Central Board of Indirect taxes and Customs (CBIC)

Department of Revenue, Ministry of Finance, Government of India

CBIC Connectivity Partner Protocol

October 2022

Table of Contents

1. Overview

Reference is invited to CBIC Notification No. 26/2009-Customs(N.T.) dated 17th March 2009 bringing into effect the "Handling of Cargo in Customs Areas Regulations 2009" (referred in short as 'Regulations') and Circulars Nos. 13/2009-Customs dated 23rd March 2009, No. 21/2009-Customs dated 4th August 2009 and Circular No.4/2011-Customs dated 10th January 2011.

The above Regulations/Circular issued by CBIC prescribe, inter-alia, that the networking, communication equipments, Uninterrupted Power Supply System, desktops, servers, printers other computer peripherals and secure connectivity to the CBIC Data Centers as specified by the Directorate General of Systems shall also be provided by the custodians. It has further been provided that these instructions apply to all the Custodians of ports, airports, Inland Container Depots (ICDs), Container Freight Stations (CFSs), Integrated Check posts (ICPs), Land Customs Stations (LCSs), the major ports notified under the Major Ports Act 1963 and the airports notified under the Airports Authority of India Act, 1994.

Furthermore, Special economic zones have also been deemed to be Ports/ICDs under section 7 of the Customs Act 1962

Here in after, Custodians and other formations for e.g. SEZ, requiring access to CBIC's Data Centers will be referred to as **"CBIC Connectivity Partner".**

This document provides the current technical details for network connectivity and IT infrastructure for "CBIC connectivity Partner".

2. Requirements:

1. The “CBIC Connectivity Partner” would be required to provide MPLS connectivity for access to the Data Centers. M/s BSNL and M/s TCL are the authorized service providers of CBIC for primary connectivity and alternate connectivity respectively as they already have presence at the Data Centers. Refer to Annexure 1 for various options of connectivity to the Data Center and Annexure 9 for details of SPOC of authorized MPLS service providers.

2. It is mandatory for the “CBIC Connectivity Partner” to take Partner MPLS connectivity to the Data Center-Delhi as well as Data Center – Chennai to ensure business continuity in the event of a contingency as well as disaster recovery.

3. In case of MPLS, the last mile connectivity to the site should preferably be through Optical Fiber Cable (OFC) or Radio Frequency(RF). In case of Optical fiber, it is suggested that the underground fiber laid should have proper ducting and the routes taken by the fiber shall avoid digging prone areas thereby ensuring minimum or no disruption to CBIC services. In case of RF, site needs to share Annexure 6 B with the required details.

4. A bandwidth estimate of about 250 kbps per user should be used while calculating the total MPLS bandwidth requirement for the whole site.

5. The “CBIC Connectivity Partner” is responsible for providing all the equipment for IT Infrastructure and connectivity, including Local Area Network (LAN) Infrastructure such as desktops, printers (including Line Printers), UPS, Routers, LAN Switches, file & print servers, air-conditioning, power backup, furniture etc. The Specifications of equipment deployed by CBIC at its locations are detailed in Annexure 2 for reference. The infrastructure procured by “CBIC Connectivity Partner” must have equivalent or higher specifications. The annual maintenance and proper upkeep of these equipments would also be the responsibility of the “CBIC Connectivity Partner”.

6. To maintain secure access to CBIC’s Data Center, the IT setup deployed at the site would have to integrate with CBIC’s security agents provided in Annexure 3.

7. The “CBIC Connectivity Partner” would be required to provision Resident Engineers (R.E.) as per their working hours who would be responsible for day-to-day support and maintenance of the Local IT Infrastructure. Minimum qualification of R.E.s (as deployed by CBIC) is provided in Annexure 4. The “CBIC Connectivity Partner” through their resident engineers would have to ensure and monitor that virus definition of antivirus is updated to latest version, DLP Agent should be online and APT Sensor is up and running fine.

8. The “CBIC Connectivity Partner” should ensure that CBIC LAN is segregated for security and not connected to their local LAN.

9. “CBIC Connectivity Partner” would be required to sign a Non-Disclosure Agreement (NDA) on a stamp paper. The NDA has to be countersigned by the Jurisdictional Principal Commissioner/Commissioner of Customs. The format of this agreement is enclosed at Annexure 5. Once the infrastructure is ready, the “CBIC Connectivity Partner” is required to fill up the Infrastructure checklist enclosed at Annexure 6 & 6A, and have it verified and signed by the concerned customs officer located at the site. The Non-Disclosure Agreement and

Infrastructure checklist in original is required to be submitted to the Jurisdictional Principal Commissioner/Commissioner of Customs.

10. The above stated documents have to be shared by Concerned Nodal Officer/System Manager over email to CBIC (cbic.lanwan@icegate.gov.in) for issue of LAN IP pool**.**

3. Important instructions for "CBIC Connectivity Partners"

1. All "CBIC Connectivity Partners" must ensure that the infrastructure at their locations is compliant with the latest guidelines as shared by CBIC under the Partner Connectivity Document.

2. In request for additional LAN IPs/ new LAN IPs, the "CBIC Connectivity Partner" should re-share the infrastructure checklist to highlight the compliance with CBIC requirements. For all additional IPs a mapping of additional users with systems needs to be shared beforehand by the respective Systems Manager/ Alternate Systems Manager

3. The "CBIC Connectivity Partner" understand and agree that the LAN IPs allotted to the site may be blocked in scenarios where in security concerns are observed for the site. Refer Annexure – 8 for details of the process for unblocking IPs.

4. In case there is any issue which is related to WAN connectivity, they need to contact their local service providers and get it resolved. Also, all LAN related issues and configurations will be site's responsibility.

5. If the "CBIC Connectivity Partner" is looking to set up a container scanner, they have to procure their own infrastructure. Kindly refer to Annexure 7 for details.

6. Audit for the security practices, implementation of security policy and vulnerability assessment can be conducted by a 3rd party appointed by CBIC as and when it is required. The report of the 3rd party auditors should rate the security implementation in three grades viz. Satisfactory, Requires Improvement and Unsatisfactory. The report of findings should be submitted to CBIC with copy to concerned "CBIC Connectivity Partner" for consideration. CBIC will randomly select few sites for security audit. For any deviation found from the policy as per the audit report, the rectification will have to be borne by the "CBIC Connectivity Partner". It is to be noted that the cost of the audit shall be borne by the "CBIC Connectivity Partner" at the prescribed rate by CBIC.

Annexure 1 – Types of Connectivity

A. Connectivity Options to the CBIC Data Centers

a) Access through the MPLS Cloud:

The "CBIC Connectivity Partner" can connect to CBIC Data Center - Delhi and CBIC Data Center – Chennai with the partner MPLS Cloud primarily through M/s BSNL and alternatively through M/s TCL. (VPN Client is not required in case of MPLS connectivity).

b) VPN over BroadBand through BSNL (VPNoBB):

In case MPLS network is not available, the site can connect to Data Center by procuring VPN over Broadband connection through M/s BSNL with "CBIC" domain (VPN Client is not required in case of this connectivity).

c) VPN over Internet (VPNoI):

VPN over internet can also be taken by procuring internet connectivity through any ISP and getting VPN IDs created for users through Saksham Seva Helpdesk. For VPN ID Creation/Modification, Users can fill the required templates (enclosed in annexure) and reach out to Saksham Seva through their Nodal Officers/System Managers (VPN client is required in this case and the link for installation of the same are provided by Saksham Seva to the user).

Note:

1) The VPNoBB and VPNoI connectivity should only be procured by sites with less than 5 users or as an alternate to the MPLS connectivity to ensure business continuity in case of frequent disruptions.
2) All the Network Switches and Routers at the location accessing CBIC's Data Centers must support 802.1x to enable integration with CBIC's Network Access Control (NAC).

B. Connectivity of stakeholders authorized by CBIC for Message Exchange

Stakeholders having voluminous and time-sensitive message exchange has an option to build point to point links between the Stakeholder's Data Center and Data Centers of CBIC at New Delhi and Chennai. In this case, partner locations will be connected to both Data Center-Delhi & Data Center-Chennai of CBIC on separate Point to Point Links. CBIC will only work as a facilitator and the responsibility for arranging the actual connectivity remains with the partner agency.

Secure File Transfer Protocol (SFTP/MFTP) can also be used as Communication Mechanism for Message Transfer with other CBIC partners. With Secure file transfer Protocol, users can pick up and drop files on the dedicated file transfer server in the directories assigned to their respective user ids in a secure manner. It may be noted that plain file transfer protocol (FTP) will not be allowed.

a) Details Required for Creation of SFTP/MFTP User ID for Message Exchange

Please fill the attached template.

SFTP-MFTP Creation Template.xlsx

Tab 1 – User creation template

Tab 2 – Firewall port opening template

After filling the required template, send a mail to the Icegate shift manager (shift.manager@icegate.gov.in), keeping copy to CBIC Lanwan Team (cbic.lanwan@icegate.gov.in) and Saksham Seva (saksham.seva@icegate.gov.in).

b) Password policy and reset procedure

i. User will be provided with a unique user-id and password at the time of user creation.
ii. Newly provided password will expire after 60 days. User will start getting the notification to reset the password within 7 days prior to the expiration.
iii. User needs to raise an interaction by sending an email to Saksham.seva@icegate.gov.in with a copy to cbic.server@icegate.gov.in. Password reset request should be routed through the Nodal officer/System Manager or along with their approval on mail.

Annexure 2 – Minimum Specifications for Equipment

Minimum Specifications for Equipment at "CBIC Connectivity Partner" Locations

1. **Specifications for Desktop**

ITEM	Specifications of equipment deployed by CBIC
Memory	8GB DDR4-2133 SODIMM (1x8GB) RAM
Processor	Intel Core i5-6500 3.2G 6M 2133 4C CPU
Operating System	Windows 10 Pro 64-bit OS
Chipset	Yes (Intel® 100 Series H Chipset)
Display	20-inch or above
Peripherals	USB Business Slim Keyboard #ACJ, USB Mouse
Network interface	10/100/1000 Mbit/s Gigabit Ethernet LAN, Broadcom BCM943228Z 802.11n M.2 noBT NIC
Network	• TCP/IP with DNS and DHCP wake on LAN • DHCP support for automatic firmware upgrades and unit configuration • PPP (PPPOE , PPPTP)
Power supply	120W External Power Supply
Bundled software (with support & upgrades)	• Office productivity suite • Mozilla Firefox (Version 38 or later) • Adobe acrobat reader • flash player • JRE 8.0 or above
Regulatory standards	ENERGY STAR Certified Label
Security	TPM 1.2 security chip, hard drive encryption

2. **Specifications for 24 Ports Switch**

S.No.	Specifications of equipment deployed by CBIC
1.	24 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T)
2.	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet
3.	Throughput- up to 95.2 MBPS Routing/Switching capacity- 160 Gbps
4.	Non-blocking and distributed forwarding hardware architecture
5.	All interfaces provide wire speed forwarding for both OFC and copper modules
6.	IP Multicast - RFC 3376 IGMPv3
7.	Switches support 8 hardware queues per port
8.	Dynamic Host Configuration Protocol (DHCP) snooping
9.	Switch supports LLDP and LLDP-MED capabilities
10.	IP source guard & Dynamic ARP Inspection/ Protection
11.	Secure Shell (SSH) Protocol and Simple Network Management Protocol Version 3 (SNMPv3) to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.
12.	1 RJ-45 serial console port 1 RJ-45 out-of-band management port
13.	Delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3
14.	Provides up to 336 Gbps of stacking throughput; each 4-port stacking module can support up to 42 Gbps in each direction per stacking port
15.	The Switch supports internal redundant power supply
16.	Advanced classifier-based QoS
17.	FTP for upgrading the operating System
18.	IEEE 802.1x support
19.	IEEE 802.3ad Link Aggregation Protocol (LACP) and HPE port trunking
20.	Supports management via CLI, Web interface SNMP v1,v2,v3 Manageable through both IPv4 & IPv6 with standard security features of both IPv4 & IPv6

21.	The stacking on the Switch provides the functionality to configure multiple switches in a single switching unit. Each unit/stack has the capability to be managed using a single IP address.
22.	Layer 3 Switch with following features like static IP routing OSPF, OSPFV3, RIP and policy based routing.
23.	– IPv6 host –Dual stack (IPv4 and IPv6) –MLD snooping – IPv6 ACL/QoS – IPv6 routing –6in4 tunneling

3. Specifications for 48 ports Switch

S.No.	Specifications of equipment deployed by CBIC
1.	48 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T)
2.	Mounts in an EIA-standard 19 in. telco rack or equipment cabinet
3.	Throughput- up to 190.5 MBPS Routing/Switching capacity- 320 Gbps
4.	Non-blocking and distributed forwarding hardware architecture
5.	All interfaces provide wire speed forwarding for both OFC and copper modules
6.	IP Multicast - RFC 3376 IGMPv3
7.	Switches support 8 hardware queues per port
8.	Dynamic Host Configuration Protocol (DHCP) snooping
9.	Switch supports LLDP and LLDP-MED capabilities
10.	IP source guard & Dynamic ARP Inspection/ Protection
11.	Secure Shell (SSH) Protocol and Simple Network Management Protocol Version 3 (SNMPv3) to provide network security by encrypting administrator traffic during Telnet and SNMP sessions.
12.	1 RJ-45 serial console port 1 RJ-45 out-of-band management port

13.	Delivers secure encryption of all access methods (CLI, GUI, or MIB) through SSHv2, SSL, and/or SNMPv3
14.	Provides up to 336 Gbps of stacking throughput; each 4-port stacking module can support up to 42 Gbps in each direction per stacking port
15.	The Switch supports internal redundant power supply
16.	Advanced classifier-based QoS
17.	FTP for upgrading the operating System
18.	IEEE 802.1x support
19.	IEEE 802.3ad Link Aggregation Protocol (LACP) and HPE port trunking
20.	Supports management via CLI, Web interface SNMP v1,v2,v3 Manageable through both IPv4 & IPv6 with standard security features of both IPv4 & IPv6
21.	The stacking on the Switch provides the functionality to configure multiple switches in a single switching unit. Each unit/stack has the capability to be managed using a single IP address.
22.	Layer 3 Switch with following features like static IP routing OSPF, OSPFV3, RIP and policy based routing.
23.	– IPv6 host –Dual stack (IPv4 and IPv6) –MLD snooping – IPv6 ACL/QoS – IPv6 routing –6in4 tunneling

4. Specification for Print/File Server

Sl No.	Item	Specifications of equipment deployed by CBIC
1	Chassis	5U Rack Mountable or Tower
2	CPU	Two numbers of latest generation Intel E5-2630v4 processor

3	CPU L3 CACHE Memory	25MB L3 cache
4	Motherboard	Intel® C610 Series Chipset
5	Memory	8 GB RAM
6	Memory Protection	Advanced ECC with multi-bit error protection and memory online spare mode
7	HDD Bays	8 HDD bays scalable up to 48 SFF max, HDD/SSD.
8	Optical drive Bay	DVD-RW Drive
9	Hard disk drive	2 x 300GB 10K SFF SAS drive.
10	Controller	PCIe 3.0 based 12Gb/s SAS Raid Controller with RAID 0/1/1+0/5/50/6/60/1 Advanced Data Mirroring/10 Advanced Data Mirroring with 2GB Flash backed write cache
11	Networking features	1Gb 4-port network adaptor supporting advanced features such as Large Send offload capability, TCP checksum and segmentation, VLAN tagging, MSI-X, Jumbo frames, IEEE 1588, and virtualization features such as VMware NetQueue and Microsoft VMQ.
12	Interfaces	Serial - 1 Micro SD slot - 1 USB 2.0 Ports 5 (2 front, 2 rear, 1 internal) USB 3.0 3 (2 rear, 1 internal)
13	Bus Slots	Nine PCI-Express 3.0 slots, atleast three x16 slots
14	Power Supply	Redundant platinum Power Supplies
15	Fans	Redundant hot-plug system fans
16	Graphics	16 bit color: maximum resolution of 1600 x 1200 Integrated Matrox G200 video standard 32 bit color: maximum resolution of 1280 x 1024 16 MB Flash 256 MB DDR3
17	Industry Standard Compliance	ACPI 2.0b Compliant PCIe 3.0 Compliant PXE Support WOL Support Novell Certified

		IPMI 2.0, SMASH CLP, DCMI 1.0 compliant Microsoft® Logo certifications USB 3.0 Support SMBIOS 2.7.1 ASHRAE A3/A4 Energy Star
18	Embedded system management	Supports monitoring ongoing management, service alerting, reporting and remote management with embedded Gigabit out of band management port Server supports configuring and booting securely with industry standard Unified Extensible Firmware System supports RESTful API integration System management should support provisioning servers by discovering and deploying 1 to few servers with Intelligent Provisioning System supports embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support
19	Security	Power-on password Setup password Serial interface control Power switch security Administrator's password TPM 1.2 UEFI
20	Operating Systems and Virtualization Software Support	Microsoft Windows Server Canonical Ubuntu Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware Citrix XenServer
21	Secure encryption	Supports Encryption of the data on both the internal storage and cache module of the array controllers using encryption keys.
22	Warranty	Server Warranty includes 3-Year Parts, 3-Year Labor, 3-Year Onsite support with next business day response.

23	Provisioning	Essential tools, drivers, agents to setup, deploy and maintain the server embedded inside the server.
24	Remote Management	1. System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. Capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication. 2. Server should have dedicated 1Gbps remote management port. Remote management port should have 4GB NAND flash with 1GB available for user access. NAND flash should be used for keeping system logs and downloading firmware from HP website or internal repository 3. Server should support agentless management using the out-of-band remote management port. 4. The server should support monitoring and recording changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur. 5. Applications to access the server remotely using popular handheld devices based on Android or Apple IOS should be available. 6. Remote console sharing upto 6 users simultaneously during pre-OS and OS runtime operation, Console replay - Console Replay captures and stores for replay the console video during a server's last major fault or boot sequence. Microsoft Terminal Services Integration, 128 bit SSL encryption and Secure Shell Version 2 support. Should provide support for AES and 3DES on browser. Should provide remote firmware update functionality. Should provide support for Java free graphical remote console.

5. Specifications for Line Printer

S.No.	Specifications of equipment deployed by CBIC
1.	Impact type line printer
2.	Minimum printing speed of 2000 LPM
3.	Ribbon life of 30 million characters with 1 no. default ribbon + 10 nos. of additional ribbons of OEM Make
4.	MTBF of 10,000 Hours
5.	Inbuilt Parallel, Serial and add on or built in Ethernet 10/100 MBPS with signal cables of 10 feet length in each category of ports with S/w drivers under UNIX, including LINUX (Redhat & SUSE), Windows 2003 OS etc.

Note: This is the specification of the Line Printer Provided by CBIC. However, at sites where heavy duty operations are not involved, any compatible printer may be used.

6. Specifications for Printers other than Line Printer

Following guidelines should be taken into consideration while procuring standalone printers:

i. Postscript, PCL5 and PCL6 compatible printers
ii. Windows 10 compatible printers

It is suggested that once a printer model is finalized by the sites, the compatibility of the same should be confirmed from the Citrix team (email: si.citrix@icegate.gov.in) before procuring the printer.

7. Specifications for 4, 8, 12, 16 and 20 KVA UPS WITH 30 Min/1 Hr. BACKUP as per the requirement of the Location

ITEM	Specifications of equipment deployed by CBIC
Technology / Design	Redundant N+1, Advance fully Microprocessor with PWM Technology with IGBTs. Double online conversion. The UPS shall utilize modular power protection technology designed to allow internal redundancy, scalability (vertical paralleling) of power and runtime, and fast mean time to repair (MTTR).
Topology	Online Double conversion Type
UPS type	On line (to act as power conditioner as well as Backup) with Auto start Facility power walking time of 30 ms
Redundancy / Parallel Operation	N+1 parallel redundancy whereas all the power modules will be active and share the load mode.

Back up desired	Full load for specific Period of 30 min/1 hr. of the 100% rated capacity.
Upgradeable	Upgradeable to 1: 1 redundant configuration

Annexure 3 – Security Agents

List of all software agents required to be installed on Desktops/AIO are tabulated below. The agents which are required to be mandatorily integrated with CBIC's centralized security controls are marked as Mandatory and will be provided to the "CBIC Connectivity Partner" by CBIC.

S. No	Component	Mandatory	Provided by
1	End Point Protection (Antivirus)*	Yes	CBIC
2	Data Leakage Prevention (End point Agent)*	Yes	CBIC
3	Advanced Persistent Threat (APT) prevention	Yes	CBIC

*DLP Agent, Antivirus and APT sensors port will be opened from data center to get the latest virus definition and Policies by FTP/SFTP/MFTP.

Annexure 4 – Resident Engineer

Guidelines for minimum qualifications for a resource to be provisioned as a resident engineer are as follows :

Minimum Requirements of Resident Engineers
The proposed candidate should be a graduate Science/ IT.
The candidate should have diploma in Networking from an ISO certified institutes
Read/Speak/Write in English and Hindi/ Regional Language
Should have at least 1 years' experience of providing IT support, preferably as site IT Engineer
Shall be trained on support, maintenance, troubleshooting of key component supplied by CBIC in the locations
Shall be trained on using Ticketing System (HPSM).

Annexure 5 – Non-Disclosure Agreement (NDA)

NON-DISCLOSURE AGREEMENT

To
The Principal Commissioner/Commissioner of Customs

WHEREAS, we the undersigned _____, having our principal place of business/ registered office at_____, hereinafter referred to "CBIC Connectivity Partner" i.e. Custodian _____ or FPO _____ or SEZ _____ or any other formation _____, are desirous of establishing connectivity with the Data Centers of CBIC, for the purposes of electronic data interchange (hereinafter called the said 'Connectivity') and,

WHEREAS, the "CBIC Connectivity Partner" is aware and confirms that the information, software, hardware, business data, architecture schematics, designs, storage media and other documents made available by DG (Systems), CBIC during the process of establishing connectivity and thereafter, or otherwise (**confidential information** for short) is privileged and strictly confidential and/or proprietary to DG (Systems), CBIC.

NOW THEREFORE, in consideration of the foregoing, the "CBIC Connectivity Partner" agrees to all of the following conditions, in order to enable DG (Systems) to grant the "CBIC Connectivity Partner" specific access to DG (Systems)'s confidential information, property, information systems, network, databases and other data as may be required in the process of establishing connectivity.

IT IS HEREBY AGREED AS UNDER:

a) The "CBIC Connectivity Partner" agrees to hold in confidence any confidential information received by the "CBIC CONNECTIVITY PARTNER" , as part of the connectivity process or otherwise, and the "CBIC Connectivity Partner" shall maintain strictest of confidence in respect of such confidential information. The "CBIC Connectivity Partner" also agrees:

(i) to maintain and use the confidential information only for the purposes of establishing connectivity and only as permitted by DG (Systems),CBIC;

(ii) to only make copies as specifically authorized by the prior written consent of DG (Systems), CBIC and with the same confidential or proprietary notices as may be printed or displayed on the original;

(iii) to restrict access and disclosure of confidential information to such of their employees, agents, consultants and representatives (hereinafter 'Authorized Personnel') who strictly have a "need to know", and who agree in writing to maintain confidentiality of the confidential information disclosed to them in accordance with this Agreement;

(iv) to treat confidential information as confidential unless and until DG (Systems), CBIC notifies the "CBIC Connectivity Partner" of release of its obligations in relation to the said confidential information;

(v) that “CBIC Connectivity Partner” will not and shall use reasonable endeavors to ensure that its Authorized Personnel do not modify, reverse engineer, de-compile or disassemble any software programs contained in the Confidential Information unless otherwise specified in writing by DG (Systems), CBIC; and

(vi) to put in place such reasonable methods of control as “CBIC Connectivity Partner” deems necessary to ensure that no person in its employment, except the Authorized Personnel, is able to copy, transfer, or take away Confidential Information at any time unless otherwise agreed in writing by DG (Systems) CBIC. If such person leaves the “CBIC CONNECTIVITY PARTNER” ’s employment at any time or for any reason before the expiry of confidentiality obligations mentioned in this Agreement, “CBIC Connectivity Partner” shall ensure that such person is debriefed appropriately.

b) Confidential information does not include information which:

(i) the “CBIC Connectivity Partner” knew or had in its possession, prior to disclosure, without limitation on its confidentiality;

(ii) is independently developed by the “CBIC Connectivity Partner” without breach of conditions under this agreement;

(iii) information in the public domain as a matter of law;

(iv) is received from a third party not subject to the obligation of confidentiality with respect to such information provided the third party has not disclosed the information for or on behalf of CBIC or as a third party vendor of CBIC;

(v) is released from confidentiality with the written consent of DG (Systems), CBIC.

The “CBIC Connectivity Partner” shall have the burden of proving hereinabove are applicable to the information in the possession of the “CBIC CONNECTIVITY PARTNER” .

c) Notwithstanding the foregoing, the “CBIC Connectivity Partner” acknowledges that the nature of activities to be performed as part of the Connectivity process may require the “CBIC CONNECTIVITY PARTNER” ’s personnel to be present on premises of DG (Systems) or may require the “CBIC CONNECTIVITY PARTNER” ’s personnel to have access to software, hardware, computer networks, databases and storage media of DG (Systems) while on or off premises of DG (Systems). It is understood that it would be impractical for DG (Systems) to monitor all information made available to the “CBIC CONNECTIVITY PARTNER” ’s personnel under such circumstances and to provide notice to the “CBIC Connectivity Partner” of the confidentiality of all such information. Therefore, the “CBIC Connectivity Partner” agrees that any technical or business or other information of DG (Systems) that the “CBIC CONNECTIVITY PARTNER” ’s personnel, representatives or agents acquire while on DG (Systems) premises, or through access to DG (Systems) computer systems or databases while on or off DG (Systems) premises, shall be deemed confidential information.

d) Confidential information and any derivatives thereof shall at all times remain the sole and exclusive property of DG (Systems). All confidential information and derivatives thereof shall be returned to DG (Systems) promptly after receipt of request by “CBIC Connectivity Partner” from the DG (systems) in this regard, together with any available copies with “CBIC Connectivity Partner” thereof and “CBIC Connectivity Partner” shall

not retain any copy of the Confidential Information of DG (systems) with itself except as may be required by law.

e) In the event that the "CBIC Connectivity Partner" hereto becomes legally compelled to disclose any confidential information, the "CBIC Connectivity Partner" shall give sufficient notice to DG (Systems) to enable DG (Systems) to prevent or minimize to the extent possible, such disclosure. "CBIC Connectivity Partner" shall not disclose to a third party any confidential information or the contents of this Tender without the prior written consent of DG (Systems). The obligations of this Clause shall be satisfied by handling Confidential Information with the same degree of care, which the "CBIC Connectivity Partner" applies to its own similar confidential information but in no event less than reasonable care.

f) The obligations herein shall survive the completion or cancellation of the Connectivity process.

g) "CBIC Connectivity Partner" shall not assign or transfer any rights or obligations under this Agreement without the prior written consent of DG (systems). No waiver or amendment of any term or condition of this Agreement will be effective unless made in writing and signed by both parties.

h) "CBIC Connectivity Partner" acknowledges that any unauthorized disclosure or unauthorized use of the Confidential Information by the "CBIC Connectivity Partner" may cause immediate and irreparable harm to DG (systems) for which damages or injury sustained by DG (systems) may be impossible to measure accurately or remedy fully. Therefore, "CBIC Connectivity Partner" acknowledges that in the event of such a breach, DG (Systems) shall have the right to seek injunctive relief without prejudice to its all other legal rights.

i) If any provision of this Agreement is determined to be invalid in whole or in part, the remaining provisions shall continue in full force and effect as if this Agreement had been executed without the invalid provision.

j) This Agreement shall be governed by and construed in accordance with the laws of India, without giving effect to conflict of law rules. The competent courts of New Delhi shall have jurisdiction in connection with any dispute arising under this Agreement.

k) This Agreement shall come into force and effect on _____.

SIGNED for and on behalf of the President of India **By**: _____ **Signature**:_____ **Designation:** _____ **Address**: _____ **Witness**: _____ **Name**:_____ **Place**:_____ **Date**:_____	SIGNED for and on behalf of "CBIC CONNECTIVITY PARTNER" **By**: _____ **Signature**:_____ **Designation**: _____ **Address**: _____ **Witness**: _____ **Name**:_____ **Place**:_____ **Date**:_____

Annexure 6 – Infrastructure Checklist

Annexure 6- Infrastructure Checklist				
S No	**Item**	**Critical**	**Done (Yes/no)** (to be filled by requestor)	**Remarks** (to be filled by requestor)
1	**Please confirm whether the custom formation is under Customs jurisdiction i.e., not in Free Trade & Warehousing Zones (FTWZ)**	**Yes**		
2	**Connectivity**	**Yes**		
	MPLS Connectivity (Enter Bandwidth (in Mbps) in remarks column with name of Service Provider)			
	Connectivity Taken for Both Data Center-Delhi and Data Center – Chennai			
	All the Network Switches and Routers at the location accessing CBIC's Data Centers support 802.1x to enable integration with CBIC's Network Access Control (NAC).			
	Connectivity Media			
3	**LAN:**	**Yes**		
	CBIC LAN must be Insular and isolated from the local "CBIC Connectivity Partner" LAN. The local LAN should be installed with a separate switch.			
	LAN diagram must be provided showing the seating arrangements of the Customs officials and Service Centre operators			
4	**Service Centre details**	**Yes**		
	Whether Service Centre is available			
	Service Centre readiness status (includes both structural and IT infrastructure readiness)			
	Number of Service Centre users and number of nodes provided			
	Service Centre Agency name			
	Whether approval from the Jurisdictional Principal Commissioner/Commissioner for deployment of service center operators accorded			
5	**Specifications of Desktop**	**Yes**		
	Specifications of Desktops			
	Number of PC's installed for accessing CBIC application			

	Conformance to CBIC's Information Security Policy			
	List of all Desktop Agents installed			
6	**Printers**	**Yes**		
	Specifications of LAN Printer			
	Specifications of File & Print Server			
	Number of Line Printers installed			
	Number of Network Printers installed			
7	**Local Infrastructure:**	**Yes**		
	Suitable office space and Furniture			
	Air-conditioning			
	Specification of LAN Switches			
	Generator back-up			
	UPS to support all IT equipment			
	AMC for all equipments			
8	**Local Maintenance Engineers:**	**Yes**		
	Whether Local IT Engineer available at the location			
	Implementation carried out by the local maintenance engineer			
9	**Non-disclosure Agreement :**	**Mandatory**		
	Signed with the Jurisdictional Principal Commissioner/Commissioner of Customs			

Signature & Designation of the
Person In-Charge of "CBIC Connectivity Partner"

Signature & Designation of the
Verifying Customs Officer

Annexure 6A - IP request form details

Annexure 6A : IP Request Form Details		
Sl. No.	**Details**	
1	**Branch Code (If Allotted) /UNLO Code**	
2	**"CBIC Connectivity Partner" Name**	
3	**"CBIC Connectivity Partner" Address**	
4	**City**	
5	**State**	
6	**Bandwidth**	
7	**Service Provider (BSNL/TCL)**	
8	**Site Type (New/Existing)**	
9	**Last Mile (OFC/RF)**	
10	**Connectivity type (Partner MPLS/VPNoBB)**	
11	**LAN IP Pool requested by site(no. of LAN IPs)**	
12	**WAN IP**	
13	**Remarks (If existing site then LAN IP and WAN IP details)**	

Signature & Designation of the
Person In-Charge of "CBIC Connectivity Partner"

Signature & Designation of the
Verifying Customs Officer

Annexure 6B - Details regarding RF link

Note: (to be filled only if link is RF)

1. Does the login console has a default username and password?
2. Which Antenna is selected and what are the security measures and password policy followed for the Antenna?
3. Frequency on which the RF would be operating
4. Is the wireless security enabled? if yes what are the security parameters used
5. Architecture and Design document of connectivity
6. Are the user restrictions defined and ports that are used
7. Details pertaining to Security measures (like AES etc.)
8. RF configuration
9. Router configuration details

Signature & Designation of the
Person In-Charge of "CBIC Connectivity Partner"

Signature & Designation of the
Verifying Customs Officer

Annexure 7 – Container Scanner Solution

Please refer to the guidelines issued by CBIC in reference to the requirements before set up of Container Scanner Systems at Customs location

Requirements for implementing this solution at Container Scanner Divisions:

1) "CBIC Connectivity Partner" would procure an L3 manageable network switch. The "CBIC Connectivity Partner" may also opt for switch which supports GRE Tunnel technology in case they want to setup a tunnel based solution. Detailed specification sheet is as under.

   Before finalizing the switch model, the compatibility of the same should be confirmed from CBIC LANWAN team (cbic.lanwan@icegate.gov.in) before procuring.

2) It is suggested that the "CBIC Connectivity Partner" provides physical connectivity through OFC between L3 manageable switch and container scanner local server.

3) It may also be noted that it will be Scanner OEM's responsibility to do the script configuration between CBIC server and their server to pull the XML files.

   Recommended specifications of L3 Mangeable network switch

Requirement	L3 Manageable switch / L3 manageable switch which supports GRE Tunnel GRE- tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network.
Switching capacity	16 port (or higher) Multigigabit models with 2x10G uplink

Annexure 8 – Unblocking of IPs

Pre-requisites:

1. The site needs to ensure that OS used are genuine and are having Windows 10.
2. System have antivirus installed and should have latest virus definitions.

Process for unblocking:

1. Contact Saksham seva (saksham.seva@icegate.gov.in) and raise a ticket.
2. Antivirus full scan needs to be run on the system and same report need to be shared to Saksham.seva@icegate.gov.in with a copy to security team (cbic.security@icegate.gov.in) in PDF format.

Annexure 9 : Single Point of Contact (SPOC) Details

MPLS service provider	Name	Phone Number	Email Address
BSNL **(Delhi NCR- II Circle)** (for primary connectivity)	Vinay Kumar	9810186870	vinaykumareb@bsnl.co.in
TCL (for alternate connectivity)	K. Uma Mahesh	9212293732	k.umamahesh@tatacommunications.com

Saksham Seva Helpdesk for CBIC officers

a) Webportal : https://sakshamseva.cbic.gov.in
b) Email : saksham.seva@icegate.gov.in