



AT&T

IFB STPB 12-001-B, C3-B-12-10-TS-01

CalNet 3, Category 7: Network Based Managed Security

Volume 2: Response to Unique Category or Subcategory Requirements
SOW Technical Requirements Response

Amendment #1, Rev. June 4, 2015

Mark Roese
Executive Sales Director
AT&T
2700 Watt Ave
Sacramento, CA 95821
916-972-3297 (phone)
916-468-8418 (cell)
mark.roese@att.com



This Page was Intentionally Left Blank



Table of Contents

Exhibit 8: Contractor’s License Information.....	1
Exhibit 10: Bidding Preferences and Incentives	5
Exhibit 11: STD 843, DVBE Declarations	9
Exhibit 12: GSPD 05-105, Bidder Declaration.....	11
Exhibit 13: STD 830, TACPA Preference Request.....	13
Exhibit 14: Commercially Useful Function Statement.....	15
Category 7 – Network Based Managed Security.....	19
7.1 Overview.....	19
7.2 Network Based Managed Security Services	20
7.3 Service Level Agreements (SLA)	53





This Page was Intentionally Left Blank



Exhibit 8: Contractor's License Information

Attached is Exhibit 8: Contractor's License Information.



This Page was Intentionally Left Blank



EXHIBIT 8: CONTRACTOR’S LICENSE INFORMATION

(Installation Services Only)

For Category/Subcategory: 7: Network Based Managed Security

Name of Bidder: AT&T Corp.

Bidder shall complete the applicable Contractor’s license information below in accordance with the Contractor’s State License Board, Department of Consumer Affairs. A Contractor’s license of appropriate Class C-7, Low Voltage Systems Contractor, is required before any Bidder can contract business (e.g. submit a bid) which includes the installation of cable and wiring, and minor electrical modification. In addition, if structural modifications are required, a Class B, General Building Contractor, license is required. Licensee must be in the name of the firm or a Responsible Managing Employee. See IFB Section 2.3.6, Contractor’s License.

CONTRACTOR

Class C-7 and C-10 License No: 760249
 Licensee: Pacific Bell Telephone Company Expiration Date: 03/31/2015
 Relationship of Licensee to Contractor: Wholly Owned Subsidiary

SUBCONTRACTOR 1

Class _____ License No: _____
 Licensee: _____ Expiration Date: _____
 Relationship of Licensee to Subcontractor: _____

SUBCONTRACTOR 2

Class _____ License No: _____
 Licensee: _____ Expiration Date: _____
 Relationship of Licensee to Subcontractor: _____

(Use additional sheets if necessary.)





This Page was Intentionally Left Blank



Exhibit 10: Bidding Preferences and Incentives

Attached is the completed and signed Exhibit 10.



This Page was Intentionally Left Blank



Exhibit 10: BIDDING PREFERENCES AND INCENTIVES

For Category/Subcategory: 7: Network Based Managed Security

ALL BIDDERS: COMPLETE ALL SECTIONS BELOW AND SUBMIT WITH YOUR PROPOSAL.

1. SMALL BUSINESS PREFERENCE

Bidder must check the appropriate box from the choices below.

- I am a DGS certified Small Business and claim the Small Business Preference.
My DGS Small Business certification number is: _____
- I have recently filed for DGS Small Business preference but have not yet received certification, but I am claiming the Small Business preference.
- I am not a DGS certified Small Business, but 25% or more of the revenue from the award will go to DGS certified Small Business Subcontractors performing a Commercially Useful Function and therefore I am claiming the preference.
Bidder must complete and submit Exhibit 12, GSPD-05-105 Bidder Declaration, indicating the percentage of the revenue that will be received by each DGS certified Small Business Subcontractor.
Bidder must complete and submit an Exhibit 14, Commercially Useful Function Statement, for each Small Business subcontractor.
- I am not claiming the DGS Small Business preference.

2. DVBE INCENTIVE

Bidder must check the appropriate box from the choices below.

- I am a DGS certified DVBE. A copy of my STD. form 843 is attached.
- I have recently filed for DGS DVBE certification, but have not yet received certification.
- I am not a DGS certified DVBE, but a percentage of the revenue will be going to DGS certified DVBE Subcontractors performing a Commercially Useful Function, and therefore I am claiming the DVBE incentive.
Bidder must submit a complete Exhibit 12, GSPD-05-105, Bidder Declaration, indicating the percentage of the revenue that will be received by each DGS certified DVBE Subcontractor.
Bidder must also submit an Exhibit 11, STD 843 DVBE Declarations, for each DVBE Subcontractor, signed by the DVBE owner/manager.
Bidder must complete and submit an Exhibit 14, Commercially Useful Function Statement, for each DVBE subcontractor or supplier.
- I am not claiming the DVBE incentive.





EXHIBIT 10, CONTINUED

3. ADDITIONAL BIDDING PREFERENCES

The Bidder shall check the appropriate box or boxes from the choices below.

- I am not claiming the TACPA preference, the EZA preference, or the LAMBRA preference.

- I am claiming the TACPA bidding preference.
Bidder must submit Exhibit 13, STD 830.

Name of Bidder: AT&T Corp.

Signature and Date: _____ March 5, 2014



Exhibit 11: STD 843, DVBE Declarations

AT&T is not claiming a DVBE incentive



This Page was Intentionally Left Blank



Exhibit 12: GSPD 05-105, Bidder Declaration

AT& is not claiming SB preference using Subcontractors, nor claiming a DVBE incentive, nor will have any Subcontractors that will receive 15% or more revenue.



This Page was Intentionally Left Blank



Exhibit 13: STD 830, TACPA Preference Request

AT&T is not claiming TACPA preference.



This Page was Intentionally Left Blank



Exhibit 14: Commercially Useful Function Statement

Attached is a copy of AT&T's completed Exhibit 14.



This Page was Intentionally Left Blank



EXHIBIT 14: COMMERCIALLY USEFUL FUNCTION STATEMENT

All certified small business, micro business, and/or DVBE Contractors, subcontractors or suppliers must meet the commercially useful function requirements under Government Code (GC) Section 14837(d)(4)(A) (for SB) and Military and Veterans Code (MVC) Section 999(b)(5)(B) (for DVBE).

Please answer the following questions, as they apply to your company for the goods and services being acquired in this solicitation.

CALNET 3 Category or Subcategory being bid: Category 7

Subcontractor Name:

Mark all that apply: DVBE: Small Business: Micro Business:

1.	Will the subcontractor be responsible for the execution of a distinct element of the resulting CALNET Contract?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2.	Will this subcontractor be actually performing, managing, or supervising an element of the resulting CALNET Contract?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
3.	Will this subcontractor be performing work on the resulting CALNET Contract that is normal for its business, services, and functions?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
4.	Will there be any further subcontracting that is greater than that expected to be subcontracted by normal industry practices for the resulting CALNET Contract?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
5.	Will this subcontractor be responsible, with respect to products, inventories, materials, and supplies required for the contract, for negotiating price, determining quality and quantity, ordering, installing, if applicable, and making payment?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

A response of “No” in questions 1 - 3 or a response of ”Yes” in question 4, may result in your claim for Small Business Preference or DVBE Incentive being deemed non-responsive and disqualified.

The bidder must provide a written statement below detailing the role, services and goods the subcontractor(s) will provide to meet the commercially useful function requirement.

AT&T is not using any DVBE, Small Business, and Micro Business Contractors, subcontractors or suppliers in the delivery of services related to this Category.



At the State’s option prior to award, bidders may be required to submit additional written clarifying information.

Per MVC Section 999.9(a)(6) and GC 14842.5 (a)(6) it is unlawful for a person to knowingly and with intent to defraud, fraudulently represent that a commercially useful function is being performed by a disabled veteran business enterprise in order to obtain or retain a bid preference or a state contract, and that doing so shall subject the person to the penalties stated in MVC Section 999.9 and GC 14842.5.

By signing this form, the undersigned bidder certifies that the Certified Small Business or DVBE satisfies the Commercially Useful Function requirement, and will provide the role, services, and/or goods stated above.

Signature of Company
Representative:

Printed/Typed Name and Title of

Mark Roese, Executive Sale Director

Company Representative:



Category 7 – Network Based Managed Security

7.1 Overview

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

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:

AT&T Distributed Denial of Service (DDoS) Defense is designed to detect and mitigate distributed denial of service attacks on your network. DDoS Defense helps identify and block malicious packets in near real time to help you prevent possible negative affects regarding the flow of your business traffic.

DDoS Defense is the service based on the data from the AT&T IP backbone network and doesn't require you to purchase additional bandwidth or premises equipment.



Depending on your configuration, a shared or dedicated set of network mitigation devices scrub your traffic for denial of service attacks. A shared configuration allows you to share network detector devices and a farm of network mitigation devices with other AT&T customers. A dedicated configuration provides you with network mitigation devices dedicated to you.

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:

DDoS Defense leverages AT&T Internet Protect technology to help identify DDoS attacks. This technology forwards data packets to our network-based detection facility where we monitor your network traffic for the IP addresses you want us to help protect. When the detection facility identifies a DDoS attack, it sends an alarm to both an AT&T operations center and to you. Concurrently, the AT&T Global Customer Support Center (GCSC) notifies you of the attack. The AT&T GCSC reroutes the affected traffic to the network scrubbing facility within the AT&T IP backbone. This facility scrubs the traffic and passes what we determine as valid traffic to your access router. We continue to monitor the scrubbed traffic for DDoS attacks until we determine the attack has subsided, and then we restore your normal traffic routing.

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:

Distributed Denial of Service (DDoS) Defense uses these components:

- **AT&T Internet Access**—provides AT&T with access to packets going into your routers. This access allows us to divert the traffic from your attacked IP address to the AT&T network scrubbing facility. DDoS Defense requires Managed Internet Service (MIS) or MIS Plus.
- **Detection Facility**—resides in the AT&T IP backbone network. The facility analyzes your NetFlow data and helps detect and identify suspected traffic anomalies.
- **Scrubbing Facility**—receives packets after the DDoS service detects an attack. The facility scrubs the traffic for known malicious packets and passes on what is determined a legitimate packets to your access routers.
- **Complete Management**—DDoS includes equipment, monitoring, and management. You receive a cost-effective solution that helps you minimize hardware and personnel expenses and avoid unpredictable implementation and maintenance costs.

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:

DDoS Defense Reporting Portal

You can access the DDoS Defense and the Internet Protect portal website via BusinessDirect®. From this site, you can access anomaly reports, historical archived data, traffic information, and email trap alerts. You'll find a variety of security information you need, all in one place, accessible from the Internet.

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		DDOS2
Bidder's Product Description: DDoS Defense consists of detection and mitigation service components that examine your Netflow data. 1 – 2 GB Protection					
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		DDOS4
Bidder's Product Description: DDoS Defense consists of detection and mitigation service components that examine your Netflow data. 3 – 4 GB Protection					
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	Y		DDOS6





	Feature Name	Feature Description	Bidder Meets or Exceeds? Y N	Bidder's Product Identifier
		flow		
	Bidder's Product Description: DDoS Defense consists of detection and mitigation service components that examine your Netflow data. 5 – 6 GB Protection			

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
	None		
1	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:

AT&T Secure E-Mail Gateway (SEG) is a network-based Security as a Service (SecaaS) offering. SEG protects customers from internal and external email threats that can include: commercial spam, malicious attachments, direct email server connections from spammers and botnet-controlled endpoints, and email embedded URL-based attacks. SEG provides features and tools that enable customers to comply with data privacy and retention regulations, meet





legal discovery requirements, and implement data loss prevention strategies. SEG customers retain responsibility and control over much of the configuration and settings for the service.

SEG is offered with two different service levels – “Advanced” or “Premium”.

SEG Advanced

The Secure E-Mail Gateway (SEG) Advanced service helps protect customer networks from inbound messages containing spam, viruses, and malware.

The Service provides features that enable customer to manage and enforce its security policy on outbound email content.

The Service provides disaster recovery protection against lost email data in the event of a customer email server outage and provides end-user continuity functionality if the customer email server becomes unavailable.

SEG is administered by the customer through a self-service web console and provides a suite of reports.

SEG requires that the Customer own and manage their own Simple Mail Transfer Protocol (SMTP) email server or servers. The customer must also own and manage their own Internet domain(s) in order to direct email to the Service for filtering.

Standard Features – SEG Advanced

Customer Managed Administration

The primary interface to the SEG Advanced service is the Administration Center web console. This console is available 24 x 7 and allows Customer Administrators to define and manage settings and configurations for their domains, including spam treatment options, virus scanning selections, content filter settings, policy rules and user permissions.

Anti-Virus Protection

Anti-Virus Protection provides an extensive and redundant anti-virus filtering process that is designed to detect, clean, and record virus infected e-mail messages before they enter the Customer’s network. Virus Protection can be configured to scan all inbound and outbound messages for viruses as recognized by industry standard virus scanning technologies.



Spam Filtering

Spam Filtering detects Spam e-mail messages before they enter the Customer's network. Captured spam is routed to the spam quarantine and can be accessed by administrators or end users at any time through a web-based interface. The Customer administrator may configure spam quarantine notification options for messages that have that been quarantined.

Policy Enforcement

Policy enforcement supports the ability to apply the Customer's corporate messaging policies on unwanted and malicious content to e-mail messages entering and leaving the Customer's e-mail system. Policy enforcement features are definable by domain or user level. Content categories that can be filtered for policy include: keyword groups, HTML, spam beacons or web bugs, hyperlinks, attachments, deny and allow lists. The Customer can define text, referred to as an "outbound disclaimer" that will be appended to the email content. The Customer administrator may configure policy enforcement notification options for emails have been identified by policy rules.

Quarantine

The Service provides multiple quarantine areas with different security access requirements to store and support review of suspect email outside of your email network. Emails that violate configured policies and that have the quarantine action applied are sorted into multiple quarantines.

- Spam Quarantined Messages – Accessible to all users, with users with role of User or Reports Manager allowed to access only their own personal spam quarantine
- Virus Quarantined Messages – Accessible to only Administrators and Quarantine Managers
- Attachment Quarantined Messages – Accessible to only Administrators and Quarantine Managers
- Content Keyword Quarantined Messages – Accessible to only Administrators and Quarantine Managers

Disaster Recovery

Disaster Recovery provides added protection against lost emails in the case the Customer's inbound email server may be unavailable to receive email.



Disaster recovery provides:

- Automatic email fails over and rolling storage for up to sixty (60) days.
- Automatic monitoring of Customer's e-mail server to establish return of service with attempt to deliver the e-mail every 20 minutes.
- Automatic forwarding of stored e-mail once Customer's e-mail service is restored
- User access to read and send messages through a web-based interface while messages are in fail-over storage status. Messages can remain in fail-over storage for up to 60 days.

Transport Layer Security

The SEG Advanced Service supports both forced and opportunistic Transport Layer Security (TLS) connections between the Customer's email server and the SEG network. TLS is designed to provide basic network level encryption through an encrypted tunnel for message transfer.

Administrator Reports

Included in the SEG Administration Center console is access to a suite of reports providing a view into the statistics and use of the Service. All mail messages processed by the Service are recorded in these statistical reports, measured on an hourly, daily, weekly, and monthly basis. The reports furnished to Customer depend of the Service components and features in use by the Customer.

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:

Anti-Virus Protection

Anti-Virus Protection provides an extensive and redundant anti-virus filtering process that is designed to detect, clean, and record virus infected e-mail messages before they enter the Customer's network. Virus Protection can be configured to scan all inbound and outbound messages for viruses as recognized by industry standard virus scanning technologies.

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:

Spam Filtering

Spam Filtering detects Spam e-mail messages before they enter the Customer's network. Captured spam is routed to the spam quarantine and can be accessed by administrators or end users at any time through a web-based interface. The Customer administrator may configure spam quarantine notification options for messages that have that been quarantined.

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 No

Description:

Policy Enforcement

Policy enforcement supports the ability to apply the Customer’s corporate messaging policies on unwanted and malicious content to e-mail messages entering and leaving the Customer’s e-mail system. Policy enforcement features are definable by domain or user level. Content categories that can be filtered for policy include: keyword groups, HTML, spam beacons or web bugs, hyperlinks, attachments, deny and allow lists. The Customer can define text, referred to as an “outbound disclaimer” that will be appended to the email content. The Customer administrator may configure policy enforcement notification options for emails have been identified by policy rules.

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 No

Description:

Quarantine

The Service provides multiple quarantine areas with different security access requirements to store and support review of suspect email outside of your email network. Emails that violate configured policies and that have the quarantine action applied are sorted into multiple quarantines.

- Spam Quarantined Messages – Accessible to all users, with users with role of User or Reports Manager allowed to access only their own personal spam quarantine
- Virus Quarantined Messages – Accessible to only Administrators and Quarantine Managers



- Attachment Quarantined Messages – Accessible to only Administrators and Quarantine Managers
- Content Keyword Quarantined Messages – Accessible to only Administrators and Quarantine Managers

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:

Notification

The Service provides E-Mail notification when an anti-virus, anti-spam or content control function has been invoked.

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 No

Description:

Administrator Reports

Included in the SEG Administration Center console is access to a suite of reports providing a view into the statistics and use of the Service. All mail messages processed by the Service are recorded in these statistical reports, measured on an hourly, daily, weekly, and monthly basis. The reports furnished to Customer depend of the Service components and features in use by the Customer.

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		SEGA01
Bidder's Product Description: AT&T Secure E-Mail Gateway (SEG) - Advanced 1-49 seats					
2	Email Monitoring and Scanning Service, 50-74	Email managed security services seat as described in Section 7.2.2.	Y		SEGA50
Bidder's Product Description: AT&T Secure E-Mail Gateway (SEG) - Advanced 50-74 seats					
3	Email Monitoring and Scanning Service, 75-99	Email managed security services seat as described in Section 7.2.2.	Y		SEGA75
Bidder's Product Description: AT&T Secure E-Mail Gateway (SEG) - Advanced 75-99 seats					
4	Email Monitoring	Email managed security services seat as	Y		SEGA100



	Feature Name	Feature Description	Bidder Meets or Exceeds? Y N		Bidder's Product Identifier
	and Scanning Service, 100-500	described in Section 7.2.2.			
	Bidder's Product Description: AT&T Secure E-Mail Gateway (SEG) - Advanced 100-500 seats				
5	Email Monitoring and Scanning Service, 501-1000	Email managed security services seat as described in Section 7.2.2.	Y		SEGA501
	Bidder's Product Description: AT&T Secure E-Mail Gateway (SEG) - Advanced 501-1000 seats				
6	Email Monitoring and Scanning Service, 1001 and above	Email managed security services seat as described in Section 7.2.2.	Y		SEG1001
	Bidder's Product Description: AT&T Secure E-Mail Gateway (SEG) - Advanced 1001+ seats				

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

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

	Feature Name	Feature Description	Bidder's Product Identifier
1	None		
	Bidder's Product Description:		

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:

AT&T Web Security service helps create a protected and productive Internet environment for your organization. The service is designed to keep malware off your organizations network and allow you to control the use of the Web by employing Web Filtering, Web Malware Scanning and remote features. As a fully managed service, AT&T Web Security Service requires no additional hardware, upfront equipment costs or ongoing system maintenance.

Implementation is completed via conference calls with the customer. AT&T will direct the customer to perform certain software configurations onsite.

In addition to predefined reports, custom reports and analysis through the drill down tool is available to gather specific information regarding web usage.

Active Directory Integration

AT&T Web Security integrates into your active directory service with a Connector Software, provided as part of the service.

Firewall Redirection

The Proxy Settings are pushed to browsers via an Active Directory GPO, browsers connect through Firewall on port 8080 to the Connector which receives client information and queries the Active Directory Server for Group Information, it then proxies to AWS upstream.

The Firewall blocks all other GET requests this provides End User/Group granularity for applying rules and reporting.



Archiving

Archiving of historical data is 90 days for allowed traffic and 1 year for blocked. Custom reports can be created to export CSV data dumps on a monthly basis for customer archiving of historical periods longer than provided.

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:

Portal Access

AT&T provides a Web based portal to allow administrators to manage control and reporting capabilities with the ability to add additional users with specific access capabilities.

Reporting

A web based portal allows access to drill down reports to enable you to analyze:

- Applications
- Bandwidth
- Blocks
- Browse Time
- Categories
- Groups
- Hosts
- Legal Liability
- Malware



- Security
- Users

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		WSSBND
Bidder's Product Description: Web Filtering enables you to easily create, enforce, and monitor Web usage policies. Web Malware Scanning is designed to help stop Web spyware and viruses at the Internet level before they can infiltrate your network, your roaming and remote employees, and helping to ensure they no longer act as an open bridge into your internal network. Per user fee for a network-based web security service providing Web Filtering – capability for enforcing Internet user web usage policies, Malware Scanning – user protection against malicious software stopping infections before they infiltrate customer's network.					

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
	None		
1	Bidder's Product Description:		

7.2.4 Security Information and Event Management (SIEM)

Contractor shall provide a networked based SIEM service. The service shall collect, analyze, assess and correlate security events from devices located on the Customer premise. All hardware/software necessary to provide service shall reside in the Contractors network and shall be maintained, monitored and supported by the Contractor, with the





exception of equipment required to collect security events from devices located on the Customer premise. Supported devices shall include routers, network intrusion detection probes, server based firewalls, host intrusion detection management stations and unified threat management appliances. The service shall categorize and prioritize security events utilizing the Contractor's threat and risk management methodologies generated from Contractor and Customer defined standards. Security events that represent a security incident or threat shall be escalated to the Customer in accordance with the SLA requirements of Section 7.3.8.5. Contractor escalations shall consist of a security incident report as defined in Section 7.2.4.1 below.

Bidder shall describe its Security Information and Event Management offering.

Bidder understands the requirements in Section 7.2.4 and shall meet or exceed them? Yes
X No_____

Description:

Correlated Log Management Service (CLMS)

Correlated Log Management Services (CLMS) utilizes AT&T's expertise in security analysis and operations within the AT&T Security Operations Center (SOC) to correlate information from multiple devices and device types, both on premises and network based in the AT&T network.

- Provides AT&T an overview of your network by correlating alerts from multiple devices and device types across the entire enterprise.
- AT&T prioritizes security events based on threat and risk management methodologies generated from AT&T standards and customer defined standards.
- AT&T provides rapid notification to the customer when security events are detected and are identified as critical by AT&T SOC
- Includes customer access to weekly and monthly security summary analysis reports

AT&T has harnessed the power of our network, our strength in network security, and access to world class process, tools and people to offer you a Correlated Log Management Service. The service takes events from multiple security and networking devices, including security controls located in the network, correlates these alerts with proprietary technology, prioritizing them and notifying you of events identified as actionable in near real-time. The Correlated Log Management service includes standard reports, threat analysis reports, log storage, Implementation assistance and initial device policy tuning. AT&T collects the security relevant log and event information from firewalls, intrusion prevention sensors and other network devices using agent-less Parser/Aggregator technology deployed in your network. Event



collection is provided for a wide variety of security and network devices which may be located within the AT&T network or on your premises. A diverse set of “feeds” from security devices and services is recommended in order to get a better view of identified threats to your systems and take full advantage of the CLMS system’s correlation capabilities. The intelligence produced is used by AT&T’s security analysis team to make security recommendations to you. Security recommendations, in the form of an email or a phone call, may vary in detail depending on type of incident, granularity of visibility within the network and breadth of the view. The response will be both verbal (phone call) and written (e-mailed) for severe and high incidents, and written only (e-mailed) for others as appropriate.

Alerting functionality

- “Actionable” alerts are generated
 - Suppression of duplicates and false positives
 - Correlation of information from multiple sources
 - Ongoing refinement of algorithms and thresholds
- Alerts are surrounded with contextual “drill-down” information
 - English language alert names and descriptions
 - Underlying event drill downs from Alert information
 - Alerts to IP, protocol, port, and other relevant information
 - Queries are available for supplemental details
- Flexible layered design for managing correlated alerts
 - Real-time correlation engine performs short interval inspection and alarming
 - Log Center queries allow data mining over days, weeks and months

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:

CLMS Standard Reports

“Metrics” Reports	
Critical Alert Count	Displays the total number of security alerts that were presented to the CLMS Portal. Clicking on the count number will show the type of security alerts that were presented to the Security Analyst.
Top 10 Alerts	Displays the Top 10 TMS alerts and the number of times (count) the alert was presented to the portal. . Clicking on the count number will show the type of security alerts that were presented to the Security Analyst.
Top 10 Attacking IP’s	Displays the Top 10 Attacking IP addresses alerts and the number of times (count) the alert was presented to the portal. . Clicking on the count number will show the type of security alerts (for that IP address) that were presented to the Security Analyst. Also clicking on the IP address will spawn an IP address lookup query to identify the owner of the IP address.
Device/Service Alarms	Displays the devices (sources) where the alerts are being reported. Clicking on the count number will show the type of security alerts (that were presented to the Security Analyst number from that device.
Case Counts	Displays the total number of security cases that were presented to the TMS Portal. Clicking on the count number will show the type of security cases/alerts that were presented to the Security Analyst.
Case Summary	Displays the total number of security cases that were presented to the TMS Portal. Listed by Severity (Critical, High, Medium and Low) and listing the number of the cases. Clicking on the count number will show the Severity types of security cases that were presented to the Security Analyst.
Bridge Assignment Count	Displays the total number of Technical Security Conference bridges that were activated for given “critical” security related even.
Case Incident Type Summary	Displays the total number of Case Incident Type Summary by hour, day week and month. Clicking on the state (i.e., Security Incident Phone, Email) will show the cases that were reported and the hour, day, week, month will display those related cases.



“Quarterly Metrics” Reports	
Critical Alert Count	Displays the total number of security alerts that were presented to the TMS Portal. Clicking on the count number will show the type of security alerts that were presented to the Security Analyst.
Top 10 Alerts	Displays the Top 10 TMS alerts and the number of times (count) the alert was presented to the portal. . Clicking on the count number will show the type of security alerts that were presented to the Security Analyst.
Top 10 Attacking IP’s	Displays the Top 10 Attacking IP addresses alerts and the number of times (count) the alert was presented to the portal. Clicking on the count number will show the type of security alerts (for that IP address) that were presented to the Security Analyst. Also clicking on the IP address will spawn an IP address lookup query to identify the owner of the IP address.
Device/Service Alarms	Displays the devices (sources) where the alerts are being reported. Clicking on the count number will show the type of security alerts (that were presented to the Security Analyst number from that device.
Case Counts	Displays the total number of security cases that were presented to the TMS Portal. Clicking on the count number will show the type of security cases/alerts that were presented to the Security Analyst.
Case Summary	Displays the total number of security cases that were presented to the TMS Portal. Listed by Severity (Critical, High, Medium and Low) and listing the number of the cases. Clicking on the count number will show the Severity types of security cases that were presented to the Security Analyst.
Advisories	Displays the total number of Security Advisories that the SOC security team has published, file or deleted. These security advisories/bulletins are related to new vulnerabilities (i.e. Microsoft, Cisco etc) that a particular vendor publishes.
Internet Protect Alerts	Displays the total number of Internet Protect Alerts that have been published. Clicking on the count will show the Internet Protect Alerts for that given status that were published. AT&T Internet Protect provides a "network security" picture at a glance. The AT&T Internet Protect security team utilizes the latest tools and techniques to compile this information and alert on.
“Admin Alert” Reports	Include Graphical Charts which show the Alert Counts from the various sources (see below for sample sources of the data) <ul style="list-style-type: none">• E-mail• IDS• IPS• Firewall



“Quarterly Metrics” Reports	
	<ul style="list-style-type: none"> • VPN Servers • Non-security-related devices (routers, switches, etc.) • Data-leak detection • Authentication servers • Personnel / HR Database
Weekly “Threat Management” Reports	<p>A Threat Management report is produced by AT&T CSO security teams each week as a summary of published information concerning security issues and related security information.</p> <p>Note: The user has the ability to see the report for a particular day by manipulating the input at the top of the screen and to show CI Flash from a selected date.</p>
“User Stats” Report	<p>Showing the user stats for the teams that utilize the CLMS portal listed by: HR ID, ID First/Last Name, Created Cases, Closed Cases, and Messages (entered into the case).</p> <p>Note: The user has the ability to see data for a particular day by manipulating the inputs (date selection) at the top of the screen and then selecting the “Show Metrics” button</p>

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	SIEM service as described in Section	Y		CLMS1





	Feature Name	Feature Description	Bidder Meets or Exceeds? Y N	Bidder's Product Identifier
	Devices	7.2.4.		
	<p>Bidder's Product Description:</p> <p>CLMS is broken into various Service Levels depending upon the number of devices identified upon initial installation and enablement of service. Customer may increase their service level at anytime per incremental costs as described below. Tier 1 is an initial enablement of 1 – 15 devices.</p> <p>Includes: Standard CLMS storage of 30 days Raw, 90 days processed, and 1 Year archived.</p> <ul style="list-style-type: none"> • Raw - raw alerts, every alarm generated by security device. • Processed - duplicate alerts eliminated and alert data is parsed by pre-determined algorithms. • Archived - can either be raw or processed, customer can specify which to use. By default AT&T will store archived. <p>Initial enablement of the service is performed by our Managed Security Services (MSS) Security Operations Center (SOC) including planning, deployment, systems assurance, and hand-off to operations. Customer assistance is required for completion of the planning materials, as well as coordination of enablement. Including a limited scope consulting engagement in which AT&T consultants perform network mapping and identify any potential issues to the implementation of the service prior to enablement. A report will be generated to the customer at the conclusion of the engagement. Tier 1 includes 16 hours of consulting.</p>			
2	Each additional	Each additional device above 15.	Y	CLMS1A
	<p>Bidder's Product Description:</p> <p>Each additional device added after the initial enablement will incur a separate one-time charge. Each additional device above the Tier threshold will include an additional monthly recurring charge as well as the one-time charge. Tier 1 threshold is 15 devices.</p>			
3	16-40 Devices	SIEM service as described in Section 7.2.4.	Y	CLMS2
	<p>Bidder's Product Description:</p> <p>CLMS is broken into various Service Levels depending upon the number of devices identified upon initial installation and enablement of service. Customer may increase their service level at anytime per incremental costs as described below. Tier 2 is an initial enablement of 16 – 40 devices.</p> <p>Includes: Standard CLMS storage of 30 days Raw, 90 days processed, and 1 Year archived.</p> <ul style="list-style-type: none"> • Raw - raw alerts, every alarm generated by security device. • Processed - duplicate alerts eliminated and alert data is parsed by pre- 			





	Feature Name	Feature Description	Bidder Meets or Exceeds? Y N	Bidder's Product Identifier
		<p>determined algorithms.</p> <ul style="list-style-type: none"> Archived - can either be raw or processed, customer can specify which to use. By default AT&T will store archived. <p>Initial enablement of the service is performed by our Managed Security Services (MSS) Security Operations Center (SOC) including planning, deployment, systems assurance, and hand-off to operations. Customer assistance is required for completion of the planning materials, as well as coordination of enablement. Including a limited scope consulting engagement in which AT&T consultants perform network mapping and identify any potential issues to the implementation of the service prior to enablement. A report will be generated to the customer at the conclusion of the engagement. Tier 2 includes 23 hours of consulting.</p>		
4	Each additional	Each additional device above 40.	Y	CLMS2A
	<p>Bidder's Product Description:</p> <p>Each additional device added after the initial enablement will incur a separate one-time charge. Each additional device above the Tier threshold will include an additional monthly recurring charge as well as the one-time charge. Tier 2 threshold is 40 devices.</p>			
5	41-100 Devices	SIEM service as described in Section 7.2.4.	Y	CLMS3
	<p>Bidder's Product Description:</p> <p>CLMS is broken into various Service Levels depending upon the number of devices identified upon initial installation and enablement of service. Customer may increase their service level at anytime per incremental costs as described below. Tier 3 is an initial enablement of 41 – 100 devices.</p> <p>Includes: Standard CLMS storage of 30 days Raw, 90 days processed, and 1 Year archived.</p> <ul style="list-style-type: none"> Raw - raw alerts, every alarm generated by security device. Processed - duplicate alerts eliminated and alert data is parsed by pre-determined algorithms. Archived - can either be raw or processed, customer can specify which to use. By default AT&T will store archived. <p>Initial enablement of the service is performed by our Managed Security Services (MSS) Security Operations Center (SOC) including planning, deployment, systems assurance, and hand-off to operations. Customer assistance is required for completion of the planning materials, as well as coordination of enablement. Including a limited scope consulting engagement in which AT&T consultants perform network mapping and identify any potential issues to the implementation of the service prior to enablement. A report will be generated to the customer at the conclusion of the engagement. Tier 3 includes 26 hours of consulting.</p>			





IFB STPD 12-001-B, C3-B-12-10-TS-01
Vol. 2, SOW Technical Requirements Response, Category 7 –
Network Based Managed Security
Amendment #1, Rev. June 4, 2015

	Feature Name	Feature Description	Bidder Meets or Exceeds? Y N		Bidder's Product Identifier
6	Each additional	Each additional device above 100.	Y		CLMS3A
Bidder's Product Description: Each additional device added after the initial enablement will incur a separate one-time charge. Each additional device above the Tier threshold will include an additional monthly recurring charge as well as the one-time charge. Tier 3 threshold is 100 devices.					
7	101-250 Devices	SIEM service as described in Section 7.2.4.	Y		CLMS4
Bidder's Product Description: CLMS is broken into various Service Levels depending upon the number of devices identified upon initial installation and enablement of service. Customer may increase their service level at anytime per incremental costs as described below. Tier 4 is an initial enablement of 101 – 250 devices. Includes: Standard CLMS storage of 30 days Raw, 90 days processed, and 1 Year archived. <ul style="list-style-type: none"> • Raw - raw alerts, every alarm generated by security device. • Processed - duplicate alerts eliminated and alert data is parsed by pre-determined algorithms. • Archived - can either be raw or processed, customer can specify which to use. By default AT&T will store archived. Initial enablement of the service is performed by our Managed Security Services (MSS) Security Operations Center (SOC) including planning, deployment, systems assurance, and hand-off to operations. Customer assistance is required for completion of the planning materials, as well as coordination of enablement. Including a limited scope consulting engagement in which AT&T consultants perform network mapping and identify any potential issues to the implementation of the service prior to enablement. A report will be generated to the customer at the conclusion of the engagement. Tier 4 includes 31 hours of consulting.					
8	Each additional	Each additional device above 250.	Y		CLMS4A
Bidder's Product Description: Each additional device added after the initial enablement will incur a separate one-time charge. Each additional device above the Tier threshold will include an additional monthly recurring charge as well as the one-time charge. Tier 4 threshold is 250 devices.					
9	251-1000 Devices	SIEM service as described in Section 7.2.4.	Y		CLMS5
Bidder's Product Description:					





	Feature Name	Feature Description	Bidder Meets or Exceeds? Y N	Bidder's Product Identifier
		<p>CLMS is broken into various Service Levels depending upon the number of devices identified upon initial installation and enablement of service. Customer may increase their service level at anytime per incremental costs as described below. Tier 5 is an initial enablement of 251 – 1,000 devices.</p> <p>Includes: Standard CLMS storage of 30 days Raw, 90 days processed, and 1 Year archived.</p> <ul style="list-style-type: none"> • Raw - raw alerts, every alarm generated by security device. • Processed - duplicate alerts eliminated and alert data is parsed by pre-determined algorithms. • Archived - can either be raw or processed, customer can specify which to use. By default AT&T will store archived. <p>Initial enablement of the service is performed by our Managed Security Services (MSS) Security Operations Center (SOC) including planning, deployment, systems assurance, and hand-off to operations. Customer assistance is required for completion of the planning materials, as well as coordination of enablement. Including a limited scope consulting engagement in which AT&T consultants perform network mapping and identify any potential issues to the implementation of the service prior to enablement. A report will be generated to the customer at the conclusion of the engagement. Tier 5 includes 41 hours of consulting.</p>		
10	Each additional	Each additional device above 1000.	Y	CLMS5A
	<p>Bidder's Product Description:</p> <p>Each additional device added after the initial enablement will incur a separate one-time charge. Each additional device above the Tier threshold will include an additional monthly recurring charge as well as the one-time charge. Tier 5 threshold is 1,000 devices.</p>			
11	1001-2500 Devices	SIEM service as described in Section 7.2.4.	Y	CLMS6
	<p>Bidder's Product Description:</p> <p>CLMS is broken into various Service Levels depending upon the number of devices identified upon initial installation and enablement of service. Customer may increase their service level at anytime per incremental costs as described below. Tier 6 is an initial enablement of 1,001 – 2,500 devices.</p> <p>Includes: Standard CLMS storage of 30 days Raw, 90 days processed, and 1 Year archived.</p> <ul style="list-style-type: none"> • Raw - raw alerts, every alarm generated by security device. • Processed - duplicate alerts eliminated and alert data is parsed by pre-determined algorithms. • Archived - can either be raw or processed, customer can specify which to use. By default AT&T will store archived. 			





	Feature Name	Feature Description	Bidder Meets or Exceeds? Y N	Bidder's Product Identifier
	Initial enablement of the service is performed by our Managed Security Services (MSS) Security Operations Center (SOC) including planning, deployment, systems assurance, and hand-off to operations. Customer assistance is required for completion of the planning materials, as well as coordination of enablement. Including a limited scope consulting engagement in which AT&T consultants perform network mapping and identify any potential issues to the implementation of the service prior to enablement. A report will be generated to the customer at the conclusion of the engagement. Tier 6 includes 48 hours of consulting.			
12	Each additional	Each additional device above 2500.	Y	CLMS6A
	Bidder's Product Description: Each additional device added after the initial enablement will incur a separate one-time charge. Each additional device above the Tier threshold will include an additional monthly recurring charge as well as the one-time charge. Tier 6 threshold is 2,500 devices.			

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

Table 7.2.4.2.b Unsolicited SIEM Features

	Feature Name	Feature Description	Bidder's Product Identifier
1	Correlated Log Management Service (CLMS) – Tier 1 Per Incremental Year of Storage	Correlated Log Management Service (CLMS) – Tier 1 Per Incremental Year of Storage	CLMY1
	Bidder's Product Description: If customer desires longer than 1 year of archived storage, this fee applies Monthly Recurring for each additional year desired. Additional year storage for Tier 1 utilizes first in, first out log retention.		
2	Correlated Log Management Service (CLMS) – Tier 2 Per Incremental Year of Storage	Correlated Log Management Service (CLMS) – Tier 2 Per Incremental Year of Storage	CLMY2





IFB STPD 12-001-B, C3-B-12-10-TS-01
Vol. 2, SOW Technical Requirements Response, Category 7 –
Network Based Managed Security
Amendment #1, Rev. June 4, 2015

	Feature Name	Feature Description	Bidder's Product Identifier
	Bidder's Product Description: If customer desires longer than 1 year of archived storage, this fee applies Monthly Recurring for each additional year desired. Additional year storage for Tier 1 utilizes first in, first out log retention.		
3	Correlated Log Management Service (CLMS) – Tier 3 Per Incremental Year of Storage	Correlated Log Management Service (CLMS) – Tier 3 Per Incremental Year of Storage	CLMY3
	Bidder's Product Description: If customer desires longer than 1 year of archived storage, this fee applies Monthly Recurring for each additional year desired. Additional year storage for Tier 1 utilizes first in, first out log retention.		
4	Correlated Log Management Service (CLMS) – Tier 4 Per Incremental Year of Storage	Correlated Log Management Service (CLMS) – Tier 4 Per Incremental Year of Storage	CLMY4
	Bidder's Product Description: If customer desires longer than 1 year of archived storage, this fee applies Monthly Recurring for each additional year desired. Additional year storage for Tier 1 utilizes first in, first out log retention.		
5	Correlated Log Management Service (CLMS) – Tier 5 Per Incremental Year of Storage	Correlated Log Management Service (CLMS) – Tier 5 Per Incremental Year of Storage	CLMY5
	Bidder's Product Description: If customer desires longer than 1 year of archived storage, this fee applies Monthly Recurring for each additional year desired. Additional year storage for Tier 1 utilizes first in, first out log retention.		
6	Correlated Log Management Service (CLMS) – Tier 6 Per Incremental Year	Correlated Log Management Service (CLMS) – Tier 6 Per Incremental Year of Storage	CLMY6





	Feature Name	Feature Description	Bidder's Product Identifier
	of Storage		
	Bidder's Product Description: If customer desires longer than 1 year of archived storage, this fee applies Monthly Recurring for each additional year desired. Additional year storage for Tier 1 utilizes first in, first out log retention.		
	Correlated Log Management Service (CLMS) – Custom (Non-standard) Device Interface	Correlated Log Management Service (CLMS) – Custom (Non-standard) Device Interface	CLMCDI
7	Bidder's Product Description: Devices not included in the Supported Devices List incur a One-Time charge per each unique device (or group of devices). If a customer has multiple devices of the same type with the same operating environment, one fee will be levied. Development time may vary, and will be identified at time of request. Check with your AT&T Account Team to determine if your device is supported.		
	Correlated Log Management Service (CLMS) – Custom (Non-standard) Report	Correlated Log Management Service (CLMS) – Custom (Non-standard) Report	CLMRPT
8	Bidder's Product Description: Customers requiring special reports not listed in the SETA REPORTS List will incur a One-Time charge per each report. Development time may vary.		
	Custom Log Sources – Tier 1	Custom Log Sources – Tier 1	CLMC1
9	Bidder's Product Description: Custom Log Sources – Application logs and custom log sources (priced per each custom log source). Tier 1 is a threshold of 15 devices.		
	Custom Log Sources – Tier 2	Custom Log Sources – Tier 2	CLMC2
10	Bidder's Product Description: Custom Log Sources – Application logs and custom log sources (priced per each custom log source). Tier 2 is a threshold of 40 devices.		
11	Custom Log	Custom Log Sources – Tier 3	CLMC3





**IFB STPD 12-001-B, C3-B-12-10-TS-01
Vol. 2, SOW Technical Requirements Response, Category 7 –
Network Based Managed Security
Amendment #1, Rev. June 4, 2015**

	Feature Name	Feature Description	Bidder's Product Identifier
	Sources – Tier 3		
	Bidder's Product Description: Custom Log Sources – Application logs and custom log sources (priced per each custom log source). Tier 3 is a threshold of 100 devices.		
	Custom Log Sources – Tier 4	Custom Log Sources – Tier 4	CLMC4
12	Bidder's Product Description: Custom Log Sources – Application logs and custom log sources (priced per each custom log source). Tier 4 is a threshold of 250 devices.		
	Custom Log Sources – Tier 5	Custom Log Sources – Tier 5	CLMC5
13	Bidder's Product Description: Custom Log Sources – Application logs and custom log sources (priced per each custom log source). Tier 5 is a threshold of 1000 devices.		
	Custom Log Sources – Tier 6	Custom Log Sources – Tier 6	CLMC6
14	Bidder's Product Description: Custom Log Sources – Application logs and custom log sources (priced per each custom log source). Tier 6 is a threshold of 2500 devices.		
	Advanced Correlation – Tier 1	Advanced Correlation – Tier 1	CLMA1
15	Bidder's Product Description: Advanced Correlation – Correlation with external data sources - DNS, DHCP, name databases, etc. (priced per correlation source for all devices within the tier). Tier 1 is a threshold of 15 devices.		
	Advanced Correlation – Tier 2	Advanced Correlation – Tier 2	CLMA2
16	Bidder's Product Description: Advanced Correlation – Correlation with external data sources - DNS, DHCP, name databases, etc. (priced per correlation source for all devices within the tier). Tier 2 is a threshold of 40 devices.		
17	Advanced Correlation – Tier 3	Advanced Correlation – Tier 3	CLMA3





IFB STPD 12-001-B, C3-B-12-10-TS-01
Vol. 2, SOW Technical Requirements Response, Category 7 –
Network Based Managed Security
Amendment #1, Rev. June 4, 2015

	Feature Name	Feature Description	Bidder's Product Identifier
	Bidder's Product Description: Advanced Correlation – Correlation with external data sources - DNS, DHCP, name databases, etc. (priced per correlation source for all devices within the tier). Tier 3 is a threshold of 100 devices.		
18	Advanced Correlation – Tier 4	Advanced Correlation – Tier 4	CLMA4
	Bidder's Product Description: Advanced Correlation – Correlation with external data sources - DNS, DHCP, name databases, etc. (priced per correlation source for all devices within the tier). Tier 4 is a threshold of 250 devices.		
19	Advanced Correlation – Tier 5	Advanced Correlation – Tier 5	CLMA5
	Bidder's Product Description: Advanced Correlation – Correlation with external data sources - DNS, DHCP, name databases, etc. (priced per correlation source for all devices within the tier). Tier 5 is a threshold of 1000 devices.		
20	Advanced Correlation – Tier 6	Advanced Correlation – Tier 6	CLMA6
	Bidder's Product Description: Advanced Correlation – Correlation with external data sources - DNS, DHCP, name databases, etc. (priced per correlation source for all devices within the tier). Tier 6 is a threshold of 1000 devices.		
21	AT&T VSS-PRO (Vulnerability Scanning Service)	AT&T VSS-PRO (Vulnerability Scanning Service)	Multiple (see IDs below)
	Bidder's Product Description: The VSS-Pro service is used to conduct host discovery and/or vulnerability scans on external and/or internal IP-based systems and networks. A variety of scanning techniques are employed to survey the security posture of the target IP-based systems and networks. These scans proactively test for known vulnerabilities and the existence of mainstream industry practice security configurations. External scanning addresses all Internet-facing assets such as routers, firewalls, web servers, and e-mail servers for potential security weaknesses, checking for the "open doors" that could allow a hacker to gain unauthorized access to the network and exploit critical assets. Internal scanning addresses all internal assets such as workstations, intranet servers, and printers for Trojans, improper configurations, peer-to-peer (PTP) file sharing programs such as Morpheus, Kazaa, etc., and more. The VSS-Pro service also provides workflow management, host-based risk assignments,		





IFB STPD 12-001-B, C3-B-12-10-TS-01
Vol. 2, SOW Technical Requirements Response, Category 7 –
Network Based Managed Security
Amendment #1, Rev. June 4, 2015

	Feature Name	Feature Description	Bidder's Product Identifier
		<p>and remediation progress reporting. In addition, VSS-Pro includes assistance in setting up and maintaining scan profiles and scheduling, project management of the customer's remediation efforts (regardless of whether they are handled by the customer's IT staff or 3rd party provider), and provides access to AT&T's staff of security analysts for additional information and guidance regarding more complex technical issues.</p> <p>In addition to the portal view, critical vulnerabilities that are identified are forwarded on a regular basis to the CLMS systems for correlation with other events within the network. Understand the vulnerabilities that exist, and the threats against these assets can be another critical element in the detection and prevention of a successful attack from either external or internal resources or devices.</p>	
22	VSS-PRO Reconnaissance Network Appliance (RNA) Set UP - Desktop	VSS -PRO Reconnaissance Network Appliance (RNA) Set UP - Desktop	VSSDRN
	Bidder's Product Description: Desktop RNA Installation and Set Up		
23	VSS-PRO Reconnaissance Network Appliance (RNA) Set UP - Rackmount	VSS-PRO Reconnaissance Network Appliance (RNA) Set UP - Rackmount	VSSRRN
	Bidder's Product Description: Rackmount RNA Installation and Set Up		
24	VSS-PRO- Quarterly Scanning 130	VSS-PRO- Quarterly Scanning 130	VSSQ130
	Bidder's Product Description: Up to 130 devices		
25	VSS-PRO- Quarterly Scanning 250	VSS-PRO- Quarterly Scanning 250	VSSQ250
	Bidder's Product Description: Up to 250 devices		
26	VSS-PRO- Quarterly Scanning 500	VSS-PRO- Quarterly Scanning 500	VSSQ500





IFB STPD 12-001-B, C3-B-12-10-TS-01
Vol. 2, SOW Technical Requirements Response, Category 7 –
Network Based Managed Security
Amendment #1, Rev. June 4, 2015

	Feature Name	Feature Description	Bidder's Product Identifier
	Bidder's Product Description: Up to 500 devices		
27	VSS-PRO– Quarterly Scanning 1000	VSS-PRO– Quarterly Scanning 1000	VSSQ1K
	Bidder's Product Description: Up to 1000 devices		
28	VSS-PRO– Quarterly Scanning 2000	VSS-PRO– Quarterly Scanning 2000	VSSQ2K
	Bidder's Product Description: Up to 2000 devices		
29	VSS-PRO– Quarterly Scanning 3000	VSS-PRO– Quarterly Scanning 3000	VSSQ3K
	Bidder's Product Description: Up to 3000 devices		
30	VSS-PRO– Quarterly Scanning 3000+ per 1K incremental	VSS-PRO– Quarterly Scanning 3000+	VSSQ3KP
	Bidder's Product Description: Each added 1K above 3K		
31	VSS-PRO– Monthly Scanning 130	VSS-PRO– Monthly Scanning 130	VSSM130
	Bidder's Product Description: Up to 130 devices		
32	VSS-PRO– Monthly Scanning 250	VSS-PRO– Monthly Scanning 250	VSSM250
	Bidder's Product Description: Up to 250 devices		





**IFB STPD 12-001-B, C3-B-12-10-TS-01
Vol. 2, SOW Technical Requirements Response, Category 7 –
Network Based Managed Security
Amendment #1, Rev. June 4, 2015**

	Feature Name	Feature Description	Bidder's Product Identifier
33	VSS-PRO– Monthly Scanning 500	VSS-PRO– Monthly Scanning 500	VSSM500
	Bidder's Product Description: Up to 500 devices		
34	VSS-PRO– Monthly Scanning 1000	VSS-PRO– Monthly Scanning 1000	VSSM1K
	Bidder's Product Description: Up to 1000 devices		
35	VSS-PRO– Monthly Scanning 2000	VSS-PRO– Monthly Scanning 2000	VSSM2K
	Bidder's Product Description: Up to 2000 devices		
36	VSS-PRO– Monthly Scanning 3000	VSS-PRO– Monthly Scanning 3000	VSSM3K
	Bidder's Product Description: Up to 3000 devices		
37	VSS-PRO– Monthly Scanning 3000+ per 1K incremental	VSS-PRO– Monthly Scanning 3000+	VSSM3KP
	Bidder's Product Description: Each added 1K above 3K		
38	VSS-PRO– On Demand Scanning 130	VSS-PRO– On Demand 130	VSSD130
	Bidder's Product Description: Up to 130 devices		
39	VSS-PRO– On Demand Scanning 250	VSS-PRO– On Demand 250	VSSD250





	Feature Name	Feature Description	Bidder's Product Identifier
	Bidder's Product Description: Up to 250 devices		
40	VSS-PRO– On Demand Scanning 500	VSS-PRO– On Demand 500	VSSD500
	Bidder's Product Description: Up to 500 devices		
41	VSS-PRO– On Demand Scanning 1000	VSS-PRO– On Demand 1000	VSSD1K
	Bidder's Product Description: Up to 1000 devices		
42	VSS-PRO– On Demand Scanning 2000	VSS-PRO– On Demand 2000	VSSD2K
	Bidder's Product Description: Up to 2000 devices		

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 No

7.3.2 Technical Requirements Versus SLA Objectives

Section 0 (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 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 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 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)



**IFB STPD 12-001-B, C3-B-12-10-TS-01
Vol. 2, SOW Technical Requirements Response, Category 7 –
Network Based Managed Security
Amendment #1, Rev. June 4, 2015**

#	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.
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: <ul style="list-style-type: none"> 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.





#	Stop Clock Condition (SCC)	SCC Definition
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.
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 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:





**IFB STPD 12-001-B, C3-B-12-10-TS-01
Vol. 2, SOW Technical Requirements Response, Category 7 –
Network Based Managed Security
Amendment #1, Rev. June 4, 2015**

DDoS Detection and Mitigation Service		Email Monitoring and Scanning Service			
Web Security and Filtering Service		Security Information and Event Management (SIEM)			
AT&T VSS-PRO (Vulnerability Scanning Service)					
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%	S
	Email Monitoring and Scanning Service	≥ 99.9%	≥ 99.95%	≥ 99.99%	S
	Web Security and Filtering Service	≥ 99.9%	≥ 99.95%	≥ 99.99%	S
	SIEM and AT&T VSS-PRO (Vulnerability Scanning Service)	≥ 99.9%	≥ 99.95%	≥ 99.99%	S
Rights and Remedies	Per Occurrence: N/A				
	<p>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.</p>				

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)																													
<p>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.</p>																													
<p>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.</p>																													
Service(s):																													
DDoS Detection and Mitigation Service		Email Monitoring and Scanning Service																											
Web Security and Filtering Service		Security Information and Event Management (SIEM)																											
AT&T VSS-PRO (Vulnerability Scanning Service)																													
<p>Objective (s): The objective restoral time shall be:</p> <table border="1"> <thead> <tr> <th></th> <th>Basic (B)</th> <th>Standard (S)</th> <th>Premier (P)</th> <th>Bidder's Objective Commitment (B, S or P)</th> </tr> </thead> <tbody> <tr> <td>DDoS Detection and Mitigation Service</td> <td>≤ 1 hour</td> <td>≤ 30 minutes</td> <td>≤ 15 minutes</td> <td>S</td> </tr> <tr> <td>Email Monitoring and Scanning Service</td> <td>≤ 1 hour</td> <td>≤ 30 minutes</td> <td>≤ 15 minutes</td> <td>S</td> </tr> <tr> <td>Web Security and Filtering Service</td> <td>≤ 1 hour</td> <td>≤ 30 minutes</td> <td>≤ 15 minutes</td> <td>S</td> </tr> <tr> <td>SIEM and AT&T VSS-PRO (Vulnerability Scanning Service)</td> <td>≤ 1 hour</td> <td>≤ 30 minutes</td> <td>≤ 15 minutes</td> <td>S</td> </tr> </tbody> </table>						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	S	Email Monitoring and Scanning Service	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	S	Web Security and Filtering Service	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	S	SIEM and AT&T VSS-PRO (Vulnerability Scanning Service)	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	S
	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	S																									
Email Monitoring and Scanning Service	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	S																									
Web Security and Filtering Service	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	S																									
SIEM and AT&T VSS-PRO (Vulnerability Scanning Service)	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	S																									
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 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)			
AT&T VSS-PRO (Vulnerability Scanning Service)					
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 and AT&T VSS-PRO (Vulnerability Scanning Service)	≤ 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 No





IFB STPD 12-001-B, C3-B-12-10-TS-01
Vol. 2, SOW Technical Requirements Response, Category 7 –
Network Based Managed Security
Amendment #1, Rev. June 4, 2015



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

SLA Name: Email Monitoring and Scanning Services - Average Delivery Time					
<p>Definition: The delivery time is the elapsed time from when an 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.</p> <p>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.</p>					
<p>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.</p> <p>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.</p>					
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	S
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	S
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	S
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)			
AT&T VSS-PRO (Vulnerability Scanning Service)					
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	S
	Email Monitoring and Scanning Service	16 hours	12 hours	8 hours	S
	Web Security and Filtering Service	16 hours	12 hours	8 hours	S
	SIEM and AT&T VSS-PRO (Vulnerability Scanning Service)	16 hours	12 hours	8 hours	S
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 No





IFB STPD 12-001-B, C3-B-12-10-TS-01
Vol. 2, SOW Technical Requirements Response, Category 7 –
Network Based Managed Security
Amendment #1, Rev. June 4, 2015



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

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





7.3.8.9 Notification

SLA Name: Notification	
<p>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.</p>	
<p>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..</p>	
Service(s): All Services	
<p>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).</p> <p>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).</p> <p>This objective is the same for Basic, Standard and Premier commitments.</p>	
Rights and Remedies	Per Occurrence: Senior Management Escalation
	Monthly Aggregated Measurements: N/A

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





7.3.8.10 Provisioning (M-S)

SLA Name: Provisioning		
<p>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).</p> <p>Provisioning SLAs have two (2) objectives:</p> <p>Objective 1: Individual Service Request; and</p> <p>Objective 2: Successful Install Monthly Percentage by Service Type.</p> <p>Note: Provisioning timelines include extended demarcation wiring, when appropriate.</p>		
<p>Measurement Process:</p> <p>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.</p> <p>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.</p>		
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 and AT&T VSS-PRO (Vulnerability Scanning Service)	N/A	Coordinated/Managed Project





IFB STPD 12-001-B, C3-B-12-10-TS-01
Vol. 2, SOW Technical Requirements Response, Category 7 –
Network Based Managed Security
Amendment #1, Rev. June 4, 2015

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%	S
Email Monitoring and Scanning Service	N/A	≥ 90%	≥ 95%	S
Web Security and Filtering Service	N/A	≥ 90%	≥ 95%	S
SIEM and AT&T VSS-PRO (Vulnerability Scanning Service)	N/A	≥ 90%	≥ 95%	S

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 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 0.

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