Service Description: Security Design Assessment

This document describes the Security Design Assessment (SDA).

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), Advanced Services Agreement (ASA), or equivalent services agreement executed between you and Cisco. In the event of a conflict between this Service Description and your MSA or equivalent services agreement, 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/.

Cisco shall provide the Security Design Assessment 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 between the parties and that, additionally, acknowledges and agrees to the terms contained therein.

Service Summary

Security Design Assessment provides a comprehensive vendor-agnostic and industry best practices based assessment of the Customer's network infrastructure based on the Cisco Security Control Framework (Cisco SCF). The framework is consistent with international standards including the ISO 27000 series and NIST 800-53. Cisco in conjunction with Customer's representatives shall scope the assessment based on the Quote and the Customer's environment. The Security Design Assessment evaluates the capabilities of the network infrastructure to protect an identified business critical asset and provide a set of recommendations to remediate the identified asset. The recommendation includes improvements to topology, protocols, device configurations and security controls.

The Security Design Assessment includes one business critical asset and sampling of devices from one each of the following network areas: data center, internal network, perimeter network.

Security Design Assessment (SDA) Service

Cisco Responsibilities

Under this Service, Cisco shall provide the Security Design Assessment Service during Standard Business Hours, unless stated otherwise. Cisco shall provide the following General Service provisions for any SDA specified in the Quote:

General Service Responsibilities

- 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 and any 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 Project 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 SDA hereunder. Customer may 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.

  Cisco shall evaluate the capabilities of the network infrastructure to protect an identified business critical asset and provide a set of recommendations to remediate the identified security gaps for that business critical asset. The recommendations include improvements to topology, protocols, device configurations and security controls.

Specific Service Responsibilities of Cisco

Cisco Advanced Services Engineer shall conduct the SDA using the Cisco Security Control Framework. The Cisco

Engineer shall perform the following tasks, unless specifically noted n the Quote:

Scope and Collect:

- Gather information from the Customer to determine the scope of the assessment:
  - Key network assets, applications and services
  - Identification of one critical business asset for the assessment
  - Device configurations and configuration templates
  - Physical and logical network topology diagrams, including the location of the asset included in the assessment
- Conduct a three to five (3 - 5) day workshop at the Customer's site with the Customer's representatives to review assessment scope and information gathered, and to gather information related to the Customer's business environment and IT infrastructure, which may include:
  - Business and compliance requirements
  - Security concerns and previous incidents
  - Future business plans that affect the business environment or IT infrastructure
  - Security organizational structure.
- Gather network and security information which may include:
  - Network architecture description
  - Security policies, standards and procedures
  - Applications and services running over the network
  - Network Management Systems architecture
  - Empirical data (documents, key performance indicators, onsite observation etc.)
- Refine collected information remotely through e-mail and phone conversations with Customer's representatives

Assess:

- Cisco Engineer shall assess the capabilities of the Customer's network infrastructure architecture to protect the identified business critical asset from a specific set of threats with respect to the Cisco Security Control Framework. Specific activities include:
  - Assess effectiveness of the technical and operational controls
  - Identify architectural gaps in the current infrastructure
  - Evaluate how widely techniques are deployed
  - Create Security Design Assessment report with findings and recommendations that may include:
    - Identified critical business asset
    - Identified gaps in controls
    - Remediation recommendations for the identified gaps

Deliver Report:

- Cisco Engineer shall conduct a one (1) day session at the Customer's site to deliver the final report and executive presentation.

Customer Responsibilities

General Service Responsibilities

Customer shall comply with the following obligations:

- Customer shall designate a person to whom all Cisco communications may be addressed and who has the authority to act on all aspects of the Service. Customer shall also designate a back up when the Customer contact is not available who has the authority to act on all aspects of the Services in the absence of the primary contact.
- In the event the Network composition is altered, after this Exhibit is in effect, Customer is responsible to notify Cisco in writing within ten (10) days of the change. Cisco may require modifications to the fee if the Network composition has increased beyond the original pricing quote for Services.
- Provide access to the appropriate resources with knowledge and authority to provide Cisco with the following information:
  - Key business critical assets
  - Assess specific threats to identified business critical asset
  - Appropriate sample configurations from requested network areas
  - Physical and logical network topology diagrams, including the location of the devices included in the assessment
  - Network architecture description
  - Security policies, standards and procedures
  - Services that traverse the perimeter network
  - Applications and services running over the network
  - High-level architecture of data center, internal servers, user host connectivity and Internet connectivity
  - Network Management System architecture
  - Empirical data necessary to develop Cisco Security Control Framework metrics.
- Ensure key Customer networking and operational personnel are available to participate in interview sessions as required.
- Unless otherwise agreed to by the parties, Customer shall respond within two (2) business days of Cisco's request for documentation or information needed for the Service.
- Provide proper security clearances and/or escorts as required to access the Customer's facility.
- Supply the workplace policies, conditions and environment in effect at 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.