



Republic of the Philippines
DEPARTMENT OF TRANSPORTATION
OFFICE FOR TRANSPORTATION SECURITY

OFFICE FOR TRANSPORTATION SECURITY
VERIFIED TRUE COPY FROM THE ORIGINAL
DOCUMENT PRESENTED

JOANNA P. FERRELL
RECORDS SECTION, AFS
FEB 24, 2026

MEMORANDUM CIRCULAR NO. 002 Series of 2026

SUBJECT : REPORTING PROCESS FOR TRANSPORTATION SECURITY INCIDENTS

DATE : FEB 24 2026

I. REFERENCES:

- A. International Civil Aviation Organization (ICAO) Annex 17;
- B. National Civil Aviation Security Program (NCASP);
- C. ISPS (International Ship and Port Facility Security) Code;
- D. National Security Program for Sea Transport and Maritime Infrastructure (NSPSTMI);
- E. National Land Transportation Security Program (NLTSP);
- F. Confidential Voluntary Reporting System (CVRS);
- G. Republic Act No. 11479 (Anti-terrorism Act of 2020);
- H. Republic Act No. 10173 (Data Privacy Act of 2012);
- I. Executive Order No. 82 dated September 4, 2012; and
- J. National Security Policy 2023-2028.

II. PURPOSE

This Circular establishes a harmonized system for timely, secure, and structured reporting of security incidents related to acts of unlawful interference and terrorism, as well as voluntary reporting of transportation security concerns across all modes of transportation. It ensures that all reports, whether mandatory or voluntary, are properly documented, reviewed, and acted upon, including the reevaluation of security measures and implementation of corrective actions to prevent recurrence.

While the system may generate data that supports strategic planning and threat-reduction efforts, its primary purpose is operational: to strengthen incident response, coordination, and continuous improvement of security measures across the transportation network.

III. SCOPE AND COVERAGE

This Circular applies to the following:

- A. Civil Aviation Authority;
- B. Airport Authorities;
- C. Airport Operators;
- D. Aircraft Operators;

U.P. LAW CENTER
OFFICE of the NATIONAL ADMINISTRATIVE REGISTER
Administrative Rules and Regulations

R FEB 26 2026 **D**
REGISTERED
ONAR Registration No. 26-0275
TIME: 10:07 BY: [Signature]

- E. Port Authorities;
- F. Port Facility Operators;
- G. Ship Operators;
- H. Bus Operators;
- I. Bus Terminal Operators;
- J. Tollway Operators;
- K. Rail Operators; and
- L. Individual reporters (passengers, crew, drivers, dock workers, ground personnel, etc.) submitting voluntary reports.

IV. DEFINITION OF TERMS

Acts of unlawful interference - these are acts or attempted acts such as hijacking, sabotage, unauthorized access, and threats that jeopardize transport safety.

Acts of Terrorism - calculated use of violence or threat of violence to inculcate fear and panic among the populace, in order to coerce or to intimidate the government or society to give in to an unlawful demand that is generally political, religious or ideological.

Terrorism¹ - is committed by any person who, within or outside the Philippines, regardless of the stage of execution:

- (a) Engages in acts intended to cause death or serious bodily injury to any person, or endangers a person's life;
- (b) Engages in acts intended to cause extensive damage or destruction to a government or public facility, public place or private property;
- (c) Engages in acts intended to cause extensive interference with, damage or destruction to critical infrastructure;
- (d) Develops, manufactures, possesses, acquires, transports, supplies or uses weapons, explosives or of biological, nuclear, radiological or chemical weapons; and
- (e) Release of dangerous substances, or causing fire, floods or explosions

Security Incident - refers to a transportation-related event arising from an intentional act that resulted in, or is in the course of resulting in, a breach of transportation security, harm to persons, damage to transportation assets, or disruption of transportation operations, and therefore requires investigation and/or official security response, such as incidents enumerated in "Annex C".

Security Occurrence - refers to a transportation-related condition, act, omission, or observed behavior that has not resulted in an actual security

¹ RA 11479

JOANNA P. PERAZICH
RECORDS SECTION, AFS
FEB 24 2015

breach but has the reasonable potential to do so, and therefore warrants documentation, reporting, assessment, monitoring, or preventive action.

V. GUIDELINES

- A. All entities covered by this MC shall, without prejudice to and in addition to the communication and notification protocols contained in the approved contingency plans under the Airport Security Program (ASP) and Aircraft Operator Security Program (AOSP), ensure that their personnel immediately report any occurrence or suspicious activities that may be security-related.
- B. Upon receipt of a report from personnel, the designated officer or unit within the covered entity shall:
 - i. Conduct an initial evaluation to determine if the report warrants escalation as a potential security incident.
 - ii. Document the details of the reported occurrence, including the date, time, location, personnel involved, and preliminary observations.
 - iii. Ensure the information is recorded confidentially and securely in accordance with organizational protocols.
- C. The Security Officer or Manager shall act as the main point of contact for incident reporting to the OTS Operations Center and ensure that reporting is available 24/7.
- D. Each covered entity shall establish and implement a formal process or procedure outlining how its personnel shall report such security occurrences internally, including but not limited to:
 - i. Roles and responsibilities for evaluating reports.
 - ii. Steps for internal escalation.
 - iii. Coordination with designated Security Officers/Managers.
- E. All covered entities shall maintain either a physical record or a secured digital file of all incident reports submitted to OTS. These records shall be readily accessible and made available to the OTS upon request, including during oversight reviews and compliance monitoring activities.
- F. Individuals can report aviation security concerns and incidents to the Confidential Voluntary Reporting System (CVRS).
- G. All reports received shall be reviewed by the OTS for analysis to determine if further action is required. This may include an investigation, corrective action, or referral to another agency concerned.

VI. REPORTING CHANNELS

- A. Mandatory Reports (by entities):

JOANNA P. FERAER
RECORDS SECTION, AFS

FEB 24, 2025

If the reported occurrence is assessed and elevated to security incident, covered entities shall mandatory submit the following forms:

1. an Incident Notification Report (INR) (**Annex A-1**) to the OTS Operations Center (TSRMS) within one (1) hour of detection.
2. A Progress Report (PR) (**Annex A-2**) shall be submitted to OTS within 24 hours, including all pertinent information concerning the security aspects of the incident or occurrence.
3. Final Report, which shall include additional details of the incident or occurrence and its resolution, shall be submitted after the incident or occurrence is resolved.

B. Voluntary Reports (by individuals):

- a. Individuals may voluntarily submit reports by accomplishing or completing the CVRS Form (**Annex B**) and submitting or forwarding it through any of the following channels:
 - i. Website: ots.gov.ph.
 - ii. E-mail addresses: pio@ots.gov.ph.
 - iii. Mail: CMC Building, Andrews Avenue Corner Aurora Boulevard, Pasay City Philippines 1300.
 - iv. Social media (Facebook): www.facebook.com/ots.dotr.
 - v. QR Code Access: available at the airport, seaports, passenger ships/vessels, bus, bus terminals, train and rail stations.
- b. All CVRS submissions shall be treated as confidential and protected under RA 10173.

VII. REVIEW AND ACTION PROCESS

- A. All incident reports received shall be assessed by the Office for Transportation Security (OTS) for validity and urgency.
- B. Validated incidents shall be classified in accordance with the *Taxonomy of Security Events* (**Annex C**), encompassing aviation, maritime, land and rail categories.
- C. All reports submitted shall be encoded into the Transportation Security Incident Registry (TSIR) maintained by OTS.
- D. All CVRS reports received by the Public Affairs Division (PAD) and OTS Operations Center shall be forwarded to the concerned Service / Division for analysis to determine if further action is required.
- E. An investigation, corrective action, or referral to another agency concerned shall be conducted, if necessary.

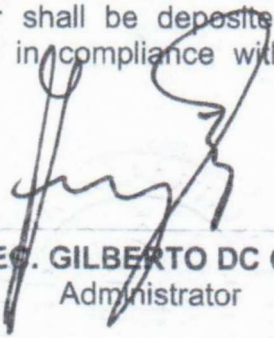
JOANNA P. PERAER
RECORDS SECTION, AFS
FEB 24, 2026

VIII. CONFIDENTIALITY AND DATA SECURITY

- A. All submitted incident reports are confidential and subject to data protection and cybersecurity protocols.
- B. Any unauthorized disclosure, tampering, or negligence in handling reports shall be subject to administrative or legal action.

IX. MISCELLANEOUS PROVISIONS

- A. **Construction.** The provisions herein shall be liberally construed in order to promote its transportation security objectives.
- B. **Reservation.** Nothing herein shall be construed as precluding OTS, through its Administrator, from prescribing additional or other requirements/criteria to meet the constantly evolving challenges in all transportation security sectors.
- C. **Amendments.** Nothing in this circular shall restrict the authority of OTS, through its Administrator, to modify, amend, or repeal any provision of the circular through subsequent issuances.
- D. **Repeal.** All orders, rules and issuances, or parts thereof, which are inconsistent with this Memorandum Circular are hereby repealed or modified accordingly.
- E. **Separability.** If any provisions or section of this Circular is declared null and void by competent authority, the remaining provisions not affected thereby shall remain in full force and effect.
- F. **Effectivity.** This memorandum circular shall take effect immediately after publication in the Official Gazette or in a newspaper of general circulation. A copy of this circular shall be deposited with the University of the Philippines Law Center in compliance with the Revised Administrative Code.


USEC. GILBERTO DC CRUZ
Administrator

Annexes:

Annex A - Mandatory Report Forms

- A-1 Incident Notification Report (INR) Format
- A-2 Progress Report (PR) Details

Annex B - Confidential Voluntary Reporting System (CVRS) Form

Annex C - Taxonomy of Security Events

- C-1 Civil Aviation
- C-2 Maritime
- C-3 Land and Rail

MC on Reporting Process for Transportation Security Incidents

JOANNA P. FERAER
RECORDS SECTION, AFS
FEB 24, 2026

ANNEX A

MANDATORY REPORT FORM



Republic of the Philippines
DEPARTMENT OF TRANSPORTATION
OFFICE FOR TRANSPORTATION SECURITY

ANNEX A-1: INCIDENT NOTIFICATION REPORT FORMAT

SECTION 1: BASIC INFORMATION (PANGUNAHING IMPORMASYON)	
Report Control Number: (to be provided by OTS)	
Date of Report Submission: Petsa ng Pagsusumite ng Ulat:	
Reporting Entity Name: Pangalan ng Nag-uulat na Ahensya:	
Type of Entity: Uri ng Ahensya: ☐ Airport Operator/Authority ☐ Aircraft Operator ☐ Port Operator ☐ Ship Operator ☐ Bus Terminal Operator ☐ Rail Operator ☐ Tollway Operator ☐ Other: _____	
Name of Reporting Officer: Pangalan ng Nag-uulat:	
Designation: Katungkulan:	
Contact Information: Impormasyon sa Pakikipag-ugnayan:	
Phone (Telepono):	

SECTION 2: INCIDENT DETAILS (DETALYE NG INSIDENTE)	
Date and Time of Incident: Petsa at Oras ng Insidente:	
Exact Location of Incident: Eksaktong Lokasyon ng Insidente:	
Mode of Transport Involved (Uri ng Transportasyong Sangkot): ☐ Aviation ☐ Maritime ☐ Land/Rail	
Nature of Incident (check all that apply): Uri ng insidente (lagyan ng tsek kung naaangkop): ☐ Aircraft Hijacking ☐ Bomb Threat / Discovery of Explosives ☐ Unauthorized Access to Restricted Area ☐ Sabotage or Vandalism ☐ Armed Attack / Shooting ☐ Cyberattack on Transport System ☐ Use or Possession of Prohibited Weapon or Explosive ☐ Suspicious Behavior or Package/Baggage ☐ Other: _____	
Source of Report (check all that apply): Pinagmulan ng Ulat (lagyan ng tsek kung naaangkop): ☐ Eyewitness Account ☐ Security/CCTV Footage	

OFFICE FOR TRANSPORTATION SECURITY
VERIFIED TRUE COPY FROM THE ORIGINAL
DOCUMENT PRESENTED

JOANNA P. FERRER
RECORDS SECTION, AFS
FEB 29, 2023

Note: This form must be submitted within one (1) hour of detection. Upon completion, kindly send the accomplished form via TSRMS viber hotline at 0923 271 5207 or email to pio@ots.gov.ph. (Ang form na ito ay dapat isumite sa loob ng isang (1) oras mula sa pagkakatuklas ng insidente. Ipadala ang kumpletong form sa pamamagitan ng email sa TSRMS viber hotline at 0923 271 5207 o pio@ots.gov.ph.)

JOANNA P. FERRER
RECORDS SECTION, AFS
FEB 24, 2026

MC on Reporting Process for Transportation Security Incidents

Damage to Property: <i>Pinasala sa Ari-arian:</i> ☐ Estimated cost (if available) : PHP _____	☐ None (Wala)
Was it covered by the media? Unknown (Hindi Tiyak) Naabisuhan ba ang media?	☐ Yes (Oo) ☐ No (Hindi) ☐
SECTION 5: ATTACHMENTS (IF AVAILABLE) (MGA KALAKIP (KUNG MERON))	
☐ CCTV Footage (file name: _____) ☐ Photos ☐ Statements / Affidavits ☐ Security Logs ☐ Other Supporting Documents: _____	
SECTION 6: CERTIFICATION AND SIGNATURE (PAGPAPATUNAY AT LAGDA)	
I certify that the information provided in this report is true and accurate to the best of my knowledge. <i>Pinatutunayan ko na ang impormasyong nakasaad sa ulat na ito ay totoo at tama ayon sa aking kaalaman.</i>	
Signature (Lagda): _____	Date (Petsa): _____
Name (Pangalan) : _____	
FOR OTS USE ONLY	
Date/ Time Report Received:	
OTS Receiving Officer:	
Remarks / Action Taken:	

☐ Intelligence Report ☐ Alarm or Security System ☐ Other: _____	
SECTION 3: IMMEDIATE RESPONSE (AGARANG PAGTUGON)	
Actions Taken by Staff/Security Personnel: <i>Mga Ginawang Hakbang:</i> ☐ Evacuation ☐ Area Secured ☐ Subject Apprehended ☐ Authorities Notified ☐ Other: _____	
Agencies/Units Notified: <i>Mga Ahensyang Naabisuhan:</i> ☐ OTS ☐ PNP ☐ CAAP ☐ MARINA ☐ PCG ☐ DOTR ☐ LTO ☐ Others: _____	
Time of Notification to OTS: <i>Oras ng Pag-abiso sa OTS:</i>	
SECTION 4: IMPACT ASSESSMENT (PAGSUSURI NG EPEKTO)	
Was there a disruption to operations? ☐ Yes (Oo) ☐ No (Hindi) <i>Nagkaroon ba ng pagkaantala sa operasyon?</i>	
Injuries / Fatalities: ☐ None (Wala) ☐ <i>May nasaktan o namatay:</i> Number of injured: _____ Number of fatalities: _____ <i>Bilang ng nasaktan:</i> _____ <i>Bilang ng namatay:</i> _____	



Republic of the Philippines
DEPARTMENT OF TRANSPORTATION
OFFICE FOR TRANSPORTATION SECURITY

OFFICE FOR TRANSPORTATION SECURITY
VERIFIED TRUE COPY FROM THE ORIGINAL
DOCUMENT PRESENTED

JOANNA P. FERRER
RECORDS SECTION, AFS
FEB 24, 2026

ANNEX A-2 : PROGRESS REPORT (PR) DETAILS

The Progress Report (PR) shall contain the following information:

Section	Required Information
A. Executive Summary	Concise overview of the incident and its significance.
B. Detailed Timeline of Events	Chronological account of events from detection to resolution.
C. Security Response and Mitigation	Details of actions taken by security personnel and supporting units.
D. Coordination Measures	List all internal/external agencies coordinated with, including timelines.
E. Assessment and Recommendations	Insights on incident handling, gaps observed, and proposed improvements.
F. SO/SM Endorsement	Name:
	Signature:
	Date:

MC on Reporting Process for Transportation Security Incident

JOANNA P. PERAER
RECORDS SECTION, AFS
FEB 24, 2025

ANNEX B

**CONFIDENTIAL VOLUNTARY REPORTING
SYSTEM (CVRS) FORM**

(VOLUNTARY REPORT BY INDIVIDUALS)

ANNEX B : CONFIDENTIAL VOLUNTARY REPORTING SYSTEM (CVRS) FORM

JOANNA P. HAER
RECORDS SECTION, AFS
FEB 24, 2015

TRANSPORTATION SECURITY CONFIDENTIAL VOLUNTARY
REPORT FORM



THIS CONFIDENTIAL VOLUNTARY REPORTING SYSTEM SHALL BE NON-PUNITIVE AND AFFORD PROTECTION TO THE IDENTITY OF SOURCES OF INFORMATION. THE OTS WILL ONLY RETAIN PERSONAL DATA AS LONG AS NECESSARY FOR THE FULFILLMENT OF THE PURPOSE.

☐ Civil Aviation ☐ Maritime ☐ Land ☐ Rail

Date of the incident:

D D M M Y Y Y Y

Time of the incident:

:
H H M M

Location: _____

Observation :

CONTACT INFORMATION

Full Name : _____

Mobile / Telephone Number : _____

E-Mail : _____

PRIVACY NOTICE:

We collect the following personal information/documents from you when you manually or electronically submit to us your report: Full Name, E-mail address, and Contact number.

Use: The collected personal information will be utilized for documentation and processing of your report to supplement the State's civil aviation quality control activities.

The OTS may also process the personal information collected in order to carry out its constitutionally and statutorily mandated functions, including, but not limited to, conduct of research for policy recommendations. (Section 4(e), R.A. 10173, or the Data Privacy Act of 2012).

OTS NOT PH

The form can be accessed by scanning the QR code available at airports, seaports, passenger ships and vessels, bus terminals, and train or rail stations, or by visiting the official OTS website at www.ots.gov.ph.

MC on Reporting Process for Transportation Security Incidents

JOANNA P. FERAER
RECORDS SECTION, AFS
FEB 24, 2026

ANNEX C

TAXONOMY OF SECURITY EVENTS



Republic of the Philippines
DEPARTMENT OF TRANSPORTATION
OFFICE FOR TRANSPORTATION SECURITY

OFFICE FOR TRANSPORTATION SECURITY
VERIFIED TRUE COPY FROM THE ORIGINAL
DOCUMENT PRESENTED

JOANNA P. FRABER
RECORDS SECTION, AFS
FEB 24, 2016

ANNEX C- TAXOMY OF SECURITY EVENTS

ANNEX C-1 : CIVIL AVIATION

Class	Category
Landside Security	Discovery or use of vehicle-borne improvised explosive
	Discovery or use of person-delivered IED
	Armed attack
	Unattended/suspicious items (also applicable airside)
	Chemical, biological and radiological (CBR) attack
	Damage to critical infrastructure/vulnerable points
	Suspicious behaviour
	Unplanned disruptions, including bomb threat or hoax
Passengers and cabin baggage	Discovery or use of prohibited item/IED
	Deficiency in the security checkpoint screening process
	Mixing of screened and unscreened passengers
	Suspicious behaviour
Staff and crew	Deficiency in the security checkpoint screening process
	Discovery or use of prohibited item/IED
	Sabotage
	Insider bypassing security controls
	Deliberate attempt to circumvent vetting/background check regime
Access control	Breach or attempted breach of perimeter
	Unauthorized access to security restricted area (SRA) or other controlled area

JOANNA FERAER
 RECORDS SECTION, AFS
 FEB 24, 2016

	(non-staff)
	Unauthorized/unescorted access within SRA (staff)
	Suspicious behaviour of staff
	Deficiency in the access control system
	Deficiency in the ID pass issuing system
	Deficiency in the vehicle access control system including application of security controls and/or screening of occupants and vehicles
Hold Baggage	Discovery or use of prohibited item/IED
	Deficiency in protecting screened hold baggage
	Evidence of tampering of screened hold baggage
	Deficiency in the hold baggage screening (HBS) system or process (including passenger baggage reconciliation)
	Deficiency in the process of transportation of dispatched weapons
In-flight supplies	Unauthorized access to in-flight supply facility
	Deficiency in protecting secure supplies
	Evidence of tampering of secured in flight supplies
	Deficiency in applying security controls
	Discovery or use of prohibited item/IED
Airport supplies	Unauthorized access to facility
	Deficiency in protecting secure supplies
	Evidence of tampering of secured airport supplies
	Deficiency in applying security controls
	Discovery or use of prohibited item/IED
Aircraft protection on the ground	Unauthorized passenger on the aircraft
	Unauthorized staff on the aircraft

JOANNA P. FETTER
 RECORDS SECTION, AFS
 FEB 24, 2025

	Deficiency in the aircraft security search/check
	Deficiency in aircraft protection measures, including where aircraft are parked overnight
	Discovery or use of prohibited item/IED in the aircraft cabin or hold
Aircraft in-flight security measures	Unruly passenger <i>Note: (to be considered for level 3 and 4 (see MAOSP and ICAO Aviation Security Manual) only to be reported)</i>
	Deficiency in the cockpit door process/protection
	Discovery or use of prohibited item/IED
	CBR attack
	Hijacking in flight
	Bomb threat in flight
Cargo and mail	Unauthorized access to cargo screening facility
	Deficiency in the screening process
	Discovery or use of prohibited item/IED
	Deficiency in protecting secured cargo
	Evidence of tampering of secured cargo
	Deficiency in the acceptance process
	Suspicious activity
Air Traffic Control	Armed attack against air traffic control (ATC) facility
	Destruction or damage of air navigation aids
	Unauthorized access
Digital information and technologies	Attack against aircraft system(s)
	Attack against air traffic management (ATM) system(s)
	Attack against airport system(s)
	Attack against other critical systems and data

JOANNA P. FORAER
 RECORDS SECTION, AFS

FEB 24, 2017

Unmanned aircraft system(s) (UAS) / Unmanned aerial vehicle (UAV) / Remotely-piloted aircraft system(s) (RPAS)	Unauthorized incursion into controlled airspace
	Near miss/Encounter with aircraft in flight
	Strike/Collision with aircraft in flight
	Sighting from aircraft/airport
	Unmanned aerial vehicle (UAV) caused threat against aircraft
	UAV caused threat against airport infrastructure
	UAV caused threat against passengers
Stand-off weapon (MANPADs, etc.)	Attack on aircraft or airport facility
	Reported sighting
Lasers ²	Attack on aircraft or airport facility
	Reported sighting
	Suspicious activity
Aviation security information	Deficiency in protecting sensitive aviation security information
	Loss of integrity and availability of information systems
General Aviation/Aeroclubs	Unauthorized access
	Discovery of prohibited item/IED

Note: This Taxonomy serves as a reference guide only and does not cover all possible security events. Entities are expected to report and document any other incidents or occurrences that may reasonably pose a threat to transportation security.

Reference: ICAO Guidance Material - Reporting of Aviation Security Occurrences and Incidents.



Republic of the Philippines
DEPARTMENT OF TRANSPORTATION
OFFICE FOR TRANSPORTATION SECURITY

OFFICE FOR TRANSPORTATION SECURITY
VERIFIED TRUE COPY FROM THE ORIGINAL
DOCUMENT PRESENTED

JOANNA PERERA
RECORDS SECTION, AFS
FEB 24, 2026

ANNEX C - TAXONOMY OF SECURITY OF EVENTS

ANNEX C-2 : MARITIME

Class	Category
Damage to or destruction of the ship or maritime facilities	Damage or destruction by explosive devices
	Damage or destruction by arson
	Damage or destruction by sabotage
	Damage or destruction by vandalism
	Chemical, Biological, Radiological and Nuclear (CBRN) attack
Use of the ship itself	As a weapon or as a means to cause damage or destruction
	Carry persons intending to cause a security incident and their equipment
Disruption of operations	Blockage of port entrances, locks, and approaches
	Sabotage of vessel monitoring or traffic management centers
	Hoaxes, threats and false information
	Civil disturbances (riots, violent demonstrations, strikes, blockading, and civil disobedience)
Tampering	Cargo theft or Cargo Pilferage
	Ship's equipment or systems
	Ship's stores
	Maritime facility's equipment or critical assets
Unauthorized Access	Breach of access control points
	Presence of unauthorized person in Restricted Areas

JOANNA P. FERRER
 RECORDS SECTION / AFS

FEB 24, 2026

	Trespassing
	Presence of stowaways
Smuggling	Weapons or military equipment
	CBRN Agents and its components including weapons of mass destruction (WMD)
	Dangerous Goods and Hazardous Materials
	Controlled substances and illegal drugs
	Moving goods in and out of the country in violation of laws
	Moving persons in and out of the country in violation of laws
Attacks from seaward whilst the ship is at berth or at anchor	Piracy/Armed Robbery
	Vessel-borne IED
	Attacks from Unmanned Underwater Vehicles
	Swimmers intending to cause security incident
	Cargo theft
Attacks whilst the ship is at sea	Piracy
	Rocket attacks
	Attacks from Unmanned Underwater Vehicles
	Vessel-borne IED
	State-sponsored armed attacks
Attacks on maritime facilities	Armed attacks
	Lone-wolf Terrorism
	Cargo theft
Passengers and baggage	Discovery or use of prohibited item/IED
	Deficiency in the security checkpoint

JOANNA P. FARER
 RECORDS SECTION, AFS

FEB 24, 2025

	screening process
	Mixing of screened and unscreened passengers
	Suspicious behaviour
Cyber attacks	Ransomware
	Attacks on Operational Technology (OT)
	Denial-of-Service (DoS/DDoS)
	Phishing and Social Engineering
	Malwares and Trojans
	Data breaches
	Attacks on ships electronic navigational equipment, communications network, cargo handling systems and automated engine and steering systems
	Attacks on vessel monitoring and traffic management systems
	GPS or AIS spoofing or jamming

Note: This Taxonomy serves as a reference guide only and does not cover all possible security events. Entities are expected to report and document any other incidents or occurrences that may reasonably pose a threat to transportation security.

Reference: Maritime Security Manual.



Republic of the Philippines
DEPARTMENT OF TRANSPORTATION
OFFICE FOR TRANSPORTATION SECURITY

OFFICE FOR TRANSPORTATION SECURITY
VERIFIED TRUE COPY FROM THE ORIGINAL
DOCUMENT PRESENTED

JOANNA P. NERAER
RECORDS SECTION, AFS
FEB 24, 2022

ANNEX C - TAXONOMY OF SECURITY EVENTS

ANNEX C-3 : LAND AND RAIL

Class	Category
BUS	
Bus and Bus Facilities Security	Unlawful seizure of facilities (e.g. depot/staging area)
	Armed occupation of bus and/or armed attacks such as shooting, stabbing, or assaulting passengers/staff
	Destruction or use of a vehicle/infrastructure to cause harm
	Vehicle-borne attacks using a bus or other large vehicle as a weapon
	Sabotage such as tampering of bus components
	Arson (setting fire to buses and/or facilities)
Bus In-Transit (Security Control of Passengers and their Baggage)	Unlawful seizure of bus units
	Hijacking of passenger, buses while in transit
	Ramming a bus into people or structures
	Deliberate collision with another vehicle
	Hostage-taking inside bus units
	CBRN attacks such as chemical, biological, radiological, or nuclear contamination in inside bus unit

Unaccompanied Baggage	Introduction of weapons, explosives, IEDs, or hazardous substance in buses and facilities
Access Control	Forcible intrusion into restricted areas e.g. depot/staging area
	Unauthorized entry into bus depots, or maintenance facilities
Digital Information and Technologies	Communication of false information
	Hoaxes (false bomb threats or misinformation to cause panic/disruption)
	Cyber-attacks (targeting automated ticketing, passenger info systems, or software)
BUS TERMINAL	
Terminal and Facilities Security	Unlawful seizure of facilities
	Armed occupation of bus terminal and/or armed attacks such as shooting, stabbing, or assaulting passengers/staff
	Destruction or use of a vehicle/infrastructure to cause harm
	Ramming a bus/vehicle into people or structures
	Deliberate collision vehicle with another vehicle inside the terminal
	Hostage-taking inside the terminal
	Vehicle-borne attacks using a large vehicle as a weapon
	Arson (setting fire to vehicle, terminal, or facilities)
Access Control	Forcible intrusion into restricted areas e.g. ticketing room, vault

OFFICE FOR TRANSPORTATION SECURITY
VERIFIED TRUE COPY FROM THE ORIGINAL

DOCUMENT PRESENTED

JOANNA P. HANER
RECORDS SECTION, AFS

FEB 24, 2026

	Unauthorized entry into ticketing room, vault
Unaccompanied Baggage	Introduction of weapons, explosives, IEDs, or hazardous substance in the terminal
Digital Information and Technologies	Communication of false information
	Hoaxes (false bomb threats or misinformation to cause panic/disruption)
	Cyber-attacks (targeting automated ticketing, passenger info systems, or software)
RAILWAY	
Railway Revenue Line, Depot, and Facilities Security	Unlawful seizure of trains
	Unlawful seizure of facilities (e.g. depot, station)
	Hijacking of passenger, trains, or light rail coaches while in-transit
	Armed occupation of railway stations and/or armed attacks such as shooting, stabbing, or assaulting passengers/staff
	Destruction or use of a vehicle/infrastructure to cause harm
	Hostage-taking inside train and/or station
	Introduction of weapons, explosives, IEDs, or hazardous substance in trains, stations, and facilities
	CBRN attacks such as chemical, biological, radiological, or nuclear contamination inside trains and subways

OFFICE FOR TRANSPORTATION SECURITY
 VERIFIED TRUE COPY FROM THE ORIGINAL
 DOCUMENT PRESENTED

JOANNA E. FERAER
 RECORDS SECTION, AFS
 FEB 24, 2026

	Arson (setting fire to trains, stations, or facilities)
Operation Command Center and Signalling System	Derailing a train by tampering with tracks or switches
	Sabotage such as tampering with tracks, switches, signaling systems, or train components
Access Control	Forcible intrusion into restricted areas e.g. depot/maintenance facility
	Unauthorized entry into rail depot, train yards, signalling control centers, or maintenance facilities
Digital Information and Technologies	Communication of false information
	Hoaxes (false bomb threats or misinformation to cause panic/disruption)
	Cyber-attacks (targeting automated ticketing, passenger info systems, or train signalling software)
TOLLWAY	
Tollway Property Lanes and Facilities Security	Unlawful seizure of infrastructure
	Armed occupation of toll plaza and/or armed attacks such as shooting, stabbing, or assaulting staff
	Destruction or use of a vehicle/infrastructure to cause harm
	Ramming vehicle into another vehicles, people or structures
	Deliberate collision of vehicle with another vehicle in toll plaza and/or property lanes

OFFICE FOR TRANSPORTATION SECURITY
VERIFIED TRUE COPY FROM THE ORIGINAL
DOCUMENT PRESENTED

JOANNA P. FERAER
RECORDS SECTION, AFS
FEB 24, 2026

	Introduction of weapons, explosives, IEDs, or hazardous substance in tollway facilities
	Vehicle-borne attacks using a large vehicle as a weapon
	CBRN attacks such as chemical, biological, radiological, or nuclear contamination in highway tunnels
	Arson (setting fire to vehicles or facilities inside property lanes)
Access Control	Forcible intrusion into restricted areas e.g. maxi booth
	Unauthorized entry into restricted areas
Digital Information and Technologies	Communication of false information
	Hoaxes (false bomb threats or misinformation to cause panic/disruption)
	Cyber-attacks (targeting automated ticketing or RFID software)

Note: This Taxonomy serves as a reference guide only and does not cover all possible security events. Entities are expected to report and document any other incidents or occurrences that may reasonably pose a threat to transportation security.

OFFICE FOR TRANSPORTATION SECURITY
VERIFIED TRUE COPY FROM THE ORIGINAL
DOCUMENT PRESENTED

JOANNA P. PERAZER
RECORDS SECTION, AFS
FEB 24, 2026