

 सत्यमेव जयते	सीमा शुल्क आयुक्त (सामान्य) का कार्यालय OFFICE OF THE COMMISSIONER OF CUSTOMS (GENERAL) सीमा शुल्क कार्गो सेवा प्रदाता सेल, Customs Cargo Service Provider (CCSP) Cell जवाहरलाल नेहरू सीमा शुल्क भवन, Jawaharlal Nehru Custom House पो: शेवा, ता: उरण, नवी मुंबई-४००७०७, PO: Sheva, Tal Uran, Navi Mumbai-400707 Email: ccsp.jnch@gov.in
---	---

Date:

Public Notice No: 120/2026

Subject: Framework for implementation of integrated technology-enabled cargo safety and security controls at Container Freight Stations under JNCH - reg.

Reference:

- i) Sections 45 and 141 of the Customs Act, 1962.
- ii) Handling of Cargo in Customs Areas Regulations, 2009, as amended (hereinafter 'HCCAR,2009').
- iii) Board's Circular No. 13/2009-Customs dated 23.03.2009.
- iv) JNCH advisories dated 25.06.2026 and 05.08.2026 concerning security, operational discipline and outsourced agencies at CFSs.

1. Jawaharlal Nehru Port Authority (JNPA), commissioned on 26.05.1989, has grown from a bulk cargo terminal into India's largest container port and one of the leading container ports globally. It is connected with more than 200 ports worldwide and handles a substantial share of the containerised cargo passing through the major ports of the country. Its development over the years has been supported by modern infrastructure, increasing automation and continuous improvement in operational and security standards.
2. JN Port operates under an ISPS compliant Port Facility Security Plan, with CISF deployment, regulated access, automated gate verification and round-the-clock CCTV monitoring. Such security cannot, however, remain confined to the port

terminals. A considerable part of the import and export cargo handled at JN Port is subsequently received, stored, examined, de-stuffed, stuffed or delivered through the CFSs operating under JNCH.

3. CFSs are, therefore, an extended arm of the port logistics system as well as the Customs cargo-custody chain. Once a container leaves a port terminal and enters a CFS, the level of safety and security available to the cargo should not be diluted. The security chain can remain effective only when the port terminal, transit movement and CFS operations are protected by compatible and reliable controls. It has accordingly become necessary for the CFSs under JNCH to upgrade their security systems in keeping with current international practices and technological developments in the maritime and logistics sector.
4. There are 33 CFSs functioning under JNCH, with differing layouts, cargo profiles, equipment and levels of digital maturity. HCCAR, 2009, however, does not prescribe different standards of responsibility for different CFSs. Every CFS approved as a Customs Cargo Service Provider, irrespective of its ownership, size, age, location or volume of cargo handled, is under the same obligation to safeguard imported goods and export cargo, regulate entry into the Customs area, maintain proper records and prevent unauthorised access, handling, removal, pilferage or tampering.
5. Under Section 45(1) of the Customs Act, 1962, all imported goods unloaded in a customs area remain in the custody of the person approved by the Principal Commissioner of Customs or Commissioner of Customs until they are cleared for home consumption, warehoused or transhipped. Section 45(2) requires that person to keep a record of such goods and send a copy of it to the proper officer. It also forbids that person to permit the goods to be removed from the customs area, or otherwise dealt with, except under and in accordance with the written permission of the proper officer or in the prescribed manner. Under Section 45(3), where imported goods are pilfered after unloading in a customs area while in the custodian's custody, the custodian is liable to pay duty on those goods. Section 141(1) places all conveyances and goods in a customs area under the control of officers of Customs. Section 141(2) provides that imported and export goods may be received, stored, delivered, dispatched or otherwise handled in a

Customs area only in the prescribed manner, and that the responsibilities of persons engaged in these activities shall be as prescribed. HCCAR, 2009 has been framed under Section 157 read with Section 141(2) to give effect to these provisions.

6. Regulation 5(1)(i)(j) of HCCAR, 2009 requires a computerized system for location and account of goods and processing of documents; Regulation 5(1)(i)(n) of HCCAR, 2009 requires security and access control to prohibit unauthorised access and to ensure the safety and security of the premises and cargo. Regulation 5(1)(i)(o) permits the Commissioner of Customs to specify any other facility considered necessary having regard to the custody and handling of imported or export goods, while Regulation 5(1)(ii) requires the Customs Cargo Service Provider to provide safe, secure and spacious premises. The responsibilities prescribed under Regulation 6(1), particularly clauses (a), (b), (c), (d), (e), (f), (g), (h), (i), (j), (k) and (l), require proper account of cargo and every related activity, regulated handling and removal, safe and secure custody, prevention of pilferage and compliance with Customs directions. The statutory custody obligations under Section 45, and the Customs control over Customs areas under Section 141, apply fully to every CFS under JNCH.
7. Recent incidents and attempted incidents examined by JNCH have involved theft or pilferage of cargo, unauthorised movement of containers or loose cargo, interference with seals, access by unauthorised persons and irregular activity during night or low-activity periods. These incidents show that the mere availability of guards, CCTV cameras or separate software applications does not provide adequate protection where the gate, yard, warehouse, equipment, surveillance and documentation systems operate independently or depend upon delayed manual entry, oral instructions or the discretion of a single user.
8. Theft or pilferage of containerised or bulky cargo is seldom possible through the act of one person. It ordinarily requires prior planning, use of a vehicle, availability of cargo-handling equipment and coordinated action by more than one person. The persons involved may include the driver, transporter, security personnel, surveyor, equipment operator, labour, warehouse personnel or other staff having access to the CFS. A container may first be moved from its recorded

position to a distant or secluded area and thereafter opened, de-stuffed or loaded into another vehicle. Absence of real-time vehicle monitoring, system-generated tasks and immediate alerts facilitates such coordinated activity and increases the risk that it goes undetected.

9. Experience indicates that an effective arrangement is one in which vehicle authorisation at entry, system-generated task control inside the CFS and independent reconciliation at the out gate operate as one connected process. This chain shall cover import containers from the port terminal to the CFS and onward delivery, as well as export cargo from carting, stuffing and sealing at the CFS until receipt of the sealed container at the nominated port terminal.
10. Vehicle management shall form the central part of this security framework. The identity of the vehicle and driver, purpose of entry, concerned Bill of Entry or Shipping Bill, cargo to be handled, authorised location, assigned task and permitted duration of stay shall remain digitally linked throughout the presence of the vehicle in the CFS. No vehicle shall be permitted to enter, approach cargo, undertake loading or unloading, or leave the CFS merely on the basis of an oral instruction or manually prepared document.
11. With the technology now available, the customer portal, gate, visitor-management system, vehicle-management system, yard-management system, warehouse, cargo-handling equipment, CCTV, control room and gate-out barrier can operate as one connected system. OCR, ANPR, QR/PIN/RFID-based credentials, GPS, geofencing, vehicle telematics and equipment telemetry, together with video analytics and data analytics, can assist in identifying, in real time or through periodic analysis, mismatches, abnormal movement, excessive dwell time, movement towards secluded areas, after-hours activity and recurring combinations of persons, vehicles and equipment.
12. Data analytics shall be used to identify defined exceptions, recurring discrepancies and unusual associations. Artificial-intelligence based tools may also be used wherever feasible. Such tools shall remain an aid to supervision and shall not be the sole basis for an adverse operational decision.

13. Accordingly, in exercise of the powers under Regulation 5(1)(i)(o) of HCCAR, 2009, read with Regulations 5(1)(i)(j) and 5(1)(i)(n) thereof, the Commissioner of Customs (General) hereby specifies the Integrated Technology-Enabled Cargo Safety and Security Framework, placed at Annexure-I, as a facility necessary for the custody and handling of imported and export goods in the customs area. The framework shall be adopted by every CFS under JNCH. It is outcome-based and does not require every CFS to use the same application. A CFS may upgrade its existing systems, integrate separate applications through secure interfaces or introduce new modules, provided that the minimum functional requirements and acceptance tests prescribed in the Annexures are met.
14. The central requirement is that an authorised event recorded in one part of the system shall automatically update all connected functions. Information already available in an authorised system shall not be re-entered by different users merely to complete the next stage. Every sensitive action shall be attributable to an authenticated user, device or equipment, and every change shall preserve the earlier value. An unauthorised transaction shall be blocked at the time it is attempted, wherever this is technically feasible. Where a physical action cannot be prevented by the system, it shall be detected and alerted in real time, and the container, cargo or vehicle concerned shall be placed on a System Security Hold.
15. The system shall operate on a job-driven basis. No container or loose cargo shall be moved, opened, loaded, unloaded, examined, de-stuffed, stuffed or delivered without a valid system-generated task arising from an eligible transaction. Completion of the earlier stage shall be validated before the next task is generated.
16. Where a validation fails, the container, cargo or vehicle shall remain blocked and the next task shall not be generated. An alert shall simultaneously be sent to the designated operational and senior staff through email, SMS, mobile application or another suitable means. If the alert is not attended to within the prescribed period, it shall automatically be escalated to the next level of management.
17. Regulatory Holds communicated to the CFS by Customs, shall operate as one common status across the gate, yard, warehouse, equipment and gate-out

systems. The CFS shall reflect every such hold in its system immediately on receipt. A free-text remark, paper instruction, local gate entry or earlier-generated gate pass shall not override an active regulatory hold.

18. The out gate shall operate as an independent final barrier. Before allowing exit, the system shall freshly verify the vehicle and driver, other admitted persons, cargo or container identity, seal, regulatory hold and release status, completed task, gate pass and unresolved alerts. A mismatch or unresolved critical alert shall prevent generation of the gate pass and operation of the exit barrier.
19. A 24×7 Security and Operations Control Room shall monitor alerts relating to port-to-CFS and CFS-to-port transit, gate operations, internal vehicle movement, yard and warehouse activity, Customs holds, surveillance, personnel presence and device health. Acknowledgement, action, escalation and closure of every material alert shall be recorded.
20. All overrides, exceptions, edits, cancellations, approvals, failed attempts and emergency actions shall remain visible in a tamper-resistant and searchable audit trail. Operational users shall not be permitted to delete transactions, alter audit evidence or bypass a system block. Any exceptional or emergency action shall require approval at the designated senior level and shall record the reason, approving staff, date, time and supporting evidence.
21. Technologies such as secure APIs, OCR/ANPR, QR/PIN/RFID credentials, GPS/geofencing, RTK/GNSS, equipment telemetry, video analytics, biometric verification and fixed or body-worn cameras may be used singly or in combination. Equivalent technology shall be acceptable where it achieves the same or a better control outcome and produces reliable audit evidence.
22. The minimum functional requirements are set out in Annexure-I. Compliance shall be established through controlled demonstrations and the minimum acceptance tests prescribed in Annexure-II. The phased implementation schedule, deliverables and post-implementation assurance requirements are prescribed in Annexure-III. These requirements constitute the minimum acceptable standard and shall not prevent a CFS from adopting stronger safeguards based on its layout, cargo profile and operational risk.

23. Each CFS shall undertake implementation in accordance with Annexure III and submit a phase-wise compliance report. Upon completion of Phase III, it shall submit a final compliance report identifying the controls implemented, controls under progress, failed or pending tests, interim safeguards and the date by which every remaining gap shall be closed. Such a gap shall be treated as a continuing non-compliance.
24. Installation of equipment, production of a vendor certificate or submission of screenshots shall not, by itself, be treated as compliance. Compliance shall be verified through process demonstration, live or controlled test transactions, retrieval of audit evidence and successful completion of the tests prescribed in Annexure II.
25. After implementation, every CFS shall carry out the quarterly and half-yearly reviews prescribed under the post-implementation assurance provisions of Annexure III. The Commissionerate may undertake live negative testing, transaction replay, surprise verification or independent audit of the system at any time. The CFS shall provide the required technical and operational assistance without making such verification dependent upon the presence of its technology vendor.
26. Where any cargo-handling, security, survey, transport, equipment, software-operation or other function is outsourced, the CFS shall continue to remain fully responsible for the acts and omissions of the outsourced agency. Written permission under Regulation 6(2), wherever applicable, and the directions contained in the advisory dated 05.08.2026 shall be complied with. Engagement of a technology vendor shall not dilute the responsibility of the CCSP for the integrity, availability, security and auditability of its systems and records.
27. As a practical illustration, the security controls introduced at M/s International Cargo Terminal Pvt. Ltd. and examined during the inspections dated 17.08.2026 and 16.09.2026 were found to have materially strengthened gate validation, vehicle and visitor control, system-generated tasking, hold management, alerts, audit trails and surveillance. Other CFSs may, on a voluntary basis, seek process-level inputs from ICTPL or any other CFS demonstrating equivalent or

stronger controls. This reference does not constitute endorsement or certification of any CFS, vendor, product or technology.

28. All CFSs shall comply with the minimum requirements prescribed in Annexures I to III within the stipulated periods and shall strengthen and continuously maintain their security infrastructure, surveillance, access control, vehicle monitoring and operational safeguards. These requirements shall be implemented in continuation of the directions contained in the Advisory dated 25.06.2026 issued vide F. No. GEN/2637/2026-CCSP concerning strengthening of security, regulatory compliance and operational discipline at CFSs. Continued dependence on manual processes, failure to introduce or maintain the prescribed controls, or any system, device or interface deficiency which results in unauthorised access, movement, handling or removal of Customs cargo, shall be viewed seriously and may invite action under the Customs Act, 1962, HCCAR, 2009 and other applicable provisions.
29. Any incident of theft or pilferage of Customs cargo within a CFS shall be viewed with the utmost seriousness. Where such an incident prima facie discloses a failure of custody, access control, surveillance, vehicle monitoring or cargo-movement controls, the Commissioner of Customs (General) may suspend the approval granted to the Customs Cargo Service Provider under Regulation 11(2) of HCCAR, 2009, if satisfied that immediate action is necessary and that an enquiry against the Customs Cargo Service Provider is pending or contemplated.
30. Difficulties in implementation, if any, may be brought to the notice of the undersigned through the Deputy/Assistant Commissioner, CCSP Cell, JNCH.

Digitally signed by
UNMESH SHARAD WAGH
Date: 30-09-2026
12:48:41

(Unmesh Sharad Wagh)

Commissioner of Customs (General)

JNCH, Nhava Sheva

Enclosure: Annexures-I, II and III

Copy to:

1. The Chief Commissioner of Customs, Mumbai Customs Zone-II, JNCH.
2. The Commissioner of Customs (NS-I, II, III, V), JNCH
3. The Assistant Commissioner of Customs, CCSP Cell, JNCH
4. The Assistant/Deputy Commissioner of Customs, EDI Section, JNCH- to upload on the JNCH website.
5. The Secretary, CFSAI for circulation to all CFSs in JNCH.
6. The CEOs/MDs/CFS Head of all the CFSs in the jurisdiction of JNCH.
7. Office Copy

ANNEXURE-I

INTEGRATED TECHNOLOGY-ENABLED CARGO SAFETY AND SECURITY FRAMEWORK FOR CFSs UNDER JNCH

Purpose and scope

1. This framework lays down minimum functional and control outcomes for the safety, security, integrity and traceability of import and export cargo handled in the Customs area of CFSs under JNCH. It covers port-to-CFS and CFS-to-port transit, vehicle and personnel access, gate operations, yard management, Customs Hold, seal cutting and examination, cargo-handling equipment, gate-out, surveillance, incident management, audit evidence and cyber-security.
2. The framework does not require all CFSs to use the same application. It requires the relevant systems including the gate, customer portal, visitor management, vehicle management, yard management, warehouse, CCTV, equipment-control and gate-out systems to exchange reliable events and act upon a common transaction status.
3. The general principles set out in the Public Notice apply to this framework and are given effect through the requirements below.

Security outcomes

1. Every activity is attributable to an authenticated person, system, device or equipment.
2. Every person and vehicle inside the Customs area has a recorded sponsor, purpose, permitted zone and time window.
3. Every container and cargo transaction has one current security state and one chronological digital chain of custody.
4. No operational movement takes place without an eligible transaction and a valid system-generated task.
5. A regulatory hold or scan requirement cannot be bypassed by a local remark, paper instruction or later data entry.
6. Cargo-handling equipment cannot independently select cargo, create its own task or alter the approved destination.
7. The gate-out remains closed until the entire transaction chain is independently reconciled.
8. Significant operational exceptions, such as a failed validation, an unauthorised movement attempt, a seal mismatch, an active-hold violation or a critical device failure, are detected in real time, escalated to the accountable CFS functionaries and closed with a recorded response.
9. Recurring exceptions, repeated variances and unusual associations of persons, vehicles and equipment are analysed periodically to identify possible collusion or systematic pilferage, and the findings are reviewed and acted upon by the designated senior functionary of the CFS.

Common system architecture and control principles

1. All relevant CFS systems including Customer Portal, Gate, EIR, Visitor/Personnel, Vehicle, ERP/Yard Management System (YMS), Customs Hold/Scan, CCTV/Control Room and Gate-Out shall operate as an integrated control environment and exchange reliable transaction events.

2. Each cargo/container transaction shall have a unique digital identity, current operational/security status and chronological chain of custody. Information captured once from an authorised source shall flow electronically to subsequent stages without repeated uncontrolled manual entry.
3. Every cargo movement, handling, examination, transfer or delivery shall require an eligible transaction and valid system-generated task. Completion/validation of the preceding activity shall be checked before the next controlled activity is permitted.
4. An active regulatory Hold or Scan requirement shall override any earlier vehicle, task, release or gate authority and shall apply consistently across all connected systems.
5. Sensitive activities shall apply appropriate segregation of duties, role-based access and maker-checker/approval controls. Operational users shall not delete audit history, silently alter validated records or bypass system blocks.
6. Controlled correction or emergency action may be permitted only through an authorised exception process preserving the original information, revised action/value, reason, responsible user, approving authority and date/time.
7. System interfaces shall authenticate their source, record success/failure, prevent duplicate business effects and detect, reject, quarantine or reconcile materially invalid or out-of-sequence events.
8. Critical systems/devices shall use appropriately synchronised time, and transaction history and evidence shall remain accessible notwithstanding change of technology vendor or service provider.
9. The CFS shall maintain a standard operating procedure for the controls under this framework. It shall train every user before granting system access, conduct refresher training at least once a year and maintain training records. Designated Senior Functionaries and control-room staff shall receive specific training on exception approval and alert handling.

Functional control requirements

Equipment Interchange Receipt (EIR) Capture and Validation

1. The EIR data shall be received electronically from the terminal or port system wherever available. Where only a physical EIR is issued, it shall be scanned/captured as an image before completion of normal gate-in. This image shall be retained as source evidence and linked to the container, vehicle and transaction.
2. Relevant EIR information shall be digitally extracted into structured data, including EIR number/date, origin Terminal, container number, vehicle/trailer number, vessel, seal, size/ISO code, Destination CFS/CFS Code, weight, Full/Empty status, special-handling indicators, damage/remarks and Scan status, whichever is available/applicable.
3. Missing/unreadable information shall not be silently assumed. Authorised corrections shall preserve original value, revised value, user, reason and date/time without altering the original EIR image.
4. The destination CFS and CFS Code shall be mandatorily validated to ensure that the destination recorded in the EIR, the authorised destination and the actual receiving CFS are identical. Any mismatch shall block normal gate-in, unless supported by valid redirection documents and approval of the designated authorised staff of the CFS.
5. The system shall read and validate the scan marking or stamp appearing on the uploaded EIR, including 'suspicious' or 'cleaned' or any other applicable status. Where the scan status is received electronically from scanning division, terminal or port system, it should be captured automatically. Any unclear, unreadable or restrictive marking shall be routed to the prescribed exception process and shall not be assumed as cleared.
6. The scan status appearing on the EIR shall be treated as an additional security input and shall not override the current Customs hold, scan or release status received from an authorised regulatory source. The latest valid regulatory instruction shall prevail. In case of any conflict or

uncertainty, the system shall automatically place the container on hold until verification by the designated CFS functionary.

7. Successful EIR validation shall not independently authorise movement or gate-out. Subsequent ERP/YMS tasks, current Customs status and independent gate-out controls shall continue to apply, with full audit/evidence retention.

Gate Management System

1. The Gate Management System shall operate as a controlled security checkpoint and shall be integrated with the EIR, Vehicle Management System, Customer Portal, ERP/YMS, Customs hold/scan/release status, ANPR/cameras and the 24×7 Security and Operations Control Room.
2. Before permitting normal entry of any cargo or container, the system shall validate, wherever applicable, the container, vehicle, driver, authorised transaction, EIR, destination CFS, current Customs hold/scan/release status and entry authorisation.
3. Any material mismatch relating to the container, vehicle, destination CFS, Customs status, EIR or entry authorisation shall automatically block normal gate-in, place the transaction on a system security hold and generate an alert for verification.
4. Cameras installed at the gate shall capture the container number and vehicle registration number, and the system shall compare the captured particulars with the authorised transaction. Where the camera is unable to read a number (a 'non-read'), the gate user shall verify and enter the number manually against the captured image. Where the number read by the camera, or entered after manual verification, differs from the authorised transaction (a 'mismatch'), the transaction shall be blocked, an alert shall be generated, and no subsequent activity or cargo- or container-handling task shall be permitted or generated until the exception is resolved through the authorised exception workflow.
5. Any manual or emergency admission shall preserve the failed validation, reason for admission, identity of the responsible user, approval of the

designated senior staff of CFS and date and time of the action. Upon successful gate-in, the validated transaction shall automatically flow to the ERP/YMS and operational-monitoring systems.

KYC and Customer Portal

1. The CFS shall maintain verified KYC records of all importers, exporters, Customs Brokers, consolidators, authorised representatives and other customers, with digital KYC being the preferred mode for onboarding and periodic revalidation.
2. Every customer shall be provided with a secure login after completion of KYC. Portal access shall be role-based and restricted to authorised transactions. Expired, suspended, blacklisted or otherwise invalid users shall not be permitted normal transaction access.
3. The portal shall automatically display only those Bills of Entry, Shipping Bills, Bills of Lading, IGM items, ex-bond documents or other transactions that belong to the logged-in customer.
4. A Bill of Entry shall become available for delivery-related work, including vehicle mapping and admission of a vehicle for delivery, only after the prescribed Customs release, including Out of Charge, and completion of the other prescribed Customs formalities, wherever applicable.
5. The customer or Customs Broker shall be able to raise a request for examination, de-stuffing, delivery, carting, stuffing, vehicle entry or any other permitted activity through the portal.
6. Every operational request shall ordinarily be submitted through the system or customer portal. An oral or paper request shall not independently result in generation of a cargo-handling task. Controlled non-digital processing may be permitted only for recorded outage, regulatory direction or authorised exceptional circumstances with proper authorization at the senior management level of CFS.

Visitor Management System

1. The CFS shall maintain a verified digital record of:

- Permanent and contractual employees;
 - Security personnel;
 - Surveyors and data-entry operators;
 - Equipment operators and labour;
 - Customs Brokers and their employees;
 - Drivers and transporters, wherever possible;
 - Maintenance personnel; and
 - Other visitors entering the Customs area.
2. The record shall contain the person's identity, employer or sponsor, assigned role, shift and validity of access.
 3. Entry shall be permitted through a QR code, PIN or equivalent digital credential. Entry or Exit should be through designated controlled point and face or biometric verification may be used to prevent use of another person's credential.
 4. The purpose of the visit shall be recorded and, wherever applicable, linked with the concerned Bill of Entry, Shipping Bill, container, cargo or job.
 5. Regular users may be given limited-period access on the request of the concerned customer. Such access shall be reviewed periodically.
 6. The system shall maintain a live count of persons present inside the CFS and generate alerts for:
 - Presence beyond the approved shift;
 - Tailgating or use of another person's credential;
 - Unexplained presence during night or holidays; and
 - Failure to record exit.
 7. Loitering inside the Customs area shall not be permitted.

Vehicle Management System

1. The request for vehicle entry in the Customs area for the purpose of carting, taking loaded delivery, delivery of de-stuffed cargo or any other reason shall ordinarily be made through the vehicle management system

in the customer portal. Where the portal/system is unavailable or an exceptional Customs-directed movement is required, a controlled exception workflow with designated senior approval and full audit trail may be used.

2. The system shall generate a one-time and time-bound PIN, QR code or equivalent authorisation for each approved vehicle movement.
3. Each authorisation shall be linked with one vehicle, one driver, one cargo transaction, one purpose and with specific cargo transaction. The identity of the driver shall be recorded at gate-in and verified at gate-out.
4. Reused, expired, cancelled, duplicated or mismatched credentials shall be rejected.
5. At gate-in, the system shall verify:
 - Vehicle registration number;
 - Cargo and document reference;
 - Purpose of entry;
 - Valid job order;
 - Customs release, hold and scan status; and
 - Whether the vehicle or cargo is already linked to another active transaction.
6. The actual vehicle number captured through the gate camera or ANPR shall be matched with the vehicle for which the credential was generated.
7. Entry of an additional or duplicate vehicle shall be blocked where the approved number of vehicles for the transaction has been exhausted, the cargo has already been delivered, or the same vehicle is already recorded as inside the CFS.
8. Vehicles entering to take delivery of de-stuffed cargo, and vehicles for export carting, shall be separately identified. The system shall check their expected empty or loaded condition, vehicle type, carrying capacity and package details. Weighment against the expected weight profile shall be carried out on a risk basis, including for high-value, sensitive or

longstanding cargo and whenever an alert or discrepancy is recorded, and for a random sample of other vehicles. For this purpose, weight profile means the expected relationship between declared cargo/package weight, vehicle tare/capacity and, where available, weighbridge or equivalent measured weight, subject to configured operational tolerance.

9. The movement, permitted zone and time spent by every vehicle inside the CFS shall be monitored. Unexplained stoppage, excessive dwell time or movement towards a secluded or unauthorized area shall generate an alert.

Yard and Equipment Management System

1. A yard task shall be generated only after successful completion of the gate-in process.
2. Every lift, offloading, grounding, shifting, loading, examination movement or warehouse transfer shall arise from a valid system task. Where other containers or packages have to be moved in order to reach the container or cargo concerned (housekeeping or shuffle moves), such moves may be carried out as part of the parent task without a separate task. A shuffle move should be confined to the same block or area, and any move beyond it shall require a separate task failing which an alert will be generated.
3. The task shall specify:
 - Container or cargo;
 - Source and destination;
 - Assigned vehicle;
 - Assigned equipment and authenticated operator, which may be associated with the task before execution or at task acceptance; and
 - Time of issue and validity.
4. An equipment operator shall not be able to create a task, change the container, substitute the receiving vehicle or alter the destination.

5. Any change in yard planning shall be made by a separately authorized CFS staff. The original task and revised task shall both remain available in the audit trail.
6. The actual block, bay, row, tier or warehouse location shall be confirmed through equipment telemetry, RTK/GNSS, RFID, cameras or equivalent technology.
7. The system shall immediately generate an alert for any movement without a valid task; movement to a location different from the assigned location; unrecorded relocation; movement, after positioning, outside the authorised task destination or route or towards a distant, secluded, dark, restricted or low-visibility area; and movement of held, high-risk or longstanding cargo during night, holiday or low-activity hours without the prescribed authority.
8. Every completed movement shall remain linked with the authenticated equipment operator and equipment identity.
9. If an equipment operator attempts to handle a container subject to a Regulatory Hold or System Security Hold, the attempt shall be blocked where technically feasible, and in every case a Critical alert shall be generated recording the equipment identity, operator identity, time, location.

Regulatory Hold, Detained and Longstanding Cargo

1. A Regulatory hold entered in one system shall automatically apply across the gate, yard, warehouse, equipment and gate-out systems.
2. While a hold is active, the system shall not permit:
 - Delivery or vehicle mapping;
 - Loading or delivery task;
 - Gate pass generation; or
 - Exit of the container or cargo.
3. Containers and cargo under intelligence or agency holds, seizure or detention, such other categories of hold as may be specified by Customs,

and longstanding cargo in the high-risk category shall be kept in a clearly identified, access-controlled and CCTV-covered Hold Zone. Containers under short-duration holds, such as a scan hold or query hold, need not be relocated to the Hold Zone, but shall remain under the system hold and the enhanced monitoring applicable to held cargo. Tasks for scanning, examination, sampling or survey of held cargo may be generated in accordance with the instructions of the proper officer. Tasks for delivery or loading shall not be generated.

4. Depending upon the risk, the CFS may provide an additional physical safeguard such as fencing, chain and lock, electronic lock or seal.
5. Release of a Regulatory hold shall be permitted only upon receipt of a written or electronic release instruction received from the competent Customs or agency authority. The designated CFS functionary may acknowledge and operationally process such release and shall upload/link the relevant direction, but shall not independently remove the regulatory hold.
6. An attempt to release or move Regulatory hold cargo without proper authority shall be treated as a critical alert.
7. Any container remaining in the CFS for more than 30 days from the date of arrival in CFS shall automatically be placed under a System Security Hold. The Release shall require reasoned approval by the designated senior staff and a complete audit trail.
8. Longstanding containers and cargo shall be placed in documented ageing and risk categories and subjected to periodic physical and system verification. The ageing thresholds and enhanced-control frequency shall be configured by the CFS in accordance with Customs requirements and made available for supervisory review.
9. For the purpose of this framework, a Regulatory Hold means a hold originating from Customs or another competent agency. A System Security Hold means a temporary operational block generated by the CFS system due to a mismatch, anomaly or security exception. A System Security Hold

shall not be represented as a Regulatory Hold and shall be cleared only through the authorized exception workflow.

Seal Cutting, Examination and Re-sealing

1. Seal cutting shall be undertaken only against a valid system task linked with examination, de-stuffing, survey, inspection or another authorised purpose.
2. Before seal cutting, the existing seal number shall be matched with the system record and a clear close-range photograph showing the seal number and the condition of the seal (preferably a video recording through a body-worn camera) shall be captured and linked to the task.
3. Where the seal number does not match the system record, or the seal shows signs of tampering or damage, the system shall:
 - Stop the seal-cutting activity;
 - Generate an alert;
 - Place the container on a System Security Hold pending verification; and
 - Prevent generation of the next task.
4. The date, time, location, reason, details of the person cutting the seal shall be recorded.
5. The new seal number and image shall be recorded before the container is allowed to move from the examination or de-stuffing area.

Warehouse, LCL and Loose Cargo Management

1. Every receipt, de-stuffing, carting, internal shift, examination, stuffing and delivery shall be covered by a system-generated task.
2. Completion of one stage shall be validated before the next task becomes available.
3. Package-level reconciliation shall be recorded digitally. The CFS may use weighment, barcode, QR or RFID tagging, image analytics or other suitable methods to support reconciliation. AI-assisted package counting may be

used as an optional aid. However, the count shall be confirmed by the authorised surveyor, and any variance shall be recorded and resolved before the next task is generated.

Export Cargo

1. Export cargo shall be carted only against a Shipping Bill or a carting request registered in the system. The packages received shall be tallied and recorded against the Shipping Bill.
2. Stuffing of export cargo shall be carried out only against a system task linked to the Shipping Bill. The container number, seal number and package count shall be recorded.
3. An export container shall not be gated out of the CFS to the port unless the Let Export Order has been granted, the seal number matches the system record and no Regulatory Hold is active.
4. Short-shipped or back-to-town cargo shall be returned only against a system task and the permission of the proper officer.

Surveillance, Transit Tracking and Control Room

1. The CFS shall provide full CCTV coverage of all gate-in and gate-out points, survey lanes, the Hold Zone, seal-cutting and examination areas, warehouses and LCL bays. It shall provide adequate CCTV coverage of internal roads, parking areas, container lanes, equipment movement areas and secluded locations.
2. The CFS shall periodically check blind spots, taking into account changes in stack height and yard configuration.
3. CCTV recordings shall be retained for at least 180 days. Recording resolution, frame rate and image quality shall be sufficient for the intended identification and evidentiary purpose and may be risk-tiered by camera location. Footage connected with an incident, hold, investigation or proceeding shall be preserved until written closure.
4. Camera, recorder, storage, network and analytics health shall be continuously monitored.

5. Import containers moving from the port terminal to the CFS and sealed export containers moving from the CFS to the nominated port terminal shall be tracked through GPS, telematics or equivalent technology. The tracking data shall be integrated with the ERP/YMS for real-time monitoring of the estimated time of arrival, route deviation, unauthorised stoppage and delay beyond the prescribed transit time.
6. The system shall monitor the approved route, geofence, stoppage, delay and loss of tracking. Any deviation shall generate an alert and be escalated to the designated staff of CFS.
7. The CFS shall maintain a 24×7 Security and Operations Control Room equipped with an integrated dashboard for real-time monitoring of material alerts and relevant information from the gate, GPS, ERP/YMS, Customs hold/scan, warehouse, CCTV and system-health modules.
8. Every transit journey shall remain open until arrival is confirmed and reconciled in the system.

Independent Gate-Out and Barrier Control

1. A gate pass shall be generated only after successful completion and validation of all required activities.
2. Gate-out shall be an independent final check and shall not merely confirm an earlier office entry.
3. Before permitting exit, the system shall freshly verify:
 - Vehicle and container number;
 - Driver and other admitted persons;
 - Seal number;
 - Customs release and hold status;
 - Completed task;
 - Gate pass and supporting documents; and
 - Pending or unresolved alerts.

4. For delivery and export-carting vehicles, the purpose of entry and expected empty or loaded condition shall also be reconciled.
5. A missing task, cargo or vehicle mismatch, seal mismatch, active hold, expired credential or unresolved critical alert shall block gate-pass generation and operation of the exit barrier.
6. A paper document, oral instruction or local security confirmation shall not override a system block.

Alerts, Incident Handling, Audit Trail and Cybersecurity

1. Alerts shall be classified as Critical, High, Medium or Low.
2. Each category shall have a prescribed response time, escalation level and closure authority.
3. Critical alerts shall be sent directly through email, SMS, mobile application or other suitable means to the designated operational and senior staff of the CFS.
4. If an alert is not acted upon within the prescribed time, it shall automatically move to the next level of management.
5. Closure of an alert shall record the action taken, supporting evidence, name of the CFS staff and date and time of closure.
6. The system shall analyse repeated failed attempts, manual exceptions, after-hours activity and recurring combinations of customer, Customs Broker, transporter, vehicle, driver, security person, surveyor, equipment operator, warehouse employee and gate user.
7. The system shall maintain searchable, append-only logs of:
 - Login and authentication;
 - Original and changed values;
 - Vehicle and cargo mapping;
 - Credential generation and use;
 - Task creation, assignment, acceptance, completion and cancellation;

- Holds and seal events;
 - Gate-in and gate-out;
 - Alerts, approvals and overrides; and
 - Interface failures and administrative changes.
8. Access shall be role-based and limited to the work assigned to each user. Privileged users shall use multi-factor authentication.
9. Access shall be immediately withdrawn when an employee or contractor is transferred, suspended or removed.
10. The CFS shall provide secure data transmission, backup, malware protection, patching, vulnerability management and monitoring of cybersecurity events.
11. Independent vulnerability assessment and penetration testing by a CERT-In empanelled auditor shall be undertaken at least once a year and after any material system change. This shall be in addition to live testing of the operational workflow.

ANNEXURE-II**MINIMUM ACCEPTANCE TESTS**

The following tests are minimum negative and positive tests. The list is not exhaustive and may be supplemented having regard to the layout, cargo profile and systems of the CFS.

S. No.	Test condition	Expected result
1.	Expired, reused or wrong vehicle details is presented at gate-in.	Entry is blocked; attempted use and identities are logged; alert is generated according to risk.
2.	A vehicle is mapped beyond the approved number of vehicles or quantity for the cargo, or the same vehicle is shown as already inside.	Duplicate/excess mapping or entry is prevented; exception is visible to the Control Room.
3.	Cargo document is ineligible, release is absent/withdrawn, or job order is missing.	Vehicle authorisation, gate-in, loading/delivery task and gate-out cannot proceed.
4.	Container appears on the received scan list or the applicable scan list for the vessel is awaited.	Automatic Scan Hold is applied; a gate remark cannot remove it; release requires the designated authorised function.
5.	Vehicle mapping, loading task or gate pass is attempted for cargo under Regulatory hold.	Transaction is rejected.

S. No.	Test condition	Expected result
6.	A user without the designated hold-release role attempts release, or the required Customs or agency reference is absent.	Release is denied; user, time and attempted action are preserved.
7.	Equipment operator attempts to move a container/cargo without a current task, on an expired task or to a different destination.	Execution is prevented; where prevention is not technically feasible, a critical real time alert is generated and a system security hold is applied.
8.	Actual yard position does not match planned block/bay/row/tier, or movement distance/time is materially abnormal.	Mismatch/abnormal movement alert is raised and movement history remains retrievable.
9.	A high-risk, held or longstanding container is moved during night/holiday without the prescribed authority.	For cargo under a regulatory hold, movement must be blocked. High risk or longstanding cargo should move only under a pre-authorized task where technically feasible, and otherwise an alert is generated.
10.	Physical container or seal does not match the seal-cutting job order or the seal shows signs of tampering or damage.	Seal cutting is stopped; event and details of the person are recorded; critical alert is opened.

S. No.	Test condition	Expected result
11.	Employee/contractor/visitor remains after shift or the digital headcount does not reconcile.	Personnel alert is raised; physical verification and reasoned closure are required.
12.	Camera is obstructed, recorder/storage fails.	Device-health alert reaches the Security and Operations Control Room.
13.	Import/export vehicle deviates from route, stops beyond threshold, loses tracking or does not reconcile at destination.	Transit alert is generated with last location/time; action and destination reconciliation remain open until closure.
14.	At gate-out, vehicle, driver, persons, container/cargo, seal, task or gate pass does not match gate-in/transaction record.	Gate out is not allowed in the system. An alert is generated.
15.	A live Regulatory hold is applied after an earlier gate pass or task was generated.	Fresh gate-out check blocks exit notwithstanding the earlier document/task.
16.	A privileged user edits a vehicle, seal, container, task, hold or release field.	Old/new values, reason, maker/checker, time and linked evidence remain searchable; deletion is not permitted.
17.	Critical network/system interruption occurs while vehicle/cargo is at gate-out.	The System fails secure; the vehicle is held until live status is verified.

ANNEXURE-III**PHASED IMPLEMENTATION AND COMPLIANCE SUBMISSION**

Stage	Target	Minimum deliverables
Phase 0 - Assessment and plan	Within 30 days	Nominate the CFS Nodal person and the designated senior functionary(ies); map import and export processes and all manual hand-offs; inventory of systems, devices and vendors; blind-spot and cyber-risk review; gap analysis against Annexure-I; 180-day CCTV retention; management-approved implementation plan and milestones.
Phase I - Core prevention controls	Within 90 days	Verified identity and vehicle pre-authorisation; time-bound transaction credential; vehicle dwell time monitoring; live regulatory hold/scan control; system task for every movement; independent gate-out block; 24×7 Security and Operations Control Room; basic audit trail; camera/device health; controlled exception process.
Phase II - Operational integration	Within 150 days	Secure system interfaces; import/export transit monitoring; yard and equipment integration; visitor and shift-based access; warehouse/LCL reconciliation; alert escalation.
Phase III - Assurance and analytics	Within 180 days	Advanced surveillance/exception analytics; anti-collusion and repeated-variance analysis; independent Vulnerability Assessment and Penetration Testing (VAPT); full acceptance testing; live-transaction audit.

*Every implementation period runs from the date of issue of this Public Notice.

Post-implementation assurance

1. The CFS shall conduct quarterly internal sampling of high-risk transactions, blocked attempts, holds, seal events, after-hours movement, manual/emergency actions and evidence retrieval.
2. User rights, vendors/contractors, alert thresholds, camera coverage and system integrations shall be reviewed at least half-yearly and whenever there is a material operational change.