Central Board of Excise & Customs
Department of Revenue, Ministry of Finance, Government of India

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

---

Version 2.0
March 2017

Document Control

1.	Document Title	CBEC Partner Connectivity Protocol – Solution for CBEC field formations managed by Custodians (under the HCCAR, 2009) requiring IT infrastructure and connectivity with CBEC Data Centre
2.	Document Code	SAKSHAM/CBEC/ CBEC 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 Excise & Customs (CBEC)

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

Reference: *Reference is invited to CBEC 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 CBEC's Circular No.4/2011-Customs dated 10th January 2011*

The above Regulations/Circular issued by CBEC prescribe, inter-alia, that the networking, communication equipments, Uninterrupted Power Supply System, desktops, servers, printers other computer peripherals and secure connectivity to the CBEC 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 CBEC's Data Centres for accessing CBEC's Customs applications. This document/specifications herein may be revised from time to time in terms of the above cited Regulations.

Requirements:

a) 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 CBEC for primary connectivity and alternate connectivity respectively and therefore already have presence at the Data Centres. However, connectivity can also be taken from any other MPLS Service provider who has presence at CBEC's Data Centres.

b) It is mandatory for the Custodian to take 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.

c) 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 150 kbps per user should be used while calculating the bandwidth requirement.

d) The Custodian shall ensure that the last mile connectivity to the Custodian site and to Data Centres would 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 CBEC services. Refer to Annexure 1 for various options of Connectivity to the Data Center.

e) The Custodian would be required to provide all requisite infrastructure including office space and furniture, Local Area Network (LAN) Infrastructure including Desktops, 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 CBEC) are detailed at 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.

f) The WAN and LAN equipment provided by Custodians shall conform to CBEC's IT Infrastructure Design and secure access policy. The local infrastructure would have to integrate with CBEC's Central End Point Protection (Anti-Virus & HIDS) gateway, Network Access Control (NAC), Active Directory, CBEC's Content Filtering Solution, 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 CBEC's centralized security controls are marked as Mandatory and will be provided to the Custodian by CBEC.

g) 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. Minimum qualification of R.E.s (as deployed by CBEC) is provided in Annexure 4.

h) The Custodian should ensure that CBEC 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 CBEC, which will be shared by CBEC with the Custodian after they have executed the required Non-Disclosure Agreement.

i) Custodian would be required to sign a "Non Disclosure Agreement" on a stamp paper with the Jurisdictional 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 Commissioner of Customs.

The System Manager or Alternate System Manager would in turn forward a scan copy of the signed Infrastructure checklist and NDA to CBEC for issue of LAN IP pool (*cbec.lanwan@icegate.gov.in*)

Annexure 1 – Connectivity Protocols

A. Connectivity Options for ICES system to the CBEC Data Centres

A. Access through the MPLS Cloud:

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

C. VPN over Internet through other ISPs:

VPN over internet can also be taken from any other ISP but since those ISPs do not have presence in CBEC'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 CBEC's Data Centres must support 802.1x to enable integration with CBEC's Network Access Control (NAC).

B. Connectivity of stakeholders authorized by CBEC 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 CBEC at New Delhi and Chennai. In this case partner locations will be connected to both Data Centre-Delhi & Data Centre-Chennai of CBEC on separate Point to Point Links. CBEC will only work as a facilitator and the responsibility for arranging the actual connectivity remains with the partner agency. CBEC 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) will be used as Communication Mechanism for Message Transfer with other CBEC 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 User ID for Message Exchange

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

- Agency Name
- Agency Type
- Static Public IP address
- Agency Address
- Authorized Single Point of Contact
- Alternate Contact Person
- Primary Contact Number (Landline)
- Alternate Contact Number (Landline)
- Primary Contact Number (Mobile)
- Alternate Contact Number (Mobile)
- Primary Email ID
- Alternate Email ID
- Alternate Contact Number (Landline)
- Technical Person details

Please provide these details in the attached template.

SFTP User Creation Template.xls

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 CBEC's policy.

Only Fully Qualified Domain Name (FQDN) should be used to connect to SFTP 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.

Annexure 2 – Specifications for Equipment at Locations

1. Specifications for Desktop

ITEM	Specifications of equipment deployed by CBEC
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 H110 Chipset)
Display	20-in Non-Touch AIO
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 Laptop

Parameter	Specifications of equipment deployed by CBEC
Memory	8GB RAM DDR4
Storage	500 GB
Processor	i7 Processor
Operating System	Windows 10 Pro 64

Display	14 Inch Screen
Network Interface	WLAN I 7265 ac 2x2 nvP +BT 4.2 WW
Ports / Slots	(a) a) 1 x VGA/ HDMI / Display Port / DVI Port
	(b) b) 1 x Headphone / microphone Combo
	(c) c) 1 x Multi-format digital media reader
	(d) d) Minimum 3 USB Ports with atleast 2 USB 3.0
Network	(a) TCP /IP with DNS and DHCP wake on LAN
	(b) DHCP support for automatic firmware upgrades & unit configuration.
	(c) PPP (PPOE,PPTP)
Power Supply	65 watt Adapter
Bundled Software (with support and upgrades)	Office Productivity Suite
	Mozilla Firefox
	Adobe Acrobat Reader, Flash player, JRE 8.0 or above
Speakers / Microphone	Integrated Stereo Speaker, Integrated dual array microphone.
Regulatory Standards	UL, FCC Compliance, EPEAT India, BEE (optional), Energy Star
Security	Integrated Fingerprint Reader, TPM 1.2, Hard Drive to be capable for software Encryption

3. Specifications for 24 Ports Switch

S.No.	Specifications of equipment deployed by CBEC
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 Mpps 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

4. Specifications for 48 ports Switch

S.No.	Specifications of equipment deployed by CBEC
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 Mpps 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

5. Specification for Print/File Server

Sl No.	**Item**	**Specifications of equipment deployed by CBEC**
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	1Gb 4-port network adaptor supporting advanced

	features	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 availabile. 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.

6. Specifications for Line Printer

S.No.	Specifications of equipment deployed by CBEC
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 CBEC. However, at sites where heavy duty operations are not involved, any compatible printer may be used.

8. 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 CBEC**
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 CBEC's centralized security controls are marked as Mandatory and will be provided to the Custodian by CBEC.

S. No	Component	Mandatory	Provided by
1	End Point Protection (Antivirus & Email Security)	Yes	CBEC
2	End point Encryption	Yes	CBEC
3	Network Access Control (NAC)	Yes	CBEC
4	Data Leakage Prevention (End point Agent)	Yes	CBEC
5	Microsoft SCCM (Patch update)	Yes	CBEC
6	Advanced Persistent Threat (APT) prevention	Yes	CBEC
7	Microsoft Server CAL Licenses for Centralized Management	Yes	CBEC
8	Office Productivity Suite like Ms Office	No	Local
9	Two Factor Authentication	Yes	CBEC

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 CBEC in the locations
Shall be trained on using the Ticketing System being proposed.

Annexure 5
NON DISCLOSURE AGREEMENT

To
The 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 Excise & Customs (CBEC) 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), CBEC 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), CBEC.

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),CBEC;

(ii) to only make copies as specifically authorized by the prior written consent of DG (Systems), CBEC 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), CBEC 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), CBEC; 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) CBEC. 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 CBEC or as a third party vendor of CBEC;

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

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 ICD/CFS is under Customs jurisdiction ie 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 CBEC's Data Centres support 802.1x to enable integration with CBEC's Network Access Control (NAC).			
	Connectivity Media			
3	**LAN:**	**Yes**		
	CBEC 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 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 CBEC'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 Commissioner of Customs.			

Signature & Designation of the Person In-Charge of CFS/ICD

Signature & Designation of the Verifying Custom Official