Offer Description - Product
Webex for Defense

This Offer Description is part of the General Terms or similar terms existing between You and Cisco (e.g., the End User License Agreement) (the "**Agreement**"). Capitalized terms, unless defined in this document, have the meaning in the Agreement. Any references to the Supplemental End User License Agreement or SEULA mean Offer Description.

1. Summary

1.1 **Description**. Webex for Defense (the "**Product**") is only available to the United States Department of Defense ("**DoD**") and DoD entities. The Product is a cloud IP-based communications system integrating voice, video, data, and mobility products and applications. It enables voice, video, and messaging communications via Cisco IP end points, mobile, and desktop soft clients. Depending upon the bundle you purchase, the Product may include some or all of the following features and functionalities:

- Cloud Calling
- Voice Messaging
- Instant Messaging and Presence ("**IM&P**")
- Mobile & Remote Access ("**MRA**")
- Emergency Call Handling
- Audio and Video Conferencing

1.2 **Bundles**. The Product is sold in the following two bundles:

- Calling (also referred to as "**D1**"). Bundle includes cloud calling and voice messaging, instant messaging and presence and mobility, licensed for multiple collaboration endpoints. A D1 subscription is intended for a single User, where a single User may be the primary user of one or multiple devices for collaboration.
- Calling & Conferencing (also referred to as "**D2**"). Bundle includes everything in D1, plus Cisco Meeting Server-powered meetings, a Cisco hosted meetings solution. A D2 subscription is for use by a single User, where that single User may be the primary user of multiple devices for collaboration and conferencing. A D2 User is authorized to schedule, host, or manage/operate an audio or video conference.

1.3 **Exclusions**. The Product does not include the following:

- Network connectivity from Defense Information Systems Agency's "Meet-me-Point" to Customer end points;
- PSTN or DSN service;
- 911 and/or E911 service;
- Provisioning of features by Cisco (e.g., dial plan configuration, end-user management, endpoint provisioning, etc.);

- Collection and/or importing of Cisco Partner data; or
- Installation and configuration outside the data centers on Cisco premises.

2. Support and Other Services

Your Cisco Partner will coordinate and ensure that You have sufficient Tier-1 and Tier-2 support as described below, provided however that (i) the Cisco Partner may agree with You that another entity besides Cisco, such as the Cisco Partner or You, may assume responsibility for its own Tier-1 and Tier-2 support (that entity will be referred to as the "**Support Entity**"), and (ii) if a Tier-2 Support Entity is unable to resolve a support issue because the issue requires support from Cisco, the Support Entity may escalate the issue to Cisco.

A Tier-1 Support Entity will:

- Provide Tier-1 support for troubleshooting as outlined below, provided that if the Support Entity fails to provide Tier-1 support as outlined below, then, upon notice from Cisco, the Cisco Partner will promptly purchase Tier-1 support from Cisco;
- Provide support for any on-premises device, endpoint, network, and non-cloud related issues; and
- Capture and provide details of reported issues, aid in replication and triaging issues as reasonably requested by Cisco; aid in testing fixes of issues, confirming issues are not related to User-provided hardware, software, applications, or other sources.

Tier-1 and Tier-2 Support includes the ability to:

- Provide general Product information;
- Explain how to use the service, devices, and soft clients;
- Provide configuration support;
- Filter non-technical problems from technical problems;
- Isolate problems and determine service defects;
- Analyze where the error occurred; and
- Restore improperly configured settings.

Cisco will provide 24x7x365 Tier-3 technical support to the Support Entity as relates to the real-time operation of the Product. Cisco is not responsible for supporting the Cisco Partner's or User's network (including network equipment) that is connected to the Product data center and/or User's premise.

3. Data Protection

Cisco shall maintain a United States Defense Information Systems Agency ("**DISA**") Provisional Authority (PA) at Impact Level 5 for the Product and maintain controls, monitoring, onshore support and reporting functions of the Product in accordance with the specifications and requirements established by DISA. Personal Data processed in connection with Your use of the Product is stored in the United States and not subject to international data transfers. If You have access to federal information, it is Your responsibility to ensure that such information is restricted to a DISA IL5 Authorized Environment.

4. Special Terms

4.1 **Conditions**. Cisco's obligation to provide the Product is dependent on the following conditions:

(1) The DISA provisions NIPRNet capacity, PSTN connectivity, and 911 and/or E911 service.

(2) Your network architecture authorizes and properly routes the Product traffic.

(3) DoD implements an approved secure network connection to NIPRNet for mobile access.

(4) Partner and/or You configure features to function properly, including when those features are dependent on other system configurations (e.g., dial plan, etc.).

(5) Calling, voice messaging, IM&P, and emergency calling features are supported between endpoints on Your network ("**IP LAN**"). (Some calling features may not be supported if they must traverse PSTN or other gateways that restrict and alter traffic.)

(6) The endpoint is a supported endpoint with capacity to support the features, as found here: https://www.cisco.com/c/en/us/solutions/industries/government/federal-government-solutions/secure-cloud-defense.html#~stickynav=2.

(7) DoD has sufficient network resources (bandwidth and latency) and routability between endpoints, and the DISA CAP functions properly. Cisco is not responsible for quality-of-service reductions or unavailability of features related to inadequate network resources or a lack of system connectivity.

(8) You use the hardwired Cisco IP Phones compatible with the Product identified here: https://www.cisco.com/c/en/us/solutions/industries/government/federal-governmentsolutions/secure-cloud-defense.html#~stickynav=2. Other Cisco IP Phones may be enabled if You are willing to accept the risk and approve an Authorization to Operate with the approved Cisco IP Phones included.

(9) You understand that the Jabber Client within the Product is supported on the following platforms: Microsoft Windows, Mac OS, Apple IOS, and Android.

(10) You and the Cisco Partner provide reasonable cooperation to Cisco and obtain the cooperation of applicable third parties.

4.2 **Access and Use**. Access and use of the Product, including the features referenced in Section 1 of this Offer Description, are dependent on the DoD providing necessary permissions and auxiliary capabilities. Cisco is not responsible for the delivery of these features if the following requirements are not met:

(A) Cloud Calling: DoD provides what Cisco determines is both a stable network connection from the User's endpoint to the Product and sufficient bandwidth between the calling parties to support the audio bandwidth requirements for the call to meet Cisco's quality standards.

(B) Audio and Video Conferencing: DoD provides network access between the User's endpoint and the Cloud Access Point ("**CAP**") with what Cisco determines is both a sufficient bandwidth and minimum network latency to allow the conference to take place. Conference traffic, both audio and video, are required to transition through the CAP to the Product data centers throughout the entire conference.

(C) Mobile & Remote Access: DoD must enable the User's mobile device to reach the Product through NIPRNet.

(D) Emergency Call Handling: DoD must provide 911/E911 services to Users. Cisco is not responsible for providing 911/E911 services directly to any Users.

4.3 **Authorized Third Party Use.** Authorized Third Parties, as defined in the Agreement, may include DoD-approved third party contractors only if the Cisco Partner ensures that, in addition to the uses authorized in the Use by Third Parties terms of the Agreement, (a) such third-party contractors are counted as a User when determining the subscription quantity, (b) Customer does not charge the third party contractor for use of the Product, and (c) Customer is responsible for all fees incurred by such third party contractor.

4.4 **License Models.** Both the D1 and D2 bundles are offered in the Enterprise Agreement model (payment for enterprise-wide use) and the Named User model (payment is per user).

(A) Enterprise Agreement model. The Enterprise Agreement license model is governed by the Cisco Enterprise Agreement Program Terms, which require Your acknowledgement when You place Your order.

(B) Named User model. Under the Named User model, Your payment obligation and right to use the Product is based on the number of Named Users on Your order, regardless of usage. If the number

of Named Users accessing the Product exceeds the number of Named Users on Your order, Your payment obligation will increase to reflect the additional Named Users. Billing reconciliation may occur at any time after You exceed the number of Named Users on Your order.

A "**Named User**" in the Named User license model, is a User as defined in the Agreement, including any devices used for add-ons (e.g., common area end devices). Each Named User receives a unique account that may not be shared or used by anyone other than the designated employee or contractor. A Named User's account may not be transferred to another person, except upon: (a) termination of the Named User's employment or (b) Cisco's prior written approval. You are solely responsible for the acts and omissions of, or any fees incurred by, Your Named Users.

4.5 **Term**. The initial term starts on the earlier of (a) 30 days from the date Cisco notifies You that any portion of the Product is ready for You to start provisioning; or (b) the date any portion of the Product has been provisioned and lasts for the Use Term.

4.6 **PSTN Requirement and Emergency Response Disclaimer - Emergency Call Handling**. If You require emergency call location identification, You can use the Cisco Unified Communications Manager Native Emergency Call Routing feature. The Native Emergency Call Routing feature provides You the ability to define Emergency Location Identification Numbers ("**ELINs**") at the device pool level or the device level, so that a device's location can be determined and identified at the public safety answering point ("**PSAP**"). This feature does not include any services with respect to the PSAP. Cisco is not responsible for confirming that (a) the ELINs are correctly configured, (b) an accurate device location has been established or (b) routing to the PSAP is occurring as intended.

4.7 **Third-Party Solutions**. If authorized by the DoD, Cisco will allow the Cisco Partner to provision third-party solutions to provide User location information for PSAP call routing, provided that if such third party integrations require an API, the Cisco Partner will utilize the APIs authorized by Cisco for this Product.

4.8 **Accounts for Personal Use**. Cisco recommends that You use Your personal email address to access the Product for personal use. If You use Your employer-issued email address to access the Product for personal use and Your employer later purchases the Product from Cisco, You will be required to update the email address associated with Your personal account to a personal email address. You can change Your email address by following these instructions. If You do nothing, Your personal account and Personal Data will be controlled by Your employer and Your use will be subject to Your employer's policies.