Central Board of Indirect taxes and Customs (CBIC)
Department of Revenue, Ministry of Finance, Government of India

CBIC Partner Connectivity Protocol – Solution for CBIC field formations managed by Custodians (under the HCCAR, 2009) requiring IT infrastructure and connectivity with CBIC Data Centre

---

Version 2.0
August 2019

Document Control

1.	Document Title	CBIC Partner Connectivity Protocol – Solution for CBIC field formations managed by Custodians (under the HCCAR, 2009) requiring IT infrastructure and connectivity with CBIC Data Centre
2.	Document Code	SAKSHAM/CBIC/ CBIC Partner Connectivity/V1.0
3.	Date of Release	February 2017
4.	Version No.	1.0
5.	Document Owner	Directorate of Systems (DoS), Central Board of Indirect taxes and Customs (CBIC)

6.	Document Title	CBIC Partner Connectivity Protocol – Solution for CBIC field formations managed by Custodians (under the HCCAR, 2009) requiring IT infrastructure and connectivity with CBIC Data Centre
7.	Document Code	SAKSHAM/CBIC/ CBIC Partner Connectivity/V2.0
8.	Date of Release	August 2019
9.	Version No.	2.0
10.	Document Owner	Directorate of Systems (DoS), Central Board of Indirect taxes and Customs (CBIC)

CBIC Partner Connectivity Protocol – Solution for CBIC field formations managed by Custodians (under the HCCAR, 2009) requiring IT infrastructure and connectivity with CBIC Data Centre

Reference: *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 and No. 21/2009-Customs dated 4th August 2009. Reference is also invited to CBIC's 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 Centres 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.

Overview: This Document provides the current revised technical details for network connectivity and IT infrastructure at ICDs/CFSs/ICPs etc. which are covered under HCCAR 2009, requiring access to CBIC's Data Centres for accessing CBIC's Customs applications. This document/specifications herein may be revised from time to time in terms of the above cited Regulations.

Requirements:

1. The Custodian would be required to provide MPLS connectivity for access to the Data Centre. M/s BSNL and M/s TCL are the authorized service providers of CBIC for primary connectivity and alternate connectivity as they already have presence at the Data Centres. The site can procure either BSNL or TCL connectivity, as their Primary connection. However, connectivity can also be taken from any other MPLS Service provider who has presence at CBIC's Data Centres. Refer Annexure – 10 for details of SPOC of various parties.

2. It is mandatory for the Custodian to take Channel Partner MPLS connectivity to the Data Centre-Delhi as well Data Centre – Chennai to ensure business continuity in the event of a contingency as well as disaster recovery. This would help the location to be connected to the services at the time of non-availability of Primary Data Centre at New Delhi.

3. The bandwidth provided should be of either 4, 8, or 16 Mbps through Optical Fiber Cable depending on the number of users. A bandwidth estimate of about 250 kbps per user should be used while calculating the bandwidth requirement.

4. The Custodian shall ensure that the last mile connectivity to the Custodian site and to Data Centres should be on Optical Fiber Cable. The Custodian shall ensure 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. Refer to Annexure 1 for various options of Connectivity to the Data Center. In case the location is procuring connectivity via RF then they need to provide details of their configurations for security check. Please refer to Annexure 6 B for the required details.

5. The Custodian would be required to provide all requisite infrastructure including office space and furniture, Local Area Network (LAN) Infrastructure including Desktops, Tablets, File & Print servers, Printers (including Line Printers as may be required), Routers, LAN Switches, air-conditioning, backup power and UPS. Specifications of equipment (as deployed by CBIC) are detailed in Annexure 2. The infrastructure supplied must conform to these specifications or higher. The annual maintenance and proper upkeep of these equipments would also be the responsibility of the Custodian.

6. The WAN and LAN equipment provided by Custodians shall conform to CBIC's IT Infrastructure Design and secure access policy. The local infrastructure would have to integrate with CBIC's Central End Point Protection (Anti-Virus) gateway, Data Leakage Prevention (DLP) and Centralized Patch Management systems etc. This is important since any violation would impact the connectivity to the data centre. List of all software agents required to be installed on Desktops are provided in Annexure 3. 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 Custodian by CBIC.

7. The Custodian 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. R.E. would be reporting to the custom's system manager of the location. Minimum qualification of R.E.s (as deployed by CBIC) is provided in Annexure 4. The custodians 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 Custodian should ensure that CBIC LAN is segregated for security and not connected to the CFS/ICD own LAN. The LAN/WAN implementation would be required to conform to the Information Security Policy of CBIC, which will be shared by CBIC with the Custodian after they have executed the required Non-Disclosure Agreement.

9. Custodian would be required to sign a "Non Disclosure Agreement" on a stamp paper with the Jurisdictional Principal Commissioner/Commissioner of Customs. The format of this agreement is enclosed at Annexure 5. Once the infrastructure is ready, the custodian is required to fill up the Infrastructure checklist enclosed at Annexure 6, and have it verified by the 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 System Manager or Alternate System Manager would in turn forward a scan copy of the signed Infrastructure checklist and NDA to CBIC for issue of LAN IP pool (cbic.lanwan@icegate.gov.in)

Important instructions for the Custodians connecting to CBIC Data Centre:

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

2. In request for additional LAN IPs/ new LAN IPs, the site should re-share the infrastructure checklist to highlight the compliance with CBIC requirements

3. The Custodians 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. The blocked IDs have to be properly checked and investigated. Refer Annexure – 9 for details of the process for unblocking IPs.

4. For all additional IPs a mapping of Customs users with systems need to be shared beforehand by the Systems Manager/ Alternate Systems Manager

5. It is the responsibility of the site to ensure that right form of MPLS connectivity i.e. Channel Partner MPLS is procured via BSNL/TCL/any connectivity which has presence at Data Centre

6. If the site faces any issues or require any changes to be done, they need to log the issues/changes via Saksham Seva with proper incident /interaction no.

7. 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.

8. If the custodian is looking to set up a container scanner, they have to procure their own infrastructure. Kindly refer to Annexure 7 for details.

9. Similarly, if the custodian is opting for Mobility solution, they have to procure their own handheld mobility device/tablets. Kindly refer to Annexure 8 for details.

10. 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 custodian for consideration. CBIC will randomly select few sites for security audit. Any deviation found from the policy as per the audit report, the rectification will be bear by the custodians.

11. It is to be noted that the cost of the audit shall be borne by the custodians at the prescribed rate by CBIC.

Annexure 1 – Connectivity Protocols

A. Connectivity Options for ICES system to the CBIC Data Centres (For CBIC locations, for all Custodian locations connectivity should be Channel Partner MPLS)

a) Access through the MPLS Cloud:

The Custodian can connect to CBIC Data Centre - Delhi and CBIC Data Centre – Chennai with the partner MPLS Cloud of either M/s BSNL or M/s TCL or any other service provider who has presence in CBIC's Data Centre. It is mandatory for the custodians to procure primary as well as alternative connectivity. VPN Client is not required in case of MPLS connectivity.
All the Network Switches and Routers at the location accessing CBIC's Data Centres must support 802.1x to enable integration with CBIC's Network Access Control (NAC).

b) VPN over BroadBand/Fibre through specified Internet Service Provider (ISP):

In case MPLS network is not available at the site, CBIC users can connect to Data Centre using VPN access over Broadband/Fibre through M/s BSNL or M/s TCL as CBIC has taken connectivity from these service providers. VPN Credentials (User id & password) in this case is to be provided by the ISP.
All the Network Switches and Routers at the location accessing CBIC's Data Centres must support 802.1x to enable integration with CBIC's Network Access Control (NAC).

c) VPN over Internet through other ISPs can be procured by sites with less than 5 users and only as alternate connectivity:

VPN over internet can also be taken from any other ISP but since those ISPs do not have presence in CBIC's Data Centres, the VPN IDs will be provided to officer concerned by SAKSHAM Seva Helpdesk. The VPN ID will be bound to the device (Desktop) and in the event that device/device credentials change, the VPN access will get impacted. In such an event, the user will again have to contact SAKSHAM Seva Helpdesk for access.

All the Network Switches and Routers at the location accessing CBIC's Data Centres must support 802.1x to enable integration with CBIC's Network Access Control (NAC).

Please provide the required details in the attached template for VPN ID creation:

VPN ID creation template.xlsx

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 Centre and Data Centres of CBIC at New Delhi and Chennai. In this case, partner locations will be connected to both Data Centre-Delhi & Data Centre-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. CBIC is only suggesting various options, which have different techno-commercial implications. The custodians may choose any option based on their business requirements.

C. Communication Mechanisms for Message Exchange

Secure File Transfer Protocol (SFTP/MFTP) will 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

Following information is required to be provided for creation of SFTP/MFTP User ID before starting the Message Exchange –

- Agency Name
- Agency Type
- SFTP/MFTP User Id
- Static Public IP address
- Agency Address
- Authorized Nodal Officer's name
- Authorized Nodal Officer's email-id
- Authorized Nodal Officer's Contact Number
- Technical Person details

Please provide these details in the attached template.

SFTP-MFTP Creation Template.xlsx

User needs to provide complete details in the SFTP/MFTP User Creation Template.xls having User_Creation sheet and Port_opening sheet and 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). Please note that User_Creation sheet is relevant for server team and Port_opening sheet is relevant for network team.

Upon receipt of duly filled template and execution of Non-Disclosure Agreement, a unique USER ID and password shall be shared with user in a confidential manner. The user shall be required to perform Password Management for their account as per CBIC's policy.
Only Fully Qualified Domain Name (FQDN) should be used to connect to SFTP/MFTP server so that in the event that the services are failed over to the Disaster Recovery Site, message exchange is not impacted. Use of IP Address is not recommended.

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 for the server team to reset the password and send a mail to cbic.server@icegate.gov.in. Password reset request should have the approval of Nodal officer i.e. Password reset request mail should either come from Nodal officer or he should be marked in that mail. Server team will reset the password and an auto generated password will be sent to the registered email-id corresponding to the requesting user.

Annexure 2 – Minimum Specifications for Equipment at Custodian 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. Post script, 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

List of all software agents required to be installed on Desktops 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 Custodian 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

The minimum qualification requirements for a resource provisioned as a resident engineer as part of Project SAKSHAM is as given below -

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 by the SI on support, maintenance, troubleshooting of key component supplied by CBIC in the locations
Shall be trained on using the Ticketing System being proposed.

Annexure 5

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 as the Custodian of ICD/ CFS/ ACU/ Port _____, are desirous of establishing connectivity with the Central Board of Indirect taxes and Customs (CBIC) data center for the purposes of electronic data interchange (hereinafter called the said 'Connectivity') and,

WHEREAS, the Custodian 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 Custodian agrees to all of the following conditions, in order to enable DG (Systems) to grant the Custodian 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 CUSTODIAN agrees to hold in confidence any confidential information received by the CUSTODIAN, as part of the connectivity process or otherwise, and the CUSTODIAN shall maintain strictest of confidence in respect of such confidential information. The CUSTODIAN 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 Custodian of release of its obligations in relation to the said confidential information;

(v) that CUSTODIAN 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 (S), CBIC; and

(vi) to put in place such reasonable methods of control as CUSTODIAN 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 (S) CBIC. If such person leaves the CUSTODIAN's employment at any time or for any reason before the expiry of confidentiality obligations mentioned in this Agreement, CUSTODIAN shall ensure that such person is debriefed appropriately.

b) Confidential information does not include information which:

(i) the CUSTODIAN knew or had in its possession, prior to disclosure, without limitation on its confidentiality;

(ii) is independently developed by the CUSTODIAN 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 CUSTODIAN shall have the burden of proving hereinabove are applicable to the information in the possession of the CUSTODIAN.

c) Notwithstanding the foregoing, the CUSTODIAN acknowledges that the nature of activities to be performed as part of the Connectivity process may require the CUSTODIAN's personnel to be present on premises of DG (Systems) or may require the CUSTODIAN'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 CUSTODIAN's personnel under such circumstances and to provide notice to the CUSTODIAN of the confidentiality of all such information. Therefore, the CUSTODIAN agrees that any technical or business or other information of DG (Systems) that the CUSTODIAN'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 CUSTODIAN from the DG (systems) in this regard, together with any available copies with CUSTODIAN thereof and CUSTODIAN 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 CUSTODIAN hereto becomes legally compelled to disclose any confidential information, the CUSTODIAN shall give sufficient notice to DG (Systems)

to enable DG (Systems) to prevent or minimize to the extent possible, such disclosure. CUSTODIAN 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 CUSTODIAN 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) CUSTODIAN 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) CUSTODIAN acknowledges that any unauthorized disclosure or unauthorized use of the Confidential Information by the CUSTODIAN 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, CUSTODAIN 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 CUSTODIAN **By**: _____ **Signature**:_____ **Designation**: _____ **Address**: _____ **Witness**: _____ **Name**:_____ **Place**:_____ **Date**:_____

Annexure 6- Custodian Infrastructure Checklist				
S No	**Item**	**Critical**	**Done**	**Remarks**
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 Centre - Delhi and Data Centre – Chennai			
	All the Network Switches and Routers at the location accessing CBIC's Data Centres 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 custodian LAN. The LAN for Customs 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 centre operators accorded			
5	**Specificatios of Desktop**	**Yes**		
	Specifications of Desktops			
	Number of PC's installed for accessing ICES 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.			

Annexure 6-A- IP request form details

Annexure 6A : IP Request Form Details		
Sl. No.	**Details**	
1	**Branch Code (If Alloted)/UNLO Code**	
2	**Custodian Name**	
3	**Custodian Address**	
4	**City**	
5	**State**	
6	**Bandwidth**	
7	**Service Provider (BSNL/TCL/Other)**	
8	**Site Type (New/Existing)**	
9	**Last Mile (OFC/RF)**	
10	**Connectivity type (MPLS/Channel Partner MPLS)**	
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)**	

Annexure 6-B- Details regarding RF link (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 Custom location

Signature & Designation of the
Verifying Custom Official

Annexure 7

Is the location looking to set up a **Container Scanner Solution (Yes/No)**

If yes, 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) Custodian would procure an L3 manageable network switch which supports GRE Tunnel technology. 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) The custodian to provide physical connectivity through OFC between L3 manageable switch and container scanner local server.

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

   Specifications of L3 Mangeable network switch

Requirement	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	176 Gbps on 48-port models (non-multigigabit models) 92 Gbps on 24-port models (non-multigigabit models) 254 Gbps on 24-port Multigigabit models with 2x10G uplink 272 Gbps on 24-port Multigigabit models with 4x10G uplink 392 Gbps on 48-port Multigigabit models with 4x10G uplink 472 Gbps on 48-port Multigigabit models with 8x10G uplink 472 Gbps on 48-port Multigigabit models with 2x40G uplink
Stacking bandwidth	160 Gbps
Total number of MAC addresses	28,000-32,000
Total number of IPv4 routes (ARP plus learned routes)	24,000
FNF entries	48,000 flow on 48-port models

	24,000 flows on 24-port models 12,000 flows on 12- port modules
DRAM	4 GB
Flash	2 GB (non-Multigigabit models) and 4GB (Multigigabit models)
VLAN IDs	4,094
Jumbo frame	9198 bytes
Total routed ports per switch stack	208
Resiliency and high availability	Available
FCoE support	Available
Command authorization	Available

Annexure 8

Solution for CBIC Customs formations and Channel Partner Locations for usage of Handhelds **for connectivity with CBIC Data Centre**

Reference: Handhelds are primarily meant for Officers working in Examination section who are mobile and require connectivity in the shed area for carrying out examinations.

Overview: This provides the current revised technical details for network connectivity and IT infrastructure for locations where Handhelds would be used like ICDs/CFSs/ICPs etc. which are covered under HCCAR 2009, requiring access to CBIC's Data Centres for accessing CBIC's Customs applications. This document/specifications herein may be revised from time to time in terms of the above cited Regulations.

Pre-requisites:

a) Each site will have a dedicated SPoC and he/she must share the user details working at the site, the same must be provided to CBIC citing User name, SSO ID, Contact Details (Phone No. & Email Id) and address in the template as per Annexure B.

b) The System Manager or Alternate System Manager would in turn forward a scanned copy of the signed Annexures to CBIC for providing access to Customs application via IP whitelisting (*cbic.lanwan@icegate.gov.in*)

c) Secure Hub application will have to be downloaded in the device so that central policies could be pushed in the device.

Annexure A – Connectivity Protocols

Connectivity using SIM and VPN over Internet through ISPs:

SIM Cards providing access to the internet may be taken from any ISP but since those ISPs do not have presence in CBIC's Data Centres, VPN IDs will have to be used to access CBIC Applications. The VPN IDs will be provided to officer concerned by SAKSHAM Seva Helpdesk by sending them the filled in VPN ID template attached. The VPN ID will be bound to the device (Handheld) and in the event that device/device credentials change, the VPN access will get impacted. In such an event, the user will again have to contact SAKSHAM Seva Helpdesk for access.

Annexure B – Specifications for handheld device:

S.No.	Feature		Minimum Requirement
1.	SIM		SIM/Nano SIM/micro SIM
2.	Operating System		Android 8 and above iOS 11 and above (auto upgradable to higher versions of Android)
3.	Display		At least 10 inch (diagonal) TFT LCD based Capacitive with Multi Touch Screen with minimum resolution of 1280x800 pixels, IPS Panel, Toughened glass, Antiglare Display
4.	Processor		Quad Core ARM 1.3 Ghz OR x86 Quad Core 1.3 GHz or better 64 bit CPU with min 2MB Cache or higher.
5.	RAM		Minimum 2 GB DDR3 or higher
6.	Graphics		Should support HD , 2D and 3D Graphics
7.	Connectivity		Built in GPRS, EDGE & 3G, LTE/VoLTE/4G DATA Capability
			Bluetooth v 4.0 or higher
			WiFi IEEE 802.11 a/b/g/n(2X2) Dual Band
			Micro / Standard USB 2.0/3.0 with OTG or higher
			A-GPS /GPS or Better
8.	Camera	Primary	Minimum 5 MP Autofocus Rear Camera
		Secondary	Front Facing camera: 2 MP or higher
		Flash	Dual-LED (for primary)
		Video	Yes (for at least primary camera)
	HD Video		Minimum 720p/30fps
	Memory		On board Memory – Minimum 16 GB or higher.

			External micro SD slot expandable up to at least 32 GB (Recommended)
9.	Communications	WLAN	Wi-Fi 802.11 a/b/g/n/ac, dual-band, hotspot
		Bluetooth	v4.0, A2DP
		GPS	Yes
		USB	microUSB v2.0/3.0, USB Host
10.	Battery	Type	Rechargeable Li-ION 4000 mAh or higher
		Charging	Yes, via USB / power adapter
11.	Security features		Bio-metric Fingerprint Reader (Software/Hardware)
12.	Sensor		Built in Accelerometer
13.	Weight		Less than 1.5 KG (including protective casing)
14.	In the Box Items		Pen Style Stylus, Battery Charger, User Manual & Documentation (Pen Style Stylus can be provided out of box)
15.	Printing		Capability to print over wireless.
16.	Protection		Protective casing is required to be provided to prevent entry of dust and water (IP 68 would be advantage Rugged Certification)
17.	Certification		BIS(INDIA), Android CTS Fingerprint / Windows Certification
18.	Barcode Scanning		Should have capability to scan barcodes with the inbuilt camera. It is expected that a barcode scanning application, which will be developed for the mobility devices through a separate project, would run from the mobility devices.

Annexure C

	User Details				Device Details			System Manager / Nodal Officer Details		
S/n	**SSOID**	**Name**	**Contact Number**	**Icegate Email**	ICETAB **Serial Number**	ICETAB **MAC Address**	Device Type **BYOD / CBIC**	**Name**	**Contact Number**	**Icegate Email**
1										
2										
3										
4										
5										

	Location Details			Geo Fencing Cordinates		
S/n	**Location Code**	**Location Address**	**End User Location (Import/Export)**	**Lattitude & Longitude**	**Geo Radius (Meters)**	**Date of Delivery**
1						
2						
3						
4						
5						

Annexure D

List of agents that will be pushed centrally in the handheld through Secure Hub

S. No	Component	Mandatory	Provided by
1	Citrix Receiver	Yes	CBIC
2	VPN Client	Yes	CBIC
3	MDM Solution (through Secure Hub)	Yes	CBIC
4	Two Factor Authentication	Yes	CBIC
5	Biometric Application	Yes (to be checked)	CBIC

Annexure 9

Pre-requisites:

1. The site needs to ensure that OS used are genuine and are having Windows 2010.
2. System have AV installed and should have latest virus definitions.

Process for unblocking:

1. Contact saksham seva (saksham.seva@icegate.gov.in) and raise a ticket
2. The site needs to share the full scan report.
3. Antivirus full scan needs to be run on the system and same report need to be shared with the security team (cbic.security@icegate.gov.in) in PDF format.
4. Once the report is verified and it is ensured that there is no further risk, security team will raise the incident and assign it to network team. The IPs will be unblocked by the network team(cbic.network@icegate.gov.in) upon receiving the request.

Annexure 10

SPOC Details:

1) **BSNL** Channel Partner Link (Chennai Circle) – B Kalaivalan – 9445195933 kalaivanans@bsnl.co.in

2) **TCL** Channel Partner Link – Ms. Ashima Bhagat – 09582433355 Ashima.bhagat@tatacommunications.com

3) **Saksham Seva** – 1800 266 2232/1800 121 4560, saksham.seva@icegate.gov.in