning, each of which can be deployed together or separately:
    - External scanning - Focuses on assets exposed directly to the Internet. External scanning provides an external attacker's view of the Customer network perimeter and highlights the level of risk the Customer is exposed to from attacks from the Internet.
    - Internal scanning - Focuses on the Customer's internal network to find vulnerabilities within the enterprise. This type of scanning is important as large number of attacks exploit weaknesses in the internal hosts once they gain a foothold in the network.
    - Authenticated scans - Verizon will utilize login credentials to the assets themselves to run host-level checks on the targets. This form of scanning produces the most meaningful results, as it can find issues such as weak passwords, missing patches or configuration weaknesses in addition to software vulnerabilities.
    - Policy Scanning Module – If the Customer elects to purchase the optional Verizon Policy Compliance (VPC), Verizon will provide operational assistance and system management

support to enable Customer to utilize this policy scanning module. The primary purpose of this Care module is for Verizon to map VPC to the required security standard the Customer wishes to apply. Verizon can analyze device configurations, web application and access control information from Customer networked devices (IP Address) based on the VVM scan. Verizon will work with the Customer to use VPC as a means to provide proof of compliance demanded by auditors across multiple compliance initiatives. In addition, Verizon will support Customer efforts to remediate the compliance gaps and modify/refine policy.

- Web application scanning - Verizon will search for typical vulnerabilities in web applications that can be exploited by attackers. This form of scanning is especially useful for Internet-facing web applications, which are typically constantly under attacks. (Note: this type of scan is offered only when the Verizon Web Application Scanning module is purchased.)

Verizon will analyze the vulnerabilities reported by the scanner and interpret and prioritize based on factors such as the severity, availability of exploit code, and business criticality of the affected asset.

- Scanning recurrence (Frequency) – Verizon will work with Customer to develop and execute an appropriate scan schedule.
- Monitor compliancy requirements. Verizon will monitor Customer's adherence to applicable compliance requirements and assist with compliance adherence planning.
- Vulnerability remediation and patch management - Verizon will oversee the vulnerability/patch management process, assign vulnerabilities to the designated asset owners for remediation, and communicate recommended remediation steps. Verizon's guidance will adhere to three primary methods of remediation:
  - Patching: Apply a security patch or software update from the vendor to repair the vulnerability.
  - Configuration adjustment: Adjust the configuration of the software to remove the vulnerability, such as changing passwords, modify permissions or change firewall rules.
  - Software removal: Removing and uninstalling the vulnerable software to eliminate the vulnerability and the associated risk.

Once the asset owners report that the vulnerability has been remediated across the environment, Verizon will conduct a specific verification scan to ensure that the chosen remediation method has been efficiently implemented and all attack vectors for a given vulnerability have been successfully eliminated.

- Monitoring and reporting – In addition to scanning for vulnerabilities, Verizon Customer Care staff will monitor the asset database and associated criticality of data to ensure the tracking process is providing current and accurate information. Verizon will provide the Customer a regular vulnerability report highlighting the current threats the Customer is exposed to by leveraging resources using the VVM tool service.
- Network documentation management – Verizon will develop and update Network Layout descriptions on a periodic, as needed basis.

- Continuous Improvement and Knowledge Transfer. Verizon will continuously improve the service based on feedback from the Customer, the results of the vulnerability scans and the feedback from Key Performance Indicators monitoring. The improvements may include changes in the processes or practices, or modification in the scanning infrastructure or configuration. Verizon will continually work with the Customer to build the body of knowledge so that the Customer can achieve self-sufficiency when desired.

Verizon VVM Customer Care will also apply to the other modules (such as Verizon Policy Compliance Service and Verizon Web Application Scanning) should they be purchased as add on options to VVM service.

	Feature Name	Feature Description	Bidder's Product Identifier
13	Vulnerability Management ≤ 256 IP's	Vulnerability Management ≤ 256 IP's	VVMS0256
	Bidder's Product Description: Provide Vulnerability Management Scanning up to 256 IP's as described above		
14	Vulnerability Management ≤ 512 IP's	Vulnerability Management ≤ 512 IP's	VVMS0512
	Provide Vulnerability Management Scanning up to 512 IP's as described above		
15	Vulnerability Management ≤ 1,024 IP's	Vulnerability Management ≤ 1,024 IP's	VVMS1024
	Bidder's Product Description: Provide Vulnerability Management Scanning up to 1,024 IP's as described above		
16	Vulnerability Management ≤ 1,536 IP's	Provide Vulnerability Management Scanning up to 1,536 IP's as described above	VVMS1536
	Bidder's Product Description: Provide Vulnerability Management Scanning up to 1,536 IP's as described above		
17	Vulnerability Management ≤ 2,048 IP's	Provide Vulnerability Management Scanning up to 2,048 IP's as described above	VVMS2048
	Bidder's Product Description: Provide Vulnerability Management Scanning up to 2,048 IP's as described above		
18	Vulnerability Management ≤ 3,072 IP's	Provide Vulnerability Management Scanning up to 3,072 IP's as described above	VVMS3072
	Bidder's Product Description: Provide Vulnerability Management Scanning up to 3,072 IP's as described above		
19	Vulnerability Management ≤ 10,000 IP's	Provide Vulnerability Management Scanning up to 10,000 IP's as described above	VVMG0000
	Bidder's Product Description: Provide Vulnerability Management Scanning up to 10,000 IP's as described above		
20	Scanner Appliance Installation	Scanner Appliance Installation provides the customer to have the option for Verizon to install the scanner appliance in the customer environment. This Scanner Appliance service installation option is available for the VVM service or Additional Scanner Appliance. VVM Service and	VSAN0000

	Feature Name	Feature Description	Bidder's Product Identifier
		Additional Scanner Appliance have pre-configured scanner appliance shipped where the customer is responsible for installation into their premise environment.	
	Bidder's Product Description: Scanner Appliance Installation provides the customer to have the option for Verizon to install the scanner appliance in the customer environment. This Scanner Appliance service installation option is available for the VVM service or Additional Scanner Appliance. VVM Service and Additional Scanner Appliance have pre-configured scanner appliance shipped where the customer is responsible for installation into their premise environment.		
21	Additional Scanner Appliance	Additional Scanner Appliance provides the customer to have the option for an additional scanning appliance deployed in the customer environment. Benefits to additional scanners include reducing scan times by keeping the scanner appliance close to the assets, load sharing, and redundancy for customer internal, non-internet facing assets. Customer is responsible for the installation of the scanner appliance on their network.	VASA0000
	Bidder's Product Description: Additional Scanner Appliance provides the customer to have the option for an additional scanning appliance deployed in the customer environment. Benefits to additional scanners include reducing scan times by keeping the scanner appliance close to the assets, load sharing, and redundancy for customer internal, non-internet facing assets. Customer is responsible for the installation of the scanner appliance on their network.		
22	Cloud Scanner Appliance	Cloud Scanner Appliance provides the customer the option of scanning their Amazon Elastic Compute Cloud or Microsoft Cloud environment. Benefit to additional cloud scanners include reaching elastic cloud environments that could not be reached from the customer's enterprise network. Scanner Appliance Installation (VSAN0000) can be used should customer require assistance with installation of the Cloud Scanner Appliance on Amazon or Microsoft network.	VASA0001
	Bidder's Product Description: Cloud Scanner Appliance provides the customer the option of scanning their Amazon Elastic Compute Cloud or Microsoft Cloud environment. Benefit to additional cloud scanners include reaching elastic cloud environments that could not be reached from the customer's enterprise network. Scanner Appliance Installation (VSAN0000) can be used should customer require assistance with installation of the Cloud Scanner Appliance on		

	Feature Name	Feature Description	Bidder's Product Identifier
	Amazon or Microsoft network.		
23	Vulnerability Management Customer Care ≤ 512 IP's	Vulnerability Management Customer Care to include up to 512 IP's as described above. Monthly efforts not to exceed 44 hours of activities.	VMCC0512
	Bidder's Product Description: Vulnerability Management Customer Care to include up to 512 IP's as described above. Monthly efforts not to exceed 44 hours of activities.		
24	Vulnerability Management Customer Care ≤ 1,536 IP's	Vulnerability Management Customer Care to include up to 1,536 IP's as described above. Monthly efforts not exceed 88 hours of activities.	VMCC1536
	Bidder's Product Description: Vulnerability Management Customer Care to include up to 1,536 IP's as described above. Monthly efforts not exceed 88 hours of activities.		
25	Vulnerability Management Customer Care ≤ 3,072 IP's	Vulnerability Management Customer Care to include up to 3,072 IP's as described above. Monthly efforts not exceed 132 hours of activities.	VMCC3072
	Bidder's Product Description: Vulnerability Management Customer Care to include up to 3,072 IP's as described above. Monthly efforts not exceed 132 hours of activities.		
26	Vulnerability Management Customer Care ≤ 10,000 IP's	Vulnerability Management Customer Care to include up to 10,000 IP's as described above. Monthly efforts not exceed 176 hours of activities.	VVMR0002
	Bidder's Product Description: Vulnerability Management Customer Care to include up to 10,000 IP's as described above. Monthly efforts not exceed 176 hours of activities.		

Verizon Security Policy Compliance (VSPC) Service is a layer on service to Verizon Vulnerability Management (VVM). VSPC enables organizations to analyze device configurations, web application and access control information from their networked devices (IP Address) based on the VVM scan. VSPC provides an organization to reduce the risk of internal and external threats, while at the same time provide proof of compliance demanded by auditors across multiple compliance initiatives. VSPC provides an efficient and automated workflow that allows IT security and compliance professionals to include:

- Define policies that describe how an organization will provide security and integrity
- Provide proof that the policies have been operationalized
- Give documented evidence that the organization has discovered and fixed any security policy compliance lapses

VSPC automatically maps this information to customer's internal security policies and external regulations in order to document compliance. VSPC provides the ability to report on current compliant status and remediate the compliance gaps via the Verizon Portal. VSPC provides compliance posture with internal security and regulatory policies to include:

- Reported in understandable format, easily accessible by business stakeholders
- Workflow and exception management allows organizations to easily produce compliance reports for internal configuration and regulatory requirements
- Security Policy Controls are mapped back to common framework templates for standards such as CIS, COBIT, FFIEC, HIPAA, ISO 17799, ISO 27001, ITIL, NERC, and NIST 800-53

VSPC is available on the Verizon Portal for customer reporting. Customer selects the number of IP's to enroll into VSPC subscription (a subset of the IP subscription for VVM). A standard template is then selected for the VSPC Library, or a custom template can be built to reflect customer own standards. The VSPC module utilized the latest VVM detailed inventory database to report on level of compliance using the standard or customized templates available on the Verizon Portal. The VSPC reporting system will provide reports from very detailed to high level executive views of compliances status to support a range of decisions from remediation to boardroom planning. Roles based access are available, controlled by the customer, for the flexibility of the access levels required to get reporting information to appropriate personal at no additional charge. Verizon provides on-line training via instructor lead net conferencing.

	Feature Name	**Feature Description**	**Bidder's Product Identifier**
27	Verizon Policy Compliance (VPC) ≤ 32 IP's	Provide Verizon Policy Compliance Scanning up to 32 IP's as described above.	VPCS0032
	Bidder's Product Description: Provide Verizon Policy Compliance Scanning up to 32 IP's as described above.		
28	Verizon Policy Compliance (VPC) ≤ 64 IP's	Provide Verizon Policy Compliance Scanning up to 64 IP's as described above.	VPCS0064
	Bidder's Product Description: Provide Verizon Policy Compliance Scanning up to 64 IP's as described above.		
29	Verizon Policy Compliance (VPC) ≤ 128 IP's	Provide Verizon Policy Compliance Scanning up to 128 IP's as described above.	VPCS0128
	Bidder's Product Description: Provide Verizon Policy Compliance Scanning up to 128 IP's as described above.		
30	Verizon Policy Compliance (VPC) ≤ 256 IP's	Provide Verizon Policy Compliance Scanning up to 256 IP's as described above.	VPCS0256
	Bidder's Product Description: Provide Verizon Policy Compliance Scanning up to 256 IP's as described above.		

	Feature Name	Feature Description	Bidder's Product Identifier
31	Verizon Policy Compliance (VPC) ≤ 1,024 IP's	Provide Verizon Policy Compliance Scanning up to 1,024 IP's as described above.	VPCS1024
	Bidder's Product Description: Provide Verizon Policy Compliance Scanning up to 1,024 IP's as described above.		
32	Verizon Policy Compliance (VPC) ≤ 2,048 IP's	Provide Verizon Policy Compliance Scanning up to 2,048 IP's as described above.	VPCS2048
	Bidder's Product Description: Provide Verizon Policy Compliance Scanning up to 2,048 IP's as described above.		
33	Verizon Policy Compliance (VPC) ≤ 3,072 IP's	Provide Verizon Policy Compliance Scanning up to 3,072 IP's as described above.	VPCS3072
	Bidder's Product Description: Provide Verizon Policy Compliance Scanning up to 3,072 IP's as described above.		

Verizon Web Application Scanning (VWAS)
Verizon Web Application Scanning (VWAS) is a layer on service to Verizon Vulnerability Management (VVM). VWAS allow organizations to discover, catalog and scan any and all of an organization's web applications. VWAS scans and analyzes custom web applications and identifies vulnerabilities that threaten underlying databases or bypass application access controls. It utilizes behavioral and static analysis to detect malware and monitor web sites that can be scheduled on the Verizon Portal with unlimited monthly scans.

VWAS Service is available on the Verizon Portal for customer reporting. Customer defines the Uniform Resource Identifiers (URL) target(s) to enroll into Web Application Scanning subscription portal. The web application scanning module identifies on vulnerabilities via the Verizon Portal to include these methods:

- Crawl web applications (Intranet, Internet)
- Fully interactive User Interface with flexible workflows and reporting
- Identify web applications' handling of sensitive or secret data
- Customize: black/white lists, robots.txt, sitemap.xml and more
- Supports these authentication schemes to include Basic, Digest, HTTP Negotiate, HTML Form-based, Single Sign On, and Client SSL Certificates
- View reports with recommended security coding practice and configuration
- Supports scanning HTML web applications with JavaScript and embedded Flash
- Comprehensive detection of custom web application vulnerabilities including Open Web Application Security Project (OWASP) Top 10 Vulnerabilities
- Differentiates exploitable fault-injection problems from simple information disclosure - Profiles custom web application behaviors
- Configures scanning performance with customizable performance level

VWAS Service excludes: Manual application code review and Manual penetration testing.

Verizon provides on-line training via instructor lead net conferencing.

	Feature Name	Feature Description	Bidder's Product Identifier
34	Verizon Web Application Scanning (VWAS) 1 URL	Provide Verizon Web Application Scanning for 1 Uniform Resource Identifier (URL) as described above.	VWAS0001
	Bidder's Product Description: Provide Verizon Web Application Scanning for 1 Uniform Resource Identifier (URL) as described above		
35	Verizon Web Application Scanning (VWAS) ≤ 5 URL's	Provide Verizon Web Application Scanning up to 5 Uniform Resource Identifier (URL) as described above.	VWAS0005
	Bidder's Product Description: Provide Verizon Web Application Scanning up to 5 Uniform Resource Identifier (URL) as described above.		
36	Verizon Web Application Scanning (VWAS) ≤ 10 URL's	Provide Verizon Web Application Scanning up to 10 Uniform Resource Identifier (URL) as described above.	VWAS0010
	Bidder's Product Description: Provide Verizon Web Application Scanning up to 10 Uniform Resource Identifier (URL) as described above.		
37	Verizon Web Application Scanning (VWAS) ≤ 25 URL's	Provide Verizon Web Application Scanning up to 25 Uniform Resource Identifier (URL) as described above.	VWAS0025
	Bidder's Product Description: Provide Verizon Web Application Scanning up to 25 Uniform Resource Identifier (URL) as described above.		
38	Verizon Web Application Scanning (VWAS) ≤ 50 URL's	Provide Verizon Web Application Scanning up to 50 Uniform Resource Identifier (URL) as described above.	VWAS0050
	Bidder's Product Description: Provide Verizon Web Application Scanning up to 50 Uniform Resource Identifier (URL) as described above.		
39	Verizon Web Application Scanning (VWAS) ≤ 100 URL's	Provide Verizon Web Application Scanning up to 100 Uniform Resource Identifier (URL) as described above.	VWAS0100
	Bidder's Product Description: Provide Verizon Web Application Scanning up to 100 Uniform Resource Identifier (URL) as described above.		

	Feature Name	Feature Description	Bidder's Product Identifier
Pre-Implementation			
40	Network Security Consultant I	Pre-implementation site survey and network security design. Provides basic consulting skills to include planning, standards based data protection assessments, design, integration, development, configuration for non-complex pre-implementation activities. Only to be sold in conjunction with the support of services specifically listed in Category 7.	NTSC0001
41	Network Security Consultant II	Pre-implementation site survey and network security design. Provides advanced consulting skills to include planning, standards based data protection assessments, design, integration, development, configuration for non-complex pre-implementation activities. Only to be sold in conjunction with the support of services specifically listed in Category 7.	NTSC0002
42	Senior Network Security Consultant	Pre-implementation site survey and network security design. Provides advanced consulting skills across multiple disciplines. Conducts assessments and design for complex installations involving multiple technologies. Provides advanced consulting skills to include planning, standards based data protection assessments, design, integration, development, configuration for complex pre-implementation activities involving multiple technologies. Only to be sold in conjunction with the support of services specifically listed in Category 7.	NTSS0000
43	Principal Network Security Architect	Pre-implementation site survey and network security design. Provides highly advanced consulting skills across multiple disciplines. Conducts assessments and design for complex installations involving multiple technologies. Provides advanced consulting skills to include planning, standards based data protection assessments, design, integration, development, configuration for complex pre-implementation activities involving multiple technologies. Only to be sold in conjunction with the support of services specifically listed in Category 7.	NSPA0000

	Feature Name	Feature Description	Bidder's Product Identifier
Implementation:			
44	Network Security Consultant I (normal business hours, Mon-Fri, 8am-5pm)	Implementation network security consultant performs basic on-site installation, assessments and tests interoperability with other products. During normal business hours, Mon – Fri 8am – 5pm. Only to be sold in conjunction with the support of services specifically listed in Category 7.	NSCN0001
45	Network Security Consultant I (outside normal business hours, Sat/Sun)	Implementation network security consultant performs basic on-site installation, assessments and tests interoperability with other products. During outside of normal business hours, Sat, Sun & Holidays. Only to be sold in conjunction with the support of services specifically listed in Category 7.	NSCO0001
46	Network Security Consultant II (normal business hours, Mon-Fri, 8am-5pm)	Implementation network security consultant performs advanced on-site installation, assessments and tests interoperability with other products. During normal business hours, Mon – Fri, 8am – 5pm. Only to be sold in conjunction with the support of services specifically listed in Category 7.	NSCN0002
47	Network Security Consultant II (outside normal business hours, Sat/Sun)	Implementation network security consultant performs advanced on-site installation, assessments and tests interoperability with other products. During outside of normal business hours, Sat, Sun & Holidays. Only to be sold in conjunction with the support of services specifically listed in Category 7.	NSCO0002
48	Network Security Project Manager (normal business hours, Mon-Fri, 8am-5pm)	Network Security implementation project manager coordinates project resources including customer staff and other VZ resources. The project manager defines the project responsibility assignments. During normal business hours, Mon – Fri 8am – 5pm. Only to be sold in conjunction with the support of services specifically listed in Category 7.	NSPN0001
49	Network Security Project Manager (outside normal business hours, Sat/Sun)	Network Security implementation project manager coordinates project resources including customer staff and other VZ resources. The project manager defines the project responsibility assignments.	NSPO0001

	Feature Name	Feature Description	Bidder's Product Identifier
		During outside of normal business hours, Sat, Sun and Holidays. Only to be sold in conjunction with the support of services specifically listed in Category 7.	

7.3 SERVICE LEVEL AGREEMENTS (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 X 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 X 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 X 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 X 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 STPD 12-001-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-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 X 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 X 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	**END-USER REQUEST**	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	**OBSERVATION**	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	**END-USER NOT AVAILABLE**	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	**WIRING**	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	**POWER**	Trouble caused by a power problem outside of the responsibility of the Contractor.
6	**FACILITIES**	Lack of building entrance Facilities or conduit structure that are the End-User's responsibility to provide.

#	Stop Clock Condition (SCC)	SCC Definition
7	**ACCESS**	Limited access or contact with End-User provided the Contractor documents in the trouble ticket several efforts to contact End-User for the following: a. Access necessary to correct the problem is not available because access has not been arranged by site contact or End-User representative; b. Site contact refuses access to technician who displays proper identification; 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, d. Site has limited hours of business that directly impacts the Contractor's ability to resolve the problem. If it is determined later that the cause of the problem was not at the site in question, then the Access SCC shall not apply.
8	**STAFF**	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	**APPLICATION**	End-User software applications that interfere with repair of the trouble.
10	**CPE**	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	**NO RESPONSE**	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	**MAINTENANCE**	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.

#	Stop Clock Condition (SCC)	SCC Definition
13	**THIRD PARTY**	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	**FORCE MAJEURE**	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 X 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)

SLA Name: Availability	
Definition: The percentage of time a CALNET 3 service is fully functional and available for use each calendar month.	
Measurement Process: 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.	
Services:	
DDoS Detection and Mitigation Service	Email Monitoring and Scanning Service
Web Security and Filtering Service	Security Information and Event Management (SIEM)
Vulnerability Management	

Objective(s):

	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%	**P**
Email Monitoring and Scanning Service	≥ 99.9%	≥ 99.95%	≥ 99.99%	**P**
Web Security and Filtering Service	≥ 99.9%	≥ 99.95%	≥ 99.99%	**P**
SIEM	≥ 99.9%	≥ 99.95%	≥ 99.99%	**P**
Vulnerability Management	≥ 99.9%	≥ 99.95%	≥ 99.99%	**P**

Rights and Remedies	Per Occurrence: N/A
	Monthly Aggregated Measurements: 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 X No_____

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

SLA Name: Catastrophic Outage 2 (CAT 2)	
Definition: 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.	
Measurement Process: 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.	
Service(s):	
DDoS Detection and Mitigation Service	Email Monitoring and Scanning Service
Web Security and Filtering Service	Security Information and Event Management (SIEM)

Vulnerability Management	

Objective (s):
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	**P**
Email Monitoring and Scanning Service	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	**P**
Web Security and Filtering Service	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	**P**
SIEM	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	**P**
Vulnerability Management	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	**P**

Rights and Remedies	**Per Occurrence:** 100 percent of the TMRC for each End-User service not meeting the committed objective for each CAT 2 fault
	Monthly Aggregated Measurements: N/A

Bidder understands the Requirement and shall meet or exceed it? Yes X No_____

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

SLA Name: Catastrophic Outage 3 (CAT 3)	
Definition: The total loss of one (1) or more CALNET 3 Network Based Managed Security services on a system wide basis.	
Measurement Process: 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.	
Service(s):	
DDoS Detection and Mitigation Service	Email Monitoring and Scanning Service
Web Security and Filtering Service	Security Information and Event Management (SIEM)
Vulnerability Management	

Objectives:

The objective restoral time shall be:

	Basic (B)	Standard (S)	Premier (P)	Bidder's Objective Commitment (B or P)
DDoS Detection and Mitigation Service	≤ 30 minutes	N/A	≤ 15 minutes	**P**
Email Monitoring and Scanning Service	≤ 30 minutes	N/A	≤ 15 minutes	**P**
Web Security and Filtering Service	≤ 30 minutes	N/A	≤ 15 minutes	**P**
SIEM	≤ 30 minutes	N/A	≤ 15 minutes	**P**
Vulnerability Management	≤ 30 minutes	N/A	≤ 15 minutes	**P**

Rights and Remedies	**Per Occurrence:** 100 percent of the TMRC for each End-User service not meeting the committed objective for each CAT 3 fault.
	Monthly Aggregated Measurements: N/A

Bidder understands the Requirement and shall meet or exceed it? Yes X No_____

7.3.8.4 Email Monitoring and Scanning Services – Average Delivery Time (M-S)

SLA Name: Email Monitoring and Scanning Services - Average Delivery Time

Definition: The delivery time is the elapsed time from when and email enters the Contractor's managed email service network to when the delivery attempt is first made to the Customer's email server. The average delivery time is the delivery time measured in minutes over a calendar month.

The End-User/Customer is responsible for opening a trouble ticket with the Contractor's Customer Service Center (helpdesk) when the Customer suspects the email monitoring and scanning service's average delivery time is not meeting the committed level as defined in this SLA.

Measurement Process: If the Customer suspects the average delivery time does not meet the committed objective level the contractor shall provide average delivery time computed using the method described herein. The Contractor shall measure and record email delivery time every five (5) minutes for one (1) month. The fastest 95% of measurements are used to create the average for the calendar month.

Trouble tickets opened as email monitoring and scanning services Delivery Time shall not count in Availability or Time to Repair measurements unless and until the End-User reports service as unusable.

Service(s):	
Email Monitoring and Scanning Services	

Objective (s):

	Basic (B)	Standard (S)	Premier (P)	Bidders Objective Commitment (B, S or P)
Email Monitoring and Scanning Services	< 2 minutes	< 1 minute	<30 seconds	**P**

Rights and Remedies	**Per Occurrence:** N/A
	Monthly Aggregated Measurements: 25 percent of the TMRC when the average delivery time exceeds the committed objective.

Bidder understands the Requirement and shall meet or exceed it? Yes X No_____

7.3.8.5 SIEM Event Notification (M-S)

SLA Name: SIEM Critical Event Notification

Definition: 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.

Measurement Process:
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.

Service(s):

SIEM	

Objective (s):

	Basic (B)	Standard (S)	Premier (P)	Bidders Objective Commitment (B, S or P)
SIEM	≤ 45 minutes	≤ 30 minutes	≤ 15 minutes	**P**

Rights and Remedies	**Per Occurrence:** 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.
	Monthly Aggregated Measurements: N/A

Bidder understands the Requirement and shall meet or exceed it? Yes X No_____

7.3.8.6 DDoS Customer Notification (M-S)

SLA Name: DDoS Customer Notification

Definition: 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.

Measurement Process:
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.

Service(s):

DDoS Detection and Mitigation	

Objective (s):

	Basic (B)	Standard (S)	Premier (P)	Bidders Objective Commitment (B, S or P)
DDoS Detection and Mitigation	≤ 45 minutes	≤ 30 minutes	≤ 15 minutes	**P**

Rights and Remedies	**Per Occurrence:** 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.
	Monthly Aggregated Measurements: N/A

Bidder understands the Requirement and shall meet or exceed it? Yes X No_____

7.3.8.7 Excessive Outage (M-S)

SLA Name: Excessive Outage

Definition: A service failure that remains unresolved for more than the committed objective level.

Measurement Process: This SLA is based on trouble ticket Unavailable Time. The service or feature is unusable during the time the trouble ticket is reported as opened until restoration of the service, minus SCC. If Customer reports a service failure as unresolved after the closure of the trouble ticket by the Contractor, the Unavailable Time shall be adjusted to the actual restoration time.

Service(s):

DDoS Detection and Mitigation Service	Email Monitoring and Scanning Service
Web Security and Filtering Service	Security Information and Event Management (SIEM)
Vulnerability Management	

Objective (s):
The Unavailable Time objective shall not exceed:

	Basic (B)	Standard (S)	Premier (P)	Bidder's Objective Commitment (B, S or P)
DDoS Detection and Mitigation Service	16 hours	12 hours	8 hours	**P**
Email Monitoring and Scanning Service	16 hours	12 hours	8 hours	**P**
Web Security and Filtering Service	16 hours	12 hours	8 hours	**P**
SIEM	16 hours	12 hours	8 hours	**P**
Vulnerability Management	16 hours	12 hours	8 hours	**P**

Rights and Remedies	**Per Occurrence:** 100 percent of the TMRC for each service or feature out of service for a period greater than the committed objective level. Upon request from the Customer or the CALNET 3 CMO, the Contractor shall provide a briefing on the excessive outage restoration.
	Monthly Aggregated Measurements: N/A

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

7.3.8.8 DDoS Time to Mitigate (M-S)

SLA Name: DDoS Time to Mitigate

Definition: The time to initiate DDoS mitigation upon the identification of an attack.

Measurement Process:

The amount of time between the detection via Customer or Contractor identification of an anomaly or attack, and the initiation of the mitigation process.

Service(s):

DDoS Detection and Mitigation	

Objective (s):
Mitigation shall begin within:

	Basic (B)	Standard (S)	Premier (P)	Bidder's Objective Commitment (B, S or P)
DDoS Detection and Mitigation	45 minutes	30 minutes	15 minutes	**P**

<table>
<tr><td>Rights and Remedies</td><td>Per Occurrence:
<table>
<tr><th>Basic
Time to Mitigate
Minutes</th><th>Standard
Time to Mitigate
Minutes</th><th>Premier
Time to Mitigate
Minutes</th><th>Percentage of
TMRC per event</th></tr>
<tr><td>46 - 75</td><td>31 -60</td><td>16 - 45</td><td>25%</td></tr>
<tr><td>76 - 135</td><td>61- 120</td><td>46- 105</td><td>50%</td></tr>
<tr><td>136 and over</td><td>121 and over</td><td>106 and over</td><td>100%</td></tr>
</table>
Monthly Aggregated Measurements: N/A</td></tr>
</table>

Bidder understands the Requirement and shall meet or exceed it? Yes X No_____

7.3.8.9 Notification

<table>
<tr><td colspan="2">SLA Name: Notification</td></tr>
<tr><td colspan="2">Definition: 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.</td></tr>
<tr><td colspan="2">Measurement Process: 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.</td></tr>
<tr><td colspan="2">Service(s): All Services</td></tr>
<tr><td colspan="2">Objective (s): 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.</td></tr>
<tr><td rowspan="2">Rights and Remedies</td><td>Per Occurrence: Senior Management Escalation</td></tr>
<tr><td>Monthly Aggregated Measurements: N/A</td></tr>
</table>

Bidder understands the Requirement and shall meet or exceed it? Yes X No_____

7.3.8.10 Provisioning (M-S)

SLA Name: Provisioning

Definition: 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).

Provisioning SLAs have two (2) objectives:

Objective 1: Individual Service Request; and

Objective 2: Successful Install Monthly Percentage by Service Type.

Note: Provisioning timelines include extended demarcation wiring, when appropriate.

Measurement Process:

Objective 1: Individual Service Request: 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.

Objective 2: Successful Install Monthly Percentage per service Type: 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.

Service (Features must be installed in conjunction with the service except when listed below)	Committed Interval Calendar Days	Coordinated/Managed Project
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
Vulnerability Management	N/A	Coordinated/Managed Project

Objective (s):

Objective 1: Individual Service Request: Service installed on or before the Committed Interval or negotiated due date.

Objective 2: Successful Install Monthly Percentage per Service:

	Basic (B)	Standard (S)	Premier (P)	Bidder's Objective Commitment (S or P)
DDoS Detection and Mitigation Service	N/A	≥ 90%	≥ 95%	**P**
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%	**P**
Vulnerability Management	N/A	≥ 90%	≥ 95%	**P**

Rights and Remedies	**Per Occurrence:** Objective 1: Individual Service Requests: 50 percent of installation fee credited to Customer for any missed committed objective.
	Monthly Aggregated Measurements: 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 X No_____

7.3.8.11 Time to Repair (TTR) (M-S)

SLA Name: Time to Repair (TTR)	
Definition: A service outage that remains unresolved for more than the committed objective level.	
Measurement Process: This SLA is based on trouble ticket Unavailable Time. The service or feature is unusable during the time the trouble ticket is reported as opened until restoration of the service or feature, minus SCC. If Customer reports a service failure as unresolved after the closure of the trouble ticket by the Contractor, the Unavailable Time shall be adjusted to the actual restoration time. This SLA is applied per occurrence.	
Service(s):	
DDoS Detection and Mitigation Service	Email Monitoring and Scanning Service
Web Security and Filtering Service	Security Information and Event Management (SIEM)

Vulnerability Management	

Objective (s):
The Unavailable Time objective shall not exceed:

Service	Basic (B)	Standard (S)	Premier (P)	Bidder's Objective Commitment (B or S)
DDoS Detection and Mitigation Service	6 hours	4 hours	N/A	**S**
Email Monitoring and Scanning Service	6 hours	4 hours	N/A	**S**
Web Security and Filtering Service	6 hours	4 hours	N/A	**S**
SIEM	6 hours	4 hours	N/A	**S**
Vulnerability Management	6 hours	4 hours	N/A	**S**

Rights and Remedies	**Per Occurrence:** 25 percent of the TMRC per occurrence for each service and feature out of service for a period greater than the committed objective level.
	Monthly Aggregated Measurements: N/A

Bidder understands the Requirement and shall meet or exceed it? Yes X 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 X No_____

7.3.8.13 Proposed Unsolicited Services

The Contractor shall provide SLAs as defined in SLA Section 7.3.8 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? Yes X 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 X No_____