

Transition Toward an Intelligent Cloud Ready Architecture

<http://github.com/ciscocodevnet/ps-crn>

Steven Carter - Principal Systems Engineer

Craig Hill - Distinguished Systems Engineer

Chris Hocker - Consulting Systems Architect

Introduction

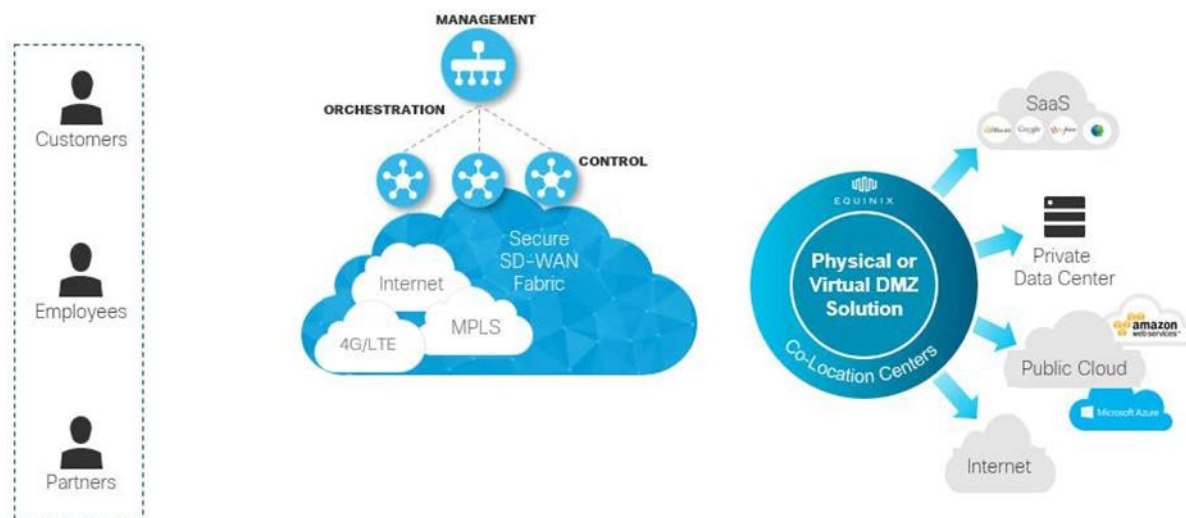
There have been several impactful architectural shifts in IT over the past several years, but none within U.S. federal agencies larger than the public cloud. The benefits and strategic “cloud first” mandates within U.S. Federal agencies have created a new set of requirements as applications move from the on-premises data center to the remote, less controlled public cloud, Infrastructure as a Service/Software as a Service (IaaS/SaaS). This transformation of application “location” is having an impact on several indirect factors – specifically how agencies approach next-generation WAN designs requirements, but also security – specifically controlling the access to applications that reside in locations with far less visibility and control (that is, in the public cloud) than they once did in their localized on-premises data centers.

The purpose of this White Paper is to provide an overview and component description of the Cloud Ready Network (CRN) architecture and introduce the concept of “cloud edge” through the use of colocation centers, and provide a generic Bill of Materials (BoM) to accelerate the process of procurement and build-out for the agency to adopt rapidly. (Note: While this document offers recommendations, readers are encouraged to leverage any variation or adjustment to the proposed solutions and/or components to best align with their agencies' requirements and needs).

Cloud Ready Network (CRN) Overview

The CRN architecture can be divided into two general domains, each of which supports critical components for securing and maintaining the Quality of Experience (QoE) needed as the applications relocate to the public cloud. The two key components include, as shown in the figure below: 1) the secure WAN domain (the SD-WAN fabric); and 2) the colocation center domain for the newly defined “cloud edge” demarcation.

Aligning WAN Design with Applications Moving the DMZ Perimeter to Colocation Centers



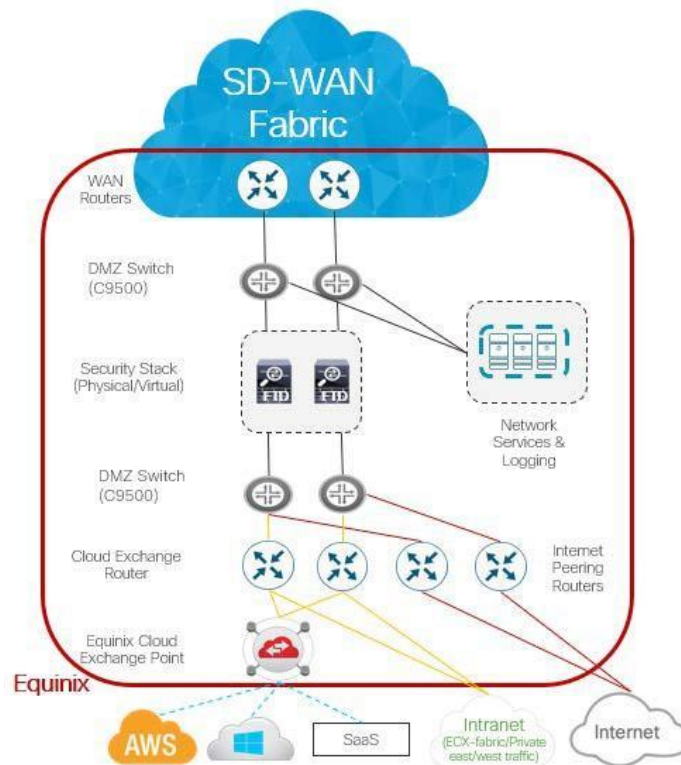
WAN Domain

The WAN domain can leverage any new or existing WAN solutions. Cisco SD-WAN [2] is transforming into a preferred solution for this CRN design because of its application-intelligent routing awareness over any transport (including MPLS, Internet, 4G/LTE/5G). This applies either to the colocation center and through the security stack, or extending the WAN edge router directly into the public cloud provider via cloud on-ramp capabilities for IaaS and SaaS [3]. Alternative WAN solutions for extending the agency WAN into the colocation center can also include private IP, MPLS, or segment routing. Cisco recommends the use of WAN MACsec [4] for securing the WAN links terminating in the agency rack inside the colocation centers.

Colocation Center Domain

The colocation center domain introduces a newer concept we define as “cloud edge,” leveraging a private cage within the colocation facility for hosting both the WAN routers (discussed above) and the remote security stack for securing and controlling access to the public cloud IaaS/SaaS resources.

The hosting facility being leveraged for this proposal is through Equinix [5]. Equinix provides cross-connection services that simplify the interconnection between the transport and public cloud service providers. This architecture proposes that a government agency leverages a private cage/rack within Equinix to establish a new “cloud edge” demarcation point for security and visibility controls for agency traffic going to, or coming from, the applications residing in public cloud IaaS/SaaS services. This establishes a tighter security domain closer to the public cloud exchange point. Furthermore, this new “cloud edge” in Equinix establishes the security controls and visibility closer to the applications (that is, the application in the cloud), eliminating the need for a back-haul to the security stack at the agency location that is not in line to the cloud edge. The strategic location using Equinix greatly reduces “hair-pinning” traffic and reduces latency and improves overall application performance to the cloud services, specifically for multicloud environments (for example, traffic traversing from cloud provider 1 to cloud provider 2).



Finally, for the purposes of this proposal, the security guidelines are based on the DHS Trusted Internet Connection Reference Architecture Document v2.2 design recommendations [6] and follow all of the required services for “External Connection Security Pattern” as stated by DHS policy.

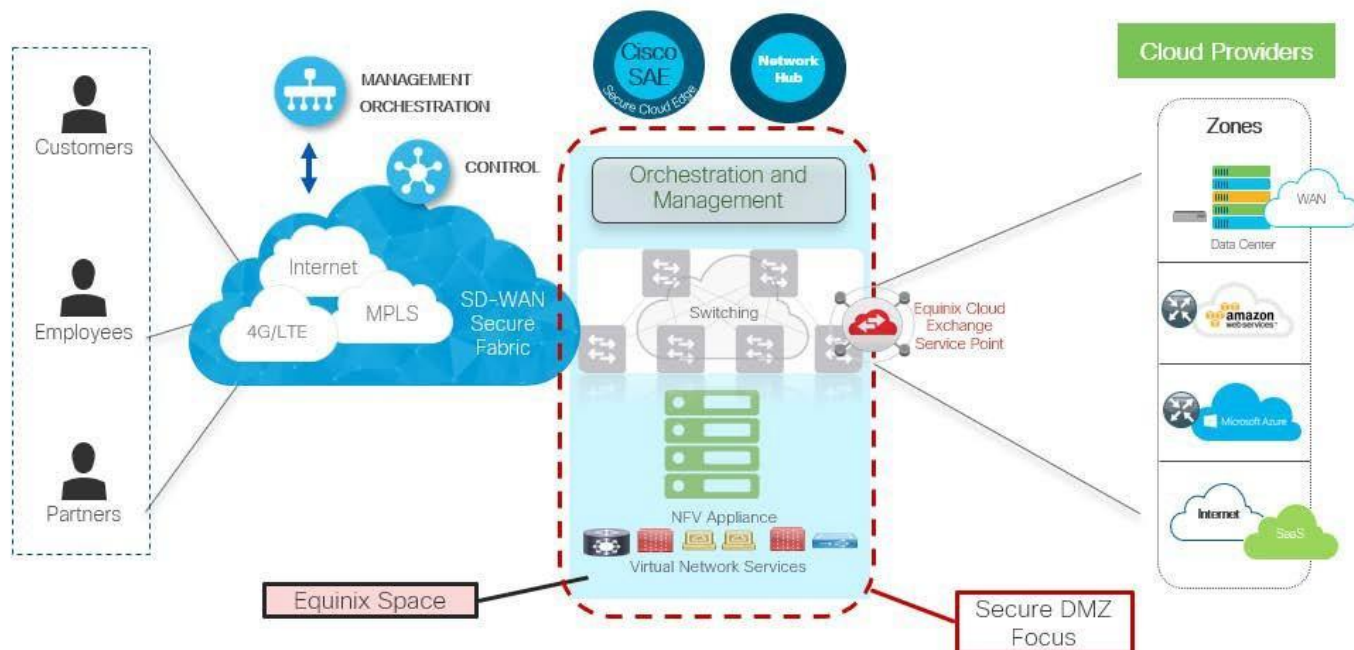
Suggested Security Stack Components

To meet the requirements for this proposal, Cisco proposes the following solutions (see Table 1 below) at both the 1 Gb [7] and the 10 Gb [8] options which fully comply with DHS guidelines as mentioned above. More details for both the 1 Gb and the 10 Gb Bill of Materials (BoM) examples can be found below in Appendix A.

Table 1 – High-Level Product Solutions

Service Function	1 Gb Solution Products	10 Gb Solution Products
Agency Routers	Cisco ASR 1001-X	Cisco ASR 1002-HX
DMZ Switches (Inside)	Cisco Catalyst 9500-40G	Cisco Catalyst 9500-40G
Security Stack Appliance	Cisco Firepower 2110 NGFW	Cisco Firepower 4140 NGFW
DMZ Switches (Outside)	Cisco Catalyst 9500-40G	Cisco Catalyst 9500-10G
Cloud Exchange Routers	Cisco ASR 1001-X	Cisco ASR 1002-HK
Internet Routers	Cisco ASR 1001-X	Cisco ASR 1002-HK
Logging/Services Compute	Cisco HyperFlex	Cisco HyperFlex

Secure Centralized DMZ Architecture



Reference Links

- [1] Public Sector Cloud Ready Network Repo:
<https://github.com/ciscodcvnet/ps-crn>
- [2] Cisco SD-WAN:
<https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/index.html>
- [3] Cisco SD-WAN – Cloud On-Ramp:
<https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/cloud-onramp.pdf>
- [4] Introduction to WAN MACsec:
<https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Security/MACsec/WP-High-Speed-WAN-Encrypt-MACsec.pdf>
- [5] Equinix Overview:
<https://www.equinix.com/interconnection-services/>
- [6] DHS Trusted Internet Connection Reference Architecture Document v2.2 Design Recommendations:
https://www.dhs.gov/sites/default/files/publications/TIC_Ref_Arch_v2.2_2017.pdf
- [7] Appendix A – 1 Gb Solution – Bill of Materials
- [8] Appendix A – 10 Gb Solution – Bill of Materials

Appendix A

1 Gb Solution - Bill of Materials

All prices shown in USD

Part Number	Description	Unit List Price	Qty	Extended Net Price
ASR1001-X	Cisco ASR1001-X Chassis, 6 built-in GE, Dual P/S, 8 Gb DRAM	17,000.00	4	68,000.00
CON-SSSNT-ASR1001X	SOLN SUPP 8X5XNBD Cisco ASR1001-X Chassis 6 built-in GE Du	2,170.49	4	8,681.96
M-ASR1001X-8 Gb	Cisco ASR1001-X 8 Gb DRAM	0.00	4	0.00
NIM-BLANK	Blank faceplate for NIM slot on Cisco ISR 4400	0.00	4	0.00
SPA-BLANK	Blank Cover for regular SPA	0.00	4	0.00
ASR1001-X-PWR-AC	Cisco ASR1001-x-AC Power Supply	0.00	8	0.00
CAB-C13-CBN	Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	0.00	8	0.00
ASR1K-CLOUD-EDGE	ASR1k - for Cloud Edge deployments - tracking only	0.00	4	0.00
CON-SSSNT-ASR1KCLE	SOLN SUPP 8X5XNBD Cisco ASR1k - for Cloud Edge deployments	0.00	4	0.00
SLASR1-IPB	Cisco ASR 1000 IP BASE License	9,000.00	4	36,000.00
CON-SSSNT-SLASR1IK	SOLN SUPP 8X5XNBD Cisco ASR 1000 IP BASE License	912.00	4	3,648.00
NETWORK-PNP-LIC-O	Network Plug-n-Play License optional zero-touch device	0.00	4	0.00
SASR1K1XUCMK9-1610	Cisco ISR ASR1K Series SD-WAN IOS XE Universal	0.00	4	0.00
LIC-DNA-ADD	Cisco DNA Subscription License for Routing	0.00	4	0.00
SDWAN-ONPREM	On Premise Deployment of SD-WAN	0.00	4	0.00
ASR1001X-DNA	ASR1001-X Platform for DNA	0.00	4	0.00
DNA-P-1G-A-3Y	Cisco DNA Advantage on Premise Lic, 2G, 3Y	16,899.84	4	67,599.36
Initial Term - 36.00 Months Auto Renewal Term - 0 Months Billing Model - Prepaid Term				
SVS-DNA-P-ADV	Embedded support- Cisco DNA Advantage On Premise LLC	0.00	4	0.00
Initial Term - 36.00 Months Auto Renewal Term - 0 Months Billing Model - Prepaid Term				
SDWAN-DNA-A	Cisco DNA Advantage for DNA Center	0.00	4	0.00
Initial Term - 36.00 Months Auto Renewal Term - 0 Months Billing Model - Prepaid Term				
FPR2110-NGFW-K9	Cisco Firepower 2110 NGFW Appliance, 1U	10,995.00	2	21,990.00
CON-SSSNT-FPR21FWN	SOLN SUPP 8X5XNBD Cisco Firepower 2110 NGFW Appliance, 1U	3,696.00	2	7,392.00
FPR2110T-TMC	Cisco FPR2110 Threat Defense Threat, Malware and URL License	0.00	2	0.00
L-FPR2110T-TMC-3Y	Cisco FPR2110 Threat Defense Threat, Malware and URL License 3Y Subs	13,460.00	2	26,920.00
CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	0.00	2	0.00
SF-F2K-TDS6.2.3-K9	Cisco Firepower Threat Defense software v6.2.3 for FPR2100	0.00	2	0.00
FPR2K-SSD100	Firepower 2000 Series SSD for FPR-2110/2120	0.00	2	0.00
FPR2K-SSD-BBLKD	Firepower 2000 Series SSD Slot Carrier	0.00	2	0.00
C9500-40X-A	Catalyst 9500 40-port 10Gig switch, Network Advantage	26,254.99	2	52,509.98
CON-SSSNT-C95004XA	SOLN SUPP 8X5XNBD Catalyst 9500 40-port 10Gig switch	1,022.85	2	20,445.70
C9500-NM-BLANK	Catalyst 9500 network module blank cover	0.00	2	0.00
S9500UK9-169	UNIVERSAL	0.00	2	0.00
C9500-NM-A	C9500 Network Stack, Advantage	0.00	2	0.00
PWR-C4-950WAC-R	950W AC Config 4 Power Supply front to back cooling	0.00	2	0.00
PWR-C4-950WAC-R/2	950W AC Config 4 Power Supply front to back cooling	2,100.00	2	4,200.00
CAB-C15-CBN	Cabinet Jumper Power Cord, 250 VAC 13A, C14-15 Connectors	0.00	2	0.00
C9500-DNA-40X-A	C9500 DNA Advantage, Term Licenses	0.00	2	0.00
C9500-DNA-A-5Y	DNA Advantage 5 Year License	19,360.00	2	38,720.00
Valid through		Product Total		182,699.98
FOB Point		Service Total		40,167.66
Note:		Subscription Total		133,239.36
		Total Price		356,107.00

I0 Gb Solution – Bill of Materials

All prices shown in USD

Part Number	Description	Unit List Price	Qty	Extended Net Price
ASR1002-HX-DNA	Cisco ASR 1002-HX, 4x10GA+4x1GE, Dual PS with DNA Support	122,500.00	4	490,000.00
CON-SSSNT-ASR100HX	SOLN SUPP 8X5XNBD Cisco ASR 1002-HX, 4x10GE+4x1GE, Dual PS	37,227.00	4	148,908.00
SL-ASR1002HX-NA	Network Advantage License for Cisco ASR1002HX-DNA	0.00	4	0.00
CON-SSSNT-SLASR12A	SOLN SUPP 8X5XNBD Network Advantage License for Cisco ASR10	0.00	4	0.00
M-ASR1002HX-16 Gb	Cisco ASR1002-HX 16 Gb DRAM	0.00	4	0.00
EPA-BLANK	Ethernet Port Adapter (EPA) Blank Cover	0.00	4	0.00
SASR1KH9K9-169	UNIVERSAL	0.00	4	0.00
ASR1002HA-IPSECHW	Cisco ASR1002-HX Crypto Module with no default throughput	0.00	4	0.00
CON-SSSNT-ASR10S2H	SOLN SUPP 8X5XNBD Cisco ASR1002-HX Crypo Module with no d	1,521.00	4	6,084.00
ASR1000X-AC-750W	Cisco ASR1002-HX 750W AC Power Supply	0.00	8	0.00
CAB-C12-C14-AC	Power cord, C13 to C14 (recessed receptacle), 10A	0.00	8	0.00
DNA-P-10G-A-3Y	Cisco DNA Advantage on Premise Lic, 20G, 3Y	72,000.00		288,000.00
Initial Term - 36.00 Months Auto Renewal Term - 0 Months Billing Model - Prepaid Term				
SVS-DNA-P-ADV	Embedded Support - Cisco DNA Advantage On Premise Lic	0.00		0.00
Initial Term - 36.00 Months Auto Renewal Term - 0 Months Billing Model - Prepaid Term				
SDWAN-DNA-A	Cisco DNA Advantage for DNA Center	0.00		0.00
Initial Term - 36.00 Months Auto Renewal Term - 0 Months Billing Model - Prepaid Term				
FPR4140-FTD-HA-BUN	Cisco Firepower 4140 Threat Defense Chss, Subs HA Bundle	0.00	1	0.00
FPR4140-NGFW-K9	Cisco Firepower 4140 NGFW Appliance, 1U, 2x NetMod Bays	209,995.00	2	419,990.00
CON-SSSNT-FPR414GK	COLN SUPP 8X5XNBD Cisco Firepower 4140 NGFW Appliance, 1U	70,560.00	2	141,120.00
FPR4K-PWR-AC-1100	Firepower4000 Series 1100W AC Power Supply	0.00	2	0.00
CAB-C130C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	0.00	4	0.00
SF-F4K-FXOS-2.3-K9	Cisco FXOS v2.3 for FPR4100	0.00	2	0.00
SF-F4K-TDS6.2.3-K9	Cisco Firepower Threat Defense software v6.2.3 for FPR4100	0.00	2	0.00
FPR4K-SSD400	Firepower 4000 Series SSD for FPR-4140/4150	0.00	2	0.00
FRP4K-SSD-BBLKD	Firepower 4000 Series SSD Slot Carrier	0.00	2	0.00
FPR4K-PWR-AC-1100	Firepower 4000 Series 1100W AC Power Supply	0.00	2	0.00
FPR4K-ACC-KIT	FPR4K Hardware Accessory Kit	0.00	2	0.00
FPR4K-FAN	Firepower 4000 Series Fan	0.00	12	0.00
Valid through		Product Total		966,699.98
FOB Point		Service Total		316,557.70
Note:		Subscription Total		725,127.50
		Total Price		2,008,385.18

All prices shown in USD

Part Number	Description	Unit List Price	Qty	Extended Net Price
FPR4K-RACK-MNT	Firepower 4000 Series Rack Mount Kit	0.00	2	0.00
GLC-TE	1000BASE-T SFP transceiver module for Category 5 copper wire	0.00	2	0.00
FPR4K-NM-BLANK	Firepower 4000 Series Network Module Blank Slot Cover	0.00	2	0.00
FPR4K-NM-BLANK	Firepower 4000 Series Network Module Blank Slot Cover	0.00	2	0.00
L-FPR-4140T-TMC=	Cisco FPR4140 Threat Defense Threat, Malware and URL License	0.00	2	0.00
L-FPR4140-TMC-3Y	Cisco FPR4140 Threat Defense, Malware and URL 3Y Subs	199,203.75	2	398,407.50
C9500-40X-A	Catalyst 9500 40-port 10Gig switch, Network Advantage	26,254.99	2	52,509.98
CON-SSSNT-C95004XA	SOLN SUPP 8X5XNBD Catalyst 9500 40-port 10Gig switch	10,222.85	2	20,445.70
C9500-NM-BLANK	Catalyst 9500 Network Module blank cover	0.00	2	0.00
S9500UK9-169	UNIVERSAL	0.00	2	0.00
C9500-NW-A	C9500 Network Stack, Advantage	0.00	2	0.00
PWR-C4-950WAC-R	950W AC Config 4 Power Supply front to back cooling	0.00	2	0.00
PWR-C4-950WAC-R/2	950W AC Config 4 Power Supply front to back cooling	2,100.00	2	4,200.00
CAB-C15-CBN	Cabinet Jumper Power Cord, 250 VAC 13A, C14-C15 Connectors	0.00	4	0.00
C9500-DNA-40X-A	C9500 DNA Advantage,Term Licenses	0.00	2	0.00
C9500-DNA-A-5Y	DNA Advantage 5 Year License	19,360.00	2	38,720.00
Valid through		Product Total		966,699.98
FOB Point	None	Service Total		316,557.70
Note:		Subscription Total		725,127.50
		Total Price		2,008,385.18

Compute System – Network Services and Logging – Bill of Materials

All prices shown in USD

Part Number	Description	Unit List Price	Qty	Extended Net Price
HXAF2X0C-M5S	Cisco Hyperconverged System	0.00	1	0.00
HXAF220C-M5SX	Cisco HyperFlex HX220c M5 All Flash Node	4,190.00	3	12,570.00
CON-SNT-AF220CM5	SNTC 8X5XNBD Cisco HyperFlex HX220c M5 All Flash Node	3,033.00	3	9,099.00
UCSC-BBLKD-S2	USC C-Series M5 SFF drive blanking panel	0.00	6	0.00
HXAF220C-BZL-M5S	HXAF220C M5 Security Bezel	0.00	3	0.00
HX-MR-Z32G2RS-H	32 Gb DDR4-2666-MHz RDIMM/PC4-21300/dual rant/x4/1.2v	2,150.00	48	103,200.00
HX-SD38T61X-EV	3.8TB 2.5 Inch Enterprise Value 6G SATA SSD	9,888.00	18	177,984.00
HX-SD16T123X-EP	1.6TB 2.5in Enterprise Performance 12G SAS SSD (3X endurance)	8,386.00	3	25,158.00
HX-SD250GM1X-EV	240 Gb 2.5 inch Enterprise Value 6G SATA SSD	734.00	3	2,202.00
HX-M2-240 Gb	240 Gb SATA M.2	535.00	3	1,605.00
HX-MLOM-C25Q-04	Cisco UCS VIC 1457 Quad Port 10/25G SFP28 CNA MLOM	2,248.00	3	6,744.00
HX-PSU1-1050W	Cisco UCS 1050W AC Power Supply for Rack Server	729.00	6	4,374.00
CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Link	0.00	6	0.00
HX-MSD-32G	32 Gb Micro SD Card for UCS M5 servers	220.00	3	660.00
HX-RAILF-M4	Friction Rail Kit for C220 M4 rack servers	175.00	3	525.00
UCSC-HS-C220M5	Heat sink for UCS C220 M5 rack servers 150W CPUs & below	0.00	6	0.00
UCS-MSTOR-M2	Mini Storage carrier for M.2 SATA/NVME (holds up to 2)	0.00	3	0.00
HX-SAS-M5	Cisco 12G Modular SAS HBA (max 16 drives)	1,031.00	3	6,093.00
HX-VSP-6-5-STD-D	Factory Installed - VMware vSphere 6.5 Std SW and Lic (2CPU)	4,589.84	3	13,769.52
CON-ECMU-HX65STDD	SWSS UPGRADES Factory Installed - VMware vSphere 6.5 Std SW	2,202.00	3	6,606.00
HX-VSP-6-5-STD-DL	Factory Installed - vSphere 6.5 SW Download	0.00	3	0.00
HX-CPU-6140	2.3 GHx 6140/150W 18C/24.75MB Cache/DDR5 2666MHz	8,000.00	6	48,000.00
HX-FI-6454	UCS Fabric Interconnect 6454	52,000.00	2	104,000.00
CON-SNT-HXFI6454	SNTC-8X5XNBD UCS Fabric Interconnect 6454	4,152.00	2	8,304.00
N10-MGT016	UCS Manager v4.0	0.00	2	0.00
SFP-H25G-CU1M	25GBASE-CU SFP28 Cable 1 Meter	125.00	6	750.00
USC-PSU-6332-AC	UCS 6332 Power Supply/100-240VAC	1,400.00	4	5,600.00
CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	0.00	4	0.00
USC-ACC-6332	USC 6332/6454 Chassis Accessory Kit	0.00	2	0.00
USC-FAN-6332	UCS 6332/6454 Fan Module	0.00	8	0.00
HXDP-S001-3YR=	Cisco HyperFlex Data Platform Standard Edition 3 Yr Subscription	0.00	3	0.00
HXDPS001-3Y	HyperFlex Data Platform Standard Edition 3 Yr Subscription	24,750.00	3	0.00
Valid through		Product Total		510,234.52
FOB Point	None	Service Total		24,009.00
Note:		Subscription Total		74,250.00
		Total Price		608,493.52