

# RAIL SECURITY INFORMATION BULLETIN

RSIB NO: 13-0001

ISSUANCE DATE: AUG 21 2013

**SUBJECT:** Reporting of Significant Security Concerns to the Transportation Security Administration (TSA) pursuant to Title 49 of the Code of Federal Regulations (CFR), Part 1580, sections 105 and 203.

**PURPOSE:** The purpose of this document is to enhance consistency in the reporting of security concerns to TSA in order to support the analysis for trends or indicators of developing threats and potential terrorist activity.

This bulletin is intended to assist regulated parties that have an obligation to report significant security concerns under 49 CFR Part 1580, but is not to be used as a substitute for the regulatory requirements to determine compliance. This information in this bulletin is not to be construed as legally binding requirements of, or official implementing guidance for, the rail security regulations. All regulated parties with reporting obligations are encouraged to share this document with all relevant personnel.

**BACKGROUND:** Since publication of the regulations affecting the rail transportation system (*see* 49 CFR Part 1580), some affected rail system operators have submitted to TSA various requests for clarification of the precise nature of the events they are required to report pursuant to 49 CFR 1580.105 and 1580.203. Additionally, in December 2012, the U.S. Government Accountability Office (GAO) published a report on Passenger Rail Security, entitled “Passenger Rail Security, Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives.” In the report, GAO stated that TSA has inconsistently overseen and enforced its rail security incident reporting requirement, because TSA does not have guidance published, leading to considerable variation in the types and number of incidents reported. GAO recommended that TSA develop guidance on the types of incidents that should be reported and this guidance should be disseminated to TSA inspectors and regulated entities, including rail and transit agencies. In response to GAO’s recommendation, TSA is disseminating this bulletin to provide clarification.

The Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Office of the Director of National Intelligence (ODNI) have initiated an effort “to support the development of a nationwide capacity for gathering, documenting, processing, analyzing and sharing terrorism-related suspicious activity reports (SARs) generated at the local, regional, state or federal levels, in a manner that rigorously protects the privacy and civil liberties of Americans.”<sup>1</sup> This concerted effort aims specifically to achieve the objectives of the National Strategy for Information Sharing (October 2007)<sup>2</sup> to prioritize, unify, and advance the sharing of terrorism-related information among Federal, State, local, and tribal Governments, the private

---

<sup>1</sup> See “Fact Sheet: Nationwide Suspicious Activities Reporting Initiative” (October 22, 2008) available at [http://ise.gov/sites/default/files/Fact\\_Sheet\\_ISE-SAR\\_Initiative\\_102208\\_FINAL.pdf](http://ise.gov/sites/default/files/Fact_Sheet_ISE-SAR_Initiative_102208_FINAL.pdf).

<sup>2</sup> Available at <http://207.245.165.145/nsc/infosharing/index.html>.

sector, and foreign partners. The collaboration has produced the Nationwide Suspicious Activity Reporting (SAR) Initiative (known as the NSI) to implement a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing information about suspicious activity that is potentially terrorism-related. In applying this approach, guiding standards have been developed, setting criteria for the types of activities that warrant reporting as suspicious and potentially terrorism-related.

These criteria recognize the capability of law enforcement and security professionals to apply their experience and expertise to identify significant security concerns by focusing on the nature of the incidents and the context in which they occur. The standardized approach among law enforcement officers and security officials with surface transportation entities produces more informative reports that can more effectively focus investigative efforts and intelligence analysis for potential trends and indicators of terrorism-related activity.

With this document, TSA is aligning information from the NSI and providing examples that could be useful to the regulated community in making a determination of whether an incident fits within the requirements for reporting under 49 CFR 1580.105 and 1580.203.

Questions regarding this document and/or other rail security matters may be submitted by e-mail to TSA at [STSIP@DHS.GOV](mailto:STSIP@DHS.GOV).

APPROVED

*for* C. M. Kalro  
Director, Surface Division  
Office of Security Policy and Industry Engagement

8/21/13  
DATE

Foto R. Garcia  
Director, Compliance Programs Division  
Office of Security Operations

8-20-13  
DATE

REGULATORY REPORTING REQUIREMENT	EXAMPLES
<p>§ 1580.105(c)(1) "Interference with the train crew."</p> <p>§ 1580.203(c)(1) "Interference with the train or transit vehicle crew."</p>	<p>Examples include activity that could interfere with the ability of train crew members to perform their duties to the extent that safety or security are threatened, such as:</p> <ul style="list-style-type: none"> <li>• Assault that causes the operator harm and interferes with the operation of the vehicle or conveyance.</li> <li>• Physically restraining an employee from performing his/her duties.</li> <li>• Physically preventing a member of the crew from calling for assistance by police or other crewmembers.</li> <li>• Use of threats or coercion to make an employee perform any task contrary to those duties assigned.</li> </ul>
<p>§ 1580.105(c)(2) and § 1580.203 (c)(2) "Bomb threats, specific and non-specific."</p>	<p>Examples include:</p> <ul style="list-style-type: none"> <li>• Communicating a spoken, written, or digitally transmitted threat to damage, disrupt, or compromise a rail or transit facility/infrastructure or operation.</li> </ul>
<p>§ 1580.105(c)(3) "Reports or discovery of suspicious items that result in the disruption of railroad operations."</p> <p>§ 1580.203(c)(3) "Reports or discovery of suspicious items that result in the disruption of rail operations."</p>	<p>In addition to activity that causes termination of operations, examples of disruption to railroad/rail operations include preventing or delaying the ability of the crew to perform its duties, activity that requires law enforcement intervention, or actions that require a train or transit vehicle to deviate from or delay its scheduled service. This includes the following types of situations in which unattended items (such as bags, packages, objects) have been deemed suspicious:</p> <ul style="list-style-type: none"> <li>• Items requiring a security response (for example, response by multiple law enforcement/security force elements).</li> <li>• Items that have a positive alert from an Explosive Detection Canine Team.</li> <li>• Items requiring Explosive Ordnance Disposal response.</li> <li>• Items that have been modified/altered or have wires/devices or suspicious objects attached that a reasonable individual would deem suspicious.</li> <li>• Items that cause partial or complete evacuations of a train, facility, or area.</li> </ul>
<p>§ 1580.105(c)(4) "Suspicious activity occurring onboard a train or inside the facility of a freight railroad carrier, rail hazardous materials shipper, or rail hazardous materials receiver that results in a disruption of operations."</p> <p>§ 1580.203(c)(4) "Suspicious activity occurring onboard a train or transit vehicle or inside the facility of a passenger railroad carrier or rail transit system that results in a disruption of rail operations."</p>	<p>In addition to activity that causes termination of operations or disruption discussed above, there is suspicious activity or behavior that could also result in a disruption of operations because it is reasonably considered as indicative of pre-operational planning related to terrorism, such as:</p> <ul style="list-style-type: none"> <li>• Observation of an individual who purposely placed objects in sensitive, operations, or vulnerable areas, in order to observe or test or probe security responses.</li> <li>• Individuals attempting to gain information: questioning crew, security, or staff at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, or security procedures, that would arouse suspicion in a reasonable person.</li> <li>• Individuals or activity that could reasonably appear to be testing or probing of security: deliberate interactions with, or challenges to, installations/infrastructure, personnel/staff, or systems that reveal or seem intended to glean information relating to physical, personnel, or cyber security capabilities or vulnerabilities.</li> </ul>

REGULATORY REPORTING REQUIREMENT	EXAMPLES
	<ul style="list-style-type: none"> <li>• Unauthorized individuals taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), and security-related equipment (such as perimeter fencing, security cameras).</li> <li>• Individuals demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (such as engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, and attempting to measure distances.</li> <li>• Discovery of theft/loss or diversion of resources, such as stealing or diverting something associated with a facility/infrastructure (for example, badges, uniforms, identification, emergency vehicles, technology or documents (classified or unclassified), which are proprietary to the facility).</li> <li>• Individuals presenting false or misusing insignia, documents, and/or identification, to misrepresent one's affiliation to cover possible illicit activity.</li> <li>• Unauthorized personnel attempting to or actually entering a restricted area or protected site.</li> <li>• Impersonation of authorized personnel (for example, police/security, or janitor). This may include individuals who attempt to or flee the area when confronted by authorized personnel.</li> </ul>
<p>§ 1580.105(c)(5) "Suspicious activity observed at or around rail cars, facilities, or infrastructure used in the operation of the railroad, rail hazardous materials shipper, or rail hazardous materials receiver."</p> <p>§ 1580.203(c)(5) "Suspicious activity observed at or around rail cars or transit vehicles, facilities, or infrastructure used in the operation of the passenger railroad carrier or rail transit system."</p>	<p>In addition to the examples provided above, examples include:</p> <ul style="list-style-type: none"> <li>• Individuals questioning crew, security, or staff at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, or security procedures, that would arouse suspicion in a reasonable person.</li> <li>• Purposeful contact with, or challenges to, infrastructure, staff, or systems that glean information relating to physical, personnel, or cyber security capabilities or vulnerabilities.</li> <li>• Theft of company-specific (proprietary) information/technology, classified information, or information relating to rail security or national defense.</li> <li>• Individuals displaying false official affiliation, or misusing items representative of official affiliation, to include identification credentials, company badges/insignia, official documents, and vehicles, intended to deceive rail staff and/or security into believing an official/legitimate association with the entity with possible nefarious intent that may pose a risk to transportation security.</li> <li>• Theft of company credentials, vehicles, uniforms, track or maintenance equipment, such as rail saw, portable derailer.</li> <li>• Suspicious actions, including accessing, attempts to access, or tampering with restricted compartments or equipment.</li> <li>• Suspicious actions, including the unauthorized entry or attempted entry of restricted areas.</li> <li>• Individuals who attempt to or flee the area when confronted by rail staff or security personnel.</li> </ul>

REGULATORY REPORTING REQUIREMENT	EXAMPLES
<p>§ 1580.105(c)(6) “Discharge, discovery, or seizure of a firearm or other deadly weapon on a train, in a station, terminal, facility, or storage yard, or other location used in the operation of the railroad, rail hazardous materials shipper, or rail hazardous materials receiver.”</p> <p>§ 1580.203(c)(6) “Discharge, discovery, or seizure of a firearm or other deadly weapon on a train or transit vehicle or in a station, terminal, facility, or storage yard, or other location used in the operation of the passenger railroad carrier or rail transit system.”</p>	<p>Examples include weapons or explosives in or around a facility, conveyance, or infrastructure of an owner/operator subject to this 49 CFR Part 1580 that may present a risk to transportation security (for example, discovery of weapons inconsistent with the type or quantity traditionally used by company security personnel).</p>
<p>§ 1580.105(c)(7) “Indications of tampering with rail cars.”</p> <p>§ 1580.203(c)(7) “Indications of tampering with passenger rail cars or rail transit vehicles.”</p>	<p>Examples include:</p> <ul style="list-style-type: none"> <li>• Placing on or attaching a foreign object to a rail car(s).</li> <li>• Disconnecting vital equipment on a rail car(s) (such as air hoses or communication cables).</li> <li>• Removal of seals, security devices, or mechanisms that are designed to secure certain equipment, compartments, or materials from access by members of the general public.</li> </ul>
<p>§ 1580.105(c)(8) “Information relating to the possible surveillance of a train or facility, storage yard, or other location used in the operation of the railroad, rail hazardous materials shipper, or rail hazardous materials receiver.”</p> <p>§ 1580.203(c)(8) “Information relating to the possible surveillance of a passenger train or rail transit vehicle or facility, storage yard, or other location used in the operation of the passenger railroad carrier or rail transit system.”</p>	<p>Examples include individuals demonstrating unusual interest in facilities, conveyances, or infrastructure owned or operated by an owner/operator subject to this part in a manner that may pose a risk to transportation or national security, such as:</p> <ul style="list-style-type: none"> <li>• Individuals demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional interest such that a reasonable person would consider the activity suspicious.</li> <li>• Individuals observing through binoculars, taking notes, attempting to measure distances.</li> <li>• Individuals noting the physical arrival and/or departure times of trains.</li> <li>• Individuals who do not appear to be conducting official or legitimate business, observed sitting in vehicles near rail operations.</li> <li>• Individuals who approach rail employees and seek information out of the ordinary, such as information concerning rail operations, rail equipment, rail fueling stations, locomotive fuel capacity, or security issues.</li> <li>• Individuals who attempt to or flee the area when confronted by rail staff or security personnel.</li> </ul>
<p>§ 1580.105(c)(9) “Correspondence received by the freight railroad carrier, rail hazardous materials shipper, or rail hazardous materials receiver indicating a potential threat. <i>Other incidents involving breaches of the security of the freight railroad carrier, rail hazardous materials shipper, or rail hazardous materials receiver's operations or facilities.</i>”</p>	<p>Threatening correspondence examples apply to any form of communication (written, spoken, or digitally transmitted), including:</p> <ul style="list-style-type: none"> <li>• Correspondence that includes any of the items enumerated in §§ 1580.105(c) or 1580.203(c).</li> <li>• Threat of any action to cause harm or injury to a rail system’s operation, personnel, passengers, or infrastructure, to include, but not limited to, such actions as active shooters, or use of an incendiary device, and use of physical intimidation.</li> </ul>

REGULATORY REPORTING REQUIREMENT	EXAMPLES
<p>[Note: for the preceding <i>italicized</i> text, please refer to “§ 1580.203(c)(10)” in the next row of this table.</p> <p>§ 1580.203(c)(9) “Correspondence received by the passenger railroad carrier or rail transit system indicating a potential threat to rail transportation.”</p>	
<p>§ 1580.203(c)(10) “Other incidents involving breaches of the security of the passenger railroad carrier or the rail transit system operations or facilities.”</p>	<p>Examples include unauthorized personnel attempting to or actually entering a restricted area or protected site relating to a transportation facility or conveyance, including an individual entering or attempting to enter by impersonation of authorized personnel (for example, police/security, janitor, vehicle owner/operator), such as:</p> <ul style="list-style-type: none"> <li>• An individual observed loitering near critical infrastructure, to include rail switches, switch stands, signal bungalows, and other potentially critical infrastructure/locations along the railroad tracks and right of way who does not appear to be there with a legitimate sense of purpose.</li> <li>• Unauthorized personnel attempting to or entering the perimeter of a restricted area or secured site.</li> <li>• Attempted or actual penetration of a rail facility, vehicle, establishment, operations site, or right of way by impersonation of authorized personnel.</li> <li>• Individuals who attempt to or flee from within a controlled/restricted area (area not open to the general public) when confronted by rail staff or security/law enforcement personnel.</li> <li>• The theft or loss of sensitive security information – such as construction design plans, operational deployment plans, engineering drawings/diagrams, and train consists, etc.</li> <li>• Cyber-attacks against the entity to include attempts or actual compromise of information/technology owned or operated by the entity.</li> </ul> <p><i>Note: Individuals who are identified through previous vetting as a non-threat need not be considered suspicious, unless events and the environment at the time of the encounter dictate otherwise.</i></p>

In submitting reports under 49 CFR Part 1580, TSA's ability to analyze the data and improve the quality of information disseminated back to its stakeholders could be enhanced if more detailed information is provided when reporting incidents to TSA. The following provides some examples of the types of information that would be most useful.

49 CFR 1580 Requirements	Examples
(1) The name of the reporting freight railroad carrier, rail hazardous materials shipper, or rail hazardous materials receiver and contact information, including a telephone number or e-mail address.	<ul style="list-style-type: none"> <li>• Company Representative: Joe BLOGGS</li> <li>• Company: ABC Rail Road Company</li> <li>• Address: XXXXX, XX (Street), XXXXX (City), XX (State), XXXXX (ZIP)</li> <li>• Phone: (111) 123-1234</li> <li>• POC E-mail: Reporting.Official@ABCRR.Com</li> </ul>
(2) The affected train, station, terminal, rail hazardous materials facility, or other rail facility or infrastructure.	<ul style="list-style-type: none"> <li>• Locomotive: ABCRR, Reporting Marks</li> <li>• Locomotive Number 1234</li> <li>• Rail Car: ABCRR Railcar Number XXXX 001234</li> <li>• Train: ABCRR Train Number XXX of XX, etc.</li> <li>• Facility: ABCRR (Rail Yard, Subway Station, Passenger Station, Storage Yard, Repair Facility, etc.) and facility physical address.</li> <li>• Right of Way: Mile Post Marker, Sub-division, and physical address (as much as known).</li> </ul>
(3) Identifying information on the affected train, train line, and route.	<ul style="list-style-type: none"> <li>• Rail Car: ABCRR Railcar Number XXXX 001234</li> <li>• Train: ABCRR Train Number XXX of XX etc.</li> <li>• Transit Vehicle: ABCRR LRV Number XXXXX etc.</li> <li>• Train Line: ABCRR X Line, etc.</li> <li>• Route: ABCRR North Corridor, XXXX Line Section.</li> </ul>
(4) Origination and termination locations for the affected train, including departure and destination city and the rail line and route, as applicable.	<ul style="list-style-type: none"> <li>• ABCRR, Northern Corridor Express – Boston to New York, XYZ Line, via X, Y and Z Cities.</li> </ul>
(5) Current location of the affected train.	<ul style="list-style-type: none"> <li>• ABCRR Train Number XXX of XX is currently located at:</li> <li>• MP 123.12, XXX Sub-division, XXXX (City), XX (State).</li> <li>• XXX Station, Street, City, State, ZIP.</li> </ul>
(6) Description of the threat, incident, or activity.	<ul style="list-style-type: none"> <li>• At XXXX hours, January 01, 2020</li> <li>• ABCRR Police Sergeant, Joe BLOGGS, badge number XXXX, ABCRR Police Department (ABCPD) reported the following:</li> <li>• At WWW hours, January 01, 2020, a suspicious person (described as a white male, approximately 6'0" tall, 190 lbs., blonde hair, approximately 35 to 40 years of age, wearing a long black knee-length coat, blue jeans, red sneakers, and a XXXX ball club baseball hat) was detected adjacent to the ticket vending machine at the street level entrance to the XX<sup>st</sup> Street and YYYYY Avenue, Station, XXXX (City), XX (State). The person was deemed suspicious because although the temperature at the time was 85 degrees, he was wearing a knee-length heavy black coat. The individual was sweating and exhibited nervousness when security officials were present (the individual looked away every time a security official appeared so as to not reveal his face). The individual had a black "Traveler," "Expandable" suitcase with him (estimated measurements: 36" W X 24"H X 12"D) with a red piece of ribbon tied to the handle. At WWW5 hours, the individual rapidly departed the area when a security official began to approach him, leaving the black suitcase behind. A review of the CCTV surveillance system determined the individual had</li> </ul>

	<p>arrived at the station at VV30 hours in a Red, 4 door, Land Rover, VA License Plate XX123XXXX, which was parked adjacent to the XXXXX. CCTV revealed the vehicle was being driven by a white female with shoulder length blonde hair, approximately 35 years of age. A check of the VA DOT License registry revealed the vehicle is registered to Joe DOE, DOB: XX/XX/XXXX, POB: XXXXX (City), XX (State) and Jane (NEE: SMITH) DOE, DOB: XX/XX/XXXX, POB: XXXXX (City), XX (State) of 1234 West Disobedience Street, Anytown, VA 202XX, Phone Number: (XXX)XXX-XXXX. A check of the VA driver's license registry revealed similar/matching descriptions of Joe and Jane DOE to those persons identified during the incident. At ZZZZ hours, a XXXX City Police Explosive Ordnance Demolition (EOD) team conducted an examination of the black suitcase with x-ray equipment and determined the suitcase contained an unknown device comprised of wiring and circuitry. EOD disrupted the suitcase, which yielded negative secondary results. EOD's examination of the suitcase's contents revealed limited amounts of women's clothing and what appeared to be the inner workings of a radio. At ZZZ1 hours, the scene was cleared by XXXX City Police EOD Sergeant Jeff BOMBGARTEN, badge number XXXX who secured the suitcase and its contents and transported them away from the facility.</p>
<p>(7) The names and other available biographical data of individuals involved in the threat, incident, or activity.</p>	<ul style="list-style-type: none"> <li>• Witness: Joe SMITH, DOB: XX/XX/XXXX, POB: XXXX City, XX State, Address: XXXXX, XX Street, XXXX City, XX State, Phone Number (XXX)XXX-XXXX, ABCRR, XXXX (Address), (XXX)XXX-XXXX.</li> <li>• Security: Fred ARRESTER, Sergeant, XXXX (City) Police Department, Badge # XXXX, Phone Number: (XXX)XXX-XXXX</li> <li>• Suspected Associate: Mrs. Jane DOE</li> <li>• DOB: XX/XX/XXXX, POB: XXXX City, XX State, Address: XXXXX, XX Street, XXXX City, XX State, Phone Number (XXX)XXX-XXXX, ABCRR, XXXX (Address), (XXX)XXX-XXXX.</li> </ul>
<p>(8) The source of any threat information.</p>	<ul style="list-style-type: none"> <li>• Jane DOE, DOB: XX/XX/XXXX, POB: XXXX City, XX State, Address: XXXXX, XX Street, XXXX City, XX State, Phone Number (XXX)XXX-XXXX, ABCRR, XXXX (Address), (XXX)XXX-XXXX.</li> </ul>