Canada Border
Services Agency

Agence des services
frontaliers du Canada

Canada

Joint report on CBSA IT outages

between September 28 and October 5, 2025.

Canada Border
Services Agency

Agence des services
frontaliers du Canada

PS38-143/2025E-PDF
ISBN 978-0-660-97776-8

Aussi disponible en français sous le titre :
Rapport conjoint sur les pannes informatiques de l'ASFC ayant eu lieu du 28 septembre au 5 octobre 2025.

Canada Border Services Agency Agence des services frontaliers du Canada

Joint Report on CBSA IT Outages between September 28 and October 5, 2025

Canada Border Services Agency and Shared Services Canada

Prepared for
the Minister of Public Safety and
the Minister of Government Transformation, Public Works and Procurement

October 31, 2025

Canada

CBSA – SSC IT Outage Summary Report

This report was prepared jointly by Shared Services Canada and the Canada Border Services Agency, following an investigation into information technology incidents and related outages to CBSA business and operations from September 28 to October 5, 2025.

Submitted to the Minister of Public Safety and the Minister of Government Transformation, Public Works and Procurement on October 31, 2025.

Scott Jones
President
Shared Services Canada

Erin O’Gorman
President
Canada Border Services Agency

1. Executive Summary

This report details findings of an investigation into IT incidents and subsequent service outages at the Canada Border Services Agency (CBSA) that occurred between September 28 and October 5, 2025.

The CBSA experienced multiple outages to major IT systems supporting most Travellers and Commercial programs and services, including the primary inspection kiosks at major airports, primary and secondary inspection systems for officers in airports and at highway crossings, the Interactive Advance Passenger Information system and Passenger Protect Program, which allow airlines to board or not board passengers. Additionally, client service portals and electronic data exchange systems for commercial shipments which permit importers to submit manifests electronically, communicate with government departments for regulated goods and to obtain clearances in all modes, including air, marine, rail, highway, and postal, were significantly impacted.

The overlapping outages were caused by two separate planned IT changes, specifically:

1. Database Upgrade

   On September 28, an upgrade was initiated by Shared Services Canada (SSC) to the databases supporting most CBSA traveller and commercial systems. A pre-requisite patch was not applied to the databases prior to the upgrade (human error) which led to significant corruption of live traveller and commercial data. Subsequent system performance issues and intermittent outages continued until October 5, resulting in delays in airports for international air passengers, a week-long backlog of commercial shipments at highway border crossings, marine ports, and air and rail yards.

2. Firewall Patch

   On September 29, an emergency security patch on CBSA firewalls was implemented by SSC which caused a break in communications with some commercial airlines trying to access the Interactive Advance Passenger Information and Passenger Protect Program systems. This led to a disruption in international and domestic air travel as airlines had difficulty and delays boarding passengers for flights.

Lessons learned from the root causes, impacts and resolutions of the outages have been determined and a comprehensive action plan has been prepared to move forward. These critical lessons are categorized into three areas: people and organizational factors, process factors and technology factors.

The CBSA and SSC remain committed to ensuring that CBSA IT services are reliable and fully support Canada's economic and national security needs.

2. Incident One – Database Upgrade

2.1 Summary

A planned routine database upgrade by SSC, intended to be non-disruptive to service, was started on September 28, at 02:30 ET. The upgrade failed and caused corruption to live data in multiple key CBSA traveller and commercial systems.

This corruption led to outages to major traveller systems: the primary inspection kiosks at international airports, primary and secondary inspection systems for border services officers at international airports and highway border crossings, and the Interactive Advance Passenger Information System and Passenger Protect Program.

The outages to these traveller systems were as follows (all times ET):

- September 28, 13:30 – 16:00 (partial outage; ~2.5 hours),
- September 28, 16:30 – September 29, 01:30 (full outage; ~9 hours),
- October 2, 10:40 – 12:45 (full outage; ~2 hours),
- October 2, 17:15 – 18:20 (full outage; ~2 hours), and
- October 4, 00:00 – 01:00 (full outage; 1 hour).

This corruption also led to outages and/or performance degradation of the CBSA's main commercial systems: client service portals and electronic data interchange systems, both used by trade chain partners to share manifest and other information with the CBSA.

The outages and/or degradations to these commercial systems were as follows (all times ET):

- September 28, 13:30 – September 30, 12:00 (partial outage; 46.5 hours), and
- September 29, morning – October 6, morning (significant performance degradation).

The CBSA and SSC support teams, with vendor support, rolled back the failed upgrade and made significant repairs to corrupted data, allowing system operations to be restored. While substantial repairs to corrupted data have been made, this work remains on-going.

2.2 Impact

This outage resulted in delays for airlines, airports, and returning international travellers on Sunday, September 28, until early Monday morning, September 29. There were delays boarding certain passengers in foreign and domestic airports, as airlines reverted to standard outage procedures to obtain board/no-board recommendations manually from the CBSA and from Transport Canada's "no-fly list". There were delays in domestic airports due to PIK machines being offline, as returning international travellers waited for processing through Customs in long queues and on planes.

This outage also resulted in long delays clearing commercial shipments at highway border crossings, airports, rail yards and marine ports. The delays created significant border wait times at most commercial highway border crossings across the country, with ports of entry in southern Ontario and Manitoba reporting delays of hours or days for trucks between September 29 and October 6.

Contrary to public comments, lookouts in the system were not missed but were communicated manually. While targeting data was not available during some of the outage, border services officers used their training and experience, as well as indicators obtained on the ground, to conduct risk assessments on both people and goods, consistent with contingency plans.

2.3 Root Cause

This upgrade had been previously rehearsed successfully in a test environment, thus both SSC and CBSA expected minimal to no operational impacts. However, during the upgrade to the live production systems on the morning of September 28, a critical pre-requisite change to enable the upgrade was not done by SSC. The vendor’s upgrade process did not check for this patch. The fact that this pre-requisite change was not made led directly to the corruption of live data, in a manner that prevented recovery from backups. The data corruption led to cascading system failures and service outages.

2.4 Resolution

With the assistance of the database software vendor, SSC and CBSA teams reverted the upgrade to the previous version in order to return the affected systems and services to operational status. Significant technical intervention has resolved the majority of the data corruption, however as of October 25, 2025, some recovery efforts continue.

3. Incident Two – Firewall Patch

3.1 Summary

On the afternoon of September 29, 2025, SSC applied a critical and known security patch to CBSA systems that are used to enable communications with domestic and foreign airlines using the Interactive Advance Passenger Information system and the Passenger Protect Program for passenger manifest data exchange and board/no-board instructions. This patch led to a break in communications between airlines and the CBSA. This communications break led to a full outage of the Interactive Air Passenger Information and Passenger Protect Program services to airlines for about 7 hours on September 29 from 14:00 – 20:55 ET.

3.2 Impact

In the afternoon/evening of Monday, September 29, in particular, there were delays boarding passengers in foreign and domestic airports, and missed flights. Airlines reverted to outage protocols but were also unable to receive manual confirmation regarding certain travellers for

Transport Canada's "no-fly list" in a timely enough manner to support regular boarding processes.

3.3 Root Cause

The critical security patch was applied to the CBSA's systems by SSC without proper notice being provided to the CBSA, leaving no possibility of coordination with airlines for readiness or to find a more quiet time to implement. Additionally, there was no indication from the software vendor that airlines (or any other parties) would be required to make changes to their systems in advance of SSC's change in order to maintain communications. The change was thought by SSC to be non-disruptive, but clearly was not.

3.4 Resolution

CBSA and SSC technicians connected with the technicians for all affected airlines to guide them through the process to update the security protocols on their respective systems which enabled the resumption of communication for the IAPI and PPP systems.

4. Lessons Learned and Action Plan

This section summarizes the critical lessons learned from the CBSA IT outages and the corresponding action to move forward.

4.1 People and Organizational Factors	
Lessons Learned	**Actions**
4.1.1 Quality controls surrounding SSC and CBSA employees making key IT changes are lacking.	Conduct a joint SSC - CBSA review to identify and implement improvements to the oversight, requisite training and experience for employees in key IT change management roles. [*March 2026*]
4.1.2 Collaboration related to IT change management between CBSA, SSC and air industry and trade chain partners is insufficient.	Establish joint IT change management with CBSA, SSC and air industry partners, and also with trade chain partners, for the discussion and coordination of all upcoming IT system changes, in order to re-establish trust and to avoid unexpected service disruptions. [*November 2025*]
4.1.3 The CBSA's internal communications about incidents lack definition and rigour.	Improve internal communications protocols, to facilitate timely, effective, and consistent communication across the Agency. [*November 2025*]
4.1.4 CBSA communications and engagement with industry partners is inadequate.	Adjust industry partner communications, engagement channels and protocols, to include the establishment of live channels for immediate communication, and to improve the quality, consistency, and usefulness of messaging. [*November 2025*]
4.1.5 CBSA communications and engagement to update government partners regarding significant CBSA incidents, outages and events must be strengthened.	Building on recent updates to communications protocols, examine means of engaging and updating government partners regarding significant CBSA incidents, outages and events, and revise or strengthen where required. [*November 2025*]

4.1.6 SSC is not sufficiently aware of the real world business impacts of CBSA system outages and the concomitant potential national and economic security risks Canada is exposed to when CBSA digital tools are unavailable.	Enhance SSC personnel awareness of CBSA operations, with a view to initiating cultural change that will improve personal and collective accountability. This will improve scrutiny, review, collaboration and communication to avoid similar human error in the future. [*March 2026*]
4.2 Process Factors	
Lessons Learned	**Actions**
4.2.1 CBSA and SSC IT change and incident management are not well-integrated.	Improve CBSA and SSC IT change and incident management including tight process integration; establish clear approval processes, levels, and timelines. [*November 2025*] Ensure that CBSA's critical business applications and services, as well as their IT infrastructure dependencies are well-documented and understood. [*March 2026*]
4.2.2 CBSA and SSC IT change and incident management processes have gaps that impact their effectiveness.	Augment controls on the execution of system updates and upgrades to mitigate the risk of human error. [*November 2025*] Conduct a joint internal audit of IT change management and incident management by CBSA and SSC Chief Audit Executives. [*October 2026*]
4.2.3 The coordinated CBSA response to the sudden, widespread and ongoing IT outages was inadequate.	Adjust the CBSA emergency management plans and procedures based on recent events, and ensure broad awareness and adherence. [*March 2026*]
4.2.4 Protocols and steps taken at the front line to manage the impact of the outage were inconsistent across ports of entry.	Review, improve, and exercise CBSA business line outage protocols and business continuity plans to better prepare for large and sustained digital disruption, and ensure broad awareness. [*March 2026*]
4.3 Technology Factors	
Lessons Learned	**Actions**
4.3.1 The CBSA IT ecosystem is fragile and lacks resiliency to changes and incidents in some areas.	Review the architecture and implementation of the CBSA's IT applications and systems, as well as the IT infrastructure hosted by SSC. Bolster the IT environment by identifying and correcting single points of failure, ensuring that technical backups and redundancy function as intended, and improving automated reporting and alerts. Find ways to insulate front-line operations from back-end service disruption and outages. [*October 2026*]
4.3.2 Neither SSC nor the CBSA are clearly identifying or sufficiently prioritising the remediation or renewal of aging CBSA systems and technologies.	Work with central agencies to ensure that the CBSA's technical debt is clearly identified as a top government risk and prioritised for renewal by both SSC and the CBSA. [*March 2026*]