Service Description: Cisco Safety & Security Optimization Service

This document describes Cisco Safety & Security Optimization Service.

Related Documents: This document should be read in conjunction with the following documents also posted at www.cisco.com/go/servicedescriptions/: (1) Glossary of Terms; (2) List of Services Not Covered; and (3) Severity and Escalation Guidelines. All capitalized terms in this description have the meaning ascribed to them in the Glossary of Terms.

Direct Sale from Cisco. If you have purchased these Services directly from Cisco, this document is incorporated into your Master Services Agreement (MSA) with Cisco. In the event of a conflict between this Service Description and your MSA, this Service Description shall govern.

Sale via Cisco-Authorized Reseller. If you have purchased these Services through a Cisco-Authorized Reseller, this document is for description purposes only; is not a contract between you and Cisco. The contract, if any, governing the provision of this Service will be the one between you and your Cisco Authorized Reseller. Your Cisco Authorized Reseller should provide this document to you, or you can obtain a copy of this and other Cisco service descriptions at www.cisco.com/go/servicedescriptions/

Service Summary
The Cisco Safety & Security Optimization Service is intended to supplement a current support agreement for Cisco products. Cisco shall provide the Safety & Security Optimization Service described below as selected and detailed on the Purchase Order for which Cisco has been paid the appropriate fee. Cisco shall provide a Quote for Services ("Quote") setting out the extent of the Services and duration that Cisco shall provide such Services. Cisco shall receive a Purchase Order that references the Quote agreed upon between the parties and that, additionally, acknowledges and agrees to the terms contained therein.

Cisco Safety and Security Optimization Service

General Service Responsibilities of Cisco

Cisco shall provide the following General Service provisions for any Safety & Security Optimization Service specified in the Quote:

- Under this Service, Cisco shall provide the Safety & Security Optimization Service during Standard Business Hours, unless stated otherwise.
- Provide a single point of contact ("Cisco Project Manager") for all issues relating to the Services.
- Participate in regularly scheduled meetings with the Customer to discuss the status of the Services.
- Ensure Cisco employees (including Cisco subcontractors) conform to Customer's reasonable workplace policies, conditions and safety regulations that are consistent with Cisco's obligations herein and that are provided to Cisco in writing prior to commencement of the Services; provided, however, that Cisco's personnel or subcontractors shall not be required to sign individual agreements with Customer or waive any personal rights.
- Supply Cisco project team personnel with a displayable form of identification to be worn at all times during services activities at Customer's facility.
- Cisco reserves the right to determine which of its personnel shall be assigned to a particular project, to replace or reassign such personnel and/or subcontract to qualified third persons part or all of the performance of any Safety & Security Optimization Service hereunder. Should Customer request the removal or reassignment of any Cisco personnel at any time; however Customer shall be responsible for extra costs relating to such removal or reassignment of Cisco personnel. Cisco shall not have any liability for any costs, which may occur due to project delays due to such removal or reassignment of Cisco personnel.

Specific Service Responsibilities of Cisco

In addition to the General Responsibilities, Cisco shall provide the following:

Physical Safety and Security Project Assurance
Cisco will provide project oversight, project management and overall coordination of a Physical Safety and Security deployment project, aligning to Customer's stated business objectives. Cisco will collaborate with Customer and its other partners and vendors involved in the full project rollout to create the following as necessary:

- Customer Requirements Document
- Network Readiness Assessment
- Site Survey & Deployment Checklist Templates
- Design and Test Plan Review
- Deployment Validation
- Project Plan

Safety & Security Technology Planning Support
Cisco provides strategic as well as tactical guidance through participation in periodic safety & security technical planning meetings. Meetings topics are aligned to Customer's business goals and objectives and may cover a range of topics from

near-term solutions to evolving security threats and longer-term management planning.

- Participate in two (2) safety & security technology planning meetings per year.
- Provide collateral / technical reference material (white papers, technical specifications) as requested for specific technologies or for security architectural approaches.
- Develop a Safety & Security Technology Planning Meeting Report, providing a synopsis of the meeting and documenting significant recommendations. Two (2) reports delivered per year.

Safety & Security Technology Readiness Assessment
Cisco analyzes implementation requirements for a new safety & security solution and assess the readiness of Customer's network devices, operations, security policies, and architecture to support the solution.

- Conduct one (1) design workshop to gather business, technical, and operational requirements including current network design documents and future security technology plans to support the readiness assessment.
- Develop one (1) Safety & Security Readiness Assessment Report to document findings and recommendations including recommendations for modifications to the network infrastructure and to the parameters for application performance and availability.

Safety & Security Design Support
Cisco conducts an in-depth analysis of the safety & security design to determine its effectiveness for meeting Customer's safety & security business and IT strategies. As part of this design support, Cisco shall:

- Conduct one (1) design workshop to gather data and initiate the
- Analyze safety security design against organizational security strategy and requirements.
- Develop one (1) Design Report to document the findings and recommendations to improving the strength and security of the given design.

Safety & Security Performance Tuning Support
Cisco provides periodic, ongoing system analysis to maintain, tune and optimize a secure, high-performance network.

- Analyze configurations and align them with corporate safety & security policies and procedures, and Cisco best practices
  - Analyze up to three (3) safety & security device types
  - Analyze up to six (6) individual safety & security devices
- Recommend tuning changes to device configurations to optimize system performance and fully leverage safety & security features of Cisco devices.
- Conduct three (3) interactive tuning sessions with customer to implement recommendations.

Safety & Security Change Support
Cisco provides expertise when making critical changes to the network's advanced security technologies. Change support typically involves reviewing and recommending any needed changes to the design, implementation plan, test plan, and rollback plan for the change, implementation support during the change window, and post implementation support including stabilization, troubleshooting incidents and root cause analysis for unscheduled network outages.

- Cisco will provide a designated engineer when Customer is making changes it deems critical to the Advanced security technologies (VSMS, VSVM, VSOM,IPICS, and CPAM).
- The Cisco designated engineer acts as the primary technical contact to with Customer and Cisco Technical Assistance Center (TAC).
  - Scheduled Change Support: Cisco will make available, upon receipt of not less than twenty-one (21) days prior written request by Customer to Cisco, a designated support contact that can consult with Customer on a 24-hour 7-day standby basis to provide remote engineering support during scheduled change window, not to exceed one (1) per quarter.
  - Unscheduled Change Support: Cisco will provide remote engineering support to provide support during an unscheduled change window, not to exceed one (1) per quarter, to Network to Customer to minimize the impact of individual device failures on the overall Network. Customer must open a service request with the Cisco's TAC prior to contacting Advanced Service Engineer for any unscheduled change support. To support any unscheduled changes to Network, Cisco will:
    - Provide technical evaluation of initial TAC problem diagnosis based on knowledge of Customer's Network.
    - Provide technical evaluation of proposed unscheduled change to Network.
    - Provide technical representation in regularly scheduled conference calls.

Safety & Security Knowledge Transfer and Mentoring
Cisco prepares Customer staff to effectively operate, maintain, manage, and tune its Cisco Self-defending Network through ongoing knowledge transfer sessions.

- Conduct an evaluation working session (1) to gather Customer's requirements for knowledge transfer to support design and configuration tasks.
- Provide a summary report of knowledge transfer requirements coming from the workshop including a proposed twelve (12) month schedule of knowledge transfer activities.

- Provide four (4) quarterly onsite chalk talks and technical presentations on advanced security technologies during quarterly review visits as requested.
- Provide informal mentoring during security technology design and configuration tasks.
- Provide two (2) – three (3) hour knowledge transfer sessions delivered remotely. Sessions support up to twenty-five (25) students.

Responsibilities of Customer

General Services

Customer shall comply with the following obligations for General Services for any Safety & Security Optimization Service specified in the Quote:

- Designate at least two (2) but not more than six (6) technical representatives, who must be Customer's employees in a centralized Network support center (Customer's technical assistance center), to act as the primary technical interface to the Cisco designated engineer. Customer will designate as contacts senior engineers with the authority to make any necessary changes to the Network configuration. One individual, who is a senior member of management or technical staff, will be designated as Customer's primary point of contact to manage the implementation of services under this Service Description (e.g., chair the weekly conference calls, assist with prioritization of projects and activities).
- Ensure key engineering, networking and operational personnel are available to participate in interview sessions and review reports as required by Cisco in support of Service.
- Customer's technical assistance center shall maintain centralized network management for its Network supported under this Service Description, capable of providing Level 1 and Level 2 support.
- Provide reasonable electronic access to Customer's Network to allow the Cisco designated engineer to provide support.
- Customer agrees to make its production, and if applicable, test Network environment available for installation of Data Collection Tools. Customer shall ensure that Cisco has all relevant Product information needed for an assessment.
- If Cisco provides Data Collection Tools or scripts located at Customer's site, Customer shall ensure that such Data Collection Tools or scripts are located in a secure area, within a Network environment protected within a firewall and on a secure LAN, under lock and key and with access restricted to those Customer employee(s) or contractor(s) who have a need to access the Data Collection Tools and/or a need to know the contents of the output of Data Collection Tools. In the event Data Collection Tool provided by Cisco is Software, Customer agrees to make appropriate computers available and download Software as needed. Customer shall remain responsible for any damage to or loss or theft of the Data Collection Tools while in Customer's custody.
- Provide a Network topology map, configuration information, and information of new features being implemented as needed.
- Notify Cisco of any major Network changes (e.g., topology, configuration, new IOS releases.).
- In the event the Network composition is altered, after this Service Description is in effect, Customer is responsible to notify Cisco in writing within ten days (10) of the change. Cisco may require modifications to the fee if the Network composition has increased beyond the original pricing quote for Services.
- Create and manage an internal email alias for communication with Cisco.
- Retain overall responsibility for any business process impact and any process change implementations.
- Supply the workplace policies, conditions and environment in effect at the Customer's facility.
- Provide proper security clearances and/or escorts as required to access the Customer's facility.
- Customer agrees that it will not hire a current or former employee of Cisco, who is involved in the Services under this Service Description, during the term of the Service and for a period of one (1) year after the termination of the Service. As liquidated damages, and not as a penalty, should Customer hire a current or former Cisco employee who is involved in the Services under this Service Description, Customer shall pay to Cisco three (3) times the annual compensation of such employee on the date the employee is hired. If payment is not made on such date, the liquidated damage payment shall be six (6) times the annual compensation of such employee.

Specific Service Responsibilities

Customer shall comply with the following obligations as required specific to the security Services specified in the Quote:

Safety & Security Technology Planning Support

- Establish and inform Cisco of dates at least sixty (60) days in advance strategic planning meetings per year.
- Provide technology roadmaps necessary to support the planning sessions.

Safety & Security Technology Readiness Assessment

- Assessment data collection support.
    - Customer shall advise Cisco immediately of all adds, moves and changes of the Product within Customer's Network.
    - Assemble and provide all necessary Network availability data to enable Cisco to calculate quarterly Network availability. The type of data required to perform the calculations includes the following:
        - Outage Start Time (date/time)
        - Service Restore Time (date/time)
        - Problem Description
        - Root Cause
        - Resolution
        - Number of end users impacted
        - Equipment Model
        - Component/Part
        - Planned maintenance activity/unplanned activity
        - Total end user/ports on network

Safety & Security Design Support

- Provide the low level design document describing the specific set of technical requirements and design goals and specifying the resulting Customer Network architecture and build-out plans to meet those requirements. The level of details must be sufficient to be used as input to an implementation plan.
- Ensure key detailed design stakeholders and decision-makers are available to participate during the course of the Service.
- Provide or extract additional information required in the design effort (e.g., current and planned traffic characteristics).
- Provide documentation of any business requirements and technical requirements for the new design.
- Provide information on any current and planned traffic characteristics or constraints.

Safety & Security Performance Planning Support

- Provide the low level design document describing the specific set of technical requirements and design goals and specifying the resulting Customer Network architecture and build-out plans to meet those requirements. The level of details must be sufficient to be used as input to an implementation plan.
- Ensure key detailed design stakeholders and decision-makers are available to participate during the course of the Service.
- Provide or extract additional information required in the design effort (e.g., current and planned traffic characteristics).
- Provide documentation of any business requirements and technical requirements for the new design.
- Provide Information on any current and planned traffic characteristics or constraints.

Safety & Security Change Support

- Designate person(s) from within its technical support organization to serve as a liaison to the Cisco designated engineer.
- Provide its designated person(s) with instructions on process and procedure to engage the Cisco designated engineer.
- Provide information on Network architecture (which may include remote sites and size of remote sites).
- Identify low risk and high risk areas of the Network based on Customer's Network traffic.
- Information on Customer Implementation plan and implementation schedule
- Provide maintenance window information and any other constraints.
- Provide information on Customer change control process.
- Provide contact information and the Customer escalation process.
- Review details of planned changes with the Cisco designated engineer.
- Advise Cisco of its standard operating procedures related to its business practices, its internal operational nomenclature and Network to allow Cisco to effectively communicate and discuss changes with Customer in the context of Customer's business environment.
- Provide all necessary information to enable Cisco to perform root cause analysis.
- Provide reasonable electronic access to Customer's Network to assist Cisco in providing support.

Safety & Security Knowledge Transfer and Mentoring

- Provide details on desired/requested topics Customer wants to see covered during the knowledge transfer and mentoring sessions.
- Provide background information on the Customer participant skill sets for the knowledge transfer or mentoring sessions.
- Provide Customer facilities and equipment (such as conference rooms, white boards, projectors) and make them available to host the informal technical update sessions.
-