Service Level Agreements
Category 7 – Network Based Managed Security

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 for each application of a SCC.

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

Table 7.3.7 – Stop Clock Conditions (SCC)

#	Stop Clock Condition (SCC)	SCC Definition
1	**END-USER REQUEST**	Periods when a restoration or testing effort is delayed at the specific request of the End-User. The SCC shall exist during the period the Contractor was delayed, provided that the End-User's request is documented and time stamped in the Contractor's trouble ticket or Service Request system and shows efforts are made to contact the End-User during the applicable Stop Clock period.
2	**OBSERVATION**	Time after a service has been restored but End-User request ticket is kept open for observation. If the service is later determined by the End-User to not have been restored, the Stop Clock shall continue until the time the End-User notifies the Contractor that the Service has not been restored.
3	**END-USER NOT AVAILABLE**	Time after a service has been restored but End-User is not available to verify that the Service is working. If the service is later determined by the End-User to not have been restored, the Stop Clock shall apply only for the time period between Contractor's reasonable attempt to notify the End-User that Contractor believes the service has been restored and the time the End-User notifies the Contractor that the Service has not been restored.
4	**WIRING**	Restoration cannot be achieved because the problem has been isolated to wiring that is not maintained by Contractor or any of its Subcontractors or Affiliates. If it is later determined the wiring is not the cause of failure, the SCC shall not apply.
5	**POWER**	Trouble caused by a power problem outside of the responsibility of the Contractor.
6	**FACILITIES**	Lack of building entrance Facilities or conduit structure that are the End-User's responsibility to provide.

#	Stop Clock Condition (SCC)	SCC Definition
7	**ACCESS**	Limited access or contact with End-User provided the Contractor documents in the trouble ticket several efforts to contact End-User for the following: a. Access necessary to correct the problem is not available because access has not been arranged by site contact or End-User representative; b. Site contact refuses access to technician who displays proper identification; c. Customer provides incorrect site contact information which prevents access, provided that Contractor takes reasonable steps to notify End-User of the improper contact information and takes steps to obtain the correct information ; or, d. Site has limited hours of business that directly impacts the Contractor's ability to resolve the problem. If it is determined later that the cause of the problem was not at the site in question, then the Access SCC shall not apply.
8	**STAFF**	Any problem or delay to the extent caused by End-User's staff that prevents or delays Contractor's resolution of the problem. In such event, Contractor shall make a timely request to End-User staff to correct the problem or delay and document in trouble ticket.
9	**APPLICATION**	End-User software applications that interfere with repair of the trouble.
10	**CPE**	Repair/replacement of Customer Premise Equipment (CPE) not provided by Contractor if the problem has been isolated to the CPE. If determined later that the CPE was not the cause of the service outage, the CPE SCC will not apply.
11	**NO RESPONSE**	Failure of the trouble ticket originator or responsible End-User to return a call from Contractor's technician for on-line close-out of trouble tickets after the Service has been restored as long as Contractor can provide documentation in the trouble ticket substantiating the communication from Contractor's technician.
12	**MAINTENANCE**	An outage directly related to any properly performed scheduled maintenance or upgrade scheduled for CALNET 3 service. Any such stop clock condition shall not extend beyond the scheduled period of the maintenance or upgrade. SLAs shall apply for any maintenance caused outage beyond the scheduled maintenance period. Outages occurring during a scheduled maintenance or upgrade period and not caused by the scheduled maintenance shall not be subject to the Maintenance SCC.
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.

#	Stop Clock Condition (SCC)	SCC Definition
14	**FORCE MAJEURE**	Force Majeure events, as defined in the PMAC General Provisions - Telecommunications, Section 28 (Force Majeure).

TECHNICAL SERVICE LEVEL AGREEMENTS

The Contractor shall provide and manage the following Technical SLAs.

7.3.8.1 Availability (M-S)

SLA Name: Availability	
Definition: The percentage of time a CALNET 3 service is fully functional and available for use each calendar month.	
Measurement Process: The monthly Availability Percentage shall be based on the accumulative total of all Unavailable Time derived from all trouble tickets closed, for the affected service (includes Contractor provided web portal, dashboard and reports), and feature per calendar month. The monthly Availability Percentage equals the Scheduled Uptime per month less Unavailable Time per month divided by Scheduled Uptime per month multiplied by 100. Scheduled Uptime is 24 x number of days in the month. All Unavailable Time applied to other SLAs, which results in a remedy, will be excluded from the monthly accumulated total.	
Services:	
DDoS Detection and Mitigation Service	Email Monitoring and Scanning Service
Web Security and Filtering Service	Security Information and Event Management (SIEM)
Vulnerability Management	

Objective(s):

	Basic (B)	Standard (S)	Premier (P)	Bidder's Objective Commitment (B, S or P)
DDoS Detection and Mitigation Service	≥ 99.9%	≥ 99.95%	≥ 99.99%	**P**
Email Monitoring and Scanning Service	≥ 99.9%	≥ 99.95%	≥ 99.99%	**P**
Web Security and Filtering Service	≥ 99.9%	≥ 99.95%	≥ 99.99%	**P**
SIEM	≥ 99.9%	≥ 99.95%	≥ 99.99%	**P**
Vulnerability Management	≥ 99.9%	≥ 99.95%	≥ 99.99%	**P**

Rights and Remedies	Per Occurrence: N/A
	Monthly Aggregated Measurements: First month the service fails to meet the committed SLA objective shall result in a 15 percent rebate of the TMRC. The second consecutive month the service fails to meet the committed SLA objective shall result in a 30 percent rebate of TMRC. Each additional consecutive month the service fails to meet the committed SLA objective shall result in a 50 percent rebate of the TMRC.

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

SLA Name: Catastrophic Outage 2 (CAT 2)

Definition: Failure of any part of the Network Based Managed Security Services architecture components (hardware, software, and interconnection of components) based on a common cause that results in a total failure of a service for two (2) or more CALNET 3 Customers.

Measurement Process: The Outage Duration begins when a network alarm is received by the Contractor from an outage-causing event or the opening of a trouble ticket by the Customer or Contractor, whichever occurs first. Upon notification from the Customer or network alarm, the Contractor shall compile a list for each End-User service and feature affected by a common cause for tracking and reporting of the SLA rights and remedies. Outage Duration shall be measured on a per-End-User service basis from information recorded from the network equipment/system or Customer reported trouble ticket. Each End-User service is deemed out of service from the first notification until the Contractor determines the End-User service is restored. Any End-User service reported by the End-User/Customer as not having been restored shall have the outage time adjusted to the actual restoration time.

Service(s):

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

Objective (s):
The objective restoral time shall be:

	Basic (B)	Standard (S)	Premier (P)	Bidder's Objective Commitment (B, S or P)
DDoS Detection and Mitigation Service	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	**P**
Email Monitoring and Scanning Service	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	**P**
Web Security and Filtering Service	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	**P**
SIEM	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	**P**
Vulnerability Management	≤ 1 hour	≤ 30 minutes	≤ 15 minutes	**P**

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

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

SLA Name: Catastrophic Outage 3 (CAT 3)

Definition: The total loss of one (1) or more CALNET 3 Network Based Managed Security services on a system wide basis.

Measurement Process: The Outage Duration begins when a network alarm is received by the Contractor from an outage-causing event or the opening of a trouble ticket by the Customer or Contractor, whichever occurs first. Upon notification from the Customer or network alarm, the Contractor shall compile a list for each End-User service and feature affected by a common cause. Outage Duration shall be measured on a per-End-User service basis from information recorded from the network equipment/system or trouble ticket. Each End-User service is deemed out of service from the first notification until the Contractor determines the End-User service is restored. Any End-User service reported by the End-User/Customer as not having been restored shall have the outage time adjusted to the actual restoration time.

Service(s):

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

Objectives:

The objective restoral time shall be:

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

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

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

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

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

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

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

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

Service(s):

Email Monitoring and Scanning Services	

Objective (s):

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

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

7.3.8.5 SIEM Event Notification (M-S)

SLA Name: SIEM Critical Event Notification

Definition: The Contractor shall notify the Customer via a verbal person-to-person telephone call to authorized users when a critical security event that represents a security incident or threat to the Customer, within the objective timeframe.

Measurement Process:
The amount of time between the identification of a critical security event and the notification (or when the Contractor initially attempts to notify) of the customer.

Service(s):

SIEM	

Objective (s):

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

Rights and Remedies	**Per Occurrence:** Customer will receive a credit equal to 25 percent of the SIEM Service TMRC for each event in which a Customer is not notified within the committed objective.
	Monthly Aggregated Measurements: N/A

7.3.8.6 DDoS Customer Notification (M-S)

SLA Name: DDoS Customer Notification

Definition: The Contractor shall notify the Customer via an e-mail and a verbal person-to-person telephone call to authorized users when an anomaly or attack is detected, within the objective timeframe.

Measurement Process:
The amount of time between the identification of an anomaly or attack, and the notification (or when the Contractor initially attempts to notify) of the customer.

Service(s):

DDoS Detection and Mitigation	

Objective (s):

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

Rights and Remedies	**Per Occurrence:** Customer will receive a credit equal to 25 percent of the DDoS Detection and Mitigation Service TMRC for each event in which a Customer is not notified within the committed objective.
	Monthly Aggregated Measurements: N/A

7.3.8.7 Excessive Outage (M-S)

SLA Name: Excessive Outage

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

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

Service(s):

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

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

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

Rights and Remedies

Per Occurrence: 100 percent of the TMRC for each service or feature out of service for a period greater than the committed objective level.

Upon request from the Customer or the CALNET 3 CMO, the Contractor shall provide a briefing on the excessive outage restoration.

Monthly Aggregated Measurements: N/A

7.3.8.8 DDoS Time to Mitigate (M-S)

SLA Name: DDoS Time to Mitigate

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

Measurement Process:

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

Service(s):

DDoS Detection and Mitigation	

Objective (s):
Mitigation shall begin within:

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

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

7.3.8.9 Notification

SLA Name: Notification	
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.	
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.	
Service(s): All Services	
Objective (s): Within 60 minutes of the above mentioned failures' start time, the Contractor shall notify CALNET 3 CMO and designated stakeholders using a method defined in IFB STPD 12-001-B Business Requirements Section B.3.3 (Network Outage Response). At 60 minute intervals, updates shall be given on the above mentioned failures via the method defined in IFB STPD 12-001-B Business Requirements Section B.3.3 (Network Outage Response). This objective is the same for Basic, Standard and Premier commitments.	
Rights and Remedies	**Per Occurrence:** Senior Management Escalation
	Monthly Aggregated Measurements: N/A

7.3.8.10 Provisioning (M-S)

SLA Name: Provisioning

Definition: Provisioning shall include new services, moves, adds and changes completed by the Contractor on or before the due dates. The Provisioning SLA shall be based on committed installation intervals established in this SLA or due dates negotiated between Customer and Contractor documented on the Contractor's order confirmation notification or Contracted Service Project Work SOW in accordance with IFB STPD 12-001-B Business Requirements Section B.2.5.4 #7 (Provisioning and Implementation). The Contractor shall meet the committed interval dates or due date negotiated with the Customer. If the Customer agrees to a negotiated due date, the negotiated due date supersedes the committed interval. At the Customer's discretion, if the scope of the Service Request(s) meets the Coordinated or Managed Project criteria, negotiated due dates will be established and documented in the Project Schedule per IFB STPD 12-001-B Business Requirements Section B.6 (Contracted Service Project Work).

Provisioning SLAs have two (2) objectives:

Objective 1: Individual Service Request; and

Objective 2: Successful Install Monthly Percentage by Service Type.

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

Measurement Process:

Objective 1: Individual Service Request: Install intervals are based on the committed installation intervals established in this SLA or due dates negotiated between Customer and Contractor documented on the Service Request. This objective requires the Contractor to meet the due date for each individual Service Request.

Objective 2: Successful Install Monthly Percentage per service Type: The Contractor shall sum all individual Service Requests per service, as listed below, meeting the objective in the measurement period (per month) and divide by the sum of all individual Service Requests due per service in the measurement period and multiply by 100 to equal the percentage of Service Requests installed on time. The Contractor must meet or exceed the objective below in order to avoid the rights and remedies.

Service (Features must be installed in conjunction with the service except when listed below)	Committed Interval Calendar Days	Coordinated/Managed Project
DDoS Detection and Mitigation Service	N/A	Coordinated/Managed Project
Email Monitoring and Scanning Service	N/A	Coordinated/Managed Project
Web Security and Filtering Service	N/A	Coordinated/Managed Project
SIEM	N/A	Coordinated/Managed Project
Vulnerability Management	N/A	Coordinated/Managed Project

Objective (s):

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

Objective 2: Successful Install Monthly Percentage per Service:

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

Rights and Remedies	**Per Occurrence:** Objective 1: Individual Service Requests: 50 percent of installation fee credited to Customer for any missed committed objective.
	Monthly Aggregated Measurements: Objective 2: 100 percent of the installation fee credited to Customer for all Service Requests (per service type) that did not complete on time during the month if the Successful Install Monthly Percentage is below the committed objective.

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

SLA Name: Time to Repair (TTR)

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

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

Service(s):

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

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

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

Rights and Remedies

Per Occurrence: 25 percent of the TMRC per occurrence for each service and feature out of service for a period greater than the committed objective level.

Monthly Aggregated Measurements: N/A