

# **PRESIDIO®**

Future. Built.

**MANAGED SERVICES CONTRACT**  
**SELECT SERVICES: NETWORK & UC**  
**ESSENTIAL SERVICES: DATA CENTER**  
**LEE COUNTY BOARD OF COUNTY COMMISSIONERS**

**May 17 , 2021**

**REVISION HISTORY**

Revision	Revision Date	Name	Notes
1.0	05-04-2021	Meredith Kirkwood	Initial Proposal for Select Managed Services
2.0	05-17-2021	Meredith Kirkwood	Revised MMSA to Reference NASPO Agreement

Notices: © 2021 Presidio. All Rights Reserved. This document and its contents are the confidential and proprietary intellectual property of PRESIDIO and may not be duplicated, redistributed, or displayed to any third party without the express written consent of PRESIDIO.

Other product and company names mentioned herein may be the trademarks of their respective owners.

TABLE OF CONTENTS

1. SERVICE SUMMARY ..... 4

2. SERVICE DELIVERY CENTER ..... 5

3. MONITORING.....10

4. CLIENT PORTAL & STANDARD REPORTS .....12

5. CHANGE MANAGEMENT .....13

6. PROBLEM MANAGEMENT .....15

7. PATCH MANAGEMENT .....16

8. CARRIER CASE MANAGEMENT .....17

9. DISPATCH SERVICES .....18

10. VENDOR MANAGEMENT .....19

11. SERVICE DELIVERY MANAGEMENT .....20

12. SERVICE TRANSITION MANAGEMENT.....21

13. CLIENT RESPONSIBILITIES.....23

14. PRICING & CONTRACT TERM .....25

15. COVERED EQUIPMENT LIST .....27

MANAGED SERVICES TERMS AND CONDITIONS .....28

APPENDIX A: NETWORK SERVICES .....31

APPENDIX B: UNIFIED COMMUNICATION MANAGEMENT - CISCO .....33

APPENDIX C: DATA CENTER SERVICES (ESSENTIAL).....36

GENERAL DEFINITIONS .....38

ATTACHMENT 1: COVERED EQUIPMENT LIST.....41

## 1. SERVICE SUMMARY

Service Elements drive the level of service for each of the Presidio Managed Services offerings and are defined in the sections that follow. Details for the specific service deliverables are outlined in the Service Appendices. Your Managed Services Support Solution will include the following:

### Service Elements

Select Services (Network and UC Only)
<ul style="list-style-type: none"><li>• Service Delivery Center</li><li>• 7 x 24 x 365 Monitoring</li><li>• Client Portal</li><li>• Standard Reports</li><li>• Change Management<ul style="list-style-type: none"><li>○ Device-Level MACDs (Move, Add, Change, Delete)</li></ul></li><li>• Problem Management</li><li>• Patch Management</li><li>• Dispatch Services</li><li>• Vendor Management</li><li>• Carrier Case Management</li><li>• Full-time, dedicated Project Manager to facilitate Client project needs</li></ul>

### NOTES:

- **User-Level MACDs are not included in the scope of this Statement of Work.**
- **Data Center Services will be delivered at the Essential Service level**, which excludes the following service elements from the table above:
  - Problem Management
  - Patch Management
  - Dispatch Services
  - Carrier Care Management
  - Device-Level MACDs

**This Statement of Work is in accordance with NASPO Master Agreement Number AR3113 (FL# 43230000-NASPO-16-ACS).**

## 2. SERVICE DELIVERY CENTER

The Service Delivery Center (SDC), also generally referred to as the Network Operations Center (NOC) is the main point of contact for reporting incidents (disruptions in service availability and/or quality) and for Clients making service requests (routine requests for services). Presidio's Service Delivery Center team is staffed 24 hours a day, 7 days a week, 365 days a year in three primary locations including Orlando, FL, Dallas, TX, and Minneapolis, MN.

Presidio defines technical support levels as follows:

### **Tier 1: Technician Support**

The Service Delivery Technician (Tier 1) is responsible for effective Client service support using workflow and incident management tools. Tier 1 technicians follow Presidio's standard ITIL-based processes, as well as specific Client processes as defined by Service Delivery Management. Technicians utilize our incident management system to manage the incident queue for resolution or follow up, interface with Tier 2 engineering for advanced engineering support as needed and maintain Client communication during escalations. Initial support for basic Client issues is supported at Tier 1.

### **Tier 2: Engineering Support**

The Service Delivery Engineer (Tier 2) is responsible for effective Client service using advanced engineering skills. Tier 2 engineers use defined ITIL-based processes for effective Incident and Change Management. In addition, the engineer interfaces with vendor support engineering or Presidio Professional Services to provide timely resolution.

### **Tier 3: Advanced Technical Support**

Tier 3 is the highest level of support in a three-tiered technical support model responsible for handling the most difficult or advanced incidents and overseeing problem management for Clients.

The Client may communicate incidents to the Service Delivery Center using the following methods (in addition to auto-generated incidents):

- Telephone (P1 Incidents must be opened via a call into the SDC)
- Opening a ticket on the Client Portal (defaults to a Priority 4 incident)
- Email (defaults to a Priority 4 incident)

Client personnel contacting the Presidio SDC must be authorized to do so as defined in the Capture Template. The Capture Template is a set of defined procedures developed during the Service Transition Management process for maintaining the everyday operation of the Client environment. The SDC cannot respond to support requests from non-authorized personnel and will not engage with the Client through indirect methods for incident notification. Client personnel authorized to contact the SDC must be qualified to interact on a technical basis at a level required to support efforts by Managed Services.

Once an incident has been opened, an email notification will be sent to the caller and all contacts subscribed to receive notifications that match the conditions of the incident.

## 2.1. Incident Management

Presidio will perform the following during the management of incidents identified through monitoring of the environment or by direct Client notification:

- Event identification, logging, and management
- Alert Review to assess if it is an actual alert or system anomaly
- Clear system anomalies and close the incident
- Group related relevant events into a single incident to reduce notifications (parent/child incident correlation)
- Prioritize incidents based on impact and urgency
- Notify Client of the incident within the notification service level
- Restore Service
  - Take complete ownership of service restoration or remotely assist onsite personnel as needed to facilitate service restoration.
  - Remotely facilitate hardware replacement and software updates determined to be required by Presidio.
  - Remotely apply patches to remediate an incident or problem identified by Presidio.
  - Interact with third-party support providers which requires a Client-signed Letter of Agency (LOA) processed during the Service Transition Management phase. Carrier Case Management is only included in the Select tier of services

### Incident Prioritization Classification and Prioritization

Incidents need proper classification and prioritization. Classification and prioritization are described as follows:

- Classification - Determined by choosing the correct service offering, category, and subcategory as it pertains to the incident.
- Prioritization - Assigning impact and urgency calculates the appropriate priority.

#### 2.1.1. Determining Classification and Prioritization

Based on the information placed in the incident during its creation, the incident is reviewed, and the correct classification, urgency and impact are selected.

Priority is based on the combined Impact and Urgency assignments, reflecting the level of adverse impact to the Client systems.

#### 2.1.2. . Impact Definition

Impact refers to the business impact of the system impacted. The initial impact is pre-defined from the alerting tool based on the type of alarm received or Client request.

There are three categories of impact:

1. **High:** Incident affecting an entire site or multiple sites.
2. **Medium:** Incident affecting multiple users.



3. **Low:** Incident affecting one or few users.

### 2.1.3. Urgency Definition

Urgency is the extent to which the incident's resolution can bear delay. The initial urgency is pre-defined from the alerting tool based on the type of alarm received or Client request.

Presidio Incident and Problem urgency and corresponding priority levels are defined as follows:

1. **High:** Complete service outage of a critical system or VIP is affected, requires urgent response.
2. **Medium:** Client's ability to function is partially impacted, requires the SDC to respond as soon as possible.
3. **Low:** No impact on the Client's ability to function; is more informational in nature and a response is not critical.

The incident shall be closed by Presidio or Client upon validation of issue remediation and the CI's return to operational stability. Incidents may be closed if no communication from client is received after three (3) attempts

### 2.1.4. Priorities for Tools Generated Incidents

Presidio monitoring tools apply the following priorities for auto-generated incidents, generally indicating the condition shown (the actual condition is determined by several factors as defined in the thresholds).

**Incident Priorities**

IMPACT				
URGENCY		High	Medium	Low
	High	P1	P2	P3
	Medium	P2	P3	P4
	Low	P3	P4	P4

### 2.1.5. Incident Escalation

Incidents are escalated according to a defined process, and at any point, the Client may request escalation via the Presidio SDC to address concerns about the handling of the incident. If service restoration requires activities by a third-party provider, Presidio initiates and manages the process.

For a High Severity (P1 or P2), Clients are asked to call Presidio Managed Services. The SDC will initiate a live handoff to an engineer, if requested

## 2.2. Service Level Agreement

Service Level Agreements (SLA) are specifically aligned to incident priorities and response times for service requests. Presidio categorizes each issue by priority reflecting the level of adverse impact to Client systems. Priority provides a reasonable and accurate reflection of the number and complexity and business impact of systems affected. Clients can set or change the priority level of an incident at any time, based on the impact to their specific business.

### Priority Levels

Level	Description
● <b>P1 / Critical</b>	Systems at one or many Client sites are completely unavailable. Affected systems cause significant business impact.
● <b>P2 / High</b>	Systems at one or many Client sites are partially unavailable. Affected systems cause some business impact.
● <b>P3 / Medium</b>	Operational performance of Client sites is impaired while most business operations remain functional.
● <b>P4 / Low</b>	Client is requesting information or a logical change that is covered under their service agreement.

### Service Credits

Service Credits shall be awarded beginning with the first full month following thirty (30) days of Service based on the criteria outlined below.

The service level table with credits identifies a credit equal to a percentage of MRC if the Acknowledgement, First Access Response Time and Resolution Time service levels are not met for P1s and P2s. A percentage is assigned to each category for a maximum credit of 10% of MRC per month.

Credits apply if the number of incidents allow for measurement per month.

**A table on the following page outlines Service Level Objectives, and achievement percentage is calculated as follows:**

**Acknowledgement Response Time** achievement percentage is calculated as follows:

Total Incidents acknowledged within Service Level Target / Total Incidents (for each priority).

**First Access Response Time** achievement percentage is calculated as follows:





Total Incidents within First Access Response Time Service Level Target / Total Incidents (for each priority).

**Resolution Time** achievement percentage is calculated as follows:

Total Incidents within Resolution Time Service Level Target / Total Incidents (for each priority).



**Service Level Objectives with Service Credits**

Service Level Objective	P1 	P2 	P3 	P4 
<b>Acknowledgement Response Time*</b> The amount of elapsed time between Client initiation of an issue, or the time Presidio Managed Services (MS) detects a fault, and the time Presidio MS creates an incident report and notifies Client via e-mail that an incident has been created.	15 minutes  >95% (20 Incidents required)	30 minutes  >90% (10 Incidents required)	4 hours  >80% (5 Incidents required)	8 hours  NA
<b>SLA Penalty - Acknowledgement</b> (% of Monthly Recurring Charge).	1% of MRC	1% of MRC	NA	NA
<b>First Access Response Time</b> The amount of elapsed time between Client initiation of an issue, or the time Presidio MS detects a fault, and the time an assigned Presidio MS technician connects to the system, or otherwise contacts Client, and begins remote diagnosis and troubleshooting.	30 minutes  >95% (20 Incidents required)	1 hour  >90% (10 Incidents required)	8 hours  >80% (5 Incidents required)	3 days  NA
<b>SLA Penalty – First Access Response</b> (% of Monthly Recurring Charge)	2% of MRC	2% of MRC	NA	NA
<b>Resolution Time</b> The amount of elapsed time between Client initiation of an issue, or the time Presidio Managed Services detects a fault, and the time Presidio Managed Services resolves the incident or provides a workaround. The SLA timer pauses if it is dependent on third party intervention or if input or an approval is required from the client.	4 hours  >95% (20 Incidents required)	24 hours  >90% (10 Incidents required)	3 days  >80% (5 Incidents required)	14 days  NA
<b>SLA Penalty – Resolution</b> (% of Monthly Recurring Charge)	2% of MRC	2% of MRC	NA	NA
<b>MACD Request Completion Time</b> The amount of elapsed time between Client request of a User Change and the completion of the change measured in US business hours.	8 business hours			

\* Requires customer subscription to notifications.

## 3. MONITORING

The Presidio Managed Services Framework, Presidio Monitoring and Operation teams integrates directly into the customer environment, providing on-site collection of all the critical information required to proactively manage customer components. The Managed Services Framework, combines industry know-how with robust processes and procedures, underpinned with many of the best practices in the Information Technology Infrastructure Library (ITIL). Presidio aligns these proven processes with top technologies to create the interlocking framework that serves as the basis for all of Presidio's offerings.

The central-based processing and consolidation capability is implemented through an extensive set of integrated tools that work in unison to manage a customer's environment. These tools provide device health monitoring and reporting, provide an interface for remote diagnostics, and exchange information with the IT Service Management (ITSM) platform to support advanced capabilities such as automated incident creation. The Presidio Data Collection Agent (DCA) comes pre-configured with all the Presidio monitoring tools. Once installed, DCA communicates back to the primary collection point where all the customer data is collected and automatically analyzed.

Inside of Presidio's ITIL compliant Service Desk system, every component managed is defined as a configuration item in the Configuration Management Database.

Threshold values are set for all device types and all devices under collection. The customer can identify critical devices/resources in which they would like to be contacted. Any exceptions to these thresholds are collected and reported.

Presidio will monitor the health and performance via multiple avenues including SNMP polling at set intervals, SNMP traps for critical alerts, when viable other methods as determined by the technology being monitored. Utilization metrics include standard MIB-II and some private enterprise MIB information supported by the application such as LAN utilization, WAN utilization, CPU Utilization, Collisions, Discards.

Presidio's monitoring tools provide device health monitoring and reporting, enable event consolidation, provide an interface for remote diagnostics and exchange information with the IT Service Management (ITSM) platform to support advanced capabilities such as automated incident creation.

Inside of Presidio's ITIL compliant Service Desk system, every component managed is defined as a configuration item in the Configuration Management Database (CMDB) and all events and data are tracked back to the individual Configuration Items.

### 3.1. Service Details

- 24X7 Collection of Monitored Component Data
- Real-time Threshold Monitoring and Exception Notification Event management

Presidio provides monitoring and instrumentation problem resolution services with best-practice processes supported by a state-of-the-art toolset. The service starts with a component, and then performs polling for events. Alarms are consolidated and efficiency is optimized for root cause analysis. Presidio provides full console services and incident workflow.

## 3.2. Presidio Data Centers

Presidio's Managed Services data center space includes two redundant facilities. Each facility features dual home connectivity to two network carriers and a data center infrastructure consisting of independent compute, storage, security and network infrastructure.

## 3.3. Presidio DCA

The monitoring framework requires installation of the Presidio Data Collection Appliance (DCA) on the Client network. Each DCA contains a complete copy of Presidio monitoring tools, including the core monitoring framework software and a local collection database.

The DCA is installed on the Client premises on a single subnet configured with Secure Socket Layer (SSL) tunnel to the Presidio monitoring framework. It is recommended that the DCA be installed within the Client data center at the network core. Additional Presidio appliances may be required, depending on the services the Client purchased and the number, type and location of monitored devices and systems.

## 4. CLIENT PORTAL & STANDARD REPORTS

Presidio Managed Services includes a Web-based Management Portal. The Client Portal is remotely accessible by Clients and provides access to key information and services with respect to their managed services. Capability includes:

- Facilitating communication with the Presidio Service Desk, including request management.
- Viewing progress of service activities and the level of service being delivered.
- Viewing, creating and updating incident tickets and change requests.
- Viewing the status of CIs under contract.

Instructions to access and navigate the portal are provided in the remote training session during Service Transition.

Presidio Managed Services come with a suite of standard reports. Presidio provides reports for managed CIs, including performance, availability, and inventory reports. The Client reports are accessible via the Client Portal. Report details are provided in the Service Appendices and are specific to each service contracted with Presidio.

## 5. CHANGE MANAGEMENT

Change Management ensures that changes to managed CIs are evaluated, coordinated, and communicated to all impacted parties to minimize adverse impact on the Client Production environment.

Changes fall into four categories:

1. Standard Changes
2. Normal Changes
3. Emergency Changes
4. Customer Maintenance Changes

### 5.1. Standard Changes

A Standard Change is a change to a service or infrastructure for which the approach is pre-authorized by Change Management and that has an accepted and established procedure to provide a specific change requirement. Standard Changes do not require authorization from Technical, Customer or Change Management Approvers prior to implementation. Standard Changes have low to no risk and have no impact to the Production environment when performed. Standard Changes should not have outages associated with them. There is no designated Lead Time for Standard Changes.

### 5.2. Normal Changes

A Normal Change is a change to a service or infrastructure planned and implemented within designated Lead Times. They follow the Normal Change process defined in the Change Management Policy. Normal Changes require authorization from the Technical Approver (designated by who is performing the implementation), Customer Approver and Change Manager Approver. Normal Changes require fully detailed implementation plans, back out plans, test plans and justification for performing the change.

The Lead Time for a Normal Change is 2 days (48 hours) from the time the Change Request is submitted until the time it can be implemented. This allows time for the Change Request to be reviewed and approved by all appropriate parties. It also allows time for Presidio Managed Services to properly assign resources to the Change Request.

If a Normal Change is required to be processed sooner than the 2-day lead time, it is flagged as Expedited. All requests for Expedited Normal Changes require a valid business-related justification.

### 5.3. Emergency Changes

An Emergency Change is a change to a service or infrastructure that requires implementation as soon as possible due to a critical issue or service or infrastructure outage. Emergency Changes must be related to a Priority 1 (P1) or Priority 2 (P2) incident or request and may be logged after the P1 or P2 is resolved.

If an Emergency Change is logged after the resolution of a P1 or P2, it must be logged within 24 hours of the Incident, Request, or Problem Resolution. Approval of an after the fact Emergency Change is a validation that the Emergency Change was required at the time it was performed. Emergency Changes are approved by the Emergency Change Advisory Board. There is no designated Lead Time for Emergency Changes.



## 5.4. Customer Maintenance Changes

A Customer Maintenance Change is a change to a service or infrastructure being performed directly by the customer and not Presidio that has the potential for alerts to be created. This type of Change Request is submitted for the purpose of suppressing monitoring for qualifying alerts at the following levels: the entire company, a specific location or the specific CIs listed in the Change Request (for those events that have a location or CI associated with them). Customer Maintenance Change Requests are submitted either by the customer through the Presidio Customer Portal or by a member of the Service Delivery team for the customer.

## 5.5. Moves, Additions, Changes, Deletions (MACD)

Presidio offers Request Management for Managed CIs. The MACD process provides a model for managing and executing moves, additions, changes and deletions of hardware and software configuration items in the Client's environment. MACD service is defined as Device-Level Changes. A Definition is provided below with additional details for contracted services within the Service Appendices (if applicable). **User-Level MACDs are NOT included in the scope of this proposal.**

### 5.5.1. Device-Level Changes

Device-level changes are defined as configuration requests that typically impact multiple users based on the change, such as configuration. Device-level MACD support is only provided to equipment specified in the CEL. Device-level MACD efforts are reviewed by Presidio relative to the contract for each device-level request and Presidio determines if it falls outside of the scope as defined below:

1. Takes less than 2 hours of time to complete which includes validation, scheduling, execution, and testing
2. Does not require planning, design or installation efforts.
3. Does not include any activity with a material operational impact. (i.e., the change cannot affect the normal physical operation of the device).
4. Not a major upgrade or a client request for feature addition.
5. Not an individual project or part of an individual project regardless whether Presidio Professional Services, internal client or 3<sup>rd</sup> party is performing services.
6. Any new functionality that requires engineering development due to the addition of hardware or software, would require proper planning, designing and execution and would be considered a 'net-new' addition is considered a project.
7. Does not require a Solution Architect or Project Manager to facilitate scheduling and planning.
8. Proactive patching for CVSS scores under 9 is not considered a device level change and will be subject to a separate statement of work per the Patch Management section.

For changes not covered by this agreement, Presidio provides a Block of Hours from Professional Services. A single device-level change (MACD) is defined as one change per device; multiple changes to a single device are considered multiple MACDs regardless of whether it is made on the same service request. Presidio reserves the right to determine if the activity qualifies as a MACD activity. Device-level changes are allowed and limited to a total equivalent of two (2) per device, per month, per device type (example: firewalls, routers, switches, application). A cumulative change example would be 40 routers which would allow 80 configuration changes per month across all routers. Any change allocations remaining at the end of a service month are considered forfeited and do not roll to subsequent service months.



## 6. PROBLEM MANAGEMENT

Problem Management is a process that supports Incident Management. A problem is created for tracking activities that lead to identifying a root cause and resolution to the incident's underlying error. Presidio Managed Service Problem Management process also helps identify, diagnose, and resolve large scale Incident trends.

Presidio's Problem Management Policy objectives are as follows:

- To identify, diagnose, resolve, and report on Problems
- To update Presidio's Knowledge Base with Problem resolutions and workarounds to Known Errors so they are searchable for information to resolve similar issues

### 6.1. Problem Management Stakeholders

- **Problem Manager** –Overall accountability of the Problem Management Policy.
- **Problem Requestor** – The person who requested the initiation of a Problem Investigation.
- **Problem Management Review Team** – The group who meets weekly to provide status updates of current open Problems.
- **Solutions Provider Group** – Engineers assigned to investigate and resolve Problems.

### 6.2. Problem Management Process

#### Problem Identification

Analyzing available data, identifying\recording problems, and classifying problems according to impact, urgency, and status. Potential problems are identified through proactive and reactive methods:

- Proactive – Auto-generation of problems based on established criteria or reviewing scheduled reports for Incident trends
- Reactive – Responding to an identified large-scale and/or recurring incident trend or an issue identified as a problem during incident diagnosis

#### Problem Diagnosis

The Problem is assessed to determine potential resolutions, which can include both temporary workarounds as well as permanent fixes. If a permanent fix is possible and cost-justifiable, a recommendation is made to the Client to correct the error by initiating a change via Change Management.

#### Problem Resolution

If a fix is discovered and can be reasonably implemented, the member of the Solutions Provider Group initiates the Change Management Process to implement the fix. If a fix is discovered and cannot be reasonably implemented due to factors such as cost, it should be notated in the Known Error Database and reported to the Problem Management Review Team for discussion.

#### Problem Closure

Once the resolution to a Problem is implemented and confirmed as fixed, the Problem will be closed with appropriate details included within the Problem record.

## 7. PATCH MANAGEMENT

Presidio provides Patch Management to customers who have contracted for Select Level services. There are two areas where patch management is applied: 1) Incident Remediation and 2) Vulnerability Management.

### 1) Incident Remediation

Patch management for incidents is applied when a Presidio engineer identifies, or a vendor support case directs Presidio to apply a version consistent with a fix for a known error. Patch application is a cooperative decision between the customer and Presidio. Patches are evaluated to ensure that current environmental stability is maintained, and are handled as Change Requests

### 2) Vulnerability Management

Vulnerabilities are defined as a defect reported by a manufacturer that has the potential to affect the overall security of a client device(s). Vulnerability patches are applied when there is a CVSS score that is a 9.0 or higher (Critical) as defined by the CVSS specifications listed at <https://www.first.org/cvss/specification-document>. Vulnerability patches below Critical level are not considered MACD activity and are billed as a separately negotiated addendum to the original SOW as applicable. Not all vendors provide CVSS scores or acknowledge vulnerabilities, and as such, Presidio is not able to notify/remediate unpublished vendor vulnerabilities.

As part of the Patch process, Presidio completes the following:

- For incident remediation patches, Presidio will work with the manufacturer/vendor to determine impact and urgency to the Client system and existing software levels.
- For vulnerabilities classified as Critical per the Common Vulnerability Scoring System, CVSSv3.x, with a score of 9.0 – 10.0, Presidio will assess impacts to the Client and provide recommendations for remediation as applicable. Engagement times may vary dependent on the client environment and will include configuration validation before notification. Presidio allows 5-10 business days as a standard when being notified that the client infrastructure is affected by a vulnerability.
- For critical security vulnerabilities and incident remediation as defined above, Presidio remotely applies updates to affected CIs
- Patches that cover many devices and require the coordination of multiple teams and/or multiple outage windows are performed with the appropriate urgency and scheduled with respect to Presidio resource availability. More than fifteen (15) devices or five (5) locations will require the customer to provide a Point of Contact to assist in the coordination of scheduling the patch application. If the customer cannot provide the appropriate resource, Presidio will provide Project Management oversight at mutually agreeable rate.

If the Patch application necessitates a full upgrade in version level, requires a physical change to the existing hardware configuration or impacts dependent technologies, the effort is deemed out of scope and will require a separate statement of work. Covered equipment with software where the software maintenance has reached end of support or has lapsed, is not covered by the Patch Management element.

Client-requested patches for obtaining additional features or functions are out of scope of this section and must be handled as a separate agreement as referenced in “Device Level Changes” under the Change Management section of this document.

## 8. CARRIER CASE MANAGEMENT

Presidio provides operational handling of carrier cases with third-party data and voice carriers for incident remediation. For most Clients under management by Presidio, there is a strong telecommunication vendor dependency. This service element enables Presidio to open tickets, for Clients who have provided a signed Letter of Agency (LOA) and the requisite circuit information, on behalf of the Client for any circuits directly connected to devices under Presidio management. Presidio manages the case throughout the incident resolution process.

---

## 9. DISPATCH SERVICES

Dispatch Services include scheduling qualified field technicians to replace failed equipment associated with an RMA only. Prior to the dispatch, Presidio coordinates with the Client to set proper expectations for timing of the replacement work. The service objectives are either a 7x24x4 hour response or an 8x5xNext Business Day (NBD) response depending on the associated vendor maintenance attached to the failed component. The 4-hour response objective is typically provided to locations within 50 miles of a major metropolitan area.

International locations or 4-hour response guarantees for US locations require a separate customer agreement for coverage, due to additional cost.

Dispatch services not associated with an RMA replacement, which are customer requests for assistance, are billable engagements at a rate that is based upon the level of effort and location and will be reviewed with the client prior to engagement.

## 10. VENDOR MANAGEMENT

Presidio provides operational coordination of incident resolution involving products supported by third-party vendors as specified in the device list of this contract. Presidio support requires the Client to provide necessary account, contract, and support information at the time of on-boarding. Support information includes, but is not limited to, vendor support hours of operation, contact numbers, escalation contacts and any applicable SLAs.

For incidents involving third-party vendors, Presidio can only commit to SLA attainment consistent with the Client's service level agreements with the vendor and is dependent on vendor resource availability. For incident management involving third-party vendors, Presidio will open tickets with the vendor and manage the case throughout the incident resolution process.

Note: Dispatches by Presidio for vendor managed products/devices are not covered, including RMAs.

## 11. SERVICE DELIVERY MANAGEMENT

The assigned Service Delivery Manager (SDM) manages client satisfaction in the delivery of IT services and ensures program objectives are met. This person provides the client a primary point of contact within Presidio Managed Services and provides operational leadership to the account team and client stakeholders. The SDM also ensures that the team understands the various technology services that Presidio delivers to the client.

The Service Delivery Manager provides management to multiple service delivery projects within the account and assumes responsibility for all aspects of account performance (technical, contractual, and administrative). The following are standard SDM responsibilities:

- Maintain configuration management database, support documentation and any agreed upon special procedures
- Work with other Managed Services departments to maintain and improve customer SLO metrics
- Manage Customer satisfaction
- Meet agreed upon client deliverable schedules and manage expectations
- Manage appropriate internal and external resources to meet deadlines
- Facilitate customer meetings and teleconferences
- Maintain active communication internally and externally
- Deliver Quarterly Business Review (QBR) to the client (can be remote or on-site per client discretion)



## 12. SERVICE TRANSITION MANAGEMENT

Service Transition Management is a phased process in which Presidio implements Managed Services. It includes uploading information into the Monitoring Framework, including the Service Management System and configuration of the DCA. This consists of all steps required to activate and onboard Managed Services.

### 12.1. Kickoff Meeting

Presidio assigns a Project Manager (PM) to act as a single point-of-contact during the Service Transition Management phase. The external Kickoff Meeting indicates the initiation of the kickoff phase and is typically conducted via web or voice conferencing. The Kickoff Phase, as well as all remaining phases within Service Transition Management, is typically facilitated by the PM in collaboration with a Presidio Engineer.

This Service Transition Management phase includes the following activities:

- Coordinating, scheduling, and executing the Kickoff Meeting.
- Reviewing deliverables included in this Managed Service Contract.
- Reviewing services purchased per the signed Statement of Work.
- Aligning Presidio and Client on all major activities, risks, and milestones during Service Transition Management phase.
- Reviewing and scheduling a timeline for completing the Capture Template and covered equipment list (CEL).

### 12.2. Capture Template

Reviewing the Capture Template components and key information is critical to success for Service Transition Management. Contained in the Capture Template is the CEL, which identifies Managed and Monitored CIs. The PM develops a Project Plan for subsequent steps with distribution to project contacts. The required information must be uploaded into the Monitoring Framework. The Client is responsible for providing the information included in the Capture Template, which is provided as part of Service Transition process.

### 12.3. Presidio Monitoring Framework

The DCA is configured to monitor Managed CIs per the CEL included in the contract. During the network discovery process, the PM communicates any discrepancies between identified CIs and requested Managed CIs in the CEL. Additional documentation specifying addressing, ports, and protocols is provided and reviewed with Client during kickoff.

Requested additions beyond the Managed CIs defined in the PO are subject to incremental service fees and additional Service Transition Management intervals. The PM communicates with sales personnel to add any additional items via an Addendum.

Implementing the Monitoring Framework includes the following:

- Preparing, configuring, and testing DCA.
- Shipping DCA to the designated Client premise.
- Remotely assisting Client with DCA installation; on-site installation support is available at client request.

- Establishing SSL over HTTP connectivity between Presidio and the Client premises.
- Configuring Presidio internal systems in preparation for service delivery.

Presidio inputs managed and monitored-only CI information into Monitoring Framework and the Service Management system. Service, support and escalation processes are also configured in the Service Management system during the Transition phase with input and agreement from the Client. This completes the implementation of the Monitoring Framework.

## 12.4. Managed Device Preparation

The Monitoring Service element is dependent upon:

1. Network connectivity to Managed CIs.
2. Configuration of SNMP.
3. Trap Receiver destination IP address.
4. Provision of login and enable passwords.

A required device-specific configuration is supplied to Client, including community strings and host destination addresses.

## 12.5. Setup and Modeling of the Application

Setup and modeling of the application is 100% Presidio's responsibility and includes the installation software components of the Monitoring Framework. Managed device information from the collection stage is loaded, and each individual device is configured for required monitoring statistics/reporting. Presidio and the Client resolve any network connectivity, firewall, or routing issues between CIs and DCA.

## 12.6. Remote Training Session

The PM will schedule remote training sessions as necessary. These sessions are conducted via WebEx provided by Presidio.

The objectives of the training session are reviews of:

- Services to be delivered.
- Service documentation.
- Presidio and Client responsibilities during the service delivery process.
- Processes for obtaining service.
- Service escalation process.
- Client Portal overview.
- Change management process.

## 12.7. Start of Service (SOS)

The SOS milestone begins the Service Term and is contingent on the timely completion of all activities as identified in the Capture Template project schedule. Presidio works with the Client to meet the Start Date milestone and validate that the Service Transition Management phase is complete before Managed Services commences. Notification/Escalation and Event Management does not occur until a detailed operations handover has been performed, all required documentation and procedures are put in place. At the agreed-upon start date, the PM and the Client execute a Certificate of Acceptance, concluding the Service Transition Management phase, and the Service Delivery phase commences.

## 13. CLIENT RESPONSIBILITIES

### 13.1. Install Monitoring Framework

Client shall provide the following with respect to the installation of the DCA:

- Customer to provide two external IP addresses and a shipping address.
- Provide appropriate secure rack-mount location for the DCA with suitable environmental conditions.
- Install the DCA and network connectivity per Presidio-supplied guidelines or allow Presidio to access appropriate location to deploy the DCA.
- Provide communications facilities and services including internet and network configuration. Communication facilities and services must be maintained for the duration of the service term.
- Provide a resource to support the installation of the DCA. These activities include:
  - Installing the DCA in a suitable equipment rack and connecting to network.
  - Power connection to Uninterruptible Power System (UPS) or other facility with continuous uninterrupted power.
  - Power-up.
  - Notification to Presidio that installation is complete.
- Provide suitable commercial power and recommends UPS or other acceptable power back-up facilities providing a minimum of 1kVA dedicated to each appliance.

### 13.2. Training

The Client shall provide training coordination support, including identifying trainees and trainee contact information.

### 13.3. Transition Management

To ensure Presidio's ability to provide services for Managed CIs, Presidio requires the Client to:

- Assign a Project Manager or equivalent to represent the Client during the Service Transition Management phase.
- Assign a Technical Lead or equivalent to assist Presidio with establishing the network access required for Managed Services.
- The Client Project Manager and Technical Lead must attend the Project Kickoff Meeting and training sessions.

### 13.4. Capture Template

Utilizing the required information provided by the client, Presidio will complete the Capture Template, which provides the key information critical to success for the Service Transition Management phase. The Capture Template provides information, such as:

- Detailed CI inventory information.
- Definition of Client-specific support policies including:

- Points of contact and profile data
  - Change management procedures
  - Notification policy
  - Escalation policy
- Manufacturer maintenance and support contract information and contract number (e.g., Cisco SMARTnet).
- Provide as-built documentation including detailed design, network implementation plan(s), site survey(s), and bill of materials (if available).

## 13.5. Service Connectivity and Network Access

The Client is required to provide Read and Write management access to Managed CIs as defined by the Capture Template. Access must be implemented in a timely manner in accordance to the Capture Template. This includes SNMP, syslog, and other defined protocols as necessary to support services.

The Client will maintain manufacturer maintenance and support contracts covering hardware and/or software as may be applicable on all Managed CIs for the duration of the Managed Services contract. Client must provide support contract details, LOA and all other Client documentation and authorization required to facilitate incident resolution.

If the Client elects not to maintain such coverage, Presidio provides reasonable business effort only and may not have access to necessary manufacturer resources, such as support and software updates to facilitate repair.

In cases of special support arrangements; e.g., Client stocking their own spares (self-insuring), Client acquiring manufacturer support on a Time and Materials (T&M) basis, or instances of no manufacturer maintenance and support, the Client must provide a sparing strategy for replacement of devices, and the replacement and recovery of device functionality is the sole responsibility of the Client.

## 13.6. Communication and Change Management

Presidio has a co-management approach to Managed Services, allowing the Client and other Client-approved vendors to retain access to Managed CIs. Because multiple parties can make changes to the environment, Presidio requires anyone with access to the Client's environment to follow a consistent and documented Change Management process. This process is reviewed and agreed-upon prior to completion of the Service Transition Management phase.




The Client will:

- Notify Presidio in advance if scheduled or unscheduled maintenance of Client's Managed and Monitored-Only CIs will impact the:
  - DCA monitoring of Managed CIs.
  - Proper operation or network connectivity of Managed CIs.
- Maintain responsibility for informing Presidio of Client employee status changes.
- Provide and maintain a list of Client employees authorized to request changes.
- Provide and maintain an escalation path within the Client's employee base.



## 14. PRICING & CONTRACT TERM

A Pricing Summary for this contract is provided below. Recurring fees begin on the Start of Service (SOS) date and remain fixed unless an Addendum is approved by the Client and Presidio. Changes in the Covered Equipment List (CEL) result in a change in the recurring pricing. Any net change in the device list results in a prorated change to the cost structure and is reflected in the subsequent invoice. Pricing included in this Agreement is valid for 30 days from the date issued.

Coverage Period				
Term	1 Year	Estimated Coverage Period	Start: 8/1/2021	End: 7/31/2022
Billing Frequency			Amount (\$) per Period	
Monthly			\$84,473.37	
Base Managed Services		Base Monthly Service Fees		
	Collaboration Services	\$19,554.10		
	Data Center Services	\$11,537.80		
	Network Services	\$27,381.47		
	Workplace Services: Project Manager (2080 Hours per Year)	\$26,000.00		
Subtotal		\$84,473.37		
Non-Recurring Fees				
Service Transition Management		(billed upon execution of contract)		\$35,000.00
Bucket of 50 Engineering Hours				\$11,250.00
Subtotal		\$46,250.00		
Total Fees				
Year 1		\$1,059,930.44		
Total Contract		\$1,059,930.44		

A bucket of engineering hours is included in the non-recurring service fee detailed above. This bucket contains 50 hours to be used over the 1-year term at Client's discretion. Additional hours may be purchased once the bucket has been consumed, and unused hours may be rolled over into the first quarter of any renewal period.

**This Statement of Work is in accordance with NASPO Master Agreement Number AR3113 (FL# 43230000-NASPO-16-ACS).**

## 14.1. Statement of Work Term

The term of this Statement of Work (SOW) ("Term") shall commence on the Actual Coverage Period Start of Service date ("Effective Date") and continue in effect until the end of term as noted in the above table. This SOW is non-cancelable. In the event of an early termination of this SOW for breach, Presidio shall be entitled, without limiting its other remedies under this SOW, at law or equity, to recover any remaining unpaid Service Transition and Installation Fees, along with the remaining cost of any hardware, software, licenses, volume-based subscription or subscriptions for agents purchased by Presidio to provide services described within this contract.

The Client may renew services for up to four additional one (1)-year periods, with consistent pricing assuming no increased scope of work, by providing at least 30 days' written notice before the then-current Term expiration date.

In the event the term of this SOW expires without a Client termination or renewal, services and monthly recurring charges outlined within this SOW will continue on a month-to-month basis until a termination or renewal is received from the customer with a 60-day notification period.



## 15. COVERED EQUIPMENT LIST

A complete Covered Equipment List is provided in Attachment 1 to this Statement of Work (starting on page 45).

All end-of-support/end-of-life devices are supported on a best reasonable-effort basis.

## MANAGED SERVICES TERMS AND CONDITIONS

This Statement of Work is governed by the NASPO Master Agreement Number AR3113 (FL# 43230000-NASPO-16-ACS) and the following additional Terms and Conditions specific to Managed Services.

### 1. Client Information

Client Company:	Lee County Board of County Commissioners	POC:	Ashley Mason
Billing Address:	1825 Hendry Street, 3 <sup>rd</sup> FL Fort Myers, FL 33901	POC Phone #:	239-533-7378
		POC E-mail:	masona@leegov.com

### 2. Scope; Coverage Period and Fees

Presidio shall provide the services ("Services") as defined in each attached Statement of Work (each, an "SOW") and the associated Service Appendix, with respect to the software ("Software") and/or related hardware ("Hardware") (collectively, the "Equipment") referenced in the Covered Equipment List ("CEL"), and subject to Presidio's acceptance of such Equipment as eligible for Services coverage pursuant to Section 5 below. The Equipment covered by this Agreement includes only the items on the CEL. The Start of Service ("SOS") date will be specified in the SOW, provided that for service management offerings, including Presidio Support Services ("PSS") for Cisco and other vendors, the SOS begins on the date that Presidio submits a purchase order to its vendor for the underlying support contract. A PSS agreement is independent from other Presidio Managed Services, and does not necessarily co-terminate with other managed services agreements.

### 3. Billing

Immediately upon (or prior to) execution of each SOW, Client shall issue a purchase order to Presidio for the Services requested therein. Presidio will have the right to withhold performance of the Services until such time as a purchase order, issued in conformance with this Agreement, is provided by Client. Presidio will reference the purchase order number on all invoices submitted to Client. Any preprinted terms and conditions on Client's purchase order (or other forms) which are in addition to or in conflict with this Agreement shall be null and void, even if purportedly acknowledged in writing by Presidio. Presidio will bill Client as specified in each SOW. Unless otherwise specified in an SOW, recurring Services will begin billing on the earlier of: (a) forty-five (45) business days from full execution of the SOW, or (b) the SOS, as determined by Presidio and communicated to Client. Service transition management fees, as specified in the SOW, shall be billed upon full execution of this Agreement and the applicable SOW. Client shall be invoiced thirty (30) days in advance of the current Service period. Cisco Partner Shared Support(PSS) offerings will be billed in advance for the duration of that agreement, for all years of the agreement. All invoices issued under this Agreement are due thirty (30) days from the date received by Client. All past due amounts shall bear interest at the rate of one percent (1.0%) per month or, if less, the maximum permissible rate under applicable law. In addition to the charges due for the Services or otherwise hereunder, Client shall pay or reimburse Presidio for any taxes, duties, fees and/or charges resulting from Presidio's performance of this Agreement which are levied by any taxing or other governing authority, except for taxes based upon Presidio's net income. Quotes provided by Presidio are valid for 30 days from the date issued.

### 4. Additional Services and Fees

The parties recognize that from time to time, Client may request maintenance and support or other Presidio services that fall outside the scope of this Agreement. The parties will discuss any requested out-of-scope services and negotiate the terms therefor in good faith. Services specifically considered outside the scope of this Agreement include, without limitation, the following: (a) correction of errors not attributable to Presidio or the manufacturer; (b) electrical work external to the Equipment; (c) installation, de-installation, reinstallation, or relocation; (d) supplies, accessories, or attachments; (e) "no fault found" (problem with equipment not provided by Presidio and/or not covered under this Agreement); and (f) MACD volumes or other managed services in excess of the terms per the Statement of Work and associated appendices. Additionally, material services requiring more than 2 hours will be treated as billable engagements. The threshold for services considered to be "material" is based on the time required for resolution. Client will be notified before billable work is performed, and such work will not begin until authorized by Client.

### 5. Equipment Configuration

Prior to the SOS, the Equipment configuration will be verified by Presidio. If the configuration cannot be verified via remote access, an on-site audit may be performed at Presidio's discretion and as agreed by Client. Client shall bear the reasonable expenses of the on-site audit, which shall be billable at Presidio's standard rates. Should this verification process indicate a change from the original configuration identified by Client, the Services Fees will be modified accordingly. Thereafter the Equipment will be reviewed ninety (90) days prior to the start of each coverage

year to verify its configuration. Should the review indicate a change from the original Agreement configuration, the Services Fees will be modified accordingly. Presidio will advise Client of any condition which would render the Equipment ineligible for the Services hereunder. Client shall be responsible for correcting, at its expense, any such condition prior to or during the term of Presidio Services being provided.

## 6. Client Responsibilities

Subject to reasonable confidentiality/security obligations as accepted by Presidio in writing, Client shall grant Presidio full and free remote and/or physical access to the Equipment at all times during the Term of each SOW, including all required access credentials (e.g. IP addresses, SNMP community strings, passwords, etc.). For monitoring tiers of service, Client shall provide Presidio with at least one publicly-routable IP address for monitoring VPN connectivity and one IP address for the Presidio monitoring collection station. Client will provide all pertinent network diagrams and documentation. Client shall provide and maintain an up-to-date list of authorized contacts and escalation information, including third-party vendor contact information, letters of authority, maintenance schedules and device configurations. Client shall ensure that the Equipment meets, at all times, the manufacturer-approved configuration specifications and is covered by a then-current vendor maintenance and support program. **Client acknowledges and agrees that the foregoing factors are critical for Presidio to perform the Services, and Presidio's performance hereunder or under any SOW may be delayed or suspended if Client does not comply with its obligations in this Section.**

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives.

LEE COUNTY BOARD OF COUNTY COMMISSIONERS

BY: [Signature]

NAME: FRANK MAW

TITLE: BOCC-For Chair

DATE: 6-28-21

PRESIDIO NETWORKED SOLUTIONS LLC

BY: [Signature]

NAME: JACKIE ARNETT

TITLE: DIRECTOR, CONTRACTS ADMINISTRATION

DATE: 5-19-2021

Approved as to Form for the  
Reliance of Lee County Only

By: [Signature]  
Office of the County Attorney

## Letter of Agency

July 1, 2021

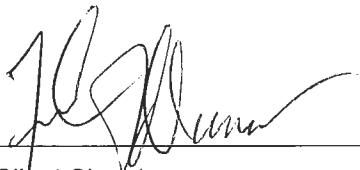
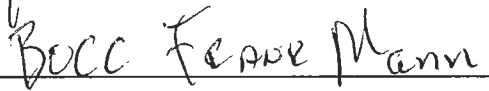
To Whom It May Concern,

Subject: Letter of Agency

The undersigned, Lee County Board of County Commissioners, appoints Presidio Networked Solutions as agent (the "Agent") with respect to the following:

- To access and utilize all features and benefits of active maintenance, support or equipment manufacturer agreements Lee County Board of County Commissioners has purchased from you.
- To perform maintenance on carrier circuits related to the Presidio Managed environment to allow Presidio to restore service or improve performance problems with carriers.
- To dispatch field maintenance technicians to service equipment, if any, under active maintenance, support or equipment manufacturer agreements Lee County Board of County Commissioners has purchased from you.
- Other:

You may deal directly with the Agent on all matters pertaining to the issues set out above and should follow the Agent's instructions with reference thereto. This authorization will remain in effect until further notice.

  
\_\_\_\_\_  
Client Signature  
\_\_\_\_\_  
Client Name/Title (Please Print)  
For Chair



## APPENDIX A: NETWORK SERVICES

The Presidio Network Services Portfolio includes both Network Management and Security Device Management.

### Network Management

Network Management service provides monitoring and management of a Client's network infrastructure. The Service Offering covers and supports Core/Access Switches, Routers, WAN Accelerators, Data Center Networks, and Wireless Access Points and Controllers.

### Security Device Management

The Security Device Management service manages a variety of security devices, including firewalls and Intrusion Prevention and Detections Systems (IPS/IDS).

A key aspect to Security Device Management is administration and monitoring at the device level to ensure availability and functionality. Inclusive in the service is the administration of critical security parameters, including firewall rule set administration, IDS/IPS signature management, and VPN tunnel management.

This service covers and supports Firewalls, Intrusion Prevention Appliances, Access Control Appliances, and Identity Services Engines.

### Network Services Monitoring

The Network Management and Security Device Management Services include standard device-level monitoring.

The following are examples of the standard monitoring elements for the Network and Security Device Management Managed Services.

Operational Status\System Uptime

- CPU Statistics
- Memory Statistics
- Hardware Environmental Status
- Interface Statistics
- SNMP Down

### Standard Reports

The Client Portal allows Standard reports to be viewed online. The Standard Reports include four pre-configured reports, and data is retained for 6 months.

**Client Portal for Network and Security Device Management Services Reports**

Title	Description
Device Availability	Availability is based on uptime. Lists each managed CI, IP address, availability percentage, and actual downtime if applicable
CPU Utilization	Measures the average and the maximum CPU utilization for each CI in the report period. A graphical representation of the top CI is also included.
Interface Bandwidth Utilization	Measures the average and maximum bandwidth utilization by interface on each of the applicable managed CIs. The report ranks each interface. A graphical representation of the top interfaces is also included.
Memory Utilization	Measures the average and maximum memory utilization percentage for each managed CIs during the report period. A graphical representation of the top CIs is also included in the report.

---

**NETWORK AND SECURITY DEVICE MANAGEMENT SERVICES**

---

Title	Description
System Backups	Presidio shall perform back-up processes for Cisco routers, switches, and other supported Command Line Interface (CLI) based CIs. This includes definition and execution of service restoration process for Managed CIs. The configuration back-ups are stored on the Presidio Monitoring Framework and available for use by Presidio in bringing current or replacement Managed CI to service. Device-based backups are not performed for Monitored-Only or Vendor Managed devices.
Moves, Adds, Changes, and Deletions (MACDs)	<p>With the Select Service level, Presidio offers device-level changes. The MACD section within this Statement of work defines the scope of these changes, along with any associated volume limitations.</p> <p>The following are <b>examples</b> of typical device-level changes:</p> <ul style="list-style-type: none"><li>• Router interface changes</li><li>• Firewall ACL modifications</li><li>• Switch port configurations</li><li>• Wireless access-point definition</li></ul>



## APPENDIX B: UNIFIED COMMUNICATION MANAGEMENT - CISCO

The Presidio Unified Communications Management (UCM) delivers support for a full range of collaboration services for Cisco unified collaboration, video, and third-party devices and applications. As a key offering within Presidio's Collaboration Services Portfolio, UCM enables organizations to accelerate the adoption of advanced collaboration technologies by providing Managed Services through a team of highly certified engineers combined with state-of-the-art IT Service Management facilities.

### UCM Monitoring

UCM includes standard device-level monitoring as well as advanced collaboration-specific monitoring.

#### UCM – Cisco-Specific Monitoring

UCM provides advanced monitoring of the Cisco UC solution. The table below lists examples of the elements in our current toolset can monitor. If a configured threshold for a CI is reached, the alert generates an incident for our SDC to resolve. Please note, as the Presidio Monitoring Framework evolves, this list may change.

Monitored Toolset Element	
Title	Description
Device Statistics	Gateways – Status, Reachability, Busy Call Attempts Phones – registered phone discrepancy Dial Plan – Route Group, Route List, Route Pattern, Trunk Status
Cisco Server Hardware	Disk, Fan, Power Supply, Temperature, Voltage Communications Manager Parameters Location Statistics – Bandwidth Utilization Media Resources – Hardware conferences, Media Termination Point (MTP), Music on Hold (MoH), Software Conferences, Transcoders, Video conferencing resources (/DSP based)
Communications Manager Server Alerts	Cisco Unified Call Manager (CUCM) Service Cisco Call Manager (CCM)Process CCM Agent Process Computer Telephony Integration (CTI) Manager Database Call Manager Down Server Node Communication Backup Service Failure Syslog Failures SNMP Failures Processes CPU Utilization Disk Partition Utilization SQL/Database
Unity Alerts	Critical Events Failover Service Failure Unity Port Max Unity Ports Not Registered
CCM Cluster Alerts	CDR/CMR Database Gateway registration
TFTP Alerts	TFTP Port/Network TFTP Service Failure

## Standard Reports

Our UCM Service includes a device-level reporting interface on our Presidio Client Portal that allows Standard reports to be viewed by the client. Standard Reports include four pre-configured reports and data are retained for 6 months. In addition to the Client Portal reports, the following **Collaboration Reports** are provided:

Title	Description
Trunk Availability	Availability is based on connectivity from the PBX, registration status within the PBX and the member channel status. Not all factors are available for all trunks.
Trunk Utilization	Utilization is expressed in terms of the number of channels occupied. It is calculated by dividing the total duration of all processed calls across the IP or PSTN trunk(s) by the sampling period.
Trunk Summary	Overall trunk availability Impacted trunks Trunk down time Trunk outages Trunk degraded time Trunk busy hour Trunk busy hour by percentage Trunk call types
Call Failure Report	<b>Calls attempted</b> - A call attempt is a request from a phone/device to a PBX to initiate a call, whether that call is successful or not. Calls attempted = Calls completed + Calls rejected + other failures. <b>Calls completed</b> - A call completed is a call successfully processed by a PBX and terminated with a disconnect cause code that indicates graceful termination. <b>Calls rejected</b> - A rejected call is either a call attempt that is received but not processed by a PBX due to throttling when the PBX is under high load, or a call that failed due to resource limitations. <b>Call failures</b> - A failed call is a call attempt that is processed by a PBX but the call terminated abnormally with a disconnect cause code indicating that the call failed. <b>Call failure ratio</b> - The call failure ratio is the percentage of processed calls that failed. <b>Calls processed</b> - A processed call is a call attempt that is processed by a PBX regardless whether the call completed successfully or not. <b>Disconnect cause code</b> - The disconnect cause code indicates why a call terminated abnormally. It may be attributed to either the origination or destination device. <b>Report data</b> - Calls with an origination time within the reporting period.
Long Duration Calls Report	Lists calls with duration exceeding the long duration threshold. This list of calls may help to identify device malfunctions, configuration errors or abuses of the system. Calls with a disconnection time within the reporting period are included in this report. Disconnection time is chosen to ensure these long calls will be captured in the report, as CDRs are only generated at the end of a call.
Node Utilization Report	High CPU Utilization Node CPU Utilization Call Load Balance Phone Load Balance Call Load Report Busy hour statistics Busy hour call attempts Busy hour grade of service Calls attempted Calls rejected Node call load Phone Report Phones configured and registered Call types Call statistics Phone utilization Phones inactive

Route Pattern Availability	<p>Availability is derived from availability of trunk members belonging to the route pattern. Trunk availability is based on connectivity from the PBX, registration status within the PBX and the member channel status. Not all factors are available for all route patterns.</p> <p>Overall route pattern availability</p> <p>Route pattern availability</p> <p>Impacted route patterns</p> <p>Route pattern down time</p> <p>Route pattern outages</p> <p>Route pattern degraded time</p>
----------------------------	---

## UCM Service Management

In addition to the details in the main Contract, the following information specifically applies to the UCM.

### System Backups

Presidio performs back-up processes for Cisco ASR and ISR-based voice gateways, VG-series analog gateways, and other IOS-based voice CIs. This includes definition and execution of service restoration process for Managed CIs. The configuration back-ups are stored on the Monitoring Framework and available for use by Presidio in bringing current or replacement Managed CI's to service. Device-based backups are not performed for Monitored-Only CI's.

Presidio provides best practice recommendations to the Client in support of their Unified Communications applications backups. The Client is responsible for the configuration and storage of the backup jobs. Presidio monitors the backup services utilizing Cisco RTMT and will alert/troubleshoot service failures and related incidents.

### Responsibility Matrix (RACI): R = Responsible A = Accountable C = Consulted I = Informed

Device	Task	MS	PS	Client
CME	Add DN to existing hunt group	R,A		C,I
CUCM	Major Version Upgrade		R,A	C,I
CUCM	Minor Version (SU) upgrade	R,A		C,I
CUCM	Device Pack Installation	R,A		C,I
CUCM	New Circuit Turnup (Requiring configuration)		R,A	C,I
UCCX	Assign skill to agent	R,A		C,I
UCCX	Add agent to team	R,A		C,I
UCCX	Create/modify/delete agents	R,A		C,I

## APPENDIX C: DATA CENTER SERVICES (ESSENTIAL)

### Systems and Virtualization Management

Presidio Systems and Virtualization Management offering provides comprehensive Managed Services for operating your compute and virtualization infrastructures. This includes the storage systems, compute hardware, and hypervisor.

### Storage Management

Presidio Storage Management provides Managed Services for all storage infrastructure needs across back-up, replication, recovery, de-duplication, and cloud storage needs. Presidio's team of Managed Services professionals work with Clients to ensure the proper storage tier is used to maximize cost efficiency while ensuring storage performance – all governed by predictable service levels.

### Data Center Monitoring

The specific Monitoring Services related to our Data Center Managed Services monitors and alerts on many parameters throughout the Data Center Device Portfolio. When a threshold or alert is triggered, an incident is generated, and our Service Delivery Center team responds.

**Data Center Monitoring Conditions**

Condition	Status
SAN (EMC/NetApp)	<ul style="list-style-type: none"> <li>• Hardware status</li> <li>• LUN Status</li> <li>• Disk state</li> </ul>
Server Hardware (Cisco UCS)	<ul style="list-style-type: none"> <li>• Chassis alerts</li> <li>• Blade alerts</li> <li>• IO Module alerts</li> <li>• Fabric Status</li> </ul>
Virtual Machines (VMWare)	<ul style="list-style-type: none"> <li>• CPU Statistics</li> <li>• Memory Usage</li> <li>• Snapshots</li> </ul>

Please note, as our Presidio Monitoring Framework evolves, this list may change.

### Reports

The Client Portal allows Standard reports to be viewed. Reports include four pre-configured reports and data is retained for 6 months.

**Standard Reports**

Report	Description
Device Availability	Availability is based on uptime. Lists each managed device, IP address, availability percentage, and actual downtime if applicable.
CPU Utilization	Measures the average and the maximum CPU utilization for each device in the report period. A graphical representation of the top devices is also included.
Memory Utilization	Measures the average and maximum memory utilization percentage for each managed device during the report period. A graphical representation of the top devices is also included in the report.

### Data Center Service Management

In addition to the main Contract details, the following information specifically applies to the Data Center Service.

## **System Backups**

Presidio shall perform back-up processes for Cisco routers, switches, and other supported Command Line Interface (CLI) based CIs. This includes definition and execution of service restoration process for Managed CIs. The configuration back-ups will be stored on the Presidio Monitoring Framework and available for use by Presidio in bringing current or replacement Managed CI to service. Device-based backups are not performed for Monitored-Only or Vendor Managed devices. The client is responsible for backup of all systems that are not running an IOS operating system.

## **Standard Services**

### **Typical Support Operations Performed- Data Center Managed Services**

Tasks	
Troubleshoot Ethernet profile issues	Troubleshoot FC performance
Troubleshoot Port Blocking Issues	Troubleshoot host presentation issues
Troubleshoot SVS connection	Troubleshoot vSan/FCOE issues
Troubleshoot Ethernet port profile issues	Troubleshoot Zone
Replace faulted drive	Troubleshoot Zone set
Troubleshoot hardware issues	Troubleshoot Ethernet profile issues
Troubleshoot blade discovery issues	Troubleshoot Port Blocking Issues
Troubleshoot chassis discovery issues	Troubleshoot SVS connection
Troubleshoot CIMC Issues	Troubleshoot Ethernet port profile issues
Troubleshoot Fabric Interconnect (FI)	Troubleshoot data mover export
Troubleshoot FCOE issues	Troubleshoot failover for appliance
Troubleshoot IO Module (IOM) Issues	Troubleshoot failover for VSB
Troubleshoot Service Profile Issues	Troubleshooting replication of Datadomain node
Troubleshoot upstream connectivity	Troubleshoot performance Ethernet
Troubleshoot VHBA issues	Troubleshoot performance R/W
Troubleshoot VM-FEX	Troubleshoot Snap View issues
Troubleshoot VNIC issues	Troubleshoot trespass issues
Troubleshooting replication of Avamar node	Troubleshoot data mover RBAC permissions
Troubleshoot backup performance issues	Troubleshoot LUN presentations
Troubleshooting failed backup of virtual machine	Troubleshoot Mirror View issues
Troubleshooting node/backup consistency	Troubleshoot performance issues
Troubleshoot storage contention /IOPS performance issues	Troubleshoot Auto support
Troubleshoot storage over-commitment issues	Troubleshoot filer failover
Troubleshoot VM Memory swapping/performance issues	Troubleshoot non-optimal access
Troubleshoot VM Network performance issues	Troubleshoot performance issues
Troubleshoot vMotion/Storage vMotion migration issues	Troubleshoot Snapshot Issues
Troubleshoot ESX PSODs	Troubleshoot CPU Ready issues

Presidio Storage Management does not include altering datasets, managing asset IDs, analyzing security vulnerabilities, nor making design recommendations to storage environment upgrades. Presidio assists in these areas through Professional Services engagements.



---

## GENERAL DEFINITIONS

**Advanced Logic Profile:** Set of patented elements performing processing on millions of simultaneous, complex systems and network management flows to determine the precise root cause of an incident.

**Auto-Generated Incident:** Ticket opened in the Incident Management System as a result of the monitoring tools. It differs from manual cases, which are manually opened by a system user through the Client Portal, email or via phone.

**Business Hours:** Normal business hours for a company operating in the United States based upon local office time, i.e., traditionally 8 a.m. to 5 p.m. Monday through Friday.

**Business Reviews:** Regularly scheduled meeting led by the Service Delivery Manager to provide metrics on Client performance during the previous period. The data presented is also used to obtain the Clients' insight into areas of Service Delivery improvements. Depending on contact specifics, this is typically a Quarterly Business Review (QBR).

**Capture Template:** Document completed by the Client during the Service Transition Management phase. Document contains information about the managed equipment covered in this agreement and includes but is not limited to make, model, serial number, access credentials and IP addresses.

**Carrier:** Provider of voice and data transport services.

**Change Advisory Board (CAB):** Group or committee of stakeholders responsible to analyze and review submitted change requests and take action to accept or reject the change.

**Change Management:** Presidio process to receive, authorize, execute, and communicate changes to managed components.

**Change Request:** Client request for service, as related to Agreement, made by electronic format.

**Client Notification:** Communication to inform the Client that an Incident has been recorded.

**Client Portal:** Online Web user interface supplied for Client to receive and submit information to and from the Presidio Service Desk.

**Client Premise(s):** Physical Client location(s) where the DCA resides.

**Configuration Item (CI):** Component that needs to be managed to deliver an IT service.

**Contract:** Statement of Work (SOW).

**DCA:** Monitoring and management solution used in the delivery of Managed Services. It consists of one or more appliances containing system and application software.

**Elements:** Basic network service when unbundled and an enhanced service when bundled into a service tier.

**Incident:** Event not part of the standard operation of a service and causes or may cause an interruption to, or reduction in, the quality of that service.

**Incident Management:** Process to detect an incident, notify the Client about the incident, and resolve the incident.



**Incident Resolution:** Process to restore services on managed components.

**Known Error:** Incident with a defined root cause and resolution.

**Letter of Agency (LOA):** Formal document that authorizes Presidio to act as the Client's agent for purposes of facilitating, tracking and/or providing services with carriers, maintenance contract providers, and other general-service providers.

**Management Hub:** Core of the Monitoring Framework system; provides an aggregation point for data compiled from multiple probes and integrates with tools data base and Client Portal.

**Management Services:** Service that provides Monitoring, Incident Resolution, Reactive Problem Management, Service Level management and Standard Changes to resolve all Incidents.

**Manual Cases:** Cases that a system user manually opens on the Client Portal or via phone.

**Manufacturer Field Notice:** Electronic notification from the manufacturer about product-related issues.

**Manufacturer Maintenance and Support Contract:** Contractual agreement between Client and Managed Components manufacturer that grants access to manufacturer-provided services, such as Managed Element hardware replacement, software patches, and technical support, necessary to maintain good working order.

**Message Bus:** Connects data collected from Probes with the Management Hub.

**Monitoring:** Detecting events on Managed CIs or Monitored-Only CIs.

**Monitoring Framework:** Presidio's integrated technology and tools required for delivering monitoring and managed services.

**Monitored-Only CI:** CI monitored by Monitoring Framework but not fully managed by Presidio Managed Services.

**Patch:** Small fix to a problem using a piece of software code.

**Problem:** Underlying cause of one or more Incidents.

**Problem Analysis:** Investigating problems to determine root cause.

**Problem Management:** Process to find and resolve the root cause of a Problem and prevention of Incidents.

**Service Addendum:** Bilaterally agreed to document modifying scope of agreement.

**Service Delivery Center Supervisor:** Role within the Presidio Service Desk with management responsibilities for Client issues, escalations and staff.

**Service Delivery:** Phase after Transition Management when Presidio begins to deliver Managed Services.

**Service Delivery Center (SDC):** Network Operations Center (NOC) is the primary facilities where Presidio technicians and engineers remotely support Clients.

**SLO:** Service Level Objective.

**Service Management System:** Presidio Incident Management Platform where Client CI information and Incident Management information is maintained.

**Vendor Management:** Presidio provides monitoring only (if monitoring framework is deployed), first-level support (triage only), alert and notification of monitored faults, and coordination of the supporting vendor/support teams on the Client's behalf throughout the troubleshooting process. Presidio does not provide second- and third-level troubleshooting and support for these devices. This support can only be provided on equipment with an existing manufacturer's warranty or current maintenance support contract.

# PRESIDIO

## ATTACHMENT 1: COVERED EQUIPMENT LIST

The following devices are covered under the scope of this proposal.

NASPO Part Title	Model Number	IP Address	Hostname	N F
NETWORK SERVICES				
Access Point - Lightweight	AIR-AP2802L-B-K9	10.1.101.132	BNLIBRY-2M-AP-01	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.1.101.139	BNLIBRY-1M-AP-06	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.1.101.162	BNLIBRY-2M-AP-10	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.1.101.163	BNLIBRY-1M-AP-04	
Access Point - Lightweight	AIR-AP1562D-B-K9	10.1.101.171	BNLIBRY-1M-AP-EXT	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.1.101.176	BNLIBRY-1M-AP-03	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.1.101.177	BNLIBRY-1M-AP-02	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.1.101.178	BNLIBRY-1M-AP-01	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.1.101.180	BNLIBRY-2M-AP-09	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.1.101.183	BNLIBRY-2M-AP-08	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.1.101.184	BNLIBRY-2M-AP-03	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.1.101.185	BNLIBRY-1M-AP-05	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.1.101.186	BNLIBRY-2M-AP-04	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.9.2.211	LHSRCTR-1M-AP-03	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.9.2.212	LHSRCTR-1M-AP-02	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.9.2.213	LHSRCTR-1M-AP-01	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.9.13.166	NFLIBRY-1M-AP-10	
Access Point - Lightweight	AIR-AP1562D-B-K9	10.9.13.175	NFLIBRY-1M-AP-EXT	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.9.13.176	NFLIBRY-1M-AP-09	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.9.13.177	NFLIBRY-1M-AP-12	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.9.13.178	NFLIBRY-1M-AP-11	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.9.13.179	NFLIBRY-1M-AP-04	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.9.13.180	NFLIBRY-1M-AP-03	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.9.13.184	NFLIBRY-1M-AP-02	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.9.13.185	NFLIBRY-1M-AP-01	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.9.13.186	NFLIBRY-1M-AP-05	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.9.13.187	NFLIBRY-1M-AP-08	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.9.13.188	NFLIBRY-1M-AP-07	
Access Point - Lightweight	AIR-AP2802L-B-K9	10.9.13.193	NFLIBRY-1M-AP-06	
Access Point - Lightweight	AIR-CAP2602L-A-K9	10.1.1.0.81	REDSOXX-CB-AP-01	

# PRESIDIO

Access Point - Lightweight	AIR-AP2802I-B-K9	10.11.11.133	HEAVYEQ-1M-AP-01	
Access Point - Lightweight	AIR-CAP2602E-A-K9	10.11.11.223	FLEET-PTS-AP-TEMP	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.16.109	NFMRECR-1M-AP-11	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.16.110	NFMRECR-ID-AP-27	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.16.111	NFMRECR-1M-AP-07	
Access Point - Lightweight	AIR-CAP2602E-A-K9	10.11.16.112	NFMRECR-1M-AP-13	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.16.114	NFMRECR-ID-AP-29	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.16.115	NFMRECR-ID-AP-35	
Access Point - Lightweight	AIR-CAP2602E-A-K9	10.11.16.116	NFMRECR-1M-AP-19	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.16.117	NFMRECR-ID-AP-31	
Access Point - Lightweight	AIR-CAP2602E-A-K9	10.11.16.118	NFMRECR-1M-AP-15	
Access Point - Lightweight	AIR-CAP2602E-A-K9	10.11.16.119	NFMRECR-1M-AP-17	
Access Point - Lightweight	AIR-CAP2602E-A-K9	10.11.16.120	NFMRECR-1M-AP-09	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.16.121	NFMRECR-1M-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.16.122	NFMRECR-ID-AP-33	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.16.123	NFMRECR-1M-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.16.125	NFMRECR-ID-AP-37	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.16.126	NFMRECR-1M-AP-05	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.22.199	LEETRIM-1M-AP-01	
Access Point - Lightweight	AIR-CAP2602E-A-K9	10.11.22.200	LEETRIM-1M-AP-02	
Access Point - Lightweight	AIR-CAP3502E-A-K9	10.11.22.216	LEETREM-1M-AP-02	
Access Point - Lightweight	AIR-CAP3502E-A-K9	10.11.22.217	LEETREM-1M-AP-03	
Access Point - Lightweight	AIR-CAP2702E-B-K9	10.11.22.228	LEETRCA-1M-AP-02	
Access Point - Lightweight	AIR-CAP2702E-B-K9	10.11.22.229	LEETRCA-1M-AP-01	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.11.22.242	LEETRFMB-1M-AP-02	
Access Point - Lightweight	AIR-AP2802E-B-K9	10.11.22.243	LEETRFMB-1M-AP-01	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.11.32.74	Hough-1M-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.32.79	RECCNTR-1M-AP-07	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.32.80	RECCNTR-1M-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.32.81	RECCNTR-1M-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.32.82	RECCNTR-1M-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.32.83	RECCNTR-1M-AP-06	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.11.32.84	RECCNTR-1M-AP-05	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.11.32.86	RECCNTR-1M-AP-04	
Access Point - Lightweight	AIR-AP3802I-B-K9	10.11.64.164	EMS6MPK-MD-AP-06	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.15.126.187	HUMANSV-1M-AP-05	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.15.126.188	HUMANSV-1M-AP-01	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.15.126.189	HUMANSV-1M-AP-04	



# PRESIDIO

Access Point - Lightweight	AIR-AP2802I-B-K9	10.15.126.190	HUMANSV-1M-AP-02	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.15.126.191	HUMANSV-1M-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.135	FMREGLB-2M-AP-08	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.18.60.144	FMREGLB-B2-AP-06	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.146	FMREGLB-2M-AP-04	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.148	FMREGLB-B2-AP-02	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.18.60.150	FMREGLB-B2-AP-05	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.151	FMREGLB-1M-AP-03	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.18.60.154	FMREGLB-B2-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.156	FMREGLB-B2-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.157	FMREGLB-2M-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.160	FMREGLB-1M-AP-08	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.166	FMREGLB-2M-AP-11	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.167	FMREGLB-2M-AP-06	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.171	FMREGLB-1M-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.172	FMREGLB-1M-AP-04	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.173	FMREGLB-2M-AP-09	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.174	FMREGLB-2M-AP-05	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.178	FMREGLB-2M-AP-03	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.18.60.180	FMREGLB-2M-AP-14	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.181	FMREGLB-2M-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.184	FMREGLB-1M-AP-05	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.186	FMREGLB-2M-AP-07	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.189	FMREGLB-1M-AP-07	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.190	FMREGLB-1M-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.191	FMREGLB-2M-AP-12	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.60.192	FMREGLB-2M-AP-10	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.18.64.151	LEETRHO-2D-AP-dae0	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.64.190	LEETRHO-4D-AP-00	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.18.64.210	LEETRHO-1M-AP-1900	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.18.64.218	LEETRHO-2D-AP-53a0	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.18.64.219	LEETRHO-1D-AP-e740	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.18.64.225	LEETRHO-1M-AP-0260	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.18.64.236	LEETRHO-1D-AP-0b60	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.18.64.239	LEETRHO-2D-AP-f180	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.18.64.240	LEETRHO-1M-AP-06a0	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.18.64.244	LEETRHO-1M-AP-cec0	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.68.74	LEETR-HQ-2	



# PRESIDIO

Access Point - Lightweight	AIR-CAP1552E-A-K9	10.18.68.114	LEETRHHQ-4D-AP-9020	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.68.183	LEETR-HQ	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.7	LEETRHHQ-2D-AP-05	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.8	LEETRHHQ-1D-AP-05	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.9	LEETRHHQ-1D-AP-07	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.10	LEETR-HQ-1M-AP	
Access Point - Lightweight	AIR-CAP3602I-A-K9	10.18.74.11	LEETRHHQ-1D-AP-17	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.12	LEETRHHQ-1D-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.13	LEETRHHQ-1D-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.14	LEETRHHQ-1D-AP-19	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.15	LEETRHHQ-1D-AP-13	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.16	LEETRHHQ-1D-AP-09	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.17	LEETRHHQ-1D-AP-11	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.18	LEETRHHQ-1M-AP-05	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.19	LEETRHHQ-1M-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.20	LEETRHHQ-1M-AP-07	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.21	LEETRHHQ-1M-AP-11	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.22	LEETRHHQ-1M-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.23	LEETRHHQ-1M-AP-09	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.24	LEETRHHQ-2D-AP-07	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.25	LEETRHHQ-2D-AP-04	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.26	LEETRHHQ-2D-AP-08	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.27	LEETRHHQ-2D-AP-06	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.29	LEETRHHQ-2D-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.30	LEETRHHQ-2D-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.31	LEETRHHQ-2D-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.32	LEETRHHQ-3D-AP-07	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.33	LEETRHHQ-3D-AP-06	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.34	LEETRHHQ-2D-AP-09	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.18.74.35	LEETRHHQ-2D-AP-BR	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.36	LEETRHHQ-3D-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.37	LEETRHHQ-3D-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.38	LEETRHHQ-3D-AP-04	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.39	LEETRHHQ-3D-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.18.74.40	LEETRHHQ-3D-AP-05	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.19.3.144	HAMSTAD-MB-AP-01	
Access Point - Lightweight	AIR-CAP3502E-A-K9	10.28.1.84	TERRYPK-AN-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.28.1.85	TERRYPK-ST-AP-01	

# PRESIDIO

Access Point - Lightweight	AIR-CAP3502I-A-K9	10.28.1.86	TERRYPK-MB-AP-01	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.28.1.87	TERRYPK-AN-AP-01	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.28.18.134	EOC2MDF-R2C5-AP-18	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.28.18.135	EOC2MDF-R2C5-AP-05-SR	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.28.18.139	EOC2MDF-R2C5-AP-16	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.28.18.152	EOC2MDF-R2C5-AP-15	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.28.18.157	EOC2MDF-R2C5-AP-02-SR	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.28.18.171	EOC2MDF-R2C5-AP-04-SR	
Access Point - Lightweight	AIR-CAP1552E-A-K9	10.28.18.172	EOC2MDF-R2C5-AP-20	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.28.18.181	EOC2MDF-R2C5-AP-03-SR	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.28.18.186	EOC2MDF-R2C5-AP-01-SR	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.28.57.229	EOC2MDF-R2C5-AP--SR	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.28.59.218	EOC2MDF-R2C5-AP-01	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.28.63.83	EOC2MDF-R2C5-AP-09	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.28.63.143	EOC2MDF-R2C5-AP-03	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.28.63.144	EOC2MDF-R2C5-AP-10	
Access Point - Lightweight	AIR-AP3802I-B-K9	10.29.1.86	CON2020-1M-AP-01	
Access Point - Lightweight	AIR-AP3802I-B-K9	10.29.1.89	CON2020-1M-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.58.3.2	MARSXXX-MB-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.58.3.3	MARSXXX-HW-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.58.3.4	MARSXXX-CS-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.58.3.5	MARSXXX-CS-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.58.3.6	MARSXXX-MB-AP-01	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.69.42.27	DETARXX-1M-AP-02	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.92.33.35	CPUTILS-BS-AP-02	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.92.33.36	CPUTILS-BS-AP-03	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.92.33.37	CPUTILS-BS-AP-01	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.92.33.46	CPUTILS-MB-AP-01	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.92.33.47	CPUTILS-MB-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.92.33.69	ENVLABS-1M-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.92.33.72	ENVLABS-1M-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.92.33.220	VETPARK-1M-AP-04	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.92.33.222	VETPARK-1M-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.92.33.223	VETPARK-1M-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.92.33.224	VETPARK-1M-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.95.1.221	GUARDAL-3M-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.95.1.222	GUARDAL-3M-AP-02	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.96.5.125	PLAYERS-1M-AP-01-EXT	

# PRESIDIO

Access Point - Lightweight	AIR-CAP2602I-A-K9	10.96.6.221	MEDSTAR-1M-AP-02	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.96.8.131	CPALMSP-1M-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.96.13.126	ENVLABS-1M-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.96.14.79	FLEETMG-1M-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.96.14.88	FLEETMG-1M-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.96.24.45	NATRESC-1M-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.96.24.64	NATRESC-1M-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.96.28.56	BOCAGRN-CC-AP-06	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.96.28.77	BOCAGRN-CC-AP-02	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.96.28.78	BOCAGRN-CC-AP-04	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.96.28.118	BOCAGRN-CC-AP-03	
Access Point - Lightweight	AIR-CAP3502E-A-K9	10.96.28.122	BOCAGRN-CC-AP-01	
Access Point - Lightweight	AIR-AP3802I-B-K9	10.96.34.66	SOLIDWS-SH2-AP-02	
Access Point - Lightweight	AIR-AP3802I-B-K9	10.96.34.67	SOLIDWS-RP-AP-01	
Access Point - Lightweight	AIR-AP3802I-B-K9	10.96.34.68	SOLIDWS-RP-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.96.34.169	SOLIDWS-VM-AP-01	
Access Point - Lightweight	AIR-AP3802I-B-K9	10.96.34.172	SOLIDWS-SH1-AP-01	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.96.34.191	SOLIDWS-VM-AP-02	
Access Point - Lightweight	AIR-AP3802I-B-K9	10.96.34.235	SOLIDWS-TS-AP-02	
Access Point - Lightweight	AIR-AP3802I-B-K9	10.96.34.244	SOLIDWS-IN-AP-03	
Access Point - Lightweight	AIR-AP3802I-B-K9	10.96.34.246	SOLIDWS-TS-AP-01	
Access Point - Lightweight	AIR-AP3802I-B-K9	10.96.34.249	SOLIDWS-IN-AP-01	
Access Point - Lightweight	AIR-AP3802I-B-K9	10.96.34.251	SOLIDWS-IN-AP-02	
Access Point - Lightweight	AIR-CAP2602I-B-K9	10.100.129.213	ANMLSVC-1M-AP-06	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.100.129.214	ANMLSVC-1M-AP-04	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.100.129.215	ANMLSVC-1M-AP-12	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.100.129.216	EMS6MPK-MD-AP-05	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.100.129.217	ANMLSVC-1M-AP-03	
Access Point - Lightweight	AIR-CAP2602E-A-K9	10.100.129.218	ANMLSVC-1M-AP-10	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.100.129.219	ANMLSVC-1M-AP-07	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.100.129.220	ANMLSVC-1M-AP-05	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.100.129.221	ANMLSVC-1M-AP-01	
Access Point - Lightweight	AIR-CAP2602E-A-K9	10.100.129.222	ANMLSVC-1M-AP-08	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.100.129.223	ANMLSVC-1M-AP-02	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.100.130.184	DOTENG-1M-AP-01	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.100.130.185	DOTENG-1M-AP-02	
Access Point - Lightweight	AIR-CAP2602E-A-K9	10.100.130.186	DOTENG-1M-AP-10	
Access Point - Lightweight	AIR-CAP2602E-A-K9	10.100.130.187	DOTENG-1M-AP-09	



# PRESIDIO

Access Point - Lightweight	AIR-AP2602I-B-K9	10.100.130.188	DOTOPS-TR-1M-AP-01	
Access Point - Lightweight	AIR-CAP2602E-A-K9	10.100.130.189	DOTTRWH-1M-AP-01	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.100.130.190	DOTTRAF-1M-AP-02	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.100.130.191	DOTTRAF-1M-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.3.35	NWREGLB-1M-AP-04	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.3.36	NWREGLB-1M-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.3.37	NWREGLB-1M-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.3.38	NWREGLB-1M-AP-05	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.3.39	NWREGLB-1M-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.3.40	NWREGLB-1M-AP-06	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.4.98	ESTROPK-1M-AP-05	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.4.100	ESTROPK-1M-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.4.105	ESTROPK-1M-AP-04	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.4.108	ESTROPK-1M-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.4.109	ESTROPK-1M-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.12.98	FLEETEMS-WH-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.12.99	FLEETMG-1M-AP-02	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.102.16.136	MEDSTAR-1M-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.17.56	PUBWRKS-4N-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.17.58	PUBWRKS-4N-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.17.59	PUBWRKS-4N-AP-03	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.102.17.67	PUBWRKS-1M-SW-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.17.69	PUBWRKS-4S-AP-02	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.102.17.70	PUBWRKS-3S-AP-02	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.102.17.73	PUBWRKS-3S-AP-05	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.102.17.74	PUBWRKS-3S-AP-03	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.102.17.75	PUBWRKS-3S-AP-01	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.102.17.76	PUBWRKS-3S-AP-04	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.102.17.78	PUBWRKS-3N-AP-03	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.102.17.79	PUBWRKS-3N-AP-01	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.102.17.80	PUBWRKS-3N-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.17.81	PUBWRKS-2N-AP-07	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.17.82	PUBWRKS-2S-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.17.83	PUBWRKS-2S-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.17.84	PUBWRKS-2N-AP-06	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.17.85	PUBWRKS-2S-AP-05	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.17.86	PUBWRKS-2S-AP-04	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.102.17.87	PUBWRKS-2S-AP-03	

# PRESIDIO

Access Point - Lightweight	AIR-CAP35021-A-K9	10.102.17.88	PUBWRKS-1N-AP-01	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.102.17.89	PUBWRKS-1N-AP-02	
Access Point - Lightweight	AIR-CAP36021-A-K9	10.102.17.90	PUBWRKS-1M-AP-05	
Access Point - Lightweight	AIR-CAP26021-A-K9	10.102.17.91	PUBWRKS-1S-AP-01	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.102.17.112	PUBWRKS-4S-AP-03	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.102.17.126	PUBWRKS-4M-AP-01	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.102.48.5	MEDEXAM-1M-AP-01	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.102.48.9	MEDEXAM-1M-AP-03	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.102.48.13	MEDEXAM-1M-AP-07	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.102.48.14	MEDEXAM-1M-AP-05	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.102.48.15	MEDEXAM-1M-AP-02	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.102.48.17	MEDEXAM-1M-AP-06	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.102.48.19	MEDEXAM-1M-AP-04	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.102.49.13	CPALMSP-3M-AP-02	
Access Point - Lightweight	AIR-AP38021-B-K9	10.102.255.57	WAKEHCH-1M-AP-05	
Access Point - Lightweight	AIR-CAP26021-A-K9	10.102.255.58	WAKEHCH-1M-AP-02	
Access Point - Lightweight	AIR-CAP26021-A-K9	10.102.255.59	WAKEHCH-1M-AP-03	
Access Point - Lightweight	AIR-CAP26021-A-K9	10.102.255.60	WAKEHCH-1M-AP-04	
Access Point - Lightweight	AIR-AP1562D-B-K9	10.102.255.61	WAKEHCH-1M-AP-07	
Access Point - Lightweight	AIR-CAP26021-A-K9	10.102.255.62	WAKEHCH-1M-AP-01	
Access Point - Lightweight	AIR-AP28021-B-K9	10.128.5.10	SOLIDWSTPZ-B2-AP-01	
Access Point - Lightweight	AIR-AP28021-B-K9	10.128.5.11	SOLIDWSTPZ-1M-AP-03	
Access Point - Lightweight	AIR-AP28021-B-K9	10.128.5.12	SOLIDWSTPZ-1M-AP-02	
Access Point - Lightweight	AIR-AP28021-B-K9	10.128.5.13	SOLIDWSTPZ-1M-AP-01	
Access Point - Lightweight	AIR-AP28021-B-K9	10.128.5.14	SOLIDWSTPZ-B2-AP-02	
Access Point - Lightweight	AIR-AP38021-B-K9	10.163.2.98	JCANNEX-1M-AP-02	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.164.9.53	ADMEAST-6M-AP-01	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.164.9.54	ADMEAST-6M-AP-05	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.164.9.55	ADMEAST-6M-AP-03	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.164.9.56	ADMEAST-6M-AP-06	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.164.9.57	ADMEAST-6M-AP-07	
Access Point - Lightweight	AIR-CAP35021-A-K9	10.164.9.58	ADMEAST-5M-AP-03	
Access Point - Lightweight	AIR-AP28021-B-K9	10.164.9.59	ADMEAST-5M-AP-04	
Access Point - Lightweight	AIR-AP38021-B-K9	10.164.9.62	ADMEAST-5M-AP-01	
Access Point - Lightweight	AIR-AP38021-B-K9	10.164.9.63	ADMEAST-1M-AP-01	
Access Point - Lightweight	AIR-AP38021-B-K9	10.164.9.64	ADMEAST-1M-AP-02	
Access Point - Lightweight	AIR-AP28021-B-K9	10.164.10.7	PSUTVHS-1M-AP-04	



# PRESIDIO

Access Point - Lightweight	AIR-AP2802I-B-K9	10.164.10.8	PSUTWHS-1M-AP-05	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.164.10.15	PSUTWHS-1M-AP-02	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.164.10.24	PSUTWHS-1M-AP-01	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.164.10.31	PSUTWHS-1M-AP-03	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.164.16.57	JUSCNTR-2B-AP-01	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.168.3.123	SIXMISL-1M-AP-04	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.168.3.137	SIXMISL-1M-AP-02	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.168.3.138	SIXMISL-1M-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.168.3.139	SIXMISL-1M-AP-01	
Access Point - Lightweight	AIR-CAP3602I-A-K9	10.168.3.150	6MILE-SLOUGH-TempAP-01	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.168.12.30	EMSVERO-1M-AP-01	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.168.15.14	EMS02-3M-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.168.15.32	EMS81-3M-AP-01	
Access Point - Lightweight	AIR-AP3802I-B-K9	10.168.24.97	PINERDG-1M-AP-01	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.168.24.106	EMS6MPK-MD-AP-03	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.196.1.199	DETARXX-1M-AP-03	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.196.8.237	EDC-1M-AP-0	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.196.8.243	EDC-1M-AP-04	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.200.1.53	DOTOPSB-1M-AP-01	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.200.1.73	DOTOPSB-1M-AP-02	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.200.9.34	EDC-1M-AP-03	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.200.9.223	OLD-EOC-911-AP-01	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.200.9.247	E911-1M-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.210.120.41	CAPEGOV-3M-AP-02	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.210.120.57	CAPEGOV-3M-AP-01	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.224.16.131	HNDRYST-2M-AP-02	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.224.16.132	HNDRYST-3M-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.224.16.133	HNDRYST-3M-AP-02	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.224.16.135	HNDRYST-2M-AP-03	
Access Point - Lightweight	AIR-AP3802I-B-K9	10.224.16.136	HNDRYST-3M-AP-01	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.224.16.137	HNDRYST-2M-AP-01	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.224.16.231	ADMINXX-1E-AP-01	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.224.16.232	ADMINXX-1E-AP-02	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.224.16.233	ADMINXX-1M-AP-02	
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.224.16.234	ADMINXX-6W-AP-03	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.224.16.235	ADMINXX-4M-AP-03	
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.224.16.236	ADMINXX-CB-AP-06	
Access Point - Lightweight	AIR-AP2802I-B-K9	10.224.16.237	ADMINXX-4M-AP-01	

# PRESIDIO

Access Point - Lightweight	AIR-AP2802I-B-K9	10.224.16.238	ADMINXX-1W-AP-04	:
Access Point - Lightweight	AIR-AP2802I-B-K9	10.224.16.239	ADMINXX-1W-AP-01	:
Access Point - Lightweight	AIR-AP2802I-B-K9	10.224.16.240	ADMINXX-4M-AP-02	:
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.224.16.242	ADMINXX-6W-AP-01	:
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.224.16.243	ADMINXX-6W-AP-02	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.224.16.244	ADMINXX-6E-AP-01	:
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.224.16.245	ADMINXX-CB-AP-03	:
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.224.16.246	ADMINXX-CB-AP-02	:
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.224.16.249	ADMINXX-CB-AP-04	:
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.224.16.251	ADMINXX-CB-AP-01	:
Access Point - Lightweight	AIR-AP2802I-B-K9	10.224.16.252	ADMINXX-1W-AP-03	:
Access Point - Lightweight	AIR-AP2802I-B-K9	10.224.16.254	ADMINXX-1W-AP-02	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.78	RIVERDL-1M-AP-01	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.79	RIVERDL-1M-AP-03	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.80	RIVERDL-1M-AP-02	:
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.253.0.111	CAPTIVA-1M-AP-02	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.112	CAPTIVA-1M-AP-01	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.143	PINEISL-1M-AP-01	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.168	EASTLIB-1M-AP-06	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.169	EASTLIB-1M-AP-03	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.170	EASTLIB-1M-AP-02-YS	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.171	EASTLIB-1M-AP-04	:
Access Point - Lightweight	AIR-CAP3502I-A-K9	10.253.0.172	EASTLIB-1M-AP-02	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.174	EASTLIB-1M-AP-05	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.176	EASTLIB-1M-AP-01	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.195	LAKELIB-1M-AP-13	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.200	LAKELIB-1M-AP-15	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.201	LAKELIB-1M-AP-17	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.202	LAKELIB-1M-AP-09	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.203	LAKELIB-1M-AP-03	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.204	LAKELIB-1M-AP-20	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.207	LAKELIB-1M-AP-02	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.208	LAKELIB-1M-AP-11	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.236	FUSTLIB-1M-AP-05	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.237	FUSTLIB-1M-AP-03	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.238	FUSTLIB-1M-AP-01	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.0.239	FUSTLIB-1M-AP-04	:
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.15.141	LIBADMN-1M-AP-02	:

# PRESIDIO

Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.15.144	L1BADMN-1M-AP-01	\$
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.15.176	DUNBARL-1M-AP-02	\$
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.15.177	DUNBARL-1M-AP-01	\$
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.15.197	CAPELB-1M-AP-01	\$
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.15.200	CAPELB-1M-AP-02	\$
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.15.204	CAPELB-1M-AP-03	\$
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.15.207	CAPELB-CA-AP-01	\$
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.15.209	CAPELB-CA-AP-03	\$
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.15.236	SOUTHRG-1M-AP-04	\$
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.15.237	SOUTHRG-1M-AP-03	\$
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.15.238	SOUTHRG-1M-AP-02	\$
Access Point - Lightweight	AIR-CAP2602I-A-K9	10.253.15.239	SOUTHRG-1M-AP-01	\$
Cisco Wireless Controller – Medium (CT5500 series)		10.29.2.116	Cisco Controller	\$
Cisco Wireless Controller – Medium (CT5500 series)	AIR-CT5508-K9	10.228.7.162	JUSCNTR-6M-WC-01	\$
Firewall - Large HQ/Complex		10.169.10.130	JUSCNTR-6M-FW-01	\$
Firewall - Large HQ/Complex		10.169.10.131	JUSCNTR-6M-FW-02	\$
Firewall - Medium Branch Office/Small HQ	PA-820	10.1.101.66	BNLBRY-2M-FW-01	\$
Firewall - Medium Branch Office/Small HQ	PA-820	10.9.13.50	NFLBRY-1M-FW-01	\$
Network Device: Router Large	CISCO2901/K9	10.92.33.129	PLAYERS-1M-RT-01	\$
Network Device: Router Large	ISR4451	172.21.18.137	LEETRHQ-1M-CUBE-01	\$
Network Device: Router Large	ISR4451	172.21.28.34	EEOCDC-CAB32-CUBE-01	\$
Network Device: Router Large	ISR4431	10.1.99.129	BNLBRY-1M-RT-01	\$
Network Device: Router Large	ISR4431	10.80.255.65	LEETRIM-1M-RT-01	\$
Network Device: Router Large	ISR4431	10.102.48.65	MEDEXAM-1M-RT-01	\$
Network Device: Router Large	ISR4431	10.160.0.35	NFLBRY-1M-RT-01	\$
Network Device: Router Large	ISR4431	10.160.255.16	HUMANSV-1M-RT-01	\$
Network Device: Router Large	ISR4431	10.166.0.193	SIXMISL-1M-RT-01	\$
Network Device: Router Large	ISR4431	10.166.0.237	PORTAUT-MB-RT-01	\$
Network Device: Router Large	ISR4431	10.166.0.246	DETARXX-1M-RT-01	\$
Network Device: Router Large	ISR4431	10.166.2.17	TERRYPK-MB-RT-01	\$
Network Device: Router Large	ISR4431	10.9.2.193	LHSRCTR-1M-RT-01	\$
Network Device: Router Large	ASR1001-X	10.92.16.42	JUSCNTR-6M-RT-01	\$
Network Device: Router Medium	WS-C3560G-24TS	172.21.86.168	JC-CLEKVOIP-3-COURT-B	
Network Device: Router Medium	CISCO3925-CHASSIS	10.166.0.253	JUSCNTR-6M-RT-02	
Network Device: Router Medium	CISCO3925-CHASSIS	10.166.0.254	JUSCNTR-6M-RT-04	
Network Device: Router Medium	CISCO2921/K9	10.160.0.4	LEETRHQ-1M-RT-01	



# PRESIDIO

Network Device: Router Medium	CISCO2921/K9	10.160.0.5	LEETRHQ-1M-RT-02	
Network Device: Router Medium	CISCO2921/K9	10.11.103.254	FUSTLIB-1M-RT-01	
Network Device: Router Medium	CISCO2921/K9	10.98.5.17	LEETREM-1M-RT-01	
Network Device: Router Medium	CISCO2921/K9	10.11.0.33	REDSOXX-1M-RT-01	
Network Device: Router Medium	CISCO2921/K9	10.11.18.1	NFMRECR-1M-RT-01	
Network Device: Router Medium	CISCO2921/K9	10.11.32.10	HOUGHST-1M-RT-01	
Network Device: Router Medium	CISCO2921/K9	10.18.53.3	FMREGLB-2M-RT-02	
Network Device: Router Medium	CISCO2921/K9	10.92.33.33	CPUTILS-MB-RT-01	
Network Device: Router Medium	CISCO2921/K9	10.166.0.29	DUNBARL-1M-RT-01	
Network Device: Router Medium	CISCO2921/K9	10.166.0.30	MARSXXX-1M-RT-01	
Network Device: Router Medium	CISCO2921/K9	10.230.0.50	FMREGLB-2M-RT-01	
Network Device: Router Medium	CISCO2911/K9	10.28.3.4	EOC2MDF-R3C1-VG-04	
Network Device: Router Medium	CISCO2911/K9	10.28.3.1	EOC2MDF-R3C1-VG-01	
Network Device: Router Medium	CISCO2911/K9	10.28.3.2	EOC2MDF-R3C1-VG-02	
Network Device: Router Medium	CISCO2911/K9	10.28.3.7	EOC2MDF-R3C1-VG-07	
Network Device: Router Medium	CISCO2911/K9	10.28.3.6	EOC2MDF-R3C1-VG-06	
Network Device: Router Medium	CISCO2911/K9	10.28.3.134	EOC2MDF-R3C1-VG-05	
Network Device: Router Medium	CISCO2911/K9	10.28.3.3	EOC2MDF-R3C1-VG-03	
Network Device: Router Medium	CISCO3845	192.168.72.1	ELECTSO-1M-RT-01	
Network Device: Router Medium	CISCO2821	10.19.0.4	HAMSTAD-1M-RT-01	
Network Device: Router Medium	CISCO2821	10.28.1.113	CON2020-1M-RT-01	
Network Device: Router Medium	CISCO2821	10.28.3.11	EOC2MDF-R5C2-RT-01	
Network Device: Router Medium	CISCO2821	10.80.1.129	SWTOPAZ-1M-RT-01	
Network Device: Router Medium	CISCO2821	10.92.16.118	NWREGLB-1M-RT-01	
Network Device: Router Medium	CISCO2821	10.92.24.4	CAPELIB-1M-RT-01	
Network Device: Router Medium	CISCO2821	10.92.33.25	RIVERDL-1M-RT-01	
Network Device: Router Medium	CISCO2821	10.92.65.1	SOLIDWS-RP-RT-01	
Network Device: Router Medium	CISCO2821	10.96.8.1	CPALMSP-1M-RT-01	
Network Device: Router Medium	CISCO2821	10.96.22.1	PINEISL-1M-RT-01	
Network Device: Router Medium	CISCO2821	10.96.24.1	NATRESC-1M-RT-01	
Network Device: Router Medium	CISCO2821	10.100.128.57	WAKEHCH-1M-RT-01	
Network Device: Router Medium	CISCO2821	10.102.11.193	BOCAGRN-CC-RT-01	
Network Device: Router Medium	CISCO2821	10.102.36.1	CAPTIVA-1M-RT-01	
Network Device: Router Medium	CISCO2821	10.160.0.21	PSUTWHS-1M-RT-01	
Network Device: Router Medium	CISCO2821	10.166.0.1	PINERDG-1M-RT-01	
Network Device: Router Medium	CISCO2821	10.167.0.65	FLEETMG-1M-RT-01	
Network Device: Router Medium	CISCO2821	10.252.0.2	DRMIAMI-3M-RT-01	
Network Device: Router Medium	CISCO2811	10.96.15.1	VETPARK-1M-RT-01	

# PRESIDIO

Network Device: Router Medium		10.29.2.132	APC_ISX_Central	
Network Device: Router Medium		10.110.0.11	EOCDDCTR-R4C26-SW-02	
Network Device: Router Medium		10.110.0.88	lcfdns02	
Network Device: Router Medium		10.110.0.129	lcfnet00	
Network Device: Router Medium		10.232.12.6	NPIA45D36B6C37D	
Network Device: Router Large	Nexus5010	10.232.26.24	NPI8CDDC49ED6B1	
Network Device: Switch Large	Nexus5010	10.31.0.3	DRMIAMI-3M-NX-01	\$
Network Device: Switch Large	Nexus5010	10.31.0.4	DRMIAMI-3M-NX-02	\$
Network Device: Switch Large	WS-C4503-E	10.164.9.1	ADMEAST-2M-L3-01	\$
Network Device: Switch Large	WS-C4500X-32	10.166.0.209	JUSCNTR-6M-L3-01	\$
Network Device: Switch Large	WS-C4500X-32	10.166.0.238	EOC2MDF-L3-01	\$
Network Device: Switch Large	WS-C4500X-32	10.224.16.161	ADMINXX-5M-L3-02	\$
Network Device: Switch Large	WS-C4500X-32	10.18.72.1	LEETRHQ-1M-L3-01	\$
Network Device: Switch Large	WS-C6500	10.230.0.49	PUBWRKS-2M-L3-04	\$
Network Device: Switch Medium	WS-C3750X-48P	10.11.16.34	NFMRECR-1M-SW-01	
Network Device: Switch Medium	WS-C3750X-48P	10.18.48.37	FMREGLB-2M-SW-01	
Network Device: Switch Medium	WS-C3750X-48P	10.18.48.38	FMREGLB-1M-SW-01	
Network Device: Switch Medium	WS-C3750X-24P	10.18.48.36	FMREGLB-B2-SW-01	
Network Device: Switch Medium	WS-C3750G-48PS	10.28.1.2	EOC2MDF-1D-SW-01	
Network Device: Switch Medium	WS-C3750G-48PS	10.92.32.2	NWREGLB-1M-SW-01	
Network Device: Switch Medium	WS-C3750G-48PS	10.92.32.3	NWREGLB-ID-SW-01	
Network Device: Switch Medium	WS-C3750G-48PS	10.92.32.35	CAPELIB-CA-SW-01	
Network Device: Switch Medium	WS-C3750G-48PS	10.102.3.2	NWREGLB-1M-SW-02	
Network Device: Switch Medium	WS-C3750G-48PS	10.102.3.3	NWREGLB-ID-SW-02	
Network Device: Switch Medium	WS-C3750G-48PS	10.224.16.38	PUBWRKS-3N-SW-01	
Network Device: Switch Medium	WS-C3750G-24T	10.11.32.35	HOUGHST-1M-SW-02	
Network Device: Switch Medium	WS-C3750G-12S	10.92.66.7	SOLIDWS-RP-SW-02	
Network Device: Switch Medium	WS-C3650-48PS-L	10.15.79.5	PSCOMMS-E9-SW-01	
Network Device: Switch Medium	WS-C3650-48PS-L	10.92.32.196	LEETRIM-1M-SW-03	
Network Device: Switch Medium	WS-C3650-48PS-L	10.224.16.93	HNDRY-3M-EMERGENCY-VOIP-CLERK	
Network Device: Switch Medium	WS-C3650-48PS	10.92.32.131	MEDEXAM-1M-SW-02	
Network Device: Switch Medium	WS-C3650-48PS	10.98.11.131	PORTAUT-1M-SW-02	
Network Device: Switch Medium	WS-C3650-48PS	10.160.16.50	SIXMISL-1M-SW-01	
Network Device: Switch Medium	WS-C3650-48FD-E	10.160.17.97	ELECTS-3M-RT-01	
Network Device: Switch Medium	WS-C3850-12S-S	10.11.84.1	PSCOMMS-1M-L3-01	
Network Device: Switch Medium	WS-C3650-24PS	10.98.11.130	PORTAUT-1M-SW-01	
Network Device: Switch Medium	WS-C3650-24PS	10.167.0.37	HUMANSV-1M-SW-04	



# PRESIDIO

Network Device: Switch Medium	WS-C3750G-48PS	10.161.0.65	EASTLIB-1M-L3-01	
Network Device: Switch Medium	WS-C3750G-48PS	10.168.22.129	HOUGHST-1M-L3-01	
Network Device: Switch Medium	WS-C3650-12X48UQ.L	10.160.16.200	ADMEAST-1M-SW-02	
Network Device: Switch Medium	WS-C3750G-48PS	10.192.0.1	DOTTRAF-1M-L3-01	
Network Device: Switch Medium	WS-C3560X-48P	10.11.96.19	FUSTLIB-1M-SW-01	
Network Device: Switch Medium	WS-C3560X-48P	10.28.1.13	EOC2MDF-SW-03	
Network Device: Switch Medium	WS-C3560X-48P	10.92.33.82	LEETREM-1M-SW-01	
Network Device: Switch Medium	WS-C3560X-48P	10.160.16.194	ADMEAST-1M-SW-01	
Network Device: Switch Medium	WS-C3560X-48P	10.160.16.196	ADMEAST-5M-SW-01	
Network Device: Switch Medium	WS-C3560X-48P	10.160.16.197	ADMEAST-6M-SW-01	
Network Device: Switch Medium	WS-C3560X-24P	10.11.0.34	REDSOXX-1M-SW-01	
Network Device: Switch Medium	WS-C3560X-24P	10.11.96.18	FUSTLIB-1M-SW-02	
Network Device: Switch Medium	WS-C3560G-48TS	10.28.1.14	EOC-PUBLIC-SW-01	
Network Device: Switch Medium	WS-C3560G-48TS	10.92.32.162	TERRYPK-MB-SW-01	
Network Device: Switch Medium	WS-C3560G-48TS	10.92.32.163	TERRYPK-MB-SW-02	
Network Device: Switch Medium	WS-C3560G-48PS	10.11.32.34	HOUGHST-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.19.0.34	HAMSTAD-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.28.1.7	EOC2MDF-R1C2-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.29.4.254	EOCDCTR-R4C29-SW-02	
Network Device: Switch Medium	WS-C3560G-48PS	10.59.1.5	MARSXXX-MB-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.60.1.11	ANMLSVC-1M-SW-02	
Network Device: Switch Medium	WS-C3750G-24PS	10.168.22.1	GARAGEX-1M-L3-02	
Network Device: Switch Medium	WS-C3560G-48PS	10.60.1.12	ANMLSVC-1M-SW-03	
Network Device: Switch Medium	WS-C3560G-48PS	10.92.32.34	CAPELIB-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.92.32.39	CAPELIB-CA-SW-03	
Network Device: Switch Medium	WS-C3560G-48PS	10.92.32.68	SOUTHRG-1M-SW-03	
Network Device: Switch Medium	WS-C3560G-48PS	10.92.32.90	PINEISL-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.92.32.178	WAKEHCH-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.92.32.195	LEETRIM-1M-SW-02	
Network Device: Switch Medium	WS-C3560G-48PS	10.92.32.210	SWTOPAZ-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.92.32.234	PSUTVHS-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.92.33.4	BOCAGRN-CC-SW-04	
Network Device: Switch Medium	WS-C3560G-48PS	10.92.33.11	CPALMSP-3M-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.92.33.18	CAPTIVA-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.92.33.26	RIVERDL-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.92.33.27	RIVERDL-1M-SW-02	
Network Device: Switch Medium	WS-C3560G-48PS	10.160.20.68	EASTLIB-1M-SW-04	
Network Device: Switch Medium	WS-C3750G-12S	172.21.68.2	JUSCNTR-6M-L3-04	

# PRESIDIO

Network Device: Switch Medium	WS-C3650-48PD-S	10.11.22.241	LEETRFMB-1M-L3-01	
Network Device: Switch Medium	WS-C3650-48PD-E	10.102.12.1	SOUTHRG-1M-L3-01	
Network Device: Switch Medium	WS-C3650-48PD	10.168.32.1	LAKELIB-1M-L3-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.160.20.83	LAKELIB-1M-SW-02	
Network Device: Switch Medium	WS-C3650-24PS-E	10.110.32.1	JCANNEX-2M-L3-02	
Network Device: Switch Medium	WS-C3650-24PS	10.168.15.65	EMS2-2M-I3-01	
Network Device: Switch Medium	WS-C3560X-48P	10.102.4.17	LIBADMN-1M-L3-01	
Network Device: Switch Medium	WS-C3560X-48P	172.21.20.1	JUSCNTR-6M-L3-06	
Network Device: Switch Medium	WS-C3560G-48TS	10.31.0.1	DRMIAMI-3M-L3-01	
Network Device: Switch Medium	WS-C3560G-48TS	10.161.0.129	JUSCNTR-2B-L3-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.160.20.84	LAKELIB-1M-SW-03	
Network Device: Switch Medium	WS-C3560G-48PS	10.167.0.34	HUMANSV-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.167.0.35	HUMANSV-1M-SW-02	
Network Device: Switch Medium	WS-C3560G-48PS	10.167.0.36	HUMANSV-1M-SW-03	
Network Device: Switch Medium	WS-C3560G-48PS	10.192.16.2	DOTENGB-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.192.16.3	DOTOPSB-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.192.16.14	DOTOPSB-1M-SW-02	
Network Device: Switch Medium	WS-C3560G-48TS	172.21.10.1	JCANNEX-2M-L3-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.192.16.130	DETARXX-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.192.16.131	DETARXX-1M-SW-02	
Network Device: Switch Medium	WS-C3560G-48PS	10.224.16.34	PUBWRKS-4S-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.224.16.35	PUBWRKS-4S-SW-02	
Network Device: Switch Medium	WS-C3560G-48PS	10.224.16.36	PUBWRKS-4N-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.224.16.37	PUBWRKS-4N-SW-02	
Network Device: Switch Medium	WS-C3560G-48PS	10.224.16.39	PUBWRKS-3S-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.224.16.40	PUBWRKS-3S-SW-02	
Network Device: Switch Medium	WS-C3560G-48PS	10.224.16.42	PUBWRKS-2S-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.224.16.49	PUBWRKS-4N-SW-03	
Network Device: Switch Medium	WS-C3560G-48PS	10.224.16.66	HNDRYST-3M-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.224.16.68	HNDRYST-3M-SW-03	
Network Device: Switch Medium	WS-C3560G-48PS	10.224.16.82	HNDRYST-3M-SW-02	
Network Device: Switch Medium	WS-C3560G-24TS	10.92.32.194	LEETRIM-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-24TS	10.160.16.243	PINERDG-1M-SW-02	
Network Device: Switch Medium	WS-C3560G-24TS	10.160.20.166	FACLMLK-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-24TS	10.192.16.6	DOTTRAF-WH-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.11.0.36	REDSOXX-DO-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.11.0.37	REDSOXX-MO-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.28.1.4	EOC2MDF-SW-05	



# PRESIDIO

Network Device: Switch Medium	WS-C3560G-24PS	10.28.1.8	EOCRADO-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.59.1.6	MARSXXX-HW-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.59.1.7	MARSXXX-CS-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.59.1.8	MARSXXX-RS-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.92.32.38	CAPELIB-CA-SW-02	
Network Device: Switch Medium	WS-C3560G-24PS	10.92.32.91	PINEISL-1M-SW-03	
Network Device: Switch Medium	WS-C3560G-24PS	10.92.32.115	DUNBARL-1M-SW-02	
Network Device: Switch Medium	WS-C3560G-24PS	10.92.32.146	VETPARK-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.92.32.211	SWTOPAZ-B2-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.92.32.226	NATRESC-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.92.33.12	CPALMSP-BO-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.92.33.14	CPALMSP-2M-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.92.65.3	SOLIDWS-RP-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.92.65.4	SOLIDWS-TS-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.92.65.5	SOLIDWS-VM-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.92.65.6	SOLIDWS-SH-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.95.1.194	JUSCNTR-6G-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.98.11.132	PORTAUT-1M-SW-03	
Network Device: Switch Medium	WS-C3560G-24PS	10.160.16.149	JCTOWER-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.160.16.154	JCTOWER-10M-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.160.16.242	PINERDG-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.160.20.69	EASTLIB-1M-SW-05	
Network Device: Switch Medium	WS-C3560G-24PS	10.160.20.167	JCANNEX-RF-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.168.14.2	EMS13ST-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.192.16.7	DOTENGB-1M-SW-02	
Network Device: Switch Medium	WS-C3560G-24PS	10.224.16.69	HNDRYST-3M-SW-04	
Network Device: Switch Medium	WS-C3560G-24PS	10.224.16.85	HNDRYST-3M-SW-09	
Network Device: Switch Medium	WS-C3560G-24PS	10.224.16.87	HNDRYST-3M-SW-07	
Network Device: Switch Medium	WS-C3560G-24PS	10.224.16.89	HNDRYST-3M-SW-10	
Network Device: Switch Medium	WS-C3560G-24PS	10.224.16.90	HNDRYST-3M-SW-11	
Network Device: Switch Medium	WS-C3560G-24PS	172.21.37.3	ADMINXX-2I-SW-01	
Network Device: Switch Medium	WS-C3560CX-12PD-S	10.92.65.8	SOLIDWS-SH2-SW-01	
Network Device: Switch Medium	WS-C3560-8PC	10.11.0.39	REDSOXX-CB-SW-01	
Network Device: Switch Medium	WS-C3560-8PC	10.160.16.235	LAKE5PK-OF-SW-01	
Network Device: Switch Medium	WS-C3560G-48TS	172.21.40.1	PUBWRKS-2M-L3-03	
Network Device: Switch Medium	WS-C3560-48PS	10.92.32.36	CAPELIB-1M-SW-02	
Network Device: Switch Medium	WS-C3560-48PS	10.92.32.37	CAPELIB-1M-SW-03	
Network Device: Switch Medium	WS-C3560-48PS	10.92.32.67	SOUTHRG-1M-SW-02	

# PRESIDIO

Network Device: Switch Medium	WS-C3560-48PS	10.92.32.114	DUNBARL-1M-SW-01	
Network Device: Switch Medium	WS-C3560-48PS	10.92.32.130	MEDEXAM-1M-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.11.64.5	EMS6MPK-MD-L3-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.29.1.18	EOCDCTR-R4C29-L3-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.92.24.3	MEDSTAR-1M-L3-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.96.13.1	ENVLABS-1M-L3-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.160.17.138	CONSBLD-2M-L3-01	
Network Device: Switch Medium	WS-C3560G-48PS	10.166.0.218	JUSCNTR-6G-L3-01	
Network Device: Switch Medium	WS-C3560-48PS	10.92.32.138	FLEETMG-1M-SW-01	
Network Device: Switch Medium	WS-C3560-48PS	10.92.33.2	BOCAGRN-CC-SW-01	
Network Device: Switch Medium	WS-C3560-48PS	10.92.65.2	SOLIDWS-IN-SW-01	
Network Device: Switch Medium	WS-C3560-48PS	10.160.20.67	EASTLIB-1M-SW-03	
Network Device: Switch Medium	WS-C3560-48PS	10.160.20.82	LAKELIB-1M-SW-01	
Network Device: Switch Medium	WS-C3560-48PS	10.224.16.88	HNDRYST-TR2-SW-01	
Network Device: Switch Medium	WS-C3560-24TS	10.92.33.3	BOCAGRN-TE-SW-01	
Network Device: Switch Medium	WS-C3560-24PS	10.11.0.35	REDSOXX-MB-SW-01	
Network Device: Switch Medium	WS-C3560-24PS	10.11.0.38	REDSOXX-IE-SW-01	
Network Device: Switch Medium	WS-C3560-24PS	10.19.0.35	HAMSTAD-ML-SW-01	
Network Device: Switch Medium	WS-C3560-24PS	10.19.0.38	HAMSTAD-2I-SW-01	
Network Device: Switch Medium	WS-C3560-24PS	10.92.33.10	CPALMSP-1M-SW-01	
Network Device: Switch Medium	WS-C3560-24PS	10.92.65.9	SOLIDWS-CD-SW-01	
Network Device: Switch Medium	WS-C3560G-48PS	172.21.32.1	ADMINXX-5M-L3-01	
Network Device: Switch Medium	WS-C3560G-48PS	172.21.79.254	ADMEAST-2M-L3-02	
Network Device: Switch Medium	WS-C3560G-48PS	172.21.98.1	HNDRYST-2M-L3-02	
Network Device: Switch Medium	WS-C3560G-24PS	10.160.0.16	EMSVERO-1M-L3-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.160.20.193	LAKESPK-1M-L3-01	
Network Device: Switch Medium	WS-C3560G-24PS	10.228.26.126	LIBADMN-1M-SW-01	
Network Device: Switch Medium	WS-C3560-48TS	172.21.51.1	CONSBLD-2M-L3-03	
Network Device: Switch Medium	WS-C3560-24PS	10.256.120.1	CAPEGOV-MB-L3-01	
Network Device: Switch Medium	IE-4010-4S24P	10.18.80.2	LEETRCA-1M-SW-02	
Network Device: Switch Medium	C9200-48P	10.9.2.19	LHSRCTR-1M-SW-01	
Network Device: Switch Medium	C9200-48P	10.15.79.4	PSCOMMS-1M-SW-01	
Network Device: Switch Medium	C9200-48P	10.60.1.13	ANMLSVC-1M-SW-01	
Network Device: Switch Medium	C9200-48P	10.92.32.242	CPUTILS-MB-SW-01	
Network Device: Switch Medium	C9200-48P	10.92.32.245	CPUTILS-B2-SW-02	
Network Device: Switch Medium	C9200-48P	10.224.16.51	PUBWRKS-1N-SW-03	
Network Device: Switch Medium	C9200-48P	172.21.77.3	HNDRYST-3M-VOICE-SW-01	
Network Device: Switch Medium	C9200-24P	10.192.16.15	DOTOPSB-1T-SW-02	



# PRESIDIO

Network Device: Switch Medium	C9200-24P	10.192.16.16	DOTOPSB-1M-SW-03	
Network Device: Switch Medium	N3K-C3548P-10GX	10.29.2.197	EOCDC-ø911-NX-01	
Network Device: Switch Medium	N3K-C3548P-10GX	10.29.2.198	EOCDC-ø911-NX-02	
Network Device: Switch Medium	N3K-C3548P-10GX	10.31.12.253	DRMIAMI-ø911-NX-01	
Network Device: Switch Medium	C9200-24P	10.224.16.46	PUBWRKS-1S-SW-02	
Network Device: Switch Medium	N3K-C3548P-10GX	10.31.12.254	DRMIAMI-ø911-NX-02	
Network Device: Switch Medium	IE-4010-4S24P	10.166.0.210	LEETRCA-1M-L3-01	
Network Device: Switch Medium	Nexus2248 FEX-128	10.110.16.1	EOCDCCTR-R5C36-NX-01	
Network Device: Switch Medium	Nexus2248 FEX-128	10.29.1.29	EOCDCCTR-R5C37-NX-02	
Network Device: Switch Medium	C9200-24P	10.255.120.2	CAPEGOV-2M-VOICE-SW-01	
Network Device: Switch Medium	C9300-24S	172.21.46.142	ADMIN-5M-VOICE-L3-01	
Network Device: Switch Medium	C9300-24S	172.21.86.154	JUSCNTR-6M-VOICE-L3-04	
Network Device: Switch Medium	C9200-48P	172.21.44.1	ADMINXX-CLERKVOIP-5-DOIT	
Network Device: Switch Medium	C9200-48P	172.21.49.137	JC-CLERKVOIP-1-COURT-C	
Network Device: Switch Medium	C9200-48P	172.21.49.161	JC-CLERKVOIP-2-COURT-B-C	
Network Device: Switch Medium	C9200-48P	172.21.49.201	ADMINXX-CLERKVOIP-3-FIN-EAST	
Network Device: Switch Medium	C9200-48P	172.21.77.34	TAXCOLL-CC-L3-01	
Network Device: Switch Medium	C9200-48P	172.21.77.39	TAXCOLL-PR-L3-01	
Network Device: Switch Medium	C9200-48P	172.21.85.129	JC-CLERKVOIP-1-COURT-D	
Network Device: Switch Medium	C9200-48P	172.21.86.164	JC-CLERKVOIP-1-COURT-B	
Network Device: Switch Medium	C9200-48P	172.21.240.1	TCTHOMP-2M-VOIP-1	
Network Device: Switch Medium	C9200-24P	172.21.45.129	ADMINXX-CLERKVOIP-3-FIN-WEST	
Network Device: Switch Medium	C9200-24P	172.21.46.141	ADMINXX-CLERKVOIP-2-REC-EAST	
Network Device: Switch Medium	C9200-24P	172.21.46.152	ADMINXX-CLERKVOIP-2-REC-WEST	
Network Device: Switch Medium	C9200-24P	172.21.77.35	TAXCOLL-NF-L3-01	
Network Device: Switch Medium	C9200-24P	172.21.77.37	TAXCOLL-BN-L3-01	
Network Device: Switch Medium	C9200-24P	172.21.79.253	ADMEAST-CLERKVOIP-3-HR	
Network Device: Switch Medium	C9200-24P	172.21.86.65	JC-CLERKVOIP-2-JURY-D	
Network Device: Switch Medium	C9200-24P	172.21.86.161	JC-CLERKVOIP-2-ADMIN-A	
Network Device: Switch Medium	C9200-24P	172.21.100.1	TCTHOMP-1M-VOIP	
Network Device: Switch Medium	C9200-24P	172.21.102.129	TAXCOLL-LH-L3-01	
Network Device: Switch Medium	C9200-24P	172.21.226.1	HNDRYST-2M-VOICE-L3-01	
Network Device: Switch Medium	C9200-24P	172.21.241.1	TCTHOMP-4M-VOIP	
Network Device: Switch Small	WS-C2960XR-48TS-I	10.11.64.66	EMS6MPK-1W-SW-01	
Network Device: Switch Small	WS-C2960XR-48FPD-I	10.160.16.146	JUSCNTR-6M-SW-01	
Network Device: Switch Small	WS-C2960XR-24PD-I	10.92.32.164	TERRYPK-AN-SW-01	
Network Device: Switch Small	WS-C2960XR-24PD-I	10.224.16.67	HNDRYST-3M-SW-06	
Network Device: Switch Small	WS-C2960XR-24PD-I	172.21.81.2	ELECTSO-1M-SW-01	



# PRESIDIO

Network Device: Switch Small	WS-C2960XR-24PD-I	192.168.65.171	ELECTBO-1M-L3-01	
Network Device: Switch Small	WS-C2960X-48FPS-L	10.160.16.199	ADMEAST-6M-SW-02	
Network Device: Switch Small	WS-C2960X-48FPS-L	10.160.20.169	JCANNEX-1M-SW-01	
Network Device: Switch Small	WS-C2960X-48FPS-L	10.224.16.2	ADMINXX-6E-SW-01	
Network Device: Switch Small	WS-C2960X-48FPS-L	10.224.16.6	ADMINXX-1E-SW-01	
Network Device: Switch Small	WS-C2960X-48FPS-L	10.224.16.7	ADMINXX-1W-SW-01	
Network Device: Switch Small	WS-C2960X-48FPS-L	10.224.16.10	ADMINXX-CB-SW-01	
Network Device: Switch Small	WS-C2960X-48FPS-L	10.224.16.14	ADMINXX-4M-SW-01	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.1.101.18	BNLIBRY-2M-SW-01	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.1.101.20	BNLIBRY-1M-SW-01	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.9.13.34	NFLIBRY-1M-SW-01	
Network Device: Switch Small	WS-C2960XR-48FPS-I	10.31.11.1	GRNMDWS-1M-L3-01	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.18.64.5	LEETRHO-1D-SW-01	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.18.64.10	LEETRHO-1M-SW-01	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.18.64.12	LEETRHO-1D-SW-02	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.18.64.13	LEETRHO-2D-SW-01	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.18.64.14	LEETRHO-3D-SW-01	
Network Device: Switch Small	WS-C2960XR-48FPD-I	172.21.81.1	ELECTSO-1M-L3-01	
Network Device: Switch Small	WS-C2960XR-24PS-I	10.11.32.97	HEAVYEQ-1M-L3-01	
Network Device: Switch Small	WS-C2960XR-24PD-I	172.21.5.6	ELECTCA-1M-L3-01	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.102.19.1	ESTROPK-1M-SW-01	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.18.64.15	LEETRHO-4D-SW-01	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.18.64.16	LEETRHO-1M-SW-02	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.18.64.17	LEETRHO-2D-SW-02	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.18.64.18	LEETRHO-5D-SW-01	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.28.1.11	EOC2MDF-SW-01	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.28.1.12	EOC2MDF-SW-02	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.28.1.114	CON2020-1M-SW-01	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.224.16.41	PUBWRKS-2N-SW-01	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.224.16.83	HNDRYST-3M-SW-08	
Network Device: Switch Small	WS-C2960X-48FPD-L	10.224.16.84	HNDRYST-2M-SW-01	
Network Device: Switch Small	WS-C2960X-24PS-L	10.1.101.19	BNLIBRY-TG-SW-01	
Network Device: Switch Small	WS-C2960X-24PS-L	10.1.101.21	BNLIBRY-MRA-SW-01	
Network Device: Switch Small	WS-C2960X-24PS-L	10.1.101.22	BNLIBRY-MRB-SW-01	
Network Device: Switch Small	WS-C2960X-24PS-L	10.1.101.23	BNLIBRY-ST-SW-01	
Network Device: Switch Small	WS-C2960X-24PS-L	10.9.13.35	NFLIBRY-TG-SW-01	
Network Device: Switch Small	WS-C2960X-24PS-L	10.9.13.36	NFLIBRY-MRA-SW-01	
Network Device: Switch Small	WS-C2960X-24PS-L	10.9.13.37	NFLIBRY-MRB-SW-01	

# PRESIDIO

Network Device: Switch Small	WS-C2960X-24PS-L	10.9.13.38	NFLIBRY-ST-SW-01	\$
Network Device: Switch Small	WS-C2960X-24PS-L	10.11.16.35	NFMRECR-ID-SW-02	\$
Network Device: Switch Small	WS-C2960X-24PS-L	10.19.0.36	HAMSTAD-MB-SW-01	\$
Network Device: Switch Small	WS-C2960X-24PS-L	10.19.0.37	HAMSTAD-SB-SW-01	\$
Network Device: Switch Small	WS-C2960X-24PS-L	10.92.33.131	PLAYERS-1M-SW-01	\$
Network Device: Switch Small	WS-C2960X-24PS-L	10.160.20.178	ADMEAST-LEETV-SW-01	\$
Network Device: Switch Small	WS-C2960X-24PS-L	10.224.16.3	ADMINXX-6W-SW-01	\$
Network Device: Switch Small	WS-C2960X-24PS-L	10.224.16.12	ADMINXX-5M-SW-01	\$
Network Device: Switch Small	WS-C2960L-8PS-LL	10.160.16.203	ADMEAST-CB-SW-01	\$
Network Device: Switch Small	WS-C2960CX-8PC-L	10.160.16.53	SIXMISL-1M-SW-02	\$
Network Device: Switch Small	WS-C2940-8TT-S	10.11.96.20	FUSTLIB-1M-SW-03	\$
Network Device: Switch Small	WS-C2940-8TT-S	10.160.16.151	JUSCNTR-3M-SW-01	\$
Network Device: Switch Small	WS-C2940-8TT-S	10.160.20.66	EASTLIB-1M-SW-02	\$
Network Device: Switch Small	WS-C2940-8TT-S	10.160.20.106	JUSCNTR-2B-SW-01	\$
Network Device: Switch Small	C1000-8FP-E-2G-L	10.92.32.246	CPUTILS-B3-SW-01	\$
Network Device: Switch Small	C1000-8FP-E-2G-L	10.92.32.247	CPUTILS-B4-SW-01	\$

## COLLABORATION SERVICES: LCG

Server - Non-blade, includes host	C240	10.29.2.205	Eocucs-01	\$
Server - Non-blade, includes host	C240	10.29.2.207	Eocucs-02	\$
Server - Non-blade, includes host	C240	10.18.64.23	Leetrucs-01	\$
Server - Non-blade, includes host	C240	10.18.64.24	Leetrucs-02	\$
Mail Control, Primary (Publisher)	CUCM Publisher	172.21.29.2	Eocucmpub-01	\$
Mail Control, Redundant (Subscriber)	CUCM Subscriber	172.21.29.4	Eocucmsub-01	\$
Mail Control, Redundant (Subscriber)	CUCM Subscriber	172.21.29.5	Eocucmsub-02	\$
Mail Control, Redundant (Subscriber)	CUCM Subscriber	172.21.18.131	Leetrucmsub-01	\$
Mail Control, Redundant (Subscriber)	CUCM Subscriber	172.21.18.132	Leetrucmsub-02	\$
Mail Control, Redundant (Subscriber)	CUCM TFTP	172.21.29.3	Eocucntftp-01	\$
Mail Control, Redundant (Subscriber)	CUCM TFTP	172.21.18.130	Leetrucmftp-01	\$
Voice Mail, Primary	Unity Publisher	172.21.29.7	Eocucupub-01	\$
Voice Mail, Redundant (HA Node)	Unity Subscriber	172.21.18.133	Leetrucucsub-01	\$
Presence, Primary	CUPS Publisher	172.21.29.8	Eocucimpub-01	\$
Presence, Redundant (HA Node)	CUPS Subscriber	172.21.18.133	Leetrucimpsub-01	\$
Contact Center Express, Primary	UCCX Primary	172.21.29.11	Eococcxpub-01	\$
Contact Center Express, Redundant (HA Node)	UCCX Redundant	172.21.18.136	Leetrucxsub-01	\$
Emergency Responder (E911), Primary	CER Primary	172.21.29.10	Eococerpub-01	\$
Emergency Responder (E911), Redundant	CER Redundant	172.21.18.135	Leetrersub-01	\$
Mail Control User	CUCM No MACDs	<b>Qty. 573</b>	Unit Price \$2.02	\$1,
Contact Center Express Agent	CCX Agents	<b>Qty. 199</b>	Unit Price \$14.54	\$2,

# PRESIDIO

S Control/Expressway Core	Expressway-C		Eocexpc-01	\$
S Control/Expressway Core - Redundant	Expressway-C		Leetexpc-01	\$
S Control/Expressway Core	Expressway-E		Eocexpe-01	\$
S Control/Expressway Core - Redundant	Expressway-E		Leetexpe-01	\$
Ice Gateway - SIP/CUBE - Complex	ISR4451 CUBE		Eoccube-01	\$
Ice Gateway - SIP/CUBE - Complex	ISR4451 CUBE		Leetcube-01	\$
teaway, Analog, Small	VG204		VG204 1	\$
teaway, Analog, Small	VG204		VG204 2	\$
teaway, Analog, Small	VG204		VG204 3	\$
teaway, Analog, Small	VG204		VG204 4	\$
teaway, Analog, Small	VG204		VG204 5	\$
teaway, Analog, Small	VG204		VG204 6	\$
teaway, Analog, Small	VG204		VG204 7	\$
teaway, Analog, Small	VG204		VG204 8	\$
Other/Third Party (Vendor Managed)	Nuance		Lcftts01	\$
COLLABORATION SERVICES: LEE TRAN				
erver - Non-blade, includes host	C220 M3	10.18.64.2	LCFVSP41	\$
erver - Non-blade, includes host	C220 M3	10.18.64.6	LCFVSP42	\$
erver - Non-blade, includes host	C220 M3	10.18.64.8	LCFVSP43	\$
erver - Non-blade, includes host	C220 M3	10.29.2.133	LCFVSP24	\$
cluded with LCFVSP41	C220 M3	10.18.64.3	CIMC - LCFVSP41	
cluded with LCFVSP42	C220 M3	10.18.64.7	CIMC - LCFVSP42	
cluded with LCFVSP43	C220 M3	10.18.64.9	CIMC - LCFVSP43	
cluded with LCFVSP44	C220 M3	10.29.2.134	CIMC - LCFVSP24	
all Control, Primary (Publisher)	CUCM Publisher	10.18.70.2	LCFUCM03	\$
all Control, Redundant (Subscriber)	CUCM Subscriber	10.110.0.164	LCFUCM04	\$
icemail, Primary	Unity Publisher	10.18.70.3	LCFCUC03	\$
icemail, Redundant (HA Node)	Unity Subscriber	10.110.0.165	LCFCUC04	\$
esence, Primary	CUPS Publisher	10.18.70.4	LCFIMP03	\$
esence, Redundant (HA Node)	CUPS Subscriber	10.110.0.166	LCFIMP04	\$
ontact Center Express, Primary	UCCX Primary	10.18.70.5	LCFCXC03	\$
ontact Center Express, Redundant (HA Node)	UCCX Redundant	10.110.0.167	LCFCXC04	\$
erver - Non-blade, includes host	Virtual Server	10.18.70.6	LCFVMA03	\$
isco WebEx Service (Vendor Managed)	WebEx Service	10.18.70.7	LCFVMM03	\$
erver - Non-blade, includes host	Virtual Server	10.18.70.8	LCFWRP03	\$
C Other/Third Party (Vendor Managed)	Virtual Server	10.110.0.168	LCFINF03	\$
C Other/Third Party (Vendor Managed)	Zoom, Xmedius, etc.	10.110.0.169	LCFRECO3	\$
C Other/Third Party (Vendor Managed)	Zoom, Xmedius, etc.	10.110.0.170	LCFTWB03	\$



# PRESIDIO

Control User	CUCM User No MACDs	Qty. 125	Unit Price \$2.02	\$
Contact Center Express Agent	CCX Agents	Qty. 59	Unit Price \$14.54	\$
oice Gateway - T1/PRI/SIP - Standard	CISCO2921	10.160.0.4	LEETRHQ-1M-RT-01	\$
oice Gateway - T1/PRI/SIP - Standard	CISCO2921	10.160.0.5	LEETRHQ-1M-RT-02	\$
ateway, Analog, Medium	VG224	10.18.70.14	LEETRHQ-1M-VG-01	\$
COLLABORATION SERVICES: EOC CORE				
Control User	CUCM User No MACDs	Qty. 487	Unit Price \$2.02	\$
DATA CENTER SERVICES: EOC **ESSENTIAL SERVICES NASPO PRICING**				
cluded with blade servers	Dell m1000e Chassis		-	
cluded with blade servers	Dell m1000e Chassis		-	
erver - Non-blade, includes host	Dell M620 Blade Servers		-	\$
erver - Non-blade, includes host	Dell M620 Blade Servers		-	\$
erver - Non-blade, includes host	Dell M620 Blade Servers		-	\$
erver - Non-blade, includes host	Dell M620 Blade Servers		-	\$
erver - Non-blade, includes host	Dell M620 Blade Servers		-	\$
erver - Non-blade, includes host	Dell M620 Blade Servers		-	\$
erver - Non-blade, includes host	Dell M620 Blade Servers		-	\$
erver - Non-blade, includes host	Dell M620 Blade Servers		-	\$
erver - Non-blade, includes host	Dell M620 Blade Servers		-	\$
erver - Non-blade, includes host	Dell M620 Blade Servers		-	\$
erver - Non-blade, includes host	Dell M630 Blade Servers		-	\$
erver - Non-blade, includes host	Dell M630 Blade Servers		-	\$
erver - Non-blade, includes host	Dell M630 Blade Servers		-	\$
erver - Non-blade, includes host	Dell R740		-	\$
erver - Non-blade, includes host	Cisco UCS C220		-	\$
erver - Non-blade, includes host	Cisco UCS C240		-	\$
erver - Non-blade, includes host	Windows 10 Enterprise			\$
erver - Non-blade, includes host	Windows 7 Enterprise			\$
erver - Non-blade, includes host	Server 2016			\$
erver - Non-blade, includes host	Server 2003			\$
erver - Non-blade, includes host	Server 2012 R2			\$
erver - Non-blade, includes host	Linux			\$
erver - Non-blade, includes host	Server 2012 R2			\$
erver - Non-blade, includes host	Server 2012 R2			\$
erver - Non-blade, includes host	Server 2016			\$
erver - Non-blade, includes host	Server 2016			\$
erver - Non-blade, includes host	Server 2012 R2			\$

---

---

[illegible]