ARLINGTON COUNTY, VIRGINIA
OFFICE OF THE PURCHASING AGENT
2100 CLARENDON BOULEVARD, SUITE 500
ARLINGTON, VIRGINIA 22201

NOTICE OF AWARD OF CONTRACT

TO: PRESIDIO HOLDINGS, INC. DBA PRESIDIO NETWORKED SOLUTIONS, LLC
12120 SUNSET HILLS ROAD, SUITE 202
RESTON, VA 20190

DATE ISSUED: October 19, 2016

CURRENT REFERENCE NO: 671-15

CONTRACT TITLE: DTS/MANAGED NETWORK SERVICES

THIS IS A NOTICE OF AWARD OF CONTRACT AND NOT AN ORDER. NO WORK IS AUTHORIZED UNTIL THE VENDOR RECEIVES A VALID COUNTY PURCHASE ORDER ENCUMBERING CONTRACT FUNDS.

Your firm is awarded the above referenced contract. The contract term covered by this Notice of Award is effective immediately and expires on June 30, 2021.

The Contract may be renewed for not more than five (5) additional 12-month periods through June 30, 2026.

The contract documents consist of the terms, conditions, and specifications of Agreement No. 671-15 including any attachments or amendments thereto.

CONTRACT PRICING:
Refer to Attachment B to the Agreement (Pricing Schedule).
Hourly rates firm through September 30, 2017. Any price adjustments shall be in accordance with paragraph 6. Contract Price Adjustments.

EMPLOYEES NOT TO BENEFIT:
NO COUNTY EMPLOYEE SHALL RECEIVE ANY SHARE OR BENEFIT OF THIS CONTRACT NOT AVAILABLE TO THE GENERAL PUBLIC.

VENDOR CONTACT: Patrick McManaman
VENDOR TEL. NO.: 202-237-2822
E-MAIL ADDRESS: pmcmanaman@presidio.com

COUNTY CONTACT: Robert Jenkins
COUNTY TEL. NO.: 703-228-3408
E-MAIL ADDRESS: rjenkins@arlingtonva.us

CONTRACT AUTHORIZATION

Krystyna Hepler, CPPB
Assistant Purchasing Agent

10/19/2016
DATE

DISTRIBUTION

BID FOLDER: 1

ARLINGTON COUNTY, VIRGINIA
OFFICE OF THE PURCHASING AGENT
SUITE 500, 2100 CLARENDON BOULEVARD
ARLINGTON, VA 22201

AGREEMENT NO. 671-15

THIS AGREEMENT is made, on the date of execution by the County, between Presidio Holdings, Inc., DBA, Presidio Networked Solutions, LLC, 12120 Sunset Hills Road, Suite 202, Reston, VA 20190 ("Contractor") a *Virginia Corporation* authorized to do business in the Commonwealth of Virginia, and the County Board of Arlington County, Virginia. The County and the Contractor, for the consideration hereinafter specified, agree as follows:

1. CONTRACT DOCUMENTS

The "Contract Documents" consist of:

This Agreement
Attachment A – Scope of Work
Attachment B –Pricing Schedule
Attachment C – Presidio Managed Network Services Agreement
Attachment D – County Nondisclosure and Data Security Agreement (Contractor)
Attachment E – County Nondisclosure and Data Security Agreement (Individual)

Where the terms and provisions of this Agreement vary from the terms and provisions of the other Contract Documents, the terms and provisions of this Agreement will prevail over the other Contract Documents, and the remaining Contract Documents will be complementary to each other. If there are any conflicts, the most stringent terms or provisions will prevail.

The Contract Documents set forth the entire agreement between the County and the Contractor. The County and the Contractor agree that no representative or agent of either party has made any representation or promise with respect to the parties' agreement that is not contained in the Contract Documents. The Contract Documents may be referred to below as the "Contract" or the "Agreement".

2. SCOPE OF WORK

The Contractor agrees to perform the services described in the Contract Documents (the "Work"). As detailed in the "Scope of Work" (Attachment A), the primary purpose of the Work is to provide the County with Managed Network Services, After-hours Service Desk support and major project support. It will be the Contractor's responsibility, at its sole cost, to provide the specific services set forth in the Contract Documents and sufficient services to fulfill the purposes of the Work. Nothing in the Contract Documents limits the Contractor's responsibility to manage the details and execution of the Work.

3. PROJECT OFFICER

The performance of the Contractor is subject to the review and approval of the County Project Officer, who will be appointed by the Director of the Arlington County department or agency requesting the Work under this Contract.

4. CONTRACT TERM

The Work will commence on the date of the execution of the Agreement by the County and must be completed no later than June 30, 2021 ("Initial Contract Term"), subject to any modifications provided in the Contract Documents. Upon satisfactory performance by the Contractor the County may, through issuance of a unilateral Notice of Award, authorize continuation of the Agreement under the same contract prices for not more than five (5) additional 12-month periods, from July 01, 2021 to June 30, 2026 (each a "Subsequent Contract Term"). The Initial Contract Term and any Subsequent Contract Term(s) are together the "Contract Term".

5. CONTRACT AMOUNT

The County will pay the Contractor in accordance with the terms of the Payment section below and of Attachment B for the Contractor's completion of the Work as required by the Contract Documents. The Contractor will complete the Work for the total amount specified in this section ("Contract Amount").

The County will not compensate the Contractor for any goods or services beyond those included in Attachment A unless those additional goods or services are covered by a fully executed amendment to this Contract. Additional services will be billed at the rates set forth in Attachment B unless otherwise agreed by the parties in writing.

6. CONTRACT PRICE ADJUSTMENT

The Project Support labor rates will remain firm until September 30, 2017, ("Project Support Price Adjustment Date") and will then increase by 4.0% at Year 2 and Year 4 of the Initial Contract Term. The Base Managed Services rates will remain firm until September 30, 2021, ("Base Managed Services Price Adjustment Date"). To request a price adjustment, the Contractor or the County must submit a written request to the other party not less than 60 days before the applicable Price Adjustment Date.

Adjustments to Project Support labor rates will be 4.0% in Year 6, Year 8 and Year 10 of the Subsequent Contract Term.

Adjustments to Base Managed Services rates will equal the percentage change of the U.S. Department of Labor Consumer Price Index, All Items, Unadjusted, Urban Areas ("CPI-U") for the 12-month period ending in June of each year of the Subsequent Contract Term or 5%, whichever is less.

Any rates that result from this provision will become effective the day after the Project Support Price Adjustment Date and will be binding for 24 months. Any rates that result from this provision will become effective the day after the Base Managed Services Price Adjustment Date and will be binding for 12 months.

If the Contractor and the County have not agreed on a requested adjustment by 30 days before the Base Managed Services Price Adjustment Date, the County may terminate the Contract, whether or not the County has previously elected to extend the Contract's term.

7. PAYMENT

The Contractor must submit invoices to the County's Project Officer, who will either approve the invoice or require corrections. The County will pay the Contractor within 30 days after receipt of an invoice for completed work that is reasonable and allocable to the Contract and that has been performed to the satisfaction of the Project Officer. The number of the County Purchase Order pursuant to which goods or services have been delivered or performed must appear on all invoices.

8. REIMBURSABLE EXPENSES

The County will not reimburse the Contractor for any expenses under this Contract. The amount in Attachment B includes all costs and expenses of providing the services described in this Contract.

9. PAYMENT OF SUBCONTRACTORS

The Contractor is obligated to take one of the two following actions within seven days after receipt of payment by the County for work performed by any subcontractor under this Contract:

a. Pay the subcontractor for the proportionate share of the total payment received from the County attributable to the work performed by the subcontractor under this Contract; or

b. Notify the County and the subcontractor, in writing, of the Contractor's intention to withhold all or a part of the subcontractor's payment, with the reason for nonpayment.

The Contractor is obligated to pay interest to the subcontractor on all amounts owed by the Contractor to the subcontractor that remain unpaid after seven days following receipt by the Contractor of payment from the County for work performed by the subcontractor under this Contract, except for amounts withheld as allowed in subsection b., above. Unless otherwise provided under the terms of this Contract, interest will accrue at the rate of 1% per month.

The Contractor must include in each of its subcontracts, if any are permitted, a provision requiring each subcontractor to include or otherwise be subject to the same payment and interest requirements with respect to each lower-tier subcontractor.

The Contractor's obligation to pay an interest charge to a subcontractor pursuant to this section may not be construed to be an obligation of the County. A Contract modification may not be made for the purpose of providing reimbursement for such interest charge. A cost reimbursement claim may not include any amount for reimbursement for such interest charge.

10. NO WAIVER OF RIGHTS

The County's approval or acceptance of or payment for any goods or services under this Contract will not waive any rights or causes of action arising out of the Contract.

11. NON-APPROPRIATION

All payments by the County to the Contractor pursuant to this Contract are subject to the availability of an annual appropriation for this purpose by the County Board of Arlington County, Virginia ("Board"). In the event that the Board does not appropriate funds for the goods or services provided under this Contract, the County will terminate the Contract, without termination charge or other liability to the County, on the last day of the fiscal year or when the previous appropriation has been spent, whichever event occurs first.

12. ESTIMATED QUANTITIES/NON-EXCLUSIVITY OF CONTRACTOR

This Contract does not obligate the County to purchase a specific quantity of items or services during the Contract Term. Any quantities that are included in the Contract Documents are the present expectations of the County for the period of the Contract; and the County is under no obligation to buy that or any amount as a result of having provided this estimate or of having had any normal or otherwise measurable requirement in the past. The County may require more goods and/or services than the estimated annual quantities, and any such additional quantities will not give rise to any claim for compensation other than at the unit prices and/or rates in the Contract.

The County does not guarantee that the Contractor will be the exclusive provider of the goods or services covered by this Contract. The items or services covered by this Contract may be or become available under other County contract(s), and the County may determine that it is in its best interest to procure the items or services through those contract(s).

13. COUNTY PURCHASE ORDER REQUIREMENT

County purchases are authorized only if the County issues a Purchase Order in advance of the transaction, indicating that the ordering County agency has sufficient funds available to pay for the purchase. If the Contractor provides goods or services without a signed County Purchase Order, it does so at its own risk and expense. The County will not be liable for payment for any purchases made by its employees that are not authorized by the County Purchasing Agent.

14. BACKGROUND CHECK

All employees or subcontractors whom the Contractor assigns to work on this Contract must pass the County's standard background check. The background check will include fingerprinting by the County Sheriff's Office and a credit check.

15. REPLACEMENT OF PERSONNEL AND SUBCONTRACTORS

The County has the right reasonably to reject staff or subcontractors whom the Contractor assigns to the project. The Contractor must then provide replacement staff or subcontractors satisfactory to the County in

a timely manner and at no additional cost to the County. The day-to-day supervision and control of the Contractor's and its subcontractors' employees is the sole responsibility of the Contractor.

The Contractor may not replace key personnel or subcontractors identified in its proposal, including the approved Project Manager, without the County's written approval. The Contractor must submit any request to remove or replace key personnel or subcontractors to the County Project Officer at least 15 calendar days in advance of the proposed action. The request must contain a detailed justification, including identification of the proposed replacement and his or her qualifications.

If the approved Project Manager must be absent for an extended period, the Contractor must provide an interim Project Manager, subject to the County's written approval.

If the approved Project Manager resigns or is terminated by the Contractor, the Contractor will replace the Project Manager with an individual with similar qualifications and experience, subject to the County's written approval.

16. EMPLOYMENT DISCRIMINATION BY CONTRACTOR PROHIBITED

During the performance of its work pursuant to this Contract:

A. The Contractor will not discriminate against any employee or applicant for employment because of race, religion, color, sex, national origin, age or disability or on any other basis prohibited by state law. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices setting forth the provisions of this nondiscrimination clause.

B. Notices, advertisements and solicitations placed in accordance with federal law, rule or regulation will be deemed sufficient for meeting the requirements of this section.

C. The Contractor will state in all solicitations or advertisements for employees that it places or causes to be placed that such Contractor is an Equal Opportunity Employer.

D. The Contractor will comply with the provisions of the Americans with Disabilities Act of 1990 ("ADA"), which prohibits discrimination against individuals with disabilities in employment and mandates that disabled individuals be provided access to publicly and privately provided services and activities.

E. The Contractor must include the provisions of the foregoing paragraphs in every subcontract or purchase order of more than $10,000.00 relating to this Contract so that the provisions will be binding upon each subcontractor or vendor.

17. EMPLOYMENT OF UNAUTHORIZED ALIENS PROHIBITED

In accordance with §2.2-4311.1 of the Code of Virginia, as amended, the Contractor must not during the performance of this Contract knowingly employ an unauthorized alien, as that term is defined in the federal Immigration Reform and Control Act of 1986.

18. DRUG-FREE WORKPLACE TO BE MAINTAINED BY CONTRACTOR

During the performance of this Contract, the Contractor must: (i) provide a drug-free workplace for its employees; (ii) post in conspicuous places, available to employees and applicants for employment, a statement notifying employees that the unlawful manufacture, sale, distribution, dispensation, possession, or use of a controlled substance or marijuana is prohibited in the Contractor's workplace and specifying the actions that will be taken against employees for violating such prohibition; (iii) state in all solicitations or advertisements for employees placed by or on behalf of the Contractor that the Contractor maintains a drug-free workplace; and (iv) include the provisions of the foregoing clauses in every subcontract or purchase order of more than $10,000.00 relating to this Contract so that the provisions will be binding upon each subcontractor or vendor.

For the purposes of this section, "workplace" means the site(s) for the performance of the work required by this Contract.

19. SAFETY

The Contractor must ensure that it and its employees and subcontractors comply with all applicable local, state and federal policies, regulations and standards relating to safety and health, including the standards of the Virginia Occupational Safety and Health program of the Department of Labor and Industry for General Industry and for the Construction Industry and the applicable Federal Environmental Protection Agency and Virginia Department of Environmental Quality standards.

20. TERMINATION

The County may terminate this Contract at any time as follows: (1) for cause, if, as determined by the County, the Contractor is in breach or default or has failed to perform the Work satisfactorily; or (2) for the convenience of the County.

Upon receipt of a notice of termination, the Contractor must not place any further orders or subcontracts for materials, services or facilities; must terminate all vendors and subcontracts, except as are necessary for the completion of any portion of the Work that the County did not terminate; and must immediately deliver all documents related to the terminated Work to the County.

Any purchases that the Contractor makes after the notice of termination will be the sole responsibility of the Contractor, unless the County has approved the purchases in writing as necessary for completion of any portion of the Work that the County did not terminate.

If any court of competent jurisdiction finds a termination for cause by the County to be improper, then the termination will be deemed a termination for convenience.

A. TERMINATION FOR CAUSE, INCLUDING BREACH AND DEFAULT; CURE

1. Termination for Unsatisfactory Performance. If the County determines that the Contractor has failed to perform satisfactorily, then the County will give the Contractor written notice of such failure(s) and the opportunity to cure them within 15 days or any other period specified by the County ("Cure Period"). If the Contractor fails to cure within the Cure Period, the County may terminate the Contract for failure to provide satisfactory performance by providing written notice with a termination date. Upon such termination, the Contractor may apply for compensation for Contract services that the County previously accepted ("Termination Costs"), unless payment is otherwise barred by the Contract. The Contractor must submit any request for Termination Costs, with all supporting documentation, to the County Project Officer within 30 days after the expiration of the Cure Period. The County may accept or reject the request for Termination Costs, in whole or in part, and may notify the Contractor of its decision within a reasonable time.

   In the event of termination by the County for failure to perform satisfactorily, the Contractor must continue to provide its services as previously scheduled through the termination date, and the County must continue to pay all fees and charges incurred through the termination date.

2. Termination for Breach or Default. If the County terminates the Contract for default or breach of any Contract provision or condition, then the termination will be immediate after notice of termination to the Contractor (unless the County provides for an opportunity to cure), and the Contractor will not be permitted to seek Termination Costs.

   Upon any termination pursuant to this section, the Contractor will be liable to the County for costs that the County must expend to complete the Work, including costs resulting from any related delays and from unsatisfactory or non-compliant work performed by the Contractor or its subcontractors. The County will deduct such costs from any amount due to the Contractor; or if the County does not owe the Contractor, the Contractor must promptly pay the costs within

15 days of a demand by the County. This section does not limit the County's recovery of any other damages to which it is entitled by law.

Except as otherwise directed by the County, the Contractor must stop work on the date of receipt the notice of the termination.

B. TERMINATION FOR THE CONVENIENCE OF THE COUNTY

The County may terminate this Contract in whole or in part whenever the Purchasing Agent determines that termination is in the County's best interest. The County will give the Contractor at least 15 days' notice in writing. The notice must specify the extent to which the Contract is terminated and the effective termination date. The Contractor will be entitled to Termination Costs, as defined above, plus any other reasonable amounts that the parties might negotiate; but no amount will be allowed for anticipatory profits.

Except as otherwise directed by the County, the Contractor must stop work on the date of receipt of the notice of the termination.

21. INDEMNIFICATION

The Contractor covenants for itself, its employees and its subcontractors to save, defend, hold harmless and indemnify the County and all of its elected and appointed officials, officers, current and former employees, agents, departments, agencies, boards and commissions (collectively the "County Indemnitees") from and against any and all claims made by third parties for any and all losses, damages, injuries, fines, penalties, costs (including court costs and attorneys' fees), charges, liability, demands or exposure resulting from, arising out of or in any way connected with the Contractor's acts or omissions, including the acts or omissions of its employees and/or subcontractors, in performance or nonperformance of the Contract. This duty to save, defend, hold harmless and indemnify will survive the termination of this Contract. If the Contractor fails or refuses to fulfill its obligations contained in this section, the Contractor must reimburse the County for any and all resulting payments and expenses, including reasonable attorneys' fees. The Contractor must pay such expenses upon demand by the County, and failure to do so may result in the County withholding such amounts from any payments to the Contractor under this Contract.

22. INTELLECTUAL PROPERTY INDEMNIFICATION

The Contractor warrants and guarantees that in providing services under this Contract neither the Contractor nor any subcontractor is infringing on the intellectual property rights (including, but not limited to, copyright, patent, mask and trademark) of third parties.

If the Contractor or any of its employees or subcontractors uses any design, device, work or material that is covered by patent or copyright, it is understood that the Contract Amount includes all royalties, licensing fees, and any other costs arising from such use in connection with the Work under this Contract.

The Contractor covenants for itself, its employees and its subcontractors to save, defend, hold harmless, and indemnify the County Indemnitees, as defined above, from and against any and all claims, losses, damages, injuries, fines, penalties, costs (including court costs and attorneys' fees), charges, liability or exposure for infringement of or on account of any trademark, copyright, patented or unpatented invention, process or article manufactured or used in the performance of this Contract. This duty to save, defend, hold harmless and indemnify will survive the termination of this Contract. If the Contractor fails or refuses to fulfill its obligations contained in this section, the Contractor must reimburse the County for any and all resulting payments and expenses, including reasonable attorneys' fees. The Contractor must pay such expenses upon demand by the County, and failure to do so may result in the County withholding such amounts from any payments to the Contractor under this Contract.

23. COPYRIGHT

By this Contract, the Contractor irrevocably transfers, assigns, sets over and conveys to the County all rights, title and interest, including the sole exclusive and complete copyright interest, in any and all copyrightable works created pursuant to this Contract. The Contractor will execute any documents that the County requests to formalize such transfer or assignment.

The rights granted to the County by this section are irrevocable and may not be rescinded or modified, including in connection with or as a result of the termination of or a dispute concerning this Contract.

The Contractor may not use subcontractors or third parties to develop or provide input into any copyrightable materials produced pursuant to this Contract without the County's advance written approval and unless the Contractor includes this Copyright provision in any contract or agreement with such subcontractors or third parties related to this Contract.

24. OWNERSHIP AND RETURN OF RECORDS

This Contract does not confer on the Contractor any ownership rights or rights to use or disclose the County's data or inputs.

All drawings, specifications, blueprints, data, information, findings, memoranda, correspondence, documents or records of any type, whether written, oral or electronic, and all documents generated by the Contractor or its subcontractors as a result of this Contract (collectively "Records") are the exclusive property of the County and must be provided or returned to the County upon completion, termination, or cancellation of this Contract. The Contractor will not use or willingly cause or allow such materials to be used for any purpose other than performance of this Contract without the written consent of the County.

The Records are confidential, and the Contractor will neither release the Records nor share their contents. The Contractor will refer all inquiries regarding the status of any Record to the Project Officer or to his or her designee. At the County's request, the Contractor will deliver all Records, including hard copies of electronic records, to the Project Officer and will destroy all electronic Records.

The Contractor agrees to include the provisions of this section as part of any contract or agreement related to this Contract into which it enters with subcontractors or other third parties.

The provisions of this section will survive any termination or cancellation of this Contract.

25. DATA SECURITY AND PROTECTION

The Contractor will hold County Information, as defined below, in the strictest confidence and will comply with all applicable County security and network resources policies, as well as all local, state and federal laws and regulatory requirements concerning data privacy and security. The Contractor must develop, implement, maintain, continually monitor and use appropriate administrative, technical and physical security measures to control access to and to preserve the confidentiality, privacy, integrity and availability of all electronically maintained or transmitted information received from or created or maintained on behalf of the County. For purposes of this provision, and as more fully described in this Contract and in the County's Non-Disclosure and Data Security Agreement (NDA), "County Information" includes, but is not limited to, electronic information; documents; data; images; financial records; personally identifiable information; personal health information (PHI); personnel, educational, voting, registration, tax and assessment records; information related to public safety; County networked resources; and County databases, software and security measures that are created, maintained, transmitted or accessed to perform the Work under this Contract.

(a) **County's Non-Disclosure and Data Security Agreement.** The Contractor and its Designees (Contractor Designees shall include, but shall not be limited to, all Contractor-controlled agents or subcontractors working on-site at County facilities or otherwise performing any work under this Contract) must sign the NDA (Attachment D before performing any work or obtaining or permitting access to County networked resources, application systems or databases. The Contractor will make copies of the signed NDAs available to the County Project Officer upon request.

(b) **Use of Data.** The Contractor will ensure against any unauthorized use, distribution or disclosure of or access to County Information and County networked resources by itself or its Designees. Use of County Information other than as specifically outlined in the Contract Documents is strictly prohibited. The Contractor will be solely responsible for any unauthorized use, reuse, distribution,

transmission, manipulation, copying, modification, access to or disclosure of County Information and for any non-compliance with this provision by itself or by its Designees.

(c) **Data Protection**. The Contractor will protect the County's Information according to standards established by the National Institute of Standards and Technology, including 201 CMR 17.00, Standards for the Protection of Personal Information of Residents of the Commonwealth and the Payment Card Industry Data Security Standard (PCI DSS), as applicable, and no less rigorously than it protects its own data and proprietary or confidential information. The Contractor must provide to the County a copy of its data security policy and procedures for securing County Information and a copy of its disaster recovery plan(s). If requested by the County, the Contractor must also provide annually the results of an internal Information Security Risk Assessment provided by an outside firm.

(d) **Security Requirements**. The Contractor must maintain the most up-to-date anti-virus programs, industry-accepted firewalls and other protections on its systems and networking equipment. The Contractor certifies that all systems and networking equipment that support, interact with or store County Information meet the above standards and industry best practices for physical, network and system security requirements. Printers, copiers or fax machines that store County Data into hard drives must provide data-at-rest encryption. The County's Chief Information Security Officer or designee must approve any deviation from these standards. The downloading of County information onto laptops, other portable storage media or services such as personal e-mail, Dropbox etc. is prohibited without the written authorization of the County's Chief Information Security Officer or designee.

(e) **Conclusion of Contract**. Within 30 days after the termination, cancellation, expiration or other conclusion of the Contract, the Contractor must, at no cost to the County, return all County Information to the County in a format defined by the County Project Officer. The County may request that the Information be destroyed. The Contractor is responsible for ensuring the return and/or destruction of all Information that is in the possession of its subcontractors or agents. The Contractor must certify completion of this task in writing to the County Project Officer.

(f) **Notification of Security Incidents**. The Contractor must notify the County Chief Information Officer and County Project Officer within 24 hours of the discovery of any unintended access to or use or disclosure of County Information.

(g) **Subcontractors**. If subcontractors are permitted under this Contract, the requirements of this entire section must be incorporated into any agreement between the Contractor and the subcontractor. If the subcontractor will have access to County Information, each subcontractor must provide to the Contractor a copy of its data security policy and procedures for securing County Information and a copy of its disaster recovery plan(s).

26. ETHICS IN PUBLIC CONTRACTING

This Contract incorporates by reference Article 9 of the Arlington County Purchasing Resolution, as well as all state and federal laws related to ethics, conflicts of interest or bribery, including the State and Local Government Conflict of Interests Act (Code of Virginia § 2.2-3100 et seq.), the Virginia Governmental Frauds Act (Code of Virginia § 18.2-498.1 et seq.) and Articles 2 and 3 of Chapter 10 of Title 18.2 of the Code of Virginia, as amended (§ 18.2-438 et seq.). The Contractor certifies that its proposal was made without collusion or fraud; that it has not offered or received any kickbacks or inducements from any other offeror, supplier, manufacturer or subcontractor; and that it has not conferred on any public employee having official responsibility for this procurement any payment, loan, subscription, advance, deposit of money, services or anything of more than nominal value, present or promised, unless consideration of substantially equal or greater value was exchanged.

27. COUNTY EMPLOYEES

No Arlington County employee may share in any part of this Contract or receive any benefit from the Contract that is not available to the general public.

28. FORCE MAJEURE

Neither party will be held responsible for failure to perform the duties and responsibilities imposed by this Contract if such failure is due to a fire, riot, rebellion, natural disaster, war, act of terrorism or act of God that is beyond the control of the party and that makes performance impossible or illegal, unless otherwise specified in the Contract.

29. AUTHORITY TO TRANSACT BUSINESS

The Contractor must, pursuant to Code of Virginia § 2.2-4311.2, be and remain authorized to transact business in the Commonwealth of Virginia during the entire term of this Contract. Otherwise, the Contract is voidable at the sole option of and with no expense to the County.

30. RELATION TO COUNTY

The Contractor is an independent contractor, and neither the Contractor nor its employees or subcontractors will be considered employees, servants or agents of the County. The County will not be responsible for any negligence or other wrongdoing by the Contractor or its employees, servants or agents. The County will not withhold payments to the Contractor for any federal or state unemployment taxes, federal or state income taxes or Social Security tax or for any other benefits. The County will not provide to the Contractor any insurance coverage or other benefits, including workers' compensation.

31. ANTITRUST

The Contractor conveys, sells, assigns and transfers to the County all rights, title and interest in and to all causes of action under state or federal antitrust laws that the Contractor may have relating to this Contract.

32. REPORT STANDARDS

The Contractor must submit all written reports required by this Contract for advance review in a format approved by the Project Officer. Reports must be accurate and grammatically correct and should not contain spelling errors. The Contractor will bear the cost of correcting grammatical or spelling errors and inaccurate report data and of other revisions that are required to bring the report(s) into compliance with this section.

Whenever possible, proposals must comply with the following guidelines:

- printed double-sided on at least 30% recycled-content and/or tree-free paper
- recyclable and/or easily removable covers or binders made from recycled materials (proposals with glued bindings that meet all other requirements are acceptable)
- avoid use of plastic covers or dividers
- avoid unnecessary attachments or documents or superfluous use of paper (e.g. separate title sheets or chapter dividers)

33. AUDIT

The Contractor must provide to the County the complete findings and all components of an independent certified public accountant's audit of its finances and program operation within two months after the close of Contractor's fiscal year. If a management letter was not prepared with the audit, the Contractor must so certify in writing as part of the audit report to the County. The Contractor must allow the County to review its records as the County deems necessary for audit purposes within 15 calendar days of the County's receipt of the findings. All accounts of the Contractor are subject to audit.

The Contractor must retain all books, records and other documents related to this Contract for at least five years after the final payment and must allow the County or its authorized agents to examine the documents during this period and during the Contract Term. The Contractor must provide any requested documents to the County for examination within 15 days of the request, at the Contractor's expense. Should the County's examination reveal any overcharging by the Contractor, the Contractor must, within 30 days of County's request, reimburse the County for the overcharges and for the reasonable costs of the County's examination, including, but not limited to, the services of external audit firm and attorney's fees; or the County rnay deduct the overcharges and examination costs from any amount that the County owes to the Contractor. If the Contractor wishes to destroy or dispose of any records related to this Contract (including confidential

records to which the County does not have ready access) within five years after the final payment, the Contractor must give the County at least 30 days' notice and must not dispose of the documents if the County objects.

34. ASSIGNMENT
The Contractor may not assign, transfer, convey or otherwise dispose of any award or any of its rights, obligations or interests under this Contract without the prior written consent of the County.

35. AMENDMENTS
This Contract may not be modified except by written amendment executed by persons duly authorized to bind the Contractor and the County.

36. ARLINGTON COUNTY PURCHASING RESOLUTION AND COUNTY POLICIES
Nothing in this Contract waives any provision of the Arlington County Purchasing Resolution, which is incorporated herein by reference, or any applicable County policy.

37. DISPUTE RESOLUTION
All disputes arising under this Agreement or concerning its interpretation, whether involving law or fact and including but not limited to claims for additional work, compensation or time, and all claims for alleged breach of contract must be submitted in writing to the Project Officer as soon as the basis for the claim arises. In accordance with the Arlington County Purchasing Resolution, claims denied by the Project Officer may be submitted to the County Manager in writing no later than 60 days after the final payment. The time limit for a final written decision by the County Manager is 30 days. Procedures concerning contractual claims, disputes, administrative appeals and protests are contained in the Arlington County Purchasing Resolution. The Contractor must continue to work as scheduled pending a decision of the Project Officer, County Manager, County Board or a court of law.

38. APPLICABLE LAW, FORUM, VENUE AND JURISDICTION
This Contract is governed in all respects by the laws of the Commonwealth of Virginia; and the jurisdiction, forum and venue for any litigation concerning the Contract or the Work is in the Circuit Court for Arlington County, Virginia, and in no other court.

39. ARBITRATION
No claim arising under or related to this Contract may be subject to arbitration.

40. NONEXCLUSIVITY OF REMEDIES
All remedies available to the County under this Contract are cumulative, and no remedy will be exclusive of any other at law or in equity.

41. NO WAIVER
The failure to exercise a right provided for in this Contract will not be a subsequent waiver of the same right or of any other right.

42. SEVERABILITY
The sections, paragraphs, clauses, sentences, and phrases of this Contract are severable; and if any section, paragraph, clause, sentence or phrase of this Contract is declared invalid by a court of competent jurisdiction, the rest of the Contract will remain in effect.

43. ATTORNEY'S FEES
The County is entitled to attorney's fees and costs that it incurs to enforce any provision of this Contract.

44. SURVIVAL OF TERMS
In addition to any statement that a specific term or paragraph survives the expiration or termination of this Contract, the following sections also survive: INDEMNIFICATION; INTELLECTUAL PROPERTY INDEMNIFICATION; RELATION TO COUNTY; OWNERSHIP AND RETURN OF RECORDS;

AUDIT; COPYRIGHT; DISPUTE RESOLUTION; APPLICABLE LAW AND JURISDICTION; ATTORNEY'S FEES, AND DATA SECURITY AND PROTECTION.

45. HEADINGS

The section headings in this Contract are inserted only for convenience and do not affect the substance of the Contract or limit the sections' scope.

46. AMBIGUITIES

The parties and their counsel have participated fully in the drafting of this Agreement; and any rule that ambiguities are to be resolved against the drafting party does not apply. The language in this Agreement is to be interpreted as to its plain meaning and not strictly for or against any party.

47. NOTICES

Unless otherwise provided in writing, all legal notices and other communications required by this Contract are deemed to have been given when either (a) delivered in person; (b) delivered by an agent, such as a delivery service; or (c) deposited in the United States mail, postage prepaid, certified or registered and addressed as follows:

TO THE CONTRACTOR:
Jackie Arnett, Executive Director
8161 Maple Lawn Boulevard, Suite 150
Fulton, MD 20759
301-313-2000

TO THE COUNTY:
Nathaniel Wentland, Project Officer
2100 Clarendon Blvd., Suite 601
Arlington, VA 22206

AND

Michael E. Bevis, Purchasing Agent
Arlington County, Virginia
2100 Clarendon Boulevard, Suite 500
Arlington, Virginia 22201

48. NON-DISCRIMINATION NOTICE

Arlington County does not discriminate against faith-based organizations.

49. INSURANCE REQUIREMENTS

Before beginning work under the Contract or any extension, the Contractor must provide to the County Purchasing Agent a Certificate of Insurance indicating that the Contractor has in force at a minimum the coverage below. The Contractor must maintain this coverage until the completion of the Contract or as otherwise stated in the Contract Documents. All required insurance coverage must be acquired from insurers that are authorized to do business in the Commonwealth of Virginia, with a rating of "A-" or better and a financial size of "Class VII" or better in the latest edition of the A.M. Best Co. Guides.

a. Workers Compensation - Virginia statutory workers compensation (W/C) coverage, including Virginia benefits and employer's liability with limits of $100,000/100,000/500,000. The County will not accept W/C coverage issued by the Injured Worker's Insurance Fund, Towson, MD.

b. Commercial General Liability - $1,000,000 per occurrence, with $2,000,000 annual aggregate covering all premises and operations and including personal injury, completed operations, contractual liability, independent contractors, and products liability. The general aggregate limit must apply to this Contract. Evidence of contractual liability coverage must be typed on the certificate.

c. Business Automobile Liability - $1,000,000 combined single-limit (owned, non-owned and hired).

a. Additional Insured – The County and its officers, elected and appointed officials, employees and agents must be named as additional insureds on all policies except workers compensation and automotive and professional liability; and the additional insured endorsement must be typed on the certificate.

b. Cancellation - If there is a material change or reduction in or cancellation of any of the above coverages during the Contract Term, the Contractor must notify the Purchasing Agent immediately and must, with no lapse in coverage, obtain replacement coverage that is consistent with the terms of this Contract. Not having the required insurance throughout the Contract Term is grounds for termination of the Contract.

c. Claims-Made Coverage - Any "claims made" policy must remain in force, or the Contractor must obtain an extended reporting endorsement, until the applicable statute of limitations for any claims has expired.

d. Contract Identification - All insurance certificates must state this Contract's number and title.

The Contractor must disclose to the County the amount of any deductible or self-insurance component of any of the required policies. With the County's approval, the Contractor may satisfy its obligations under this section by self-insurance for all or any part of the insurance required, provided that the Contractor can demonstrate sufficient financial capacity. In order to do so, the Contractor must provide the County with its most recent actuarial report and a copy of its self-insurance resolution.

The County may request additional information to determine if the Contractor has the financial capacity to meet its obligations under a deductible and may require a lower deductible; that funds equal to the deductible be placed in escrow; a certificate of self-insurance; collateral; or another mechanism to guarantee the amount of the deductible and ensure protection for the County.

The County's acceptance or approval of any insurance will not relieve the Contractor from any liability or obligation imposed by the Contract Documents.

The Contractor is responsible for the Work and for all materials, tools, equipment, appliances and property used in connection with the Work. The Contractor assumes all risks for direct and indirect damage or injury to the property used or persons employed in connection with the Work and for of all damage or injury to any person or property, wherever located, resulting from any action, omission, commission or operation under the Contract or in connection in any way whatsoever with the Work. The Contractor's insurance shall be the primary non-contributory insurance for any work performed under this Contract.

The Contractor is as fully responsible to the County for the acts and omissions of its subcontractors and of persons employed by them as it is for acts and omissions of persons whom the Contractor employs directly.

WITNESS these signatures:

THE COUNTY BOARD OF ARLINGTON COUNTY, VIRGINIA

AUTHORIZED SIGNATURE: for

NAME: MICHAEL E. BEVIS
TITLE: PURCHASING AGENT

DATE: 10/18/2016

PRESIDIO NETWORKED SOLUTIONS LLC

AUTHORIZED SIGNATURE:

NAME AND TITLE: Jackie Arnett, Executive Director

DATE: 30 September 2016

ATTACHMENT D

NONDISCLOSURE AND DATA SECURITY AGREEMENT (CONTRACTOR)

The undersigned, an authorized agent of the Contractor and on behalf of Presidio Networked Solutions, LLC ("Contractor"), hereby agrees that the Contractor will hold County-provided information, documents, data, images, records and the like confidential and secure and protect them against loss, misuse, alteration, destruction or disclosure. This includes, but is not limited to, the information of the County, its employees, contractors, residents, clients, patients, taxpayers and property as well as information that the County shares with the Contractor for testing, support, conversion or other services provided under Arlington County Agreement No. 671-15 (the "Project" or "Main Agreement") or that may be accessed through other County-owned or -controlled databases (all of the above collectively referred to as "County Information" or "Information").

In addition to the DATA SECURITY obligations set in the County Agreement, the Contractor agrees that it will maintain the privacy and security of County Information, control and limit internal access and authorization for access to such Information and not divulge or allow or facilitate access to County Information for any purpose or by anyone unless expressly authorized. This includes, but is not limited to, any County Information that in any manner describes, locates or indexes anything about an individual, including, but not limited to, his/her ("his") Personal Health Information, treatment, disability, services eligibility, services provided, investigations, real or personal property holdings and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, social security number, tax status or payments, date of birth, address, phone number or anything that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual, or the record of his presence, registration, or membership in an organization or activity, or admission to an institution.

Contractor also agrees that it will not directly or indirectly use or facilitate the use or dissemination of County information (whether intentionally or by inadvertence, negligence or omission and whether verbally, electronically, through paper transmission or otherwise) for any purpose other than that directly associated with its work under the Project. The Contractor acknowledges that any unauthorized use, dissemination or disclosure of County Information is prohibited and may also constitute a violation of Virginia or federal laws, subjecting it or its employees to civil and/or criminal penalties.

Contractor agrees that it will not divulge or otherwise facilitate the disclosure, dissemination or access to or by any unauthorized person, for any purpose, of any Information obtained directly, or indirectly, as a result of its work on the Project. The Contractor shall coordinate closely with the County Project Officer to ensure that its authorization to its employees or approved subcontractors is appropriate and tightly controlled and that such person/s also maintain the security and privacy of County Information and the integrity of County-networked resources.

Contractor agrees to take strict security measures to ensure that County Information is kept secure; is properly stored in accordance with industry best practices, and if stored is encrypted as appropriate; and is otherwise protected from retrieval or access by unauthorized persons or for unauthorized purposes. Any device or media on which County Information is stored, even temporarily, will have strict security and access control. Any County Information that is accessible will not leave Contractor's work site or the County's physical facility, if the Contractor is working onsite, without written authorization of the County Project Officer. If remote access or other media storage is authorized, the Contractor is responsible for the security of such storage device or paper files.

Contractor will ensure that any laptops, PDAs, netbooks, tablets, thumb drives or other media storage devices, as approved by the County and connected to the County network, are secure and free of all computer viruses, or running the latest version of an industry-standard virus protection program. The Contractor will ensure that all passwords used by its employees or subcontractors are robust, protected and not shared. The Contractor will not download any County Information except as agreed to by the parties and then only onto a County-approved device. The Contractor understands that downloading onto a personally owned device or service, such as personal e-mail, Dropbox, etc., is prohibited.

Contractor agrees that it will notify the County Project Officer immediately upon discovery or becoming aware or suspicious of any unauthorized disclosure of County Information, security breach, hacking or other breach of this agreement, the County's or Contractor's security policies, or any other breach of Project protocols concerning data security or County Information. The Contractor will fully cooperate with the County to regain possession of any Information and to prevent its further disclosure, use or dissemination. The Contractor also agrees to promptly notify others of a suspected or actual breach if requested.

The Contractor agrees that all duties and obligations enumerated in this Agreement also extend to its employees, agents or subcontractors who are given access to County information. Breach of any of the above conditions by Contractor's employees, agents or subcontractors shall be treated as a breach by the Contractor. The Contractor agrees that it shall take all reasonable measures to ensure that its employees, agents and subcontractors are aware of and abide by the terms and conditions of this agreement and related data security provisions in the Main Agreement.

It is the intent of this *NonDisclosure and Data Security Agreement* to ensure that the Contractor has the highest level of administrative safeguards, disaster recovery and best practices in place to ensure confidentiality, protection, privacy and security of County information and County-networked resources and to ensure compliance with all applicable local, state and federal laws or regulatory requirements. Therefore, to the extent that this *NonDisclosure and Data Security Agreement* conflicts with the Main Agreement or with any applicable local, state, or federal law, regulation or provision, the more stringent requirement, law, regulation or provision controls.

At the conclusion of the Project, the Contractor agrees to return all County Information to the County Project Officer. These obligations remain in full force and effect throughout the Project and shall survive any termination of the Main Agreement.

Authorized Signature: Jackie Arnett

Printed Name and Title: Jackie Arnett, Executive Director

Date: 30 September 2016

ATTACHMENT E

NONDISCLOSURE AND DATA SECURITY AGREEMENT (INDIVIDUAL)

I, the undersigned, agree that I will hold County-provided information, documents, data, images, records and the like confidential and secure and protect it against loss, misuse, alteration, destruction or disclosure. This includes, but is not limited to, the information of the County, its employees, contractors, residents, clients, patients, taxpayers, and property as well as information that the County shares with my employer or prime contractor for testing, support, conversion or the provision of other services under Arlington County Agreement No. 671-15 (the "Project" or "Main Agreement") or which may be accessed through County-owned or -controlled databases (all of the above collectively referred to as "County Information" or "Information").

I agree that I will maintain the privacy and security of County Information and will not divulge or allow or facilitate access to County Information for any purpose or by anyone unless expressly authorized to do so by the County Project Officer. This includes, but is not limited to, any County Information that in any manner describes, locates or indexes anything about an individual including, but not limited to, his/her ("his") Personal Health Information, treatment, disability, services eligibility, services provided, investigations, real or personal property holdings, education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, social security number, tax status or payments, date of birth, or that otherwise affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual, or the record of his presence, registration, or membership in an organization or activity, or admission to an institution.

I agree that I will not directly or indirectly use or facilitate the use or dissemination of information (whether intentionally or by inadvertence, negligence or omission and whether verbally, electronically, through paper transmission or otherwise) for any purpose other than that directly authorized and associated with my designated duties on the Project. I understand and agree that any unauthorized use, dissemination or disclosure of County Information is prohibited and may also constitute a violation of Virginia or federal law/s, subjecting me and/or my employer to civil and/or criminal penalties.

I also agree that I will not divulge or otherwise facilitate the disclosure, dissemination or access to or by any unauthorized person for any purpose of the Information obtained directly, or indirectly, as a result of my work on the Project. I agree to view, retrieve or access County Information only to the extent concomitant with my assigned duties on the Project and only in accordance with the County's and my employer's access and security policies or protocols.

I agree that I will take strict security measures to ensure that County Information is kept secure; is properly stored in accordance with industry best practices, and if stored is encrypted as appropriate; and is otherwise protected from retrieval or access by unauthorized persons or for unauthorized purposes. I will also ensure that any device or media on which County Information is stored, even temporarily, will have strict security and access control and that I will not remove, facilitate the removal of or cause any Information to be removed from my employer's worksite or the County's physical facility without written authorization of the County Project Officer. If so authorized, I understand that I am responsible for the security of the electronic equipment or paper files on which the Information is stored and agree to promptly return such Information upon request.

I will not use any devices, laptops, PDAs, netbooks, tablets, thumb drives or other media storage devices ("Device") during my work on the Project without pre-approval. I will ensure that any Device connected to the County network is free of all computer viruses or running the latest version of an industry-standard virus protection program. I will also ensure that my password, if any, is robust, protected and not shared. I will not download any County Information except as authorized by the County Project Officer and then only

onto a County-approved Device. I understand that downloading onto a personally-owned Device or service, such as personal e-mail, Dropbox etc., is prohibited.

I agree that I will notify the County Project Officer immediately upon discovery or becoming aware or suspicious of any unauthorized disclosure of County Information, security breach, hacking or other breach of this agreement, the County's or Contractor's security policies, or any other breach of Project protocols concerning data security or County Information. I will fully cooperate with the County to help regain possession of any County Information and to prevent its further disclosure, use or dissemination.

It is the intent of this *NonDisclosure and Data Security Agreement* to ensure that the highest level of administrative safeguards and best practices are in place to ensure confidentiality, protection, privacy and security of County Information and County-networked resources and to ensure compliance with all applicable local, state and federal laws or regulatory requirements. Therefore, to the extent that this *Nondisclosure and Data Security Agreement* conflicts with the underlying Main Agreement or any local, state or federal law, regulation or provision, the more stringent requirement, law, regulation or provision controls.

Upon completion or termination of my work on the Project, I agree to return all County Information to the County Project Officer. I understand that this agreement remains in full force and effect throughout my work on the Project and shall survive my reassignment from the Project, termination of the above referenced Project or my departure from my current employer.

Signed: _____

Printed Name: _____

Date: _____

Witnessed:

Contractor's Project Manager: _____

Printed Name: _____

Date: _____

PRESIDIO

MANAGED NETWORK SERVICES STATEMENT OF WORK

ARLINGTON COUNTY GOVERNMENT

ARLINGTON
VIRGINIA

June 9, 2016

CONTENTS

1. EXECUTIVE SUMMARY

Presidio will meet Arlington County Government's (ACG's) Managed Network Service requirements through the following tasks and services:

- Presidio Managed Services

  Presidio will provide ACG with Managed Services 24x7x365. During ACG's Department of Technology Services (DTS) business hours, from 7:00 a.m. to 5:00 p.m., Monday through Friday, Presidio will deliver the services onsite. At all other times, Presidio will deliver the services remotely from its US-based geo-redundant service centers.

  Presidio Managed Services includes the following service elements:

  - Service Desk
  - Monitoring
  - Customer Portal
  - Standard Reports
  - Change Management
  - MACD (Move, Add, Change, Delete)
  - Problem Management
  - Patch Management
  - Dispatch Service
  - Carrier Case Management
  - Service Delivery Management
  - Onsite Engineering
  - Service Desk Ticket Integration

  Each device or component (i.e. router, switch, server, etc.) is defined as a Configuration Item (CI). Monitored elements and standard reports for network CIs such as routers, switches, wireless, firewalls, etc., are detailed in Appendix A: Network Management Services.

  Monitored elements, standard reports, typical operations and standard MACDs for unified communications (UC) CIs such as voice gateways, UC servers, IP phones, etc., are detailed in Appendix B: Unified Communication Management Services.

- After-hours Service Desk

  Presidio's After-hours Service Desk will provide the following items after ACG's Department of Technology Services (DTS) business hours:

  - Telephone access to the After-hours Service Desk for any County employee.
  - Manage After - hours Service Requests
  - Provide Tier 1 assistance to inquiries, and escalation to Tier 2 and Tier 3 as needed.
  - Daily coordination conference calls with onsite Presidio personnel.
  - Provide Monthly After - hours Service Desk Report to ACG.

  To provide After-hours support, Presidio may engage its partner and resolver group Allied Digital Services, LLC (Allied).

- Major Project Support

Major Projects will address specific improvements to ACG's Voice and Data Network infrastructure to accommodate the advancements in technology and growth in demand.

2. PRESIDIO MANAGED SERVICES

Presidio Managed Services elements are listed below in this section:

2.1. SERVICE DESK

The Service Desk is the central point-of-contact between ACG and Presidio for daily support activity, including for ACG's IT staff to report disruptions in service and make routine requests for services. Presidio's Service Desk team is staffed 24 hours a day, 7 days a week in two primary Service Delivery Centers (SDCs) located in Orlando, FL and Lewisville, TX.

This service desk activity is used to troubleshoot hardware, software and tools issues that are applicable to the specific service offered ACG. Where applicable for third-party devices and products Presidio will collaborate with the specific Vendor to resolve the issue for ACG. The Service Desk follows a specific Incident Management process to ensure each ticket is categorized with a priority level including business impact and urgency.

The Service Desk will deliver the following Tier 1 through Tier 3 levels of technical support.

- **Tier 1: Technician Support**

  Service Delivery Center Technician (Tier 1) is responsible for initial support of basic issues. Tier 1 technicians follow specific ACG processes as defined by Service Delivery Management. Technicians either resolve the issue or coordinate with Tier 2 engineers for advanced support, maintaining communication with ACG during any escalations.

- **Tier 2: Engineering Support**

  Service Delivery Center Engineer (Tier 2) is responsible for issues that require advanced engineering skills. Tier 2 engineers use defined Information Technology Infrastructure Library (ITIL) process for effective Problem and Change Management as defined by Service Delivery Management. The Tier 2 engineer suggests improvements for device stabilization and potential upgrades. In addition, the engineer interfaces with third-party vendors or Presidio Professional Services to provide timely resolution.

- **Tier 3: Advanced Technical Support**

  Tier 3 professionals are responsible for handling the most difficult or advanced incidents and overseeing problem management.

ACG may communicate incidents to the Service Desk via the following methods (in addition to incidents that the generated by the monitoring tools):

- Opening a ticket on the Customer Portal
- Telephone (P1 Incidents must be opened via telephone into Service Desk)
- Email

Only authorized ACG personnel, as defined in the Runbook (described below), may contact the Presidio Service Desk.

2.1.1 Incident Management

Presidio will perform the following during the management of incidents identified through monitoring of the environment or by direct ACG 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 (if no actual alerts exist)
- Group related relevant events into a single incident to reduce notifications
- Prioritize incidents based on impact and urgency
- Notify ACG of the incident by one or more of the following means:
  - Email
  - Auto-generated notifications to ACG contacts (if desired)
  - Presidio Service Desk
- Restore Service
  - Take ownership of service restoration or remotely assist onsite personnel as needed to facilitate service restoration.
  - Remotely facilitate hardware replacement and software updates that Presidio determines are required.
  - Remotely apply patches to remediate an incident or problem identified by Presidio and handled as a Standard Change (detailed below), if required.
  - Interact with third-party support providers (e.g., Cisco Technical Assistance Center). This requires an ACG-signed Letter of Agency (LOA) processed during the Service Transition Management phase.

2.1.1.1. Incident Prioritization Classification and Prioritization

Incidents receive a classification and prioritization based on the information in the incident log.

- Classification - choosing the correct service offering, category, and subcategory as it pertains to the incident.
- Prioritization – determining the impact and urgency relative to other issues.

2.1.1.2. Impact Definition

The initial impact on the business system is pre-defined from the alerting tool, based on the type of alarm received or ACG 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.

2.1.1.3. 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 ACG request.

There are three levels of urgency:

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

The initial case priority remains until resolution even if the severity of impact lessens. The case also may be left open while operational stability is being assessed.

The incident ticket is closed by Presidio upon issue remediation and the CI is returned to operational stability.

Complete detail for open and closed tickets resides on the Customer Portal and is used to support incident management and problem management processes.

2.1.1.4. 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 a number of factors, as defined in the thresholds).

Incident Priorities

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

Priority Descriptions

Priority Level	Description
● **P1 / Critical**	Systems at one or many ACG sites are completely unavailable. Affected systems cause significant business impact.
● **P2 / High**	Systems at one or many ACG sites are partially unavailable. Affected systems cause some business impact.
● **P3 / Medium**	Operational performance of ACG sites is impaired while most business operations remain functional.

● P4 / Low	ACG is requesting information or a logical change that is covered under their service agreement.

2.1.1.5. Incident Escalation

At any point in the incident management process, ACG may request escalation via the Presidio SDC Supervisor to address concerns about the handling of the incident. If service restoration requires activities by a third-party provider, however, Presidio initiates and manages the process.

If ACG requests escalation to a High Severity (P1 or P2), the SDC will initiate a live handoff to an engineer. If further escalation of an existing ticket or after-hours escalation is required, ACG should request to speak to the SDC Supervisor or Manager.

Upon resolution, Presidio will notify ACG that the incident is resolved and provide ACG with the opportunity to verify that services have been restored satisfactorily before Presidio closes the incident.

2.2. MONITORING

Presidio monitors key events including outages, performance bottlenecks (via thresholds) and security incidents (for security services) from each CI under management. Information about all of ACG's managed CIs is included in the Runbook. A definition of the Runbook and its contents are listed below in this section.

Monitoring includes identifying, diagnosing and remotely resolving events quickly and effectively and keeping ACG up to date throughout the life of the event through regular notifications. The CIs are monitored using either a site-to-site Virtual Private Network (VPN) connection or a dedicated connection provided by ACG.

The Monitoring Framework uses industry-standard management protocols, such as Internet Control Message Protocol (ICMP), Simple Network Management Protocol (SNMP), Hypertext Transfer Protocol (HTTP), and Syslog to remotely monitor CIs under management.

The Monitoring Service requires installation of the Presidio Data Collection Appliance (DCA) on the ACG network. The DCA contains a complete copy of Presidio monitoring tools, including the core monitoring framework software, a local collection database, and over 140 different probes.

The DCA is installed on ACG premises on a single subnet configured with a Secure Socket Layer (SSL) tunnel to the Presidio Monitoring Framework. It is recommended that the DCA be installed within the ACG data center at the network core. The DCA provides the complete hardware, software, and a suite of management applications required for service delivery.

All DCAs supplied as part of the service remain the property of Presidio; ACG must return to Presidio or allow the removal by Presidio of all associated appliances immediately upon expiration or termination of services.

ACG is required to provide timely read and write management access to managed CIs as defined by the Runbook. This includes SNMP, syslog, and other defined protocols as necessary to support services.

ACG 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. ACG must provide support contract details, LOA and all other ACG documentation and authorization required to facilitate incident resolution.

If ACG 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., ACG stocking their own spares (self-insuring), ACG acquiring manufacturer support on a Time and Materials (T&M) basis, or instances of no available manufacturer maintenance and support, ACG must provide a sparing strategy for replacement of CIs, and the replacement and recovery of CI functionality is the sole responsibility of ACG.

2.2.1 Runbook

The Runbook contains key information required to support ACG including, authorized ACG contact information, escalation procedures and change control, CI information, ACG physical locations and the Letter of Agency.

2.2.1.1. ACG Contact Information

The Contact Information section includes names, email addresses, location, the technology each contact supports, contact hours and phone numbers of all authorized ACG contacts who will be opening tickets or interacting with the Presidio support team.

2.2.1.2. Escalation Procedures and Change Control

This section of the Runbook includes distribution email addresses (if applicable), ACG escalation instructions and ACG escalation contacts. It also includes a copy of ACG's Change Control policy.

2.2.1.3. CI Information

Presidio captures the following information for each CI: hostnames, serial numbers, IP address (Loopback), SNMP string, login credentials, physical location, business priority, Cisco SMARTnet or applicable OEM contract information and circuit information.

2.2.1.4. ACG Physical Locations

The Runbook lists the street addresses for all covered ACG sites, including a local point of contact at each site where applicable. Each CI is mapped to the appropriate physical location where it resides.

2.2.1.5. Letter of Agency

The Letter of Agency allows Presidio to work with Carriers on behalf of ACG and is a requirement of the U.S. Federal Communications Commission. A sample Letter of Agency is included as Appendix E: Letter of Agency.

2.3. CUSTOMER PORTAL

Presidio Managed Services includes a Web-based Customer Portal that provides ACG access to information and capabilities with respect to their managed services. Capabilities include:

- 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, incident reports and change requests.
- Viewing status of managed and monitored-only CIs under contract.
- Generating reports for managed and monitored-only CIs under contract.

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

2.4. STANDARD REPORTS

Presidio Managed Services come with a suite of standard reports. Presidio provides reports for managed CIs, including performance, availability, and inventory reports. ACG generates reports using the reporting capabilities and tools in the Customer Portal.

2.5. CHANGE MANAGEMENT

Change Management supports the incident and problem management processes by ensuring that changes to managed CIs are evaluated, coordinated, and communicated to all impacted parties. Presidio will participate in the ACG change management process as a member of the Change Advisory Board (CAB), a group of key ACG stakeholders who provide governance over changes to the IT infrastructure.

Changes fall into three categories:

Standard Changes

A Standard Change is performed to resolve an incident on the affected CI only. A Standard Change does not require Change Advisory Board (CAB) approval. The Presidio Engineer submits a Standard Change request in the incident management system to start the Standard Change Management process.

Planned Changes

A Planned Change requires CAB approval and is executed at a specific time. The change submittal includes the planned effort, test plan and success criteria with a back-out and contingency plan.

Emergency Changes

An Emergency Change is a change that is required to remediate an incident or problem that is the organization's highest priority. All Emergency Changes require ACG approval and CAB approval, which may be obtained without waiting for a regular CAB board meeting.

Emergency Changes are defined as changes that need to be evaluated, assessed and either rejected or approved in a short amount of time with a shortened change request process.

2.6. MOVES, ADDITIONS, CHANGES, DELETIONS (MACD)

MACD is the process for moving, adding, changing and removing hardware and software configuration items (and configurations) in ACG's environment. MACDs can be divided into two categories; i.e., CI-level changes and user changes. MACD is any single activity on an individual covered CI meeting the following criteria:

1. Takes less than 2 hours of time to complete.
2. Does not require planning or design efforts.
3. Does not include any activity with a material operational impact. (i.e., the change cannot affect the normal physical operation of the CI).
4. Is not an upgrade or feature addition.
5. Is not a project or part of a project.

User Change

A User Change impacts a single user-based configuration, including moves, additions, change or deletion – for example, a request to delete a user profile.

The monthly allotment of user MACDs is calculated based on 5% of the total user base. ACG indicated in the RFP that there are 4000 standard users and 30 VIP users. The monthly allotment for user MACDs is 202 per month.

Presidio tracks the user MACD tickets for a 3-month period and notifies ACG of trends. If the average MACD counts are exceeding the target limits, it may show evidence of an operational or training issue Presidio can address with ACG. If no operational issues exist, and the MACD requests from ACG normally exceed the 5% limit, additional MACD allowances can be discussed with Presidio Managed Services.

CI Level (Change to the CI)

CI-Level Changes typically impact multiple users based on the change – for example a request to change a configuration.

Presidio reviews each CI-level request and determines if it falls within the scope of this Agreement. For changes not covered by this Agreement, Presidio provides a separate Contract from Professional Services. MACD support is only provided to equipment specified in the Covered Equipment List (CEL). The CEL includes all of the CIs to be managed under this SOW. A single MACD is defined as one change per CI; multiple changes to a single CI are considered multiple MACDs regardless if it is made on the same service request. Presidio and ACG will collaborate to determine if the activity qualifies as a MACD activity.

Device-level changes include up to two changes per CI per month. Changes are allotted monthly and must be used during the target month of service. Any change allocations remaining at the end of a service month do not roll to subsequent service months.

2.7. PROBLEM MANAGEMENT

Problem Management addresses the root causes of incidents. Problem Management is limited to Priority 1 incidents as requested by ACG.

Problem Management has three major categories:

Primary Control

Primary control identifies a root cause for the problem. The process starts with analyzing available data, identifying and recording problems, and classifying problems according to impact, urgency, and status.

Error Control

Error control takes over when a root cause of a problem has been identified. The error 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 ACG to correct the error by initiating a change via Change Management.

Chronic Problem Management

A Chronic "problem" occurs when more than three closed Incident Reports of any Severity Level are reported during the previous eight consecutive weeks for the same Managed LAN Location or on the same component, as defined by vendor part number. Presidio Managed Services delivery center engineers (Tier 2 & Tier 3 level engineers) review Incident Reports on a weekly basis to identify for AGC and to resolve chronic problems. Changes that are planned to resolve chronic problems are submitted to the Change Review board for approval and scheduling. Chronic problems detected and resolved for other customers are also applied to ACG as required.

2.8. PATCH MANAGEMENT

Patch application to remediate incidents and reduce known vulnerabilities is at the discretion of Presidio and are handled as a Standard Change. Vulnerabilities are defects reported by a manufacturer that have a potential to affect the overall security of the CI and are typically resolved with a software workaround or a patch issued by the manufacturer.

As part of the Patch process, Presidio:

- Reviews manufacturer field notices to determine impact and urgency to ACG's system and existing software levels.
- Remotely applies updates to affected CIs following the Change Management process.

Approved changes are coordinated, planned, and monitored via the ticketing system and the Service Delivery Centers. This allows coordination to minimize the potential for negative impact. The Engineer ensures that relevant stakeholders, including ACG, are notified when the change is complete and tested, after which the change is closed.

If the Patch application requires an upgrade in revision level or impacts dependent technologies, the necessary work is evaluated and may be subject to a separate agreement. If the software component of covered equipment has reached end of support, the equipment is no longer covered by Patch Management.

ACG-requested patches for obtaining additional features or functions are out of scope and must be handled as a separate agreement.

2.9. CARRIER CASE MANAGEMENT

Presidio provides operational handling of carrier cases with third-party data and voice carriers for incident remediation. This enables Presidio to open tickets for ACG with a signed LOA, on behalf of ACG. Presidio manages the case throughout the incident resolution process.

2.10. DISPATCH SERVICES

Through Dispatch Services, Presidio schedules qualified field technicians to replace failed equipment associated with a manufacturer's Return Material Authorization (RMA) form. Prior to the dispatch, Presidio coordinates with ACG to coordinate the timing of the work and access to the service location.

2.11. SERVICE DELIVERY MANAGEMENT

Presidio will conduct Quarterly Business Reviews (QBRs) with ACG contacts. The purpose of the QBR is to evaluate overall performance of the managed environment during the previous quarter and discuss any plans or objectives for the upcoming quarter. During the QBR the following reports will be reviewed as well:

- Chronic Issue and Root Cause Analysis
- Changes for prior period
- Review of Priority 1 and 2 Incidents

2.12. ONSITE ENGINEERING

Onsite engineering services provides business hours helpdesk services and troubleshooting support relating to technologies and solutions covered under this SOW.

2.13. SERVICE DESK INTEGRATION

This element provides for ACG to integrate their service desk to Presidio Managed Services' service desk and ticketing system. The tool used to integrate the ticketing systems is Cisco ServiceGrid. The checklist required to complete the integration is included as Appendix C: ServiceGrid Integration.

3. AFTER-HOURS SERVICE DESK

The After-hours Service Desk will be available to answer a call from any County employee after ACG's Department of Technology Services (DTS) business hours.

After-hours support is limited to Tier 1 issues, the most basic issues that can be solved with little or no analysis. Tier 2 issues are more complex and will be escalated by the After-hours Service Desk staff, based on the prioritized escalation structure. The Tier 1 support matrix and Tier 2 escalation structure will be identified in the Runbook.

Presidio will provide the following items as part of the After-Hours Service Desk:

- Provide Tier 1 assistance on the features, functions and use of hardware and software.
- Identify issues and escalate as necessary (e.g., Tier 2 and Tier 3 escalation).
- Manage and close incidents, including those escalated to third parties.
- Manage After-hours service requests by opening ticket for business hours resolution.
- Conduct a daily coordination conference call with the Presidio Managed Services Team.
- Provide a monthly After-hours Service Desk report to Arlington County.
- Participate in a monthly After-hours Service Desk meeting with Arlington County.

4. MAJOR PROJECTS

Throughout the duration of this contract, ACG will define major projects to address specific improvements to its Voice and Data Network infrastructure to accommodate for advancement in technology and growth in demand. Examples of major projects include Data Network implementation at new sites and future Data Network technology changes such as IPv6, Software defined Network (SDN) and Network Access Control (NAC). ACG's specific needs for major projects will be vetted together with Presidio.

Regardless of the specific project, Presidio uses its Strategic Engagement Framework (SEF) to provide engineering support for major engagements. The following summarizes the eight steps within the SEF that will be used at ACG.

1. Planning

The Planning phase creates a high-level understanding of the business, technical, physical infrastructure, and financial requirements involved in a project, including the preliminary assessment of technology and its potential to meet the business requirements. This helps narrow the field of potential solutions.

2. Requirements Analysis

The team initially collects a set of technical information in order to develop a high-level understanding of technical requirements. Through this step, Presidio develops an initial diagram, equipment list, and scope of services to be provided. Additional planning and design activities are required to refine the design.

Identify Initial High-Level Design Requirements - Review feedback collected in initial meetings to identify the high-level design requirements.

The High-Level Preliminary design starts with a definition of the requirements. Based on those requirements and a general assessment of the organization (users, locations, applications used, etc.), the next step is to determine the general deployment model(s) to use. Next, Presidio will identify additional output from the High-Level Preliminary Design, which may include determining services requirements and estimating project cost based on services and hardware/software.

Perform Initial Audit of Existing Infrastructure Architecture - The lead engineer assesses the current infrastructure to determine the optimal solution architecture approach. This provides a way of highlighting any infrastructure deficiencies in order to mitigate risk during implementation.

Perform Initial Network Analysis - Using available tools, engineers collect data about the network. They evaluate information such as the current state of network and collect data related to the high-level design requirements.

Perform an Initial Hardware and Software Gap Analysis - A hardware gap analysis should address space, power, cabling, conduits, telephony systems, switches, routers, servers, WAN connections including analog and digital voice, and points of demarcation. In addition, Presidio engineers will obtain floor plans and campus maps, including utilities and conduit systems. Deficiencies in infrastructure should be identified and addressed prior to installation. Presidio engineers pay particular attention to ensuring that the cabling infrastructure will support the cut over plans and making sure servers and operating systems, as well as switches and routers with limited resources and capabilities, are identified.

Perform Initial Legacy Integration Analysis - Collect information regarding the potential legacy system integration points for the solution from ACG. Based upon those findings, Presidio

engineers develop the high-level design considerations to allow the new solution to fit into the architecture.

Develop Initial Design - Consolidate high-level design requirements and ACG-specific infrastructure considerations to develop the high-level design. When possible, Presidio will create alternative designs for ACG to consider.

Discuss Design Requirements, Alternatives, and Deliverables - Review the high-level design requirements identified during the interviews with ACG. Discuss design alternatives and ensure Arlington understands the implications of each alternative.

3. Perform Low-Level Site Survey

Conducting a low-level site survey involves assisting in assessing the adequacy of physical infrastructure. The assessment focuses on requirements for space, cabling, conduits, racks, patch panels, power, and HVAC as they pertain to acquiring and deploying a new system. More detailed site surveys will be performed prior to installation during the implementation planning.

Develop Site Specification - Develop a complete floor plan, showing the location of all components including set and jack locations. Presidio provides details of the physical, electrical and environmental requirements required by Arlington in order to prepare the site to accommodate equipment to be deployed. This includes cable specifications, circuit specifications (site to site, ISDN remote access, etc.), and roles and responsibilities (who will be responsible for providing cables - Presidio/ACG etc.)

Survey and Inventory the Network - Engineers assess the logical configuration of the network to identify potential design considerations in the next phase.

Provide for Network Security – Engineers also establish the high-level plan for components that ensure the security and integrity of the system. This must be done in close coordination with ACG's overall network security architecture and system.

4. Technical Design

In conjunction with ACG's technical stakeholders, Presidio evaluates items such as IP and trunking protocols and identifies the materials and supplies needed for Presidio to complete the project. Information gathered in this stage is used to identify specific VLAN structure, IP subnets in use on the network and security policies per ACG's requirements.

In Technical Design, the project team focuses on developing the low-level design that will be followed during the implementation. The team reviews the design and presents the final Low-Level Design to ACG for acceptance.

Presidio often generates a primary and alternative design solution that meets or exceeds the customer's goals and expectations defined during Requirements Analysis. The design should support the customer's business and technical requirements, including security, quality of service (QoS), and system management.

The team makes decisions on:

- How to meet application, support, back-up, and recovery requirements
- Migration strategy, test plans, training plans
- CI configurations (which parameters and features to turn on or off, and which protocols to use).

The team assesses the current state of the network to identify the potential impact of the solution they plan to implement.

Generate a Low-Level Migration or Integration Strategy – Engineers develop the migration or implementation strategy for the final design deliverable. This strategy contains a detailed plan for migration from legacy equipment or for ensuring the solution interoperates with legacy equipment and provides an overview of any upgrades or configuration changes necessary to accomplish the above.

Support Strategy - Finalize the initial support strategy surrounding network monitoring and day-1 and day-2 support based upon additional findings in the Requirements Analysis. Identify and plan proper escalation procedures and processes. Address any requirements identified during the Design phase that may have changed since the initial support plan was created.

Network Security Strategy - Outline the details around components that ensure the security and integrity of the system. This strategy must be validated with the customer's overall network security architecture and system guidelines.

5. Low-Level Design

Create the low-level design (LLD) and solution design specifics. The LLD is the core of the final design deliverable. It provides the proposed solution topology and articulates how the proposed design fulfills the requirements outlined during the planning workshop.

Develop Detailed Solution Design - Use the high-level design requirements to develop the detailed design. The lead engineers outlines the detailed design considerations related to the solution's goals. Typically generated items from this design include the final parts list, network topology diagrams and proposed traffic flows.

6. Detailed Design Review

The project manager, lead engineer and customer review and discuss the details of the design to ensure that all parties are in agreement that the proposed low-level design (LLD) satisfies the business requirements. If requirements have changed, revise to create what should be the final design for developing the implementation project plan. All parties sign off on the new design.

Conduct Integration Analysis - Analyze features and protocols in the low-level design to determine if they will interoperate with the legacy hardware and components that may remain in the network. If interoperability issues are found, make recommendations for resolution and the associated testing. This task may include proof-of-concept testing for selected low-level design features to validate that the low-level design can be accepted into the current environment.

Finalize Detailed Design Documents - Consolidate all the detailed design components, which include hardware, software and support. Prepare the LLD documentation for customer presentation.

Conduct Internal Detailed Design Review – Presidio circulates the LLD within the internal team for quality assurance prior to presenting to the key decision makers.

Present and Get Acceptance of Low-Level Design to Primary Decision Maker - Arrange a design acceptance meeting between Presidio and ACG. Present the final low-level design (LLD) to ACG for acceptance.

7. Configurations

Based on the accepted design documentation, CI configurations are produced for every piece of equipment. These configurations include necessary routing protocols, VLAN's, trunking protocols, security settings, and management infrastructure.

The configurations replicate the functionality provided by the existing equipment. Improvements are made as documented in the findings and recommendations deliverable from the Requirements Analysis phase. Presidio derives all equipment configurations.

8. Implementation Planning

Presidio will use findings from the Design process to develop a high-level implementation plan that covers management of equipment, power and grounding, hardware procedures, and customer implementation expectations. Presidio will develop an implementation plan to coordinate the transition from completing the LLD to initiating the Implement phase.

In planning the implementation the focus is on clarifying the plan established in the Design phase that covers management of equipment, power and grounding, hardware procedures, and customer implementation expectations and confirms the expectations for the installation. Presidio will detail expected traffic flow and vulnerability points of the network and consider these points for testing.

Hold Implementation Planning Meeting - The implementation team (which typically includes the project manager, Managing Consultant and lead engineer) meets with the customer project-team members to discuss the implementation. This meeting provides team members and the customer a forum for confirming timeframes and decision-making processes. The team will discuss and create a plan for completing the following Deployment phase considerations:

- Design confirmation
- Implementation plan
- Migration/integration strategy
- Solution acceptance testing
- Proposed installation dates and caveats
- Customer change control process

5. SERVICE LEVEL OBJECTIVES

Network Operation Performance SLRs

DEFINITION	Provide response to network outage/alarm on 24x7x365 basis according to the Service Level Requirements identified for each category. All performance criteria are to be measured on a per circuit and component basis – criteria are not to be aggregated and averaged for all circuits and network components.

	Time to Notify	Initial Assessment Verbal Report	On-Site Response Time (OSRT)	Resolution – Assuming Access to On-site Spares
During DTS Business Hours	Within 15 minutes of the initial issue	Within 1 hour of initial issue	Within 1 hour of initial issue	Within 2 hours of onsite arrival
After DTS Business Hours for Core, Distribution and Public Safety sites	Within 15 minutes of the initial issue	Within 1 hour of initial issue	Within 4 hours of initial issue	Within 6 hours of initial issue
After DTS Business Hours for all other sites	Within 15 minutes of the initial issue	Within 1 hour of initial issue	Within 4 hours of initial issue	Within 8 hours of initial issue
External Partner Networks & Integrated Services	Within 15 minutes of the initial issue	Within 1 hour of initial issue	As per DTS Business Hours and After DTS Business Hours SLRs	Within 1 hour of issue resolution during DTS Business Hours and within 2 hours in all other instances

Network Administration Services SLRs

DEFINITION	SLR measures the 24/7 monitoring of routers and circuits using either product-specific or proprietary network monitoring and management tools. Pre-scheduled maintenance will be performed according to the published maintenance window schedule, with the ability to reschedule based on network availability requirements based on CAB approval and scheduling.

Network Administration Services SLRs			
Administration Task	**Service Measure**	**Performance Target**	**SLR**
Network Service capacity reallocation or change	Proactive monitoring and preemptive intervention to advise ACG of need to increase capacity.	Sustained avg. daily utilization reaches 60% of installed capacity	98%
MAC– Implement service packs and updates to minor releases*	Elapsed Time, based on CAB approval and scheduling	<4 hours	98.00%
MAC—service addition or change as scheduled under Change Control process	Elapsed Time, based on CAB approval and scheduling	Increases of 10% of installed capacity within 2 months; or Decreases of 10% of installed capacity within 6 months	95.00%

*Major releases or full version upgrades will be performed as a separate professional services project. However, if a full version upgrade is required to solve a security vulnerability that upgrade is included within the Managed Network services scope as long as the upgrade does not require network architecture, design or physical changes.

Network Administration Services SLRs			
Administration Task	**Service Measure**	**Administration Task**	**Service Measure**
Firewall Management Implementation of firewall changes related to changing, adding/deleting firewall rules.	Response Time	Emergencies: ≤2 hours Standard Requests: within normal change control parameters after submission by ACG	99.00%
	Formula	Transactions completed within Performance Target/Total Transactions	
	Measurement Interval	Monitor Continuously, Measure Daily, Report Monthly	
	Source Data	Cherwell Software	

Network Services Satisfaction SLRs

DEFINITION	ACG satisfaction will be measured two times each year.

Network Services Satisfaction SLRs			
Network Services Satisfaction	**Service Measure**	**Performance Target**	**SLR Performance %**
Score	50 Employee Survey Scored out of 5	Score 4 out of 5	80%
	Formula	Average Score for 50 Employees	
	Measurement Interval	Sixth month Thereafter—every year	
	Reporting Period	Seventh month Thereafter—every year	
	Measurement Tool/Source Data	Electronic Survey / Email	

After-hours Service Desk Availability SLRs

Definition	SLR measures the timeframes during which certain Services provided by the After-hours Service Desk must be available to end-users and by which responses to automatically generated After-hours Service Desk Incidents must be achieved.

After-hours Service Desk Availability	Performance Target	SLR Performance %
Password Reset	≤ 15 Minutes	98.00%
Successful Allocation of Incidents to tier 2 Support	≤ 15 Minutes	95.00%
After-hours Service Desk ACD	Availability	99.99%
1) Automated Password Support 2) End-User Support 3) IT Operations and Technical Support	≤ 15 Minutes	99.95%
Formula	Availability (%) = 100% - Unavailability (%) Where Unavailability is defined as: (□Σ Outage Duration × 100%) / (Schedule Time - Planned Outage)	
Measurement Interval	First Month – Measure Daily Thereafter – Measure Daily	
Reporting Period	First Month – Report Weekly Thereafter – Measure Daily	
Measurement Tool/ Source Data	Cherwell Software	

After-hours Service Desk Response Time SLRs

Definition	SLR measures the number of seconds or cycles it takes an end-user to connect with Contractor's After-hours Service Desk representative. Contractor will provide telephone lines in adequate quantity to handle call volume; ACD system(s) to record call date, time and duration information; and electronic interfaces to all systems for monitoring and reporting.

After-hours Service Desk Responsiveness	Service Measure	Performance Target	SLR Performance %
Speed-to-Answer after ACD	Phone Response Time	≤ 30 Seconds	85%
Call Abandonment Rate	Share of calls Abandoned	5%	100%
First Contact Resolution	First Contact Resolution Percentage	75% with ≤ 5% recalls	N/A
Email Response Rate	Email Response Time	< 30 Minutes	98%
Voice Mail Response Rate	Voice Mail Response Time	≤ 30 Minutes	98%
Incident Closure Notice (via email and/or phone)	Elapsed Time	<20 minutes following Incident Resolution	98%
Formula	Number of events per event Type within Performance Target ÷ Total number of events per Type during Measurement Interval = "Percent (%) Attained"		
Measurement Interval	First Month – Measure Daily Thereafter – Measure Daily		
Reporting Period	First Month – Report Weekly Thereafter – Measure Daily		
Measurement Tool/ Source Data	Cherwell Software		

After-hours Service Desk Satisfaction SLRs

Definition	ACG Satisfaction will be measured two times each year.

After-hours Service Desk ACG Satisfaction	Service Measure	Performance Target	SLR Performance %
Score	50 Employee Survey Scored out of 5	Score 4 out of 5	85%
Formula	Average Score for 50 Employees		
Measurement Interval	Six month Thereafter – annually		
Reporting Period	Seven month Thereafter – annually		
Measurement Tool/ Source Data	Electronic Survey / Email		

Fee Reductions

This section defines the circumstances under which the Contractor will be subject to Fee Reductions for failure to achieve the Service Level Requirements (SLRs).

For Network Operation Performance SLRs, "failure" shall mean the failure to meet any of the specific SLRs that relate to the Onsite Response Time (OSRT).

For all After-hours Service Desk SLRs for availability, responsiveness and satisfaction, "failure" shall mean the failure to meet any of the specific SLRs that relate to SLR Performance Percentages.

In each calendar month, there will be no Fee Reduction for the first Network Operation Performance SLR failure or the first After-hours Service Desk SLR failure. If the Contractor has a second failure in a calendar month, ACG will receive a Fee Reduction Credit of $2,000.00. For any subsequent failure in the same calendar month, ACG will receive a Fee Reduction Credit of $2,000.00 per failure occurrence up to a maximum of $4,000.00 in a given month. Failures will not carry over to the next month, and at the start of the next month, there will be another pass for the first failure.

6. SERVICE TRANSITION MANAGEMENT

Service Transition Management is the phased process through which Presidio implements Managed Services. The Service Transition Management process concludes at the start-of-service, as defined in this section. Detailed in the sections below are the steps for transitioning Presidio Managed Services and After Hours Support.

Presidio Managed Services

Project Management and Issue Management

- Kickoff Phase

The Kickoff meeting is scheduled upon full execution of the contract. The start of service is typically 60 days from the kick-off meeting. The Kickoff Meeting is conducted via web or voice conferencing and begins the Kickoff Phase. All phases of Service Transition Management are typically facilitated by Presidio's Regional Project Manager in collaboration with a Presidio Engineer.

The Kickoff Phase includes the following activities:

- Coordinating, scheduling, and executing the Kickoff Meeting.
- Reviewing deliverables included in the Managed Service Contract.
- Reviewing services purchased, as indicated on ACG Purchase Order (PO).
- Aligning Presidio and ACG on all major activities, risks, and milestones
- Reviewing and scheduling a timeline for completing the Runbook and CEL.

- Runbook
- The Runbook, as defined in Section 2.2, is developed and all of the information required to support ACG will be entered. Presidio Monitoring Framework

Implementing the Monitoring Framework includes the following:

- Preparing, configuring, and testing the DCA.
- Shipping DCA to the designated ACG location.
- Remotely assisting ACG with DCA installation.
- Establishing SSL over HTTP connectivity between Presidio and ACG premises.
- Configuring Presidio internal systems in preparation for service delivery.

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

The DCA is configured to monitor Managed CIs per the CEL. During the CI discovery process where the DCA scans the ACG network for the covered CIs, the Presidio PM communicates any discrepancies between identified CIs and requested Managed CIs in the CEL.

- Managed CI Preparation

The Monitoring Service element is dependent upon preparation of managed CIs, including:

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

Presidio will provide a required CI-specific configuration, including community strings and host destination addresses.

- Setup and Modeling of the Application

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

- Remote Training Session

The Presidio PM schedules one remote training session. The session is conducted via WebEx provided by Presidio.

The objectives of the training session are to review:

- Services to be delivered
- Service documentation
- Presidio and ACG responsibilities during the service delivery process, including those detailed in Appendix D: Remote Management Tasks
- Processes for obtaining service
- Service escalation process
- Customer Portal overview
- Change Management process
- Service level reporting
- Service deliverables, review meetings and scheduling

- Start of Service (SOS)

The SOS milestone begins the Managed Services Term and is contingent on the timely completion of the Runbook and the Service Transition Management phase.

Notification/Escalation and Event Management do not begin until a detailed operations handover has been performed, all required documentation and procedures are put in place, and the Monitoring Framework is successfully detecting and reporting events.

At the mutually agreed-upon start date, the Presidio PM and ACG execute a Certificate of Acceptance, concluding the Service Transition Management phase, and the Service Delivery phase commences.

Risk Management and Mitigation

The ACG Risk Management Plan will contain a thorough description of the Risk Management Process for resolving transition issues. The majority of this process occurs while defining the mitigation during the planning phase.

The Risk Management Plan deliverable is created during the planning phase and is reviewed and approved by ACG prior to project implementation. Mitigation Plans established in the Risk Management Plan are documented in the Project Workbook and become a part of the Project Management Procedures.

- Approach

The Risk Management Process assesses what can go wrong on the project (risks), determines which risks are important, and defines and implements strategies to deal with those risks. It is a continuous process and all ACG project team members have the responsibility to identify potential risks.

The Risk Management process has the following major steps:

- Identify potential risks
- Analyze the identified risks to ensure they are valid and provide information about what the impact may be
- Response Planning: determine how to react to or mitigate the risk
- Monitor and Control: monitor risks and response actions

Risks are classified into the following categories: functional, schedule, quality, resource, and cost.

Each identified risk can have one or more identified areas of impact. For example, a single risk can have a low impact on schedule but a high impact on cost. These impacts are combined with the probability to calculate the overall severity of the risk (risk exposure).

- Managing the Plan

The Presidio PM will monitor the Risk Management Plan and the corresponding mitigation plans to ensure that they are being executed successfully. If it is determined that the risk is not being successfully mitigated, new activities will be added, and an escalation will occur within Presidio management and, if required, any subcontractor's management. Presidio management includes the Manager of the Project Management team, the Sr. Director of Service Delivery and members of the Managed Services executive team (VP of Service Delivery and VP of Operations).

The Presidio PM also performs periodic evaluations to identify new risks that may arise as the project progresses. **Transition Reporting**

The Presidio PMO has various reporting responsibilities during ACG's transition to Managed Services. These reports include, but are not limited to those described in Exhibit 18.

Exhibit 18. Sample Transition Reports

Report	Content
ACG Weekly Report	• Runbook completion • Status of work completed during current period • Work scheduled for completion for the coming period • Risks/Dependencies related to meeting timeframes • Technical issues requiring attention • ACG issues requiring attention
Asset Management Report (Time of Ship)	• Asset Information • Validate that inventory in contract is visible via Managed Service toolsets
Warranty/Maintenance Record Log (Monthly)	• List of all warranty and maintenance calls and their resolution
Testing Record Log (Monthly)	• List of all testing performed and associated results
System Documentation (As necessary)	• All product documentation • Design documentation • As-built drawings • Training materials

Quality Assurance Process

Presidio's Quality Management (QM) approach establishes goals, processes, and responsibilities required for implementing effective quality project management functions. Implementation of and compliance with the ACG quality management approach is the shared responsibility of all ACG project personnel.

Quality metrics are reviewed on an ongoing basis and monitored for trends that may indicate work product quality issues. Action plans are put in place to address any issues.

- Ongoing Program/Project Manager QA Methods

The Presidio PM will monitor key exception metrics on a daily, weekly and monthly basis. Anomalies may result in change to process, staff or skill composition and management tools. The Presidio PM has significant latitude in constructing performance-enhancing actions, including through the following methods:

- Weekly staff meetings to review root cause analysis and actions taken on high impact problems. Problem ownership is clearly defined and resolution dates established.

- Monthly management reviews focused on overall quality results and trends. Issues (potential new project change requirements and existing operational problems) and potential action plans are analyzed and reviewed. New project enhancements are researched, root cause techniques are performed, alternatives are developed, cost/benefit analysis is performed and recommendations are presented to Project Management.

- The Presidio PM is responsible for program actions that enhance productivity through the contract duration. Formal plans are developed and administered that lower cost or improve contract service.

- The Presidio PM can schedule and chair regular operational reviews with ACG management; and ACG, depending upon the status of the project, may request additional formal Reviews.

- Internal Ongoing Reviews

These reviews provide the Presidio PM and the ACG Project Team with an assessment of the project status. Presidio management and subject matter experts that are not involved in or associated directly with the project conduct the formal reviews.

The review team presents the results of all Quality Assurance Reviews to the Presidio PM, who is required to immediately institute a corrective action plan to resolve any reported issues. The progress and success of the action plans are documented and become a part of the next review.

Acceptance Procedures

Presidio and ACG will agree upon activities or events that need to take place for ACG to accept project deliverables and solutions. Upon acceptance, ACG will sign a Ready For Use (RFU) document. Specific acceptance events will be made a part of the Project Management Plan as well as the Project Workbook.

After Hours Support

Project Management and Issue Management

- Transition Methods/Phases

Implementation of the Service Desk solution takes from 4 to 8 weeks depending on the size, scope and complexity of the transition. Resource availability, transition requirements and timing will affect activities.

- Discovery

The Discovery activities determine requirements and identify project resources, systems and all related data required to fully understand and support the ACG environment. This phase takes approximately 5 business days to complete.

Technical implementation discovery results are used for strategic planning and modification of service-delivery requirements. In general, the requirements analysis will include the following tasks:

- Validating current processes and the proposed processes and assumptions
- Identifying all processes and sub-processes related to current support
- Creating a process-flow diagram for each process and sub-process
- Assigning estimated cycle times for each process task, if beneficial
- Analyzing the process for potential improvement areas
- Developing process modifications/improvements

- Standard Operating Procedures (SOP)

Understanding existing procedures and identifying un-documented procedures is an important step toward ensuring that we can perform according to ACG requirements. Thus, all activities must be defined and documented in Standard Operating Procedures (SOP). The duration of this activity varies depending upon the maturity of existing documentation. We recommend that at least 90% of all defined support activities have a corresponding SOP prior to "go live".

- Supported Hardware & Software

Obtaining a list of all hardware and software requiring support is essential so that the corresponding SOPs, configuration details, warranty, maintenance contracts and other alternative support options can be documented and available to Service Desk agents.

- Communications Plan

The Communications Plan is developed collaboratively between ACG and Presidio, and defines how communication will occur between ACG and the Service Desk. Escalations, reporting requirements, and weekly and monthly meetings are included in the Communications Plan.

- Staffing

Ramp-up time for staffing is expected to take up to 3 weeks.

- Live Call Testing – Solution Shadow

ACG's and Presidio's PMs will collaboratively design the approach and parameters for testing live calls and personnel shadowing.

- Characterization Period

Characterization is the period between the Go-Live date and the Service Desk moving into steady state. Steady state is achieved once call processing, severities, priorities and escalations are fined tuned based on actual ACG call handling activity. During the Characterization period, call duration and other OLA's and SLA's will be measured and reported, but penalties will not be imposed. Characterization will not exceed 90 days.

- Typical Deliverables for Completion of Characterization Period

Completion of the Characterization Phase and full start of service will occur when the following Deliverables are completed:

- Category, Type and Item (CTI)– defined, documented and configured within Incident Management System
- Proposed Escalation Groups (resolving groups) – defined, documented and configured within Incident Management System
- Standard Operating Procedures – defined and documented for at least 90% of CTI's. (Remaining 10% of CTI's will be defined and documented within 30 days post start of service.)
- Phone line activated and tested
- Call routing from ACG number to Service Desk activated and tested
- Voice recordings setup
- Email routing setup and tested
- VIP users identified
- Standard Status Reporting and SLAs are accepted
- Continuous Process Improvement (CPI) meetings have commenced
- Acceptance of these and any other Deliverables have been agreed to and documented.

Transition Reporting (Type and Frequency)

The Presidio PMO has various reporting responsibilities during ACG's transition to the After-Hours Service Desk. These reports include, but are not limited to those described in Exhibit 18.

7. ACG RESPONSIBILITIES

Presidio suggests ACG provide a dedicated staff member for 8-16 hours, weekly, for the first two months starting with the kick off meeting. This person would assist with the Runbook completion, including validating escalation paths, personnel and contact information, correlating efforts between ACG and Presidio, testing the processes, optimizing processes after tests, and assisting with orientation to the Managed Services portal. Additional ACG responsibilities follow.

- Install Monitoring Framework

    - Provide an 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 personnel to support the installation of the DCA. These activities include:
        - Installing the DCA in a suitable equipment rack and connecting to network.
        - Turn on the Power to the DCA and confirm the connection of the DCA to the Uninterruptible Power System (UPS) or other facility with continuous uninterrupted power.
        - Notification to Presidio that installation is complete.
    - Provide suitable commercial power. Presidio recommends that ACG provide UPS or other acceptable power back-up facilities providing a minimum of 1kVA dedicated to each appliance.

- Training

ACG shall identify trainees and trainee contact information for the remote training sessions defined in the Presidio Managed Services, Project Management and Issue Management sections above.

ACG will train all Presidio staff on ACG After-hours support SOPs, Communications Plan, Supported Hardware and Software as well as other unique aspects of ACG environment. This training will be conducted remotely and facilitated collaboratively by ACG designated contacts. The purpose of the training is to ensure the After-hours support team knows how to handle After-hours calls including what items they can resolve and what items should be escalated to ACG IT staff. If desired by Presidio and ACG, multiple sessions may be conducted to fine tune the After-hours call handling procedures.

- Transition Management

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

- Assign an ACG PM or equivalent to represent ACG during the Service Transition Management phase.

- Assign a Technical Lead or equivalent to assist Presidio with establishing the network access required for Managed Services.
- ACG PM and Technical Lead must attend the Project Kickoff Meeting and training sessions.

- Runbook

ACG is responsible for providing information included in the Runbook, as defined in Section 2.2.1.

- Communication and Change Management

Presidio has a co-management approach to Managed Services, allowing ACG and other ACG-approved vendors to retain access to Managed CIs. Because multiple parties can make changes to the environment, Presidio requires anyone with access to ACG'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.

ACG will:

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

8. STAGING & WAREHOUSING

ACG may leverage Presidio's Fulton, Maryland warehouse facility for receiving product shipments prior to Presidio integration projects for up to 30 days with no storage cost to ACG. Use of the warehouse requires signature of the Storage Agreement, with the three most pertinent points of the agreement being:

- ACG ownership of the equipment upon receipt at the warehouse
- ACG payment for the equipment on net 30 terms
- ACG payment for shipping from the warehouse to the ACG-designated final destination.

It is not Presidio's intent to use anything but the Fulton facility. However, from time-to-time the Fulton warehouse could be fully occupied. If the Fulton warehouse is full or otherwise unable to receive ACG shipments, Presidio will offer an alternate storage facility with a monthly, per-pallet charge of $60.00. All other terms of the Storage Agreement will apply to the alternate site.

APPENDICES

The following Appendices are separated into the following sections:

1. **Remote & Onsite Managed Services included in this SOW:**

Appendix A: Network Management Services
Appendix B: Unified Communication Management Services
Appendix C: ServiceGrid Ticket Integration
Appendix D: Remote Management Tasks
Appendix E: Letter of Agency

APPENDIX A: NETWORK MANAGEMENT SERVICES

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

Network Management

Network Management service provides monitoring and management of ACG's network infrastructure.

The Service Offering covers and supports Core Switches, Routers, WAN Accelerators, Data Center Networks, LAN Switches, and Wireless APs and Controllers.

Security Device Management

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

A key aspect to Security CI Management is administration and monitoring at the CI 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 Engine.

Network Services Monitoring

The Network Management and Security Device Management Services include standard CI-level monitoring, as well as advanced network-specific monitoring.

The following are examples of the standard monitoring elements for the Network and Security Device Management Managed Services. Further content can be provided upon request.

Operational Status\System Uptime

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

STANDARD REPORTS

Customer Portal allows Standard reports to be viewed and scheduled for automatic report delivery. Customer Portal also allows ACG to build reports based on monitored parameters; these can also be scheduled for automatic delivery. The Standard Reports include four pre-configured reports, and data is retained for 6 months.

Exhibit A-1. Customer Portal for Network Management and Security Device Management Services Reports

Title	Description
CI 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.
Custom Reports	If custom reporting is desired, Presidio Managed Services can be engaged for report development using elective/optional services and will be scoped separately.

NETWORK AND SECURITY SERVICES MANAGEMENT

In addition to the details in the Contract on Presidio's Standard services, Exhibit A-2 specifically applies to the Network Management and Security Device Management Services.

Exhibit A-2. Network Management 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. CI-based backups are not performed for Monitored-Only or Vendor Managed devices.
Moves, Adds, Changes, and Deletions (MACDs)	Change Management is offered for Moves, Adds, Changes and Deletions (MACDs). The following are examples of typical CI-level MACDs: Router interface changes Firewall ACL modifications Switch port configurations Wireless access-point definition (lightweight)

APPENDIX B: UNIFIED COMMUNICATION MANAGEMENT SERVICES

The Presidio Unified Communications Management Service (UCMS) delivers support for a full range of collaboration services for Cisco unified collaboration, video, and third-party devices and applications.

UCMS Monitoring

UCMS includes standard CI-level monitoring as well as advanced collaboration-specific monitoring.

The following are examples of the standard monitoring elements. Further content is available upon request.

- Operational Status\System Uptime
- CPU Statistics
- Memory Statistics
- Hardware Environmental Status
- Interface Statistics
- SNMP Down

UCMS – Cisco-Specific Monitoring

In addition to the standard monitored elements above, UCMS provides advanced monitoring of the Cisco UC solution. Exhibit B-1 lists the elements in our current toolset that we 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.

Exhibit B-1. Monitored Toolset Element

Title	Description
CI Statistics	Gateways – Status, Reachability, Busy Call Attempts Gatekeeper - Out of bandwidth issues – video Phones – registered phone discrepancy Dial Plan – Route Group, Route List, Route Pattern, Trunk Status
Cisco Server Hardware	Disk, Fan, Power Supply, Temperature, Fan, 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 SNMP TFTP
Unity Alerts	Critical Events Failover Service Failure Unity Port Max Unity Ports Not Registered
CallManager Alerts	CallManager Down Database Failure Heartbeat Issues CTI Manager Down Backup Service Failure SNMP Failure Syslog Failure

Title	Description
CCM Cluster Alerts	CDR/CMR Database Issues Gateway registration issues
CCM Server Alerts	Process issues CPU Utilization Disk Partition Utilization SQL/Database Issues
TFTP Alerts	TFTP Port/Network issues TFTP Service Failure

STANDARD REPORTS

Our UCMS Service includes two levels of reporting. First, we include a network CI-level reporting interface on our Presidio Customer Portal that allows Standard reports to be viewed and scheduled for automatic report delivery. Customer Portal also allows ACG to build reports based on monitored parameters of the network level CIs; these can also be scheduled for automatic delivery. Standard Reports include four pre-configured reports and data are retained for 6 months.

In addition to Customer Portal reports, the following Collaboration Reports are provided monthly, shown in Exhibit B-2.

Exhibit B-2. Collaboration Reports

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. For example: 12 x 5-minute calls (60 minutes) divide by 10-minute sampling period = 6 channels occupied, or 12 x 5-minute calls (60 minutes), divide by 1-hour sample period = 1 channel occupied. Calls originated outside the sampling period are also counted, but only for part of the call, which falls within the period.
Trunk Summary	Overall trunk availability Trunk availability Impacted trunks Trunk down time Trunk outages Trunk degraded time Trunk utilization Trunk busy hour Trunk busy hour by percentage Trunk call types
Call Failure Report	Calls attempted - 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. Calls completed - A call completed is a call successfully processed by a PBX and terminated with a disconnect cause code that indicates graceful termination. Calls rejected - 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. Call failures - 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. Call failure ratio - The call failure ratio is the percentage of processed calls that failed. Calls processed - A processed call is a call attempt that is processed by a PBX regardless whether the call completed successfully or not. Disconnect cause code - The disconnect cause code indicates why a call terminated abnormally. It may be attributed to either the origination or destination device. Report data - Calls with an origination time within the reporting period.

Title	Description
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	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. Overall route pattern availability Route pattern availability Impacted route patterns Route pattern down time Route pattern outages Route pattern degraded time
Custom Reports	If custom reporting is desired, Presidio Managed Services can be engaged for report development using elective/optional services, which are scoped separately.

UCMS SERVICE MANAGEMENT

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

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. CI-based backups are not performed for Monitored-Only CI's.

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

Standard Services

Exhibit B-3 lists of the typical operations performed by our SDC for UCMS ACG.

Exhibit B-3. SDC Typical Operations

Device	Task
CER	DB Replication
CER	CER troubleshooting (phone tracking, ERL mapping)
CER	Integration with CUCM troubleshooting
CME	General Troubleshooting
CME	Hardware replacements
CME	Integration with CUCM troubleshooting
CUC	Call handler troubleshooting
CUC	Subscriber troubleshooting
CUC	DB Replication
CUC	Failover troubleshooting
CUC	Integration with CUCM troubleshooting
CUCM	IP Phone troubleshooting
CUCM	Jabber Client troubleshooting
CUCM	Dial plan troubleshooting
CUCM	Resource troubleshooting (Xcode, MTP, Conf)
CUCM	DB Replication
CUCM	Backup and Disaster Recovery troubleshooting
CUCM	Debugging calls on gateway
CUCM	Call failure troubleshooting
CUCM	Troubleshooting Basic QoS (limited to managed components only)
CUE	Hardware replacements
CUE	Integration with CME troubleshooting
CUPS	Subscriber troubleshooting
CUPS	DB Replication
CUPS	Failover troubleshooting
CUPS	Configuration issues
CUPS	Integration with CUCM troubleshooting
UCCX	CAD\Supervisor Client troubleshooting
UCCX	Inbound calling troubleshooting
UCCX	Outbound campaign troubleshooting
UCCX	Call Recording Troubleshooting
UCCX	DB Replication
UCS	Upgrades - Firmware - In response to a bug or vulnerability
UCS	Hardware replacements - Drives

Exhibit B-4. CI-Level Change Examples

Device	Task
CER	CER Configuration (ELIN, ERL, alerts, etc.)
CME	Configuration (dial-peers, hunt lists, other dial plan elements)
CUC	Bulk changes to subscribers
CUC	VM distribution lists
CUC	Auto attendant routing changes/menu structure changes

Device	Task
CUC	Uploading licenses
CUC	Auto attendant schedule changes
CUC	Call Handler Configuration
CUC	Scheduling, TOD routing
CUCM	Translation pattern adds/changes/deletes
CUCM	New DID assignments using number expansion
CUCM	New call blocking configurations on H323/SIP gateways
CUCM	Adding to or modifying existing call blocking configurations
CUCM	Codec manipulations
CUCM	Bulk changes to phones/users
CUCM	Building new hunt groups
CUCM	Music on Hold changes
CUCM	Uploading licenses
CUCM	Uploading new firmware
CUCM	Changes to gateways
CUCM	Generating simple CDR reports (few numbers, narrow date range)
CUCM	Creating/modifying Forced Authorization Codes/Client Matter Codes
CUCM	Translation pattern adds/changes/deletes
CUCM	Dial plan configuration
CUCM	License Activation
CUCM	Backup and Disaster Recovery Setup
CUCM	Minor updates/patching (elective, on request - no new features)
CUE	Configuration (auto attendant scripting, voicemail subscribers, etc.)
UCCX	Skill group assignments
UCCX	Team assignments
UCCX	Script modifications (holidays, hold music)
UCCX	Minor script changes (TOD Routing, trigger additions etc.)
UCS	Upgrades - Firmware - On request/coinciding with application patching
Voice GW	Dial-peer configuration
Voice GW	SIP Configuration changes (SIP Profiles, Translations, etc.)

Exhibit B-5. User MACD Changes Examples

Device	Task
CME	Create user/ephone/DN
CME	Add DN to existing hunt group
CUC	Setup/decommission voice mail
CUC	Change existing subscribers
CUCM	Create users/CIs/profiles
CUCM	Assign directory numbers
CUCM	Delete users/CIs/profiles
CUCM	Move users/CIs/profiles to new phone number
CUCM	Change existing users/CIs/profiles
CUCM	Add users to/remove users from existing hunt groups

Device	Task
CUE	Create/Modify/Delete CUE Subscribers
UCCX	Assign skill to agent
UCCX	Add agent to team
UCCX	Create/modify/delete agents

APPENDIX C: SERVICE GRID INTEGRATION

Service Summary

Presidio will deploy a business-to-business (B2B) Connection to enable ACG Service Management System to connect to Presidio's ITSM (Information Technology Service Management) instance to allow for bi-directional incident communication. Presidio utilizes the Cisco Systems Ecosystem Manager Managed B2B Connection Deployment Service to support the implementation of Cisco ServiceGrid Standard Workflows. Presidio will manage the workflow for the installation of the product utilizing both ACG and Cisco resources.

Location of Services

Services are delivered remotely to Customer.

Managed Connection: Cisco manages Cisco ServiceGrid Deployment Service Ecosystem Manager

Kick-Off Meeting

Presidio Responsibilities

Schedule a one (1) hour remote kick-off meeting with Customer and Cisco. This meeting is intended to initiate the project, review project scope, introduce the project team and commence project planning and will include the following:

- Review project schedule and timeline with Customer and Cisco
- Review configuration with Customer and Cisco and provide recommendations if system requirements are not met Compile and distribute project kick-off meeting minutes.

Customer Responsibilities

- Ensure appropriate people resources are available to participate in the kick-off meeting (including) technical resources
- Review project schedule and timeline with Presidio
- Review configuration with Presidio to ensure system requirements are met
- Read project kick-off meeting minutes and provide feedback
- Participate in status meetings with Presidio
- Review Project Plan with Presidio for accuracy
- Review project status meeting minutes and provide feedback to Presidio

Specification and Implementation Presidio Responsibilities

- Schedule up to 4 remote specification meetings (maximum total duration of 12 hours) with Customer and Cisco
- Create and update specification document to provide one B2B Connection. This includes a high level architectural overview as well as the functional and technical specification that meets the following requirements:
  - A Standard Cisco ServiceGrid Core incident, problem, change or request process that leverages up to 12 transactions.

- Cisco ServiceGrid Core Standard Workflow that supports agreed upon configurations for data mappings, error handling, event based triggers and notifications
- A transport method using post via HTTPS (Secure Hyper Text Transfer Protocol) POST or SOAP (Simplex Object Access Protocol) using Push/Pull method for both ITSM connections

- Standard Authentication: username and password within the SOAP envelope or Basic Authentication for HTTPS POST
- Request final acceptance for the specification document
- Create and update Acceptance Test Plan for the implementation
- Request final acceptance for the Acceptance Test Plan

Customer Responsibilities

- Ensure appropriate people resources are available to participate in the specification meetings
- Review specification document and provide feedback
- Review and approve final detailed specification document
- Review and approve Acceptance Test Plan
- Review and accept the Go-Live plan
- Receive declaration of testing readiness and prepare for testing

Testing

Presidio Responsibilities

- Schedule up to 6 remote testing meetings (maximum total duration of 16 hours) with Customer and Cisco. Testing Meetings are conducted in order to track the progress of testing, report on progress to plan, and document the status.
- Complete testing and prepare for go-live readiness by performing the following: Define defects that were detected during testing, and identify the defects that can and cannot be fixed during the testing phase.
- Classify defects into four classes:
  - Class 1 "critical": Non-availability of contracted Cisco ServiceGrid services or major functions for the Customer. This defect will delay go-live original date. It includes: a) system freeze without recovery b) loss of data c) destruction of data, d) incorrect results during time critical processing of mass data.
  - Class 2: "major": Service partly not available but basic functions are available. This defect will not affect go live if all parties agree to fix immediately after go live. It includes: a) incorrect or inconsistent data processing, b) slow system performance.
  - Class 3: "minor": Agreed and documented functions are not available, but do not disturb daily operations significantly. This defect doesn't delay go live and can be fixed after go live. It includes: a) wrong error messages, b) a program is in a waiting state and can only be reactivated manually.

- Class 4: "trivial": The system is not affected and the documented functions are available. The error can be bypassed without any effect on the user. This defect doesn't delay go live and can be fixed after go live. It includes: a) duplicated screen messages, b) error in documentation, c) typos.

- Declare testing finished and assess Go Live readiness
- Request final acceptance for the implementation
- Update and distribute technical implementation documentation

Customer Responsibilities

- Prepare, participate, and contribute to testing meetings.
  - Provide feedback on testing results
  - Review and provide feedback on the testing progress report.
- Perform acceptance testing and, provide test plan and results. o Review and accept the Acceptance Test Plan Document.
  - Participate in the execution of the Acceptance Test Plan providing any applicable feedback
  - Review and agree to classification of defects
- Send acceptance for implementation to project team
- Receive updated technical implementation documentation and provide feedback

Go Live

Presidio Responsibilities

- Hand-over Cisco ServiceGrid support and standard operating procedures information to Customer support and operations
- Hand-over implementation and Customer support and operations information to Cisco ServiceGrid support (Incident/Problem/Change Management) and to Cisco ServiceGrid Operations (Availability/Capacity/Continuity Management)
- Go-Live meeting is conducted in order to take the project live
  - Invite and moderate the go-live meeting
  - Compile and distribute go-live meeting minutes
  - Compile and distribute go-live note
- Request final acceptance for the project
- Receive acceptance and trigger post project assessment
- Conduct post project assessment meeting
  - Invite and moderate post project assessment meeting
  - Compile and distribute meeting minutes of post project assessment meeting

Customer Responsibilities

- Hand-over Customer support and operations information to Presidio

- Prepare and participate in the go-live meeting by performing the following:
  - Ensure appropriate people resources are available to participate in the go-live meeting
  - Go-Live Meeting is conducted in order to take the project live
  - Contribute to go-live meeting
  - Review go-live note and provide feedback
  - Read go-live meeting minutes and provide feedback
- Verify deliverables against acceptance criteria and provide feedback
- Send final acceptance to Presidio project team
- Contribute to post project assessment meeting
  - Participate in post project assessment meeting
  - Read post project assessment meeting minutes and provide feedback

Deliverables

- Kick-off PowerPoint containing all updates from actual project kick-off meeting
- All-hands Remote project status meeting
- Project status meeting task list
- Specification Document
- Test Plan Document
- Cisco ServiceGrid Setup, access to case tracking
- Go Live Plan
- Email declaration of testing readiness
- Validation of Implementation against Test Plan
- Email declaration of Go Live readiness
- Technical documentation of Implementation
- Cisco ServiceGrid Support and Standard Operating Procedures Information Document
- Smoke test ticket
- Email note of Go Live
- Post Project Assessment PowerPoint

General Customer Responsibilities

- All information (such as but not limited to: designs, topologies, requirements) provided by Customer is assumed to be up-to-date and valid for the Customer's current environment. Services are based upon information provided to Presidio by Customer at the time of the Services.
- Customer acknowledges that the completion of Services is dependent upon Customer meeting its responsibilities as indicated herein.
- Identify Customer's personnel and define their roles in the participation of the Services. Such personnel may include but is not limited to: architecture design and planning engineers, and network engineers.

- Ensure Customer's personnel are available to participate during the course of the Services to provide information and to participate in scheduled information gathering sessions, interviews, meetings and conference calls.
- Support services provided by Cisco to Customer on behalf of Presidio comprise technical advice, assistance and guidance only.
- Customer expressly understands and agrees that the Services shall take place and complete within ninety (90) calendar days from issuing a Purchase Order to Presidio for the Services herein. **Invoicing** Services will be invoiced upon completion of the Services. **Completion of Services** Presidio will provide written notification upon completion of the Services to Customer. The Customer shall within five (5) Business Days of receipt of such notification provide written acknowledgement of Presidio's completion of the Services. Customer's failure to acknowledge completion of the Services or to provide reasons for rejection of the Services within the five (5) Business Day period signifies Customer's acceptance of completion of the Services in accordance with this Service Description.
- **B2B Connection** connects an ITSM application or system to the Cisco ServiceGrid Core to enable the automation of a contracted process including data, attachments and status exchange transactions associated with a defined workflow.
- **Cisco ServiceGrid** is an integration platform in the cloud that seamlessly connects Customers to enable real time multi-party support collaboration for key workflow processes including but not limited to service request, incident, change and problem management.
- **Cisco ServiceGrid Core** is a standard component that provides a set of well-defined standard definitions to support service request, incident, change, and problem management workflow processes. Each Customer and Ecosystem Trading Partner can leverage Cisco ServiceGrid Core to create standardized integration, workflow and data mappings to other Ecosystem Trading Partners.
- **Ecosystem** consists of a Customer and at least one Ecosystem Trading Partner collaborating and managing ITSM service cases.
- **Ecosystem Trading Partner** is the general term for a Customer's business partner that has an active B2B Connection with the Customer that is enabled by Cisco ServiceGrid.
- **Information Technology Service Management (ITSM)** applications are typically used by Customer and Ecosystem Trading Partner(s) to execute and manage service cases (tickets) internally. Cisco ServiceGrid enables Customers to integrate and automate workflow processes with Ecosystem Trading Partners by creating B2B Connections between their ITSM application and the ITSM application of the Ecosystem Trading Partner(s).
- **Workflows** - Service Cases are driven through a pre-defined set of Workflow tasks and transactions triggered through a series of updates made by Customer or Ecosystem Trading Partner. Each update and its data are stored in Cisco ServiceGrid database. Workflows are the basic method to manage Service Cases. Workflow Types include:
    - **Standard** – Four Cisco ServiceGrid Core standard Workflows (including service request, incident, change and problem management) and twelve Transactions (including open, open_info, acknowledge, reject, update, process, hold, solve, assign_partner, close, cancel, error) to quickly implement your multi-party Workflow process.

- **Configured** – Four Cisco ServiceGrid Core standard Workflows (including service request, incident, change and problem management) that have been modified or extended by adding new Transactions, data lookups, specific logic, rules and event triggers.
- **Custom** - Custom Integration Workflow built from scratch using Cisco ServiceGrid features and functions including Workflow.

PRESIDIO SERVICEGRID CHECKLIST:

Summary

Evaluate the established standard B2B connection between Presidio and Cisco ServiceGrid in order to share/exchange information on Presidio tickets with future partners.

Presidio's Workflow Overview

The defined workflow establishes a B2B interface between partners ticketing system and Presidio via ServiceGrid. This implementation will set the standard way to connect with Presidio. It will enable future Partners to build integrations with ServiceGrid to bi-directionally open/update tickets with Presidio's ServiceNow ticketing system.

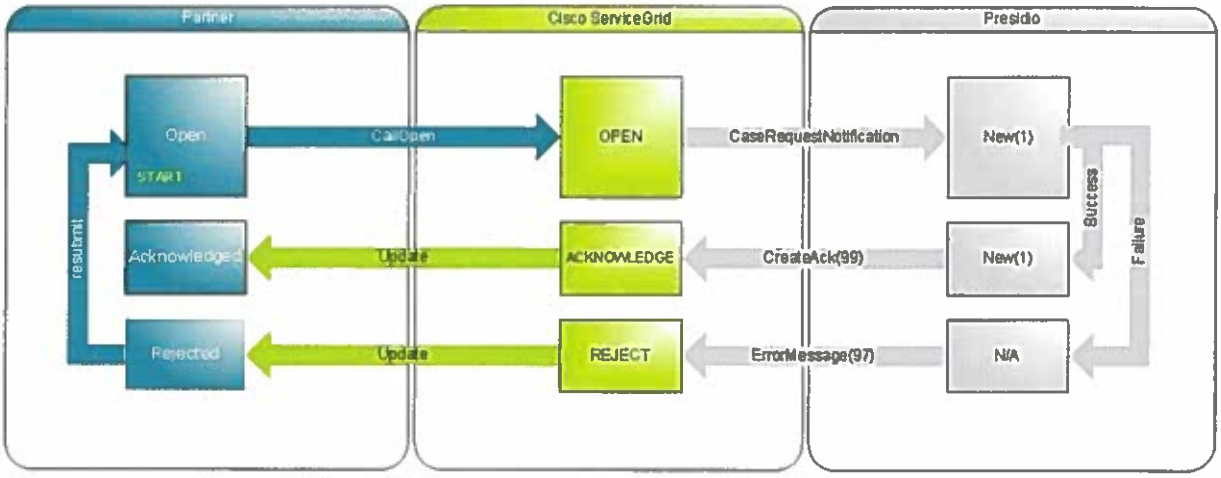
The connection between a Partner and Presidio follows a clear workflow which consist of 3 transaction types to be used between the Presidio and the partner:

- Presidio creates a new ticket
- The partner creates a new ticket
- Update between Presidio and the partner

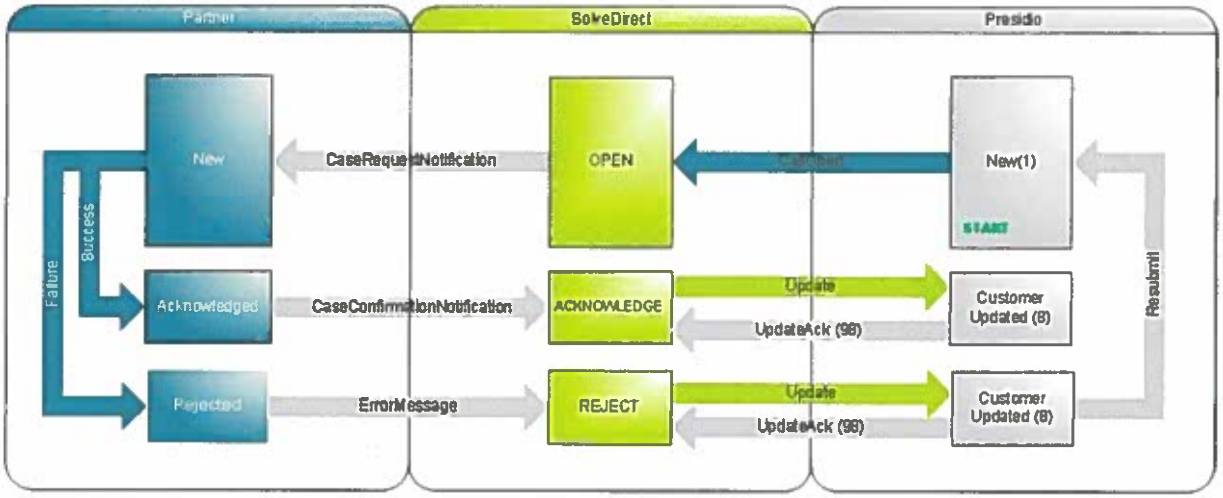
These transaction types are part the standard Presidio eBonding ecosystem providing an Incident Management process that aligns with ITIL.

Note that the arrows only represent the data flow. Presidio initiates all communications by pushing and pulling messages from the ServiceGrid message queues.

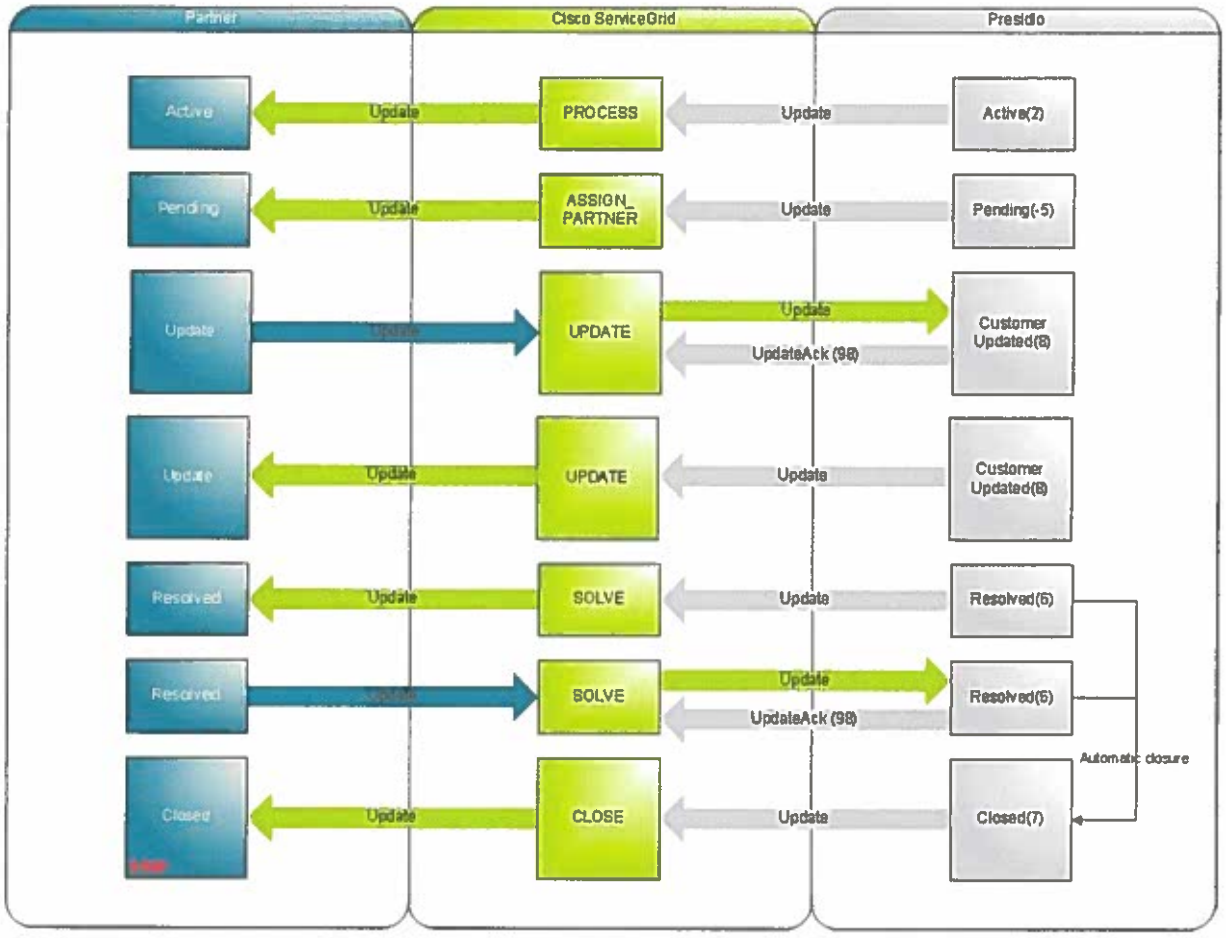
Partner Creates Case into Presidio



Presidio to Partner MessageFlow



Partner and Presidio Bidirectional MessageFlow



Process and Workflow Questions	Support (Yes/No)	Comments:
Will your business rules align to the standard transaction types?		
Is your current Incident Management practice aligned to ITIL?		
The Presidio Incident process allows for either party to open an incident… Will your ticketing system support this? If please provide details in comment section.		
Can your ticketing system send update to a service case via web services?		

Will your business rules and ticketing system allow for updates from eBonded partner to your active tickets?		
Updates to an open ticket are bidirectional in the Presidio workflow. Will your business rules and ticketing system support?		
The Presidio Incident Management process will allow either partner the ability to "resolve" open tickets based on ownership. Will your business rules and ticketing system support?		
The Presidio Incident Management process will allow either partner the ability to "close" open ticket based on ownership. Will your business rules and ticketing system support?		
The Presidio Incident process allows for the ownership to switch within the ticket life cycle between you and your service partners. Will your business rules and ticketing system support?		
The standard patterns supported by ServiceGrid are as follows: Open, Update, Acknowledgment, Solve, Close, Error, Reject, Hold. Are you aware of any other that your system requires?		
The Presidio eBonding ecosystem has enabled the Incident Management process within ServiceGrid. Additional ITIL processes such as Service Request, Change Mgmt., or Asset are out of scope but can be discussed and scoped as additional benefit.		
Is complex acknowledgment logic required?		

e.g.: Technical (HTTP Response) + Application Acknowledgment (Backend System Acknowledgment)		

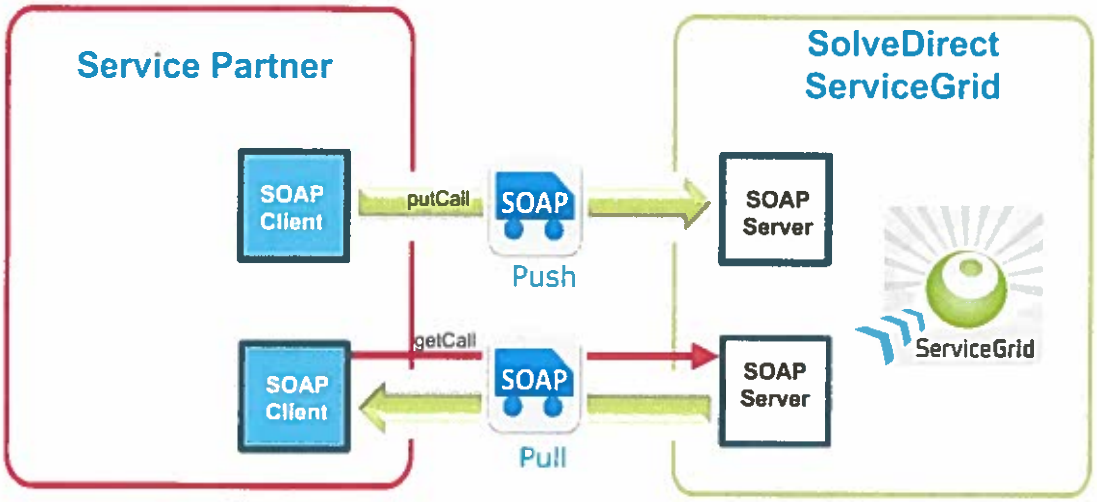
Technical details

HTTPS SOAP/POST (Push/Pull)

For the communication between the Service Partner's Service Management Tools and the ServiceGrid platform Cisco offers a standard Push/Pull transaction method. A public WSDL is published by Cisco to be used by the partner.

The advantage of this solution is that all message-queuing issues are handled by Cisco ServiceGrid. The partner initiates the "push" transactions to the ServiceGrid service and "pulls" transactions actively and periodically from the ServiceGrid web service. The partner is in control of the time interval for each transaction.

In this case the service partner will take the "active" part and ServiceGrid will take the passive part. Cisco does not need access to any server of the Service Partner removing security issues such as firewall/VPN challenges.



Syntax Questions	Partner Standard	Answers
Can your system generate and processes XML messages for a data exchange?		
Can your system send/receive a unique identifier (Ticket ID) with every update?		
Are you able to send/receive base64 encoded attachments?		
Can you initiate a Push/Pull connection to ServiceGrid using HTTPS SOAP?		

Can you send XML messages respecting the standard Presidio namespace?		
Are you aware of any VPN/Firewall constraints preventing your ITSM to access ServiceGrid's WSDL?		

Project management

General questions	Answers
What are your pain points? Why are we implementing this integration?	
Do you have any metrics regarding the current ticket creation/resolution times?	
Does your team have previous B2B integration experience?	
Do you have the technical resources to implement the integration in your ITSM?	
How many tickets per month will be created via B2B?	
What are your time constraints?	

APPENDIX D: REMOTE MANAGEMENT TASKS

General Roles and Responsibilities

RM = Remote Management; OS = Onsite

General Roles and Responsibilities	Contractor	ACG	RM or OS Or Both
1. Participate in quarterly technical and business planning sessions to establish standards, architecture and project initiatives	X	X	Both
2. Develop and present documented standards and architecture	X		OS
3. Review and approve documented standards and architecture		X	
4. Perform business liaison function for ACG's agencies		X	
5. Develop and review plan for technology refreshes and upgrades with ACG on semi annual basis	X		OS
6. Review and approve technology refresh and upgrade plan		X	
7. Analyze and recommend network capacity thresholds	X		Both
8. Approve network capacity thresholds		X	
9. Provide network and security expertise as part of service performance evaluation	X		RM
10. Develop and provide operation, performance and service level reports on a monthly basis	X		RM
11. Provide Network Health Check reports and suggest remediation on a quarterly (or bi annual) basis	X		RM
12. Plan and execute Network Health Check Remediation	X		RM
13. Approve Network Health Check Remediation		X	
14. Maintain technology certification for the staff assigned to ACG	X		RM
15. Provide ACG department specific physical security or regulatory compliance training		X	

16. Provide design, and integration support to enable end points services such as video services, System Control And Data Acquisition (SCADA), and sensor networks	X		OS
17. Provide operation and maintenance support for the UPS systems at ACG buildings listed in the Runbook	X		OS
18. Provide technology refresh support (e.g. replace and operationalize network components) as per ACG's technology refresh schedule	X		Both

Provisioning Services

The Provisioning Services includes network configuration and maintenance updates required to maintain the Service Level Requirements outlined in Section 5. Under this SOW, Provisioning Services includes only ACG's approved upgrades to existing network hardware and software at ACG offices.

Provisioning Services Roles and Responsibilities	Contractor	ACG	RM or OS Or both
1. Establish a policy for infrastructure technology lifecycle refresh		X	
2. Recommendations for the provisioning of new Voice and Data Infrastructure at ACG Offices, in accordance with ACG's technology lifecycle equipment refresh policy	X		OS
3. Approval of all new infrastructure provisioning projects		X	
4. Develop Configuration for the network components highlighted in the Runbook	X		OS
5. Document configuration files, develop and/or update Visio drawing, and backup configuration and documents on ACG's server	X		OS
6. Maintain and update inventory of IP addresses, VLAN assignment, port assignment, telephone extensions, and other configuration details	X		OS
7. Coordinate equipment delivery with major vendors including Cisco, Palo Alto and F5 Networks	X		OS
8. Configure hardware and software prior to installation	X		OS

9. Install and burn new network hardware	X		OS
10. Upon installation of any new equipment, configure the equipment for real time monitoring by ACG's monitoring systems. ACG's monitoring systems are SolarWinds, OPsManager, and WhatsUPGold	X		OS
11. Coordinate with Cisco to ensure that ACG's SmartNet service is up to date, that licenses correctly reflect that ACG is the owner of the service and that the Contractor has the ability to open, track, escalate, and close service tickets	X		OS
12. Document network provisioning requirements and policies	X		OS
13. Approve network provisioning requirements and policies		X	
14. Ensure that all new circuits, CIs and software provisioned are included in configuration management documentation	X		RM
15. Provision Virtual Routing Forwarding (VRF) network, static IP addresses and configuration support for network components	X		OS
16. Serve as a single point of contact for all network provisioning service	X		RM
17. Coordinate with Internet carriers, external partners and network technology vendors such as Cisco and Palo Alto to enable Internet connectivity to cloud based service providers	x		RM

Operations and Maintenance Support

The Contractor is required to provide operations and maintenance support for ACG's network components at all sites. Operations and Maintenance includes monitoring the status of ACG's network assets, recommending improvements, and managing all requested Moves, Adds and Changes (MACs).

Operations Support Roles and Responsibilities	Contractor	ACG	RM or OS or Both
1. Implementation and up keep of the network and security services to match industry best practices	X		OS
2. Monitor and respond to alerts associated with Network components	X		RM

3. Recommend improvements or changes in existing processes, procedures and design that yield more efficient Network performance	X		Both
4. Manage Network components moves, adds and changes (MACs)	X		RM
5. Coordinate site visits with ACG or telecommunication service providers and as required to maintain network connectivity at each site	X		RM
6. Provide network traffic analysis as required to troubleshoot problems	X		OS
7. Conduct preventative maintenance, repair and technology refresh for the network components	X		OS
8. Install, configure, and maintain network components and associated peripherals	X		OS
9. Implement and update network configuration as required to maintain service level requirements	X		OS
10. Prepare defective equipment for return to manufacturer	X		RM
11. Recommend and maintain the most current software release for the network components	X		RM
12. Approve the deployment of software releases as part of the standard network services		X	
13. Develop, document, and review network and security administration requirements with ACG	X		OS
14. Develop and document procedures for network administration that meet requirements and adhere to ACG approved policies and procedures	X		OS
15. Review and approve recommended changes to administration procedures		X	
16. Manage all network CIs in accordance with ACG policies (including security oversight and change management policies)	X		RM
17. Develop or update network documents within five days upon successful implementation of network changes	X		RM

18. Manage user accounts as needed for access and maintaining network resources (e.g. logon user id and password maintenance)	X		RM
19. Maintain public safety data/information for the VoIP environment; populated or provide data to the appropriate public safety agency as required by ACG's emergency response policies	X	X	Both
20. Develop and maintain VoIP call flow, call trees, and users extension databases	X		Both
21. Manage and maintain ACG's VoIP dial plan	X		RM
22. Maintain video services equipment at ACG offices	X		RM
23. Work with ACG's Network Team and representatives from other departments to capture video feeds for storage and/or redistribution	X		OS
24. Configuration, user level security and software maintenance of all video hosting servers that reside in the counties DMZ or internal data farm for external and internal access	X		OS
25. Maintain ACG defined backup schedule for all configuration changes, new data or software components that are added to the network	X		RM
26. Review and approve back up requirements		X	
27. Conduct annual test of the backup/restore procedure, on a schedule mutually agreed to by ACG and the Contractor, to ensure restoration of full functionality, and provide a post-test report to ACG	X		Both
28. Plan and perform failover capabilities of network services on a quarterly basis as approved by ACG	X		OS
29. Implementation of software/firmware updates and security patches	X		RM
30. Provide Subject Matter Expertise (SME) for integrated video services	X		OS
31. Support the network transport for video distribution to ensure high quality audio and video services	X		OS

32. Coordinate, conduct, monitor, and provide real -time support for planned Special Event days and ACG declared emergencies	X		OS
33. Troubleshoot and identify the source of LAN extension failure as a result of physical media failure (e.g. Fiber cut)	X		RM
34. Restore, test, and operationalize the LAN extension in accordance to incident and change management processes once the physical media has been restored	X		OS

Performance Management and Reporting

The Performance Management and Reporting Services cover the proactive monitoring of ACG's network and security infrastructure components. The Contractor will monitor the network on a 24x7 basis through an automated monitoring system to identify and remediate issues as per the Service Level Requirements outlined in Section 5.

Performance Management and Reporting Roles and Responsibilities	Contractor	ACG	RM or OS or Both
1. Provide real time monitoring of all network elements	X		RM
2. Provide real time reporting and alerting of network problem areas	X		RM
3. Coordinate repair of network components as required	X		RM
4. Develop and document network monitoring procedures including escalation thresholds that meet requirements	X		RM
5. Review and approve network monitoring procedures		X	
6. Provide and maintain tools for monitoring network CIs and traffic	X		RM
7. Perform maintenance and problem resolution activities in accordance to incident and change management processes	X		RM
8. Notify ACG immediately when the Contractor adds, moves or changes Network equipment	X		RM

9. Upon installation of any new equipment, configure the equipment for real time monitoring by ACG's monitoring systems. ACG's monitoring systems are SolarWinds, OPsManager and WhatsUPGold	X		OS
10. Coordinate with Cisco to ensure that ACG's SmartNet service is up to date, that licenses correctly reflect that ACG is the owner of the service, and that Contractor has the ability to open, track, escalate and close service tickets	X		OS
11. Monthly reporting of problem areas, hardware failures, losses of connectivity, number of trouble tickets, outages, duration of each outage, outage resolution, and time -to - repair	X		RM
12. Provide Network bandwidth analysis and utilization in absolute and percentage	X		RM
13. Provide reports for Individual CI utilization and performance as requested by ACG	X		RM
14. Perform Data Network component tuning to maintain optimum performance in accordance with Change Management procedures	X		OS
15. Manage Data Network component resources (e.g., CIs and traffic) to meet defined service Availability and performance thresholds	X		RM
16. Provide regular monitoring and reporting of Data Network component performance, utilization, and efficiency	X		RM
17. Proactively evaluate, identify, and recommend configurations or changes to configurations that will enhance performance	X		RM
18. Conducting trending analysis to recommend changes to improve the performance	X		Both
19. Provide technical advice and integration support to enable partner connectivity with network applications (i.e. Call Center, video services, etc.)	X		OS

Incident Management Services

An incident is an unplanned disruption or degradation of service that needs to be resolved immediately. Incident Management Services involve identifying and reporting incidents and

faults, and restoring normal network operations as quickly as possible with the least possible impact on ACG staff and business.

The Contractor's staff must be accessible to provide Incident Management services on a 24 x 7 basis.

Outside of DTS Business Hours, including all day on ACG holidays, the Contractor will receive automated alerts and/or voicemails from ACG or from the After -hours Service Desk concerning network issues and must resolve those issues as described in the Service Level Requirements in Section 5.

Incidents are recorded in ACG's Service Desk system. The Contractor will enter and/or update incident records in ACG's Service Desk system.

The primary activities of the network Incident Management include:

- Incident detection and recording
- Incident classification and initial support
- Incident Investigation, triage and diagnosis
- Resolution and recovery
- Incident closure
- Incident ownership, monitoring, tracking, and communication

Incident Management Roles and Responsibilities	Contractor	ACG	RM or OS Or Both
1. Establish criteria for Incident Management support, including priority levels, definitions and characteristics, incident classification and prioritization schema, and escalation requirements		X	
2. Adhere to ACG's Incident Management process and recommend Incident Management procedure to enhance service level response time and overall user experience	X		RM
3. Review and approve Incident Management policies and procedures enhancements		X	
4. Provide access to ACG's centralized Service Desk System for Incident Management tracking, in order to log and track network incidents		X	

5. Monitor ACG's Service Desk System for automatically generated and logged Incident alerts and events	X		Both
6. Resolve incidents on the first call in accordance with the Service Level requirements	X		RM
7. Log all network incidents into ACG's Service Desk System	X		Both
8. Identify, filter, and classify Events and Incidents to a priority level and handle according to Service Level requirements	X		RM
9. Diagnose and resolve incidents; Where possible, proactively implement appropriate corrective actions for known errors (e.g., workarounds for known unresolved Problems)	X		RM
10. Escalate incidents to the appropriate next level service as soon as it is clear that the incident is unable to be resolved without additional assistance or as required to comply with the Service Level Requirements	X		RM
11. Monitor and track incident resolution progress through to final closure and record/update incident record status as appropriate	X		RM
12. Troubleshoot, diagnose, and resolve incidents	X		RM
13. Investigate configuration level error and network disconnects	X		RM
14. Debug network functionality or supported applications service capabilities	X		RM
15. Provide end to end Incident Identification, Escalation, and Resolution Management; and a Closure Process including the management of those tickets escalated to third parties	X		RM
16. Provide Tier 2 and Tier 3 support for the network connectivity related issues	X		RM
17. Verify that all records (e.g., inventory, asset and configuration management records) are updated to reflect completed / resolved incident	X		RM

18. Document solutions to resolved incidents in central knowledgebase. Accurately update all information pertinent to trouble ticket including general verbiage, codes, et.al.	X		RM
19. Notify designated ACG personnel of all incidents within the designated timeframe	X		RM
20. Maintain current and historical records of all calls and the resolution of those calls for the life of the contract	X		RM
21. Track ongoing status of any incident and their corresponding problem record to ensure that identified problems are addressed and resolved	X		RM
22. Ensure incident resolution activities conform to defined Change Management procedures set forth in the Process and Procedures Manual	X		RM
23. Periodically review the status of open, unresolved incidents and related problems and the progress being made in addressing problems	X		RM
24. Conduct incident review sessions with ACG on a monthly basis to provide listing and status of Incidents and impact on the network components	X		RM
25. Participate in Incident Management review sessions		X	
26. Close out incidents that were resolved satisfactorily	X		RM
27. Provide Incident Management reporting as required	X		RM

Problem Management Services

By definition, at the root of every incident there is a problem. Problem Management services involve identifying and reporting problems and prioritizing them for resolution.

The Contractor will provide proactive Problem Management services to minimize the adverse impact of errors within the IT Infrastructure and prevent the occurrence of Incidents related to these errors. The Contractor will provide reactive Problem Management services by diagnosing and solving Problems that have been the cause of one or more reported Incidents. Problem Management services could include performing predictive analysis activities to identify potential future problems and developing and implementing recommended mitigation plans. The Contractor will also maintain, update, and disseminate information about the Problems and resolutions.

The Contractor will provide these Problem Management services for all identified Problems that are determined to be related to ACG's network components and are within the scope of the Agreement. The Contractor will also assist ACG in performing Problem Management with its External Partners.

The Contractor will also be responsible for ensuring that resolutions to problems are implemented through the appropriate control procedures, especially Change Management and Release Management, and for coordinating Problem Management activities with the various teams responsible for Configuration Management, Availability Management, Capacity Management, IT Service Continuity Management, and Service Level Management activities.

Problem Management Roles and Responsibilities	Contractor	ACG	RM or OS Or Both
1. Define requirements and policies for Problem Management (e.g., events that trigger a Root Cause Analysis, categorization and prioritization schema, etc.)		X	
2. Participate in developing Problem Management requirements and policies	X		RM
3. Develop appropriate process and procedures and methodologies that support ACG -approved Problem Management requirements and policies that comply with ACG requirements	X		RM
4. Approve appropriate process and procedures and methodologies that support ACG approved Problem Management requirements and policies that comply with ACG requirements		X	
5. Implement appropriate process and procedures and methodologies that support ACG approved Problem Management requirements and policies that comply with ACG requirements	X		RM
6. Establish and maintain a Problem Management knowledgebase that is accessible to ACG where information about Problems, Root Cause, Known Errors, Workarounds, and problem resolution actions are recorded and tracked. This knowledgebase can be the same knowledgebase as used by Incident Management	X		Both

7. Provide unrestricted access to ACG authorized staff and other ACG designated personnel to all current and historical Problem Management records and knowledgebase data	X	X	Both
8. Ensure Problem Management activities conform to defined Change Management procedures set forth in the Procedures Manual	X		RM
9. Coordinate with appropriate Incident Management teams and take ownership of Problem Management activities of all problems determined to reside in the Contractor's service area of responsibility (e.g., detection, logging, root -cause analysis, et. al.)	X		RM
10. Coordinate, escalate, and track Problem Management activities within ACG and third parties related to problems determined to reside in all IT infrastructure areas	X		RM (covered equipment only)
11. Flag all incidents that require further Root Cause Analysis be conducted (i.e., Priority 1 and Priority 2 incidents) per the agreed to procedures	X		RM
12. Ensure that recurring problems that meet defined criteria related to the Contractor's IT service responsibility area are reviewed using root cause analysis procedures	X		RM
13. Conduct proactive trend analysis of incidents and problems, and other data elements to identify recurring situations that are or may be indicative of future problems and points of failure	X		RM
14. Track and report on problems and trends or failures and identify associated consequences of problems	X		RM
15. Develop and recommend corrective actions or solutions to address recurring incidents and problems, as well as mitigation strategies and actions to take to avert potential problems identified through trend analysis	X		RM
16. Identify, develop, document, and recommend appropriate Workarounds for known errors of unresolved problems and notify ACG and other appropriate stakeholders of its availability if approved. Document the workaround in the knowledgebase	X		RM (ticket data only)

17. Review and approve Workarounds for implementation, as appropriate		X	
18. Coordinate and monitor status of Root Cause Analysis activities performed by ACG and External Partners (i.e., from other IT service areas)	X		Both
19. Document and update Problem Management knowledge base with information regarding problem resolution actions, activities and status (e.g., root cause, known errors, workarounds, etc.) and notify all appropriate stakeholders of availability of information	X		Both
20. Ensure problem resolution activities conform to defined Change Management procedures set forth in the Process and Procedures Manual	X		RM
21. Provide status reports detailing the status of corrective actions for Problems and Priority 1 and Priority 2 Incidents until closure as determined by ACG	X		RM
22. Conduct Problem Management review meetings and provide listing and status of same categorized by problem impact	X		RM
23. Participate in Problem Management review meetings and review and approve recommendations for actions, where appropriate		X	
24. Periodically review the state of open incidents and related problems and the progress being made in addressing Problems	X		RM
25. Participate in and review and approve as appropriate all Problem Management generated RFCs as part of the Change Management		X	
26. Create Request for Change (RFC) documentation with recommended corrective actions to be taken to resolve a problem and submit to ACG for review and approval	X		RM
27. Conduct periodic problem management proactive review sessions	X		RM
28. Provide Problem Management reporting as required	X		RM

Capacity Management

Capacity Management Services are the activities associated with ensuring that the capacity of the data networks matches ACG's evolving demands in the most cost -effective and timely manner. The process encompasses the following:

- Monitoring of performance and throughput of IT Services and supporting IT components
- Understanding current demands and forecasting for future requirements
- Developing capacity plans which will meet demand and SLRs
- Developing modeling and conducting simulations to manage capacity
- Conducting risk assessment of capacity recommendations
- Developing and implementing a capacity plan including the financial impact of the Data Networks
- Undertaking tuning activities

Capacity Management Roles and Responsibilities	Contractor	ACG	RM or OS Or Both
1. Develop, document and maintain in the Standards, Process and Procedures network Capacity Management procedures	X	X	Both
2. Review and approve Capacity Management process and procedures		X	
3. Identify future business requirements that will alter capacity requirements		X	
4. Develop and recommend annual capacity plan, and provide quarterly updates on the progress against the plan	X	X	Both
5. Review and approve recommended capacity plan		X	
6. Develop and implement capacity models and run simulations to validate the capacity plan	X	X	Both
7. Participate in all capacity planning activities	X	X	
8. Assess capacity impacts when adding, removing or modifying network components in scope	X	X	Both
9. Assess Incidents/Problems related to capacity and provide recommendations for resolution	X		Both

10. Recommend changes to capacity to improve service performance	X		Both
11. Assess impact/risk and cost of capacity changes	X	X	Both

Internet and External Partner Connectivity

The Contractor will manage, monitor, provision, and operationalize connectivity to External Partner Networks. In addition to roles and responsibilities identified below, the Contractor is required to monitor External Partner Network connectivity performance, evaluate the impact of External Partner Network performance on ACG's end -user experience, and recommend technology or design enhancements that would ultimately improve the performance of the External Partner Network connectivity.

Internet and External Partner Connectivity Roles and Responsibilities	Contractor	ACG	RM or OS Or Both
1. Review architecture and design for External Partner Network connectivity focusing on streamlining the technology for operational and business efficiencies	X		OS
2. Provide expertise to architect and design optimal External Partner Network connectivity to meet desired service performance requirements and end user experience	X		OS
3. Monitor performance of the External Partner Network connectivity and cloud based application	X		Both
4. Collaborate with cloud provider to establish network latency, capacity, and performance thresholds for optimal end user experience of cloud based applications	X		OS
5. Collaborate with the External Partner Network on the ways to enhance service performance; recommend relevant configuration for the network components to improve service performance	X		OS
6. Conduct on site health check session with ACG on a monthly basis to review External Partner Network connectivity performance against predefined threshold and end user experience	X		OS
7. Provide real time monitoring and reporting of External Partner Network Connectivity Performance	X		RM

8. Recommend upgrades to ACG Data Networks that would improve External Partner Network Connectivity Performance	X		RM
9. Provide recommendations to ACG on the protocol or service components that should be monitored and tracked for each External Partner Service Provider	X		OS
10. Monitor ACG's External Partner Transport circuit from its NOC and inform ACG of the existence of any outages or problems with the External Partner	X		RM
11. Approve recommended configuration for the network components		X	
12. Request modifications to network configurations via the Change Management process	X		OS
13. Provide monthly performance analysis reports	X		RM

Network Security Services

Network Security Services are the activities associated with maintaining physical and logical security of all Data Network components (hardware and software) and data, including, virus protection, network access protection, and other security services, in compliance with ACG Security requirements. Network Security Services include the provisioning and maintenance of network Firewalls and Intrusion Detection Systems (IDS).

Network Security Roles and Responsibilities	Contractor	ACG	RM or OS Or Both
1. Define Security requirements, standards, process and procedures, and policies including regulatory requirements		X	
2. Assist in developing Security standards, policies, and procedures including industry best practices	X		OS
3. Provide Security plan based on ACG's Security requirements, standards, procedures, and policies	X		OS
4. Implement the necessary controls and procedures to protect information systems assets from intentional or inadvertent modification, disclosure, or destruction	X		OS

5. Review and approve Security plans and IT infrastructure		X	
6. Recommend and perform network security design and integration	X		OS
7. Review and approve Security requirements, standards, procedures, and policies including regulatory requirements		X	
8. Recommend best practice firewall policies and configuration	X		OS
9. Review and approve firewall and ACL designs		X	
10. Provide network security, incident response, firewall and VPN management and administration	X		RM
11. Remain up to date with current Security trends, threats, common exploits and security policies and procedures and best practices	X		RM
12. Assist in the development of guidelines and procedures for administration and security best practices		X	
13. Establish access profiles and policies for adding, changing, enabling/disabling, and deleting log on access of ACG staff, agents and partners		X	
14. Administer Enterprise Security Incident Event Management (SIEM) system	X		RM
15. Assist in IT/OT Security product evaluations such as Single Sign On, Dual Factor authentication, Active Directory Federated Systems, SCADA/PLC, NAC, etc.	X		OS
16. Provide real time network security monitoring to identify any remediate possible network intrusions	X		RM
17. Report Security violations to ACG per ACG policies	X		RM
18. Resolve Security violations per ACG policies	X		RM
19. Recommend security patches relevant to ACG network and classify the need and speed in which the Security patches should be installed	X		RM

20. Install Security patches per ACG's Change Management process and procedures including acquiring required ACG approval	X		RM
21. Maintain all documentation required for Security assessments, audits, and internal control and control testing	X		Both
22. Attend bi monthly Security Compliance briefings	X		RM
23. Perform Security audits as requested by ACG	X		
24. Provide security dashboard report for the network components, including components listed in the Runbook.	X	X	Both

Documentation

The Contractor is required to develop, update, and maintain documents related to the network components.

Documentation Roles and Responsibilities	Contractor	ACG	RM or OS Or Both
1. Document and maintain network components specifications, and configurations (e.g., interconnection topology, configurations, Network diagrams)	X		RM
2. Document and maintain standard operating procedures (e.g., boot, failover, spool management, batch processing, backup)	X		RM
3. Document and maintain procedures manual, production and maintenance schedules, and NOC job schedules	X	X	Both
4. Update all appropriate documentation as necessary as a result of any network components or services changes in accordance with Change Management procedures	X		RM
5. Maintain inventory of network components, IP address management tool such as Bluecat, VLAN database, VoIP extensions, mapping of End user location and extension assignment, External Partner Network circuits, and maintenance contract	X		OS

6. Enter/upload configuration data into configuration database as required by ACG's configuration management process	X		OS
7. Provide ACG designated and authorized personnel access to all documentation	X		RM
8. Backup CI configuration, documentation and databases to centralized backup server on a weekly basis	X		RM

APPENDIX E: LETTER OF AGENCY

[date] "Effective date"

To Whom It May Concern,

Subject: Letter of Agency

The undersigned, [customer] 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 [customer] has purchased from you.
- To order changes in and maintenance on carrier circuits related to the Presidio Sentry Managed environment in order 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 [customer] 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.

Sincerely,

_____

Customer Signature

Kythyus Hopler, Assistant Purchasing Agent

Customer Name/Title (Please Print)

EXHIBIT B

PRICING SCHEDULE

Coverage Period				
Term	5 Years	Coverage Period	Start: 10/01/2016	End: 09/30/2021
			Billing Frequency:	**Annual**

Base Managed Services	Monthly	Annual
Onsite Engineering and Support Services	$113,101.50	$1,357,218.00
Remote Managed Services	$41,326.00	$495,912.00
Service Grid Ticket Integration	$2,100.00	$25,200.00
Total Recurring Fees:	**$156,527.50**	**$1,878,330.00**

Project Support Fees *(based on Project Support Labor Rates)*		
Project Costs	$185,355.50	$2,224,266.00
Total Recurring Fees:	**$185,355.50**	**$2,224,266.00**

Non-Recurring Fees *(billed upon execution of contract)*	
Service Transition Management	$20,000.00
ServiceGrid Integration Connection	$18,000.00
Total Non-Recurring Fees:	**$38,000.00**

Total Fees (Recurring and Non-Recurring)	
Year 1	**$4,140,596.00**
Year 2	**$4,102,596.00**
Year 3	**$4,102,596.00**
Year 4	**$4,102,596.00**
Year 5	**$4,102,596.00**
Total Contract:	**$20,550,980.00**

Quarterly True Ups

Pricing is based on several elements, including data provided in the RFP, conversations between Presidio and Arlington County and the following elements:

1. The quantity of managed CIs
2. The number of After Hours support calls
3. User MACDs based on 5% of 4,100 users per month
4. CI MACDs include up to 2 MACDs per CI per month, excluding emergency MACDs. There is no additional charge for emergency CI MACDs.

Each quarter these four elements will be reviewed. If the elements change based on the parameters below, Presidio will provide ACG with a proposed adjustment that reflects the change. This adjustment is called a "True-up". True-ups will be reviewed collaboratively between ACG and Presidio during Quarterly Business Reviews. The True-up will be documented via a contract addendum, and the financial adjustment will be made annually, unless the adjustment to any of these items exceed the following thresholds, in which case the financial adjustment will be made in the following quarter:

1. The quantity of managed CIs changes by more than 15%.
2. After Hours support calls exceed 200 per month for 2 consecutive months within the quarter.
3. User MACDs exceed 250 per month for 2 consecutive months within the quarter.
4. CI MACDs exceed the total number of allotted CI MACDs for 2 consecutive months within the quarter.

Price adjustments will be based on the table below:

CI/Resource Category	Unit of Measure	Monthly Unit Cost
Core Layer LAN Ports	Each Core Layer LAN Port	$3.92
Distribution Layer LAN Ports	Each Distribution Layer LAN Port	$5.64
Access Layer LAN Ports	Each Access Layer LAN Port	$1.28
Internet and Partner Network Ports	Each Internet and Partner Network Port	$0.85
Load Balancers	Each Load Balancer	$63.24
Firewalls	Each Firewall	$37.82
Wireless Access Points	Each Wireless Access Point	$8.31
UPS Devices	Each UPS Device	$21.70
VoIP Phones	Each VoIP Phone	$2.78
Analog Phones	Each Analog Phone	$2.78
Video Devices	Each Video Device	$4.67
MACDs for Phone and Video	Increases in increments of 50 MACDs/month	$2,000.00
MACDs for CIs	Increases in increments of 50 MACDs/month	$2,000.00
After-hours Service Desk calls	Increases in increments of 50 calls/month	$2,000.00

NOTE: If the average User MACD counts or After Hours support calls consistently exceed the target limits, it may show evidence of an operational or training issue that Presidio can address with ACG. If no operational issues exist, and the User MACD or After Hours support calls continue to exceed the threshold, the User MACD and After Hour support call allowances will be adjusted as agreed to by both ACG and Presidio.

Project Support

Hourly labor rates for Project Support will be based on the table below:

ACG Job Title / Labor Category	Onsite Hourly Rates	Presidio Job Title
Network Engineer	$150.33	Network Engineer
Network Analyst	$126.59	Network Analyst
Network Administrator	$107.60	Network Administrator
Network Engineer - Video	$153.68	Communications/Network Engineer
Network Engineer - Wireless	$153.68	Communications/Network Engineer
Network Engineer - Cloud Integration Architect	$199.96	Network Engineer - Cloud Integration Architect
Telecommunications Engineer	$180.48	Communications/Network Engineer
Telecommunications Technician	$147.94	Telecommunications Technician
Security Analyst	$146.11	Security Analyst
Network Security Specialist	$177.00	Network Security Specialist
Systems Security Specialist	$111.17	Systems Security Specialist
Information Security Architect	$199.96	Sr. Network Security Specialist
Program Manager	$170.48	Program Manager
Project Manager	$153.01	Project Manager
Project Leader	$121.35	Project Coordinator
Project Management Specialist	$137.52	Business Process Engineer
Infrastructure Business Analyst	$177.97	Business Case Analyst

EXHIBIT C

TERMS AND CONDITIONS

This Managed Services Agreement ("Agreement") is entered into on this day by and between Presidio Networked Solutions, LLC, with offices at 7601 Ora Glen Drive, Suite 100, Greenbelt, Maryland 20770 ("Presidio") and Arlington County Government, with offices at 2100 Clarendon Boulevard, Suite 601, Arlington, Virginia 22201 ("Customer"). In consideration of the mutual covenants and conditions herein contained, and other good and valuable consideration, receipt and sufficiency of which is hereby acknowledged, the parties hereto agree as follows:

1. **Customer Information:**

Organization:	Arlington County Government	**POC:**	Nathaniel Wentlend
Billing Address:	2100 Clarendon Blvd., Suite 600	**POC Phone #:**	703-228-4776
		POC E-mail:	nwentlend@arlingtonva.us

2. **Scope:**
Presidio shall provide the Services as defined in Exhibit A, with respect to the software ("Software") and/or related hardware ("Hardware") (collectively the "Equipment") referenced in Covered Equipment List (CEL) and subject to Presidio's acceptance of such Equipment as eligible for Services coverage pursuant to Section 11 of the Terms and Conditions.

3. **Coverage Period and Fees:**
The Start of Service (SOS) date shall be the earlier of 45 business days following the execution of this Agreement, or upon completion of the Service Transition Management process for the subscribed services, unless otherwise agreed upon by both parties in writing.

   For Service Management Offerings, including Presidio Support Services (PSS) for Cisco and Multivendor, the Start of Service commences on the date that Presidio submits a PO to vendor for the underlying support contract. The PSS agreement is independent from other Presidio Managed Services and does not necessarily co-terminate with other agreements.

4. **Additional Services and Fees:**
5. **Covered Equipment and Billing:**
   The equipment covered under this Services Agreement is listed above In Section 11 Covered Equipment List (CEL).
6. **Billing:**
7. **Term**
8. **Customer Responsibilities**
   Customer shall grant Presidio full and free access to the Equipment at all times during the Term including all required access credentials (e.g. IP addresses, SNMP community strings, passwords, etc.). Customer's selecting one of the monitoring tiers of service 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. Customer shall provide all pertinent network diagrams and documentation. Customer shall provide 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. Customer shall ensure that the Equipment meets, at all times, the manufacturer approved configuration specifications and current and covered by vendor maintenance and support program. Customer shall provide Presidio with the necessary remote access (e.g., via modem, VPN) to the Equipment.

   Immediately upon, or prior to, execution of this Agreement, Customer shall issue a purchase order to Presidio for purchase of the Services hereunder. Presidio will have the right to withhold performance of the Services until such time as a purchase order, issued in conformance with the terms and conditions of this Agreement, is provided by Customer.

9. **Payment Terms:**
10. **Acceptance of Covered Equipment:**
    Presidio reserves the right to inspect Customer's installation site with respect to the Equipment and/or to verify remote access capability at any time prior to commencement of the Services for the initial Term or any renewal of the Term. Presidio will advise Customer of any condition which would render the Equipment ineligible for the Services hereunder. Customer shall be responsible for correcting, at its expense, any such condition prior to Presidio's providing the Services.

11. **Service Limitations**
    The parties recognize that from time to time Customer may request maintenance and support services that fall outside the scope of this agreement. Maintenance and support services considered outside the scope of this Agreement include, but are not limited to, 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; and (e) no fault found (problem with equipment not provided by Presidio and/or not covered under this Agreement). In addition, Presidio does not guarantee performance for Monitored Customer if remote access to the Equipment (e.g., via modem, VPN) is not provided by Customer. In the event Customer decides to perform an out of scope task on their own, Presidio will make commercially reasonable attempts to offer guidance and reactive "help-line" assistance.

12. **Notices**
13. **Assignment**
14. **Warranties, Remedies and Limitations of Warranties and Remedies and Disclaimers of Warranties and Liabilities:**
    Presidio warrants that the Services will be performed in a good and workmanlike manner in accordance with applicable professional standards. THE WARRANTIESTHIS WARRANTY PROVIDED HEREUNDER AREIS IN LIEU OF ALL OTHER WARRANTIES, GUARANTEES OR CONDITIONS PERTAINING TO THE SERVICES, WRITTEN OR ORAL, STATUTORY, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY AS TO MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, ALL SUCH WARRANTIES ARE EXPRESSLY DISCLAIMED AND THE PROVISIONS HEREIN SHALL CONSTITUTE PRESIDIO'S SOLE OBLIGATION AND LIABILITY AND Customer'S SOLE REMEDY FOR BREACH OF WARRANTY. PRESIDIO SHALL NOT BE RESPONSIBLE FOR ANY WARRANTY OFFERED TO Customer BY ANY OTHER PARTY. IN NO EVENT SHALL PRESIDIO BE LIABLE FOR ANY INCIDENTAL, INDIRECT SPECIAL OR CONSEQUENTIAL DAMAGES RELATING TO BREACH OF WARRANTY.

15. **Force Majeure:**
16. **Non-Solicitation:**
17. **Confidentiality:**
    Both parties recognize that during the course of contract performance, one party ("Receiving Party") may acquire knowledge, confidential or proprietary business information or trade secrets ("Confidential Information") from the other party ("Disclosing Party") which: 1) has been marked as confidential, 2) whose confidential nature has been made known to the Receiving Party, or 3) that due to the nature of the information, a reasonable person under the circumstances would treat as confidential. Confidential Information, whether marked or not, shall specifically include, but not be limited, to 1) technical information such as methods, processes, formulae, compositions, systems, techniques, inventions, machines, computer programs and research projects; or 2) business information such as Customer lists, pricing data, supply sources, financial and marketing data, production, or merchandising systems or plans, business policies or practices, and 3) any non-public personal information including but not limited to personally identifiable financial or credit card information, personally identifiable medical information. The Receiving Party agrees to keep all Confidential Information in a secure place and further agrees not to publish, communicate, divulge, use, or disclose, directly or indirectly, for his or her own benefit or for the benefit of another any Confidential Information except as specifically required in accordance with performing its duties under this Agreement.

18. This obligation of confidentialityce shall not apply with respect to information that 1) was in the public domain prior to disclosure, 2) is available to the Receiving Party from third parties with legal right to do so on an unrestricted basis; 3) is disclosed by Disclosing Party to others on an unrestricted basis, 4) is developed by Receiving Party independently of any disclosure made hereunder, or 54) is required to be disclosed to a court or government body pursuant to an order.

19. **Limitations of Damages:**
20. **Default:**
21. **Subcontracting:**
22. **Indemnification:**
23. **Independent Contractor:**
24. **Publicity:**
25. **Applicable Law:**
26. **Waiver:**
27. **Invalidity:**
28. **Duplicate Originals/Counterparts:**
    This Agreement may be executed in two or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same instrument. Execution of this Agreement at different times and places by the parties hereto shall not affect the validity hereof.

29. **Entire Agreement:**

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

Arlington County Government		Presidio Networked Solutions LLC	
By:	K Hepler	By:	Jackie Arnett
Name:	Kyshyra Hepler	Name:	Jackie Arnett
Title:	Assistant Purchasing Agent	Title:	Executive Director
Date:	10/18/2016	Date:	30 September 2016