



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.2.8

JUNE 14, 2023

EFFECTIVE DATE

(06-14-2023)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.2.8, *Incident Reporting*.

MATERIAL CHANGES

- (1) Added the Insider Threat program.
- (2) Added Infectious disease incidents.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 10.2.8 dated July 25, 2019.

AUDIENCE

Servicewide

Richard L. Rodriguez
Chief
Facilities Management and Security Services

10.2.8
Incident Reporting

Table of Contents

- 10.2.8.1 Program Scope and Objectives
 - 10.2.8.1.1 Background
 - 10.2.8.1.2 Authority
 - 10.2.8.1.3 Responsibilities
 - 10.2.8.1.4 Program Management and Review
 - 10.2.8.1.5 Program Controls
 - 10.2.8.1.6 Terms and Acronyms
 - 10.2.8.1.7 Related Resources
- 10.2.8.2 Incident Report
- 10.2.8.3 Notification
- 10.2.8.4 Insider Threat
- 10.2.8.5 Infectious Disease

Exhibits

- 10.2.8-1 Incidents To Be Reported To SAMC

10.2.8.1
(06-14-2023)
Program Scope and Objectives

- (1) This IRM section discusses the Situational Awareness Management Center (SAMC) and provides guidance on the types of incidents to report, when to report an incident, and how to report an incident.
- (2) **Purpose:** This IRM provides policy and guidance to be used by IRS personnel and organizations including vendors, and outsourcing providers when reporting physical security incidents to the SAMC. Physical security incidents are incidents and/or threats (direct, indirect, or implied), office closures, loss of identification (ID) media, disruptive/disgruntled taxpayers and personnel, infectious disease exposures, and Insider Threats (InT).
- (3) **Audience:** Servicewide
- (4) **Policy Owner:** Chief, Facilities Management and Security Services (FMSS)
- (5) **Program Owner:** FMSS Associate Director (AD), Security
- (6) **Primary Stakeholders:** Senior Commissioner's Representatives (SCR), Administrative Officers (AO), FMSS ADs, FMSS Field Operations Territory Managers (TM), Security Section Chiefs (SSC), Physical Security Staff (PSS), and FMSS Security Personnel.
- (7) **Program Goals:** To ensure servicewide incident reporting for IRS Headquarters (HQ) and provide senior leader awareness and analysis.

10.2.8.1.1
(06-14-2023)
Background

- (1) SAMC is tasked with receiving and promptly reporting all physical security incidents and/or threats. SAMC's mission is to document, archive and report incidents, threats, and emergencies by supporting the Internal Revenue Service's law enforcement partners to ensure the safety of IRS personnel, facilities, and infrastructure. Additionally, SAMC disseminates, documents, and responds to inquiries from the Department of the Treasury, governmental agencies, and other federal law enforcement partners. This is important as SAMC must be kept apprised of situations that could require the immediate assistance and/or attention of the IRS Commissioner, the Chief, FMSS, and/or other IRS Leadership.
- (2) SAMC operates 24 hours 7 days a week and is the focal point for incident reporting. SAMC monitors and routes incident reports to the appropriate IRS personnel.

10.2.8.1.2
(06-14-2023)
Authority

- (1) Treasury Directive (TD), TD P 85-01, Treasury Information Technology Security Program, February 28, 2022
- (2) Restructuring and Reform Act (RRA) 98, 26 United States Code (USC) 7608 (b) and Public Law 105-206 or The Internal Revenue Service Restructuring and Reform Act of 1998
- (3) Homeland Security Act of 2002 and 40 USC 1315

10.2.8.1.3
(06-14-2023)
Responsibilities

- (1) Chief, FMSS prescribes and oversees security incident reporting, policy, and guidance.
- (2) AD, Security oversees planning, developing, implementing, evaluating, and controlling security incident reporting.

(3) Each FMSS Operations AD and TM will ensure each SSC adheres to the IRS Incident Reporting Program.

(4) Section Chief, SAMC, is responsible for:

- a. Developing and updating policy, procedures, and training documents.
- b. Serving as the Threat and Incident Response Center (TIRC) Chair.
- c. Maintaining Internal Controls for the SAMC Program.
- d. Reviewing and approving the daily Leadership View (LV) report that outlines the Level 1, Level 2, and Level 3 Physical Security Incidents along with any office closures that occurred that day.
- e. Establishing a secure process to receive physical security incidents and providing guidance to Watch Stander (WS) on proper classification, as needed.

(5) The SSC is responsible for:

- a. Monitoring all incidents and threats within their geographical area to assist in identifying the validity of the data reported.
- b. Ensuring reported incidents are properly addressed through established protocols and countermeasures.
- c. Submitting the Follow Up Incident Report (FUIR).

Note: All incidents that have been classified as a Level 1 incident and/or threat require a FUIR.

Note: The FUIR must be submitted to SAMC within 24 hours of occurrence.

Note: A Level 2 or 3 incident and/or threat may require a FUIR at the discretion of the AD of Security. The FUIR for Level 2 or 3 incidents must be completed within 72 hours.

- d. Completing and ensuring their assigned Physical Security Staff complete ITM Course 71555, *SAMC Incident Reporting*, annually.
- e. Providing updates on incidents to the FMSS TM, FMSS Operations AD, and SAMC until the incidents are completed and/or terminated.

Note: Any incident requiring the evacuation or closing of an IRS facility due to an impending threat, either natural or man-made, is considered significant. In addition to SAMC, the FMSS TM and/or SSC must also report significant incidents immediately to the Chief, FMSS, and Operations AD by telephone. This initial notification is intended to provide forewarning of impending threats and/or situations.

(6) SCR/AO is responsible for reporting facility closures affected by any major equipment failures, natural disasters, acts of nature, or severe weather.

- a. Reports of closures to SAMC must include:
 - i. Description of the incident
 - ii. Facility impacted by the incident
 - iii. Number of personnel affected
 - iv. Amount of time the facility is expected to be closed

(7) All IRS Personnel are responsible for:

- a. Familiarizing themselves with the physical security incident and emergency reporting procedures, including the reporting of all physical security incidents, to SAMC within 30 minutes of incident discovery, or when it is safe to do so.

Note: For additional information, see ITM Course 71555, *SAMC Incident Reporting*.

10.2.8.1.4
(06-14-2023)
**Program Management
and Review**

- (1) **Program Goals:** To ensure servicewide incident reporting for IRS Headquarters (HQ) and provide senior leader awareness and analysis.
- (2) **Program Reports:** Provide information regarding reporting of the program objectives. It is not intended to provide instruction for completing any reports. Identify the data sources, storage location, and the primary purpose for this data.
- (3) **Program Effectiveness:** The timely and accurate incident processing, incident reporting, and notification to appropriate stakeholders.
- (4) **Internal Control - Random Sampling Process:** Ensures that SAMC complies with the 15-minute timeframe for incident processing.
- (5) **Annual Review:** Review the processes included in this manual annually to ensure accuracy and promote consistent tax administration.

10.2.8.1.5
(07-25-2019)
Program Controls

- (1) Internal Control - Random Sampling Process – ensures that the WS complies with the 15-minute timeframe for incident processing within the TRC application.

10.2.8.1.6
(06-14-2023)
Terms and Acronyms

- (1) **Direct Threat** - A threat is made through verbal communication when an individual threatens to harm a government employee, others, themselves, or any public officials. Threat can be communicated telephonic, in writing, through the postal service, through other electronic means or by body language. A threat can also be made to a government employee away from government property when the person making the threat has identified the individual by the nature of their work. Threats must be reported to law enforcement, onsite Protective Security Officer (if available) and management.
- (2) **Federal Protective Service (FPS)** - An organization within the Department of Homeland Security (DHS) that protects federal facilities, their occupants, and visitors by providing law enforcement and protective security services/officers.
- (3) **Follow Up Incident Report (FUIR)** - Report generated and prepared by the impacted SSC and used by the TIRC to outline the actions taken by FMSS to mitigate the reported incident/threat.
- (4) **Incident** - An occurrence of an action or situation, such as an act of human intervention or an act of nature (e.g., storm or fire) that requires a physical security response.
- (5) **Indirect Threat** - Any verbal or nonverbal communication that raises a concern of potential violence. The comment is stated indirectly about a government employee, person, themselves, government officials or towards a government facility. The communications can be received in person, through body language, in writing, by telephone, by fax or other electronic means.

- (6) **Information Technology (IT) Security** - IT security service provider responsible for ensuring IRS compliance with federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
- (7) **Infrastructure** - The basic equipment and structures (e.g., phones, desks, electricity, buildings) that are needed for the IRS to function properly.
- (8) **Insider Threat** - An insider threat includes but is not limited to, Unauthorized Access (UNAX) violations; workplace violence and threats; domestic violence; concerning or inappropriate behavior; security breaches; background investigations; and information disclosures.
- (9) **Level 1 Incident** - Incidents (actual or alleged) involving a direct or imminent threat or implied threat of physical harm to employees, contractors, visitors; damage, and/or destruction of IRS facility, infrastructure, property, and/or equipment; and/or actual or potential compromise of IRS data. Incidents can be direct (e.g., face to face or via phone call); indirect (e.g., email, mail, or other social media;) or other (e.g., defacement of property, conveyed via another party or source).
- (10) **Level 2 Incident** - Incidents (actual or alleged) involving an indirect threat of physical harm to employees, contractors, visitors; damage and/or destruction of IRS facility, infrastructure, property, and/or equipment; and/or actual or potential compromise of IRS data. Incidents can be indirect (e.g., verbal via phone call, email, mail, or other social media;) or other (e.g., defacement of property, conveyed via another party or source).
- (11) **Level 3 Incident** - Incidents involving no direct or indirect physical harm to employees, contractors, visitors; damage, and/or destruction of IRS facility, infrastructure, property and/or equipment; and/or actual or potential compromise of IRS data. Example of incidents include, minimal security or management involvement, security exercises, and loss, theft, or unrecoverable ID media.
- (12) **Personally Identifiable Information (PII)** - Is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
- (13) **Personnel** - Refers to IRS employees and contractors.
- (14) **Privacy, Governmental Liaison and Disclosure (PGLD)** - An IRS organization whose mission is to protect the sensitive information and privacy of taxpayers and employees.
- (15) **Security Exercises** - Security awareness drills such as Shelter-in-Place, Fire Drill, and Active Shooter.
- (16) **SAMC** - A 24/7 program within FMSS responsible for incident and threat reporting servicewide. The SAMC also serves as the central point for all incident communications and notifications.
- (17) **Stakeholder** - IRS business unit or individual responsible for security oversight and/or with a need to know.
- (18) **Taxpayer Assistance Center (TAC)** - An IRS location that provides taxpayers with tax assistance face-to-face.
- (19) **Threat** - A person or thing likely to cause damage or danger.

- (20) **Treasury Inspector General for Tax Administration (TIGTA)** - A Treasury organization committed to the prevention and detection of fraud, waste, and abuse within the IRS and related entities.
- (21) **TIGTA Incident Notification Submittal (TINS)** - Incidents submitted by TIGTA to SAMC.
- (22) **Threat and Incident Response Center (TIRC)** - Group that monitors and reviews incidents and threats to the IRS. Stakeholder organizations, including: FMSS, TIGTA, Criminal Investigation (CI), PGLD, IT Cyber Security, and FPS.
- (23) **Threat Response Center (TRC)** - Database software application used by the Watch Standers to manage all incident and threats reported to SAMC.
- (24) **Watch Stander (WS)** - SAMC personnel that receive and process incidents and distribute to appropriate stakeholders.

Acronyms

Acronym	Definition
24/7	24 hours a day 7 days a week
AD	Associate Director
AO	Administrative Officer
CI	Criminal Investigation
COGCON	Continuity of Government Readiness Condition
DHS	Department of Homeland Security
ESC	Executive Steering Committee
FMSS	Facilities Management and Security Services
FPS	Federal Protective Service
FUIR	Follow Up Incident Report
HAZMAT	Hazardous Material
HQ	Headquarters
HVAC	Heating, Ventilation, and Air Conditioning
ID	Identification
InT	Insider Threat
IT	Information Technology
ITM	Integrated Talent Management
LV	Leadership View
PGLD	Privacy, Governmental Liaison and Disclosure
PII	Personally Identifiable Information

Acronym	Definition
POC	Point of Contact
POD	Post of Duty
PSS	Physical Security Staff
RRA	Restructuring and Reform Act
SAMC	Situational Awareness Management Center
SCR	Senior Commissioner's Representative
SIP	Shelter in Place
SSC	Security Section Chief(s)
TAC	Taxpayer Assistance Center
TD	Treasury Directive
TIGTA	Treasury Inspector General for Tax Administration
TINS	TIGTA Incident Notification Submittal
TIRC	Threat and Incident Response Center
TM	Territory Manager(s)
TRC	Threat Response Center
UNAX	Unauthorized Access
USC	United States Code
WG	Working Group
WS	Watch Stander(s)

10.2.8.1.7
(06-14-2023)

Related Resources

- (1) IRM 10.2.9, *Occupant Emergency Planning*
- (2) IRM 10.5.4, *Privacy and Information Protection, Incident Management Program*
- (3) IRM 10.8.1, *Information Technology, Policy and Guidance*
- (4) IRM 21.3.4, *Taxpayer Contacts, Field Assistance*
- (5) *Insider threat Capability Concept of Operations*

10.2.8.2
(06-14-2023)

Incident Report

- (1) All IRS personnel must report any physical security incidents to the SAMC within 30 minutes of incident discovery/identification, or when it is safe to do so.
- (2) When reporting incidents to the SAMC or to the local FMSS PSS, at a minimum, the following information must be provided:
 - a. Time and date of incident

- b. Name of facility/office
- c. Address of facility/office
- d. Details of what occurred (i.e., who, what, when, where, how, and if possible, why)
- e. Who was notified (e.g., FPS, TIGTA, local authorities, senior management, etc.)
- f. Approximate number of IRS personnel affected
- g. Whether the facility has been evacuated or closed (including the number of downtime minutes/hours)
- h. Point of Contact (POC) or an individual at the facility in the event there are follow up questions

(3) Incident Reporting (SAMC website portal) at:

- a. <https://tscc.enterprise.irs.gov/irc/>
- b. Telephone at 202-317-6124
- c. Toll free hotline at 1-866-216-4809
- d. E-mail samc@irs.gov

Note: Although it is not always possible, the website portal is the preferred method for reporting incidents to the SAMC.

- (4) Any incident requiring the evacuation or closing of an IRS facility due to an impending threat, either natural or man-made, is considered significant. In addition to SAMC, FMSS TM and/or SSC must also report significant incidents immediately to the Chief, FMSS by telephone. This initial notification is intended to provide forewarning of impending threats and/or situations.
- (5) Threats against or assaults on IRS personnel and facilities are also required to be reported to TIGTA. TIGTA is the **only** investigative agency with jurisdiction to investigate internal and external attempts to interfere with tax administration as outlined in Restructuring and Reform Act (RRA) 98, 26 United States Code (USC) 7608 (b), and (Public Law 105-206) or The Internal Revenue Service Restructuring and Reform Act of 1998.
- (6) Threats must also be reported to the assigned Federal Protective Services (FPS) Inspector. FPS protects the buildings, grounds, and property that are owned, occupied, or secured by the Federal Government (including any agency, instrumentality, or wholly owned or mixed-ownership corporation thereof) and the persons on the property.

Note: For additional information, see *Homeland Security Act of 2002* and *40 USC 1315*.

- (7) A list of incidents that must be reported to SAMC is provided in Exhibit 10.2.8-1, *Incidents to be Reported to SAMC*. The list of incidents is not all inclusive but will help provide a basis for determining which incidents must be reported.

Note: For additional guidance, contact SAMC if you are unsure as to whether to report an incident. **When there is doubt as to whether an incident should or should not be reported, the incident should be reported to the SAMC.** It is the employee's obligation and responsibility to report security incidents through the prescribed IRS incident reporting process, even if instructed not to report by an investigative agency such as FPS.

- (8) Incidents involving the inadvertent unauthorized disclosure of Personally Identifiable Information (PII) or Privacy act information must be reported to PGLD via the Personally Identifiable Information (PII) Breach Reporting Form.

Note: For additional information, see IRM 10.5.4, Privacy and Information Protection, Incident Management Program.

- (9) Incidents involving the loss of theft of IT assets must be reported to Cyber Security. Cyber Security will reach out to the employee's manager for action or follow-up.

Note: For additional information, see IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance.

10.2.8.3
(06-14-2023)
Notification

- (1) Various types of incident notifications will be sent to local FMSS PSS, and designated response personnel identified by their business unit. Designated response personnel are responsible for forwarding the incident/threat to the responsible party within their business unit, if applicable.
- (2) Requests for SAMC reports and incident information is based on a need to know. Due to the sensitivity of some information, incidents will not be disseminated or disclosed from SAMC outside of FMSS and/or TIGTA/Law Enforcement. Email requests for incident information must be sent to the SAMC Program Manager.
- (3) Daily notification of Level 1 and 2 physical security incidents with an impact to the IRS from the previous workday will be distributed through the Leadership View (LV) report. The LV report is distributed to designated personnel (e.g., executives, managers and other personnel).

10.2.8.4
(06-14-2023)
Insider Threat

- (1) In January 2021, the Insider Threat (InT) Executive Steering Committee (ESC) and Working Group (WG) confirmed that SAMC will be the primary employee and contractor reporting tool for cross-functional insider threat incidents.
- (2) SAMC staff will review each incident reported through the SAMC incident reporting platform to determine whether there is a direct link, or suggests the potential of being linked, to an insider threat activity and create a SAMC Incident Report and send to the Insider Threat (InT) Team Members via encrypted email.

Note: Insider Threats incidents involving Classified National Security Information (CNSI, e.g., Confidential, Secret, or Top Secret) must be reported to the Treasury Inspector General for Tax Administration (TIGTA) and the CNSI Program Managers instead of SAMC.

10.2.8.5
(06-14-2023)
Infectious Disease

- (1) Managers must report a confirmed or suspected disease through SAMC. Managers must submit a SAMC report as noted in the *Infectious Disease in the Workplace* document. Examples of Communicable or Infectious Diseases include:
 - a. Chickenpox
 - b. Coronavirus (COVID 19)
 - c. Influenza (Flu)

- d. Hand, Foot and Mouth Disease (HFMD)
- e. Measles
- f. Methicillin-Resistant Staphylococcus Aureus (MRSA)
- g. Mononucleosis
- h. Tuberculosis (TB)
- i. Monkeypox

(2) Reports of an Infectious Disease should include:

- a. Test result status (positive, negative, or unknown)
- b. Post of Duty (POD) Name
- c. Last day in the office
- d. Areas accessed

Note: Do not include PII, such as the employee's name.

(3) Managers should report updated information upon medical clearance as being no longer contagious and able to return to work via telephone at 866-216-4809, email to samc@irs.gov or through the *Incident Entry Form*.

This Page Intentionally Left Blank

Exhibit 10.2.8-1 (06-14-2023)**Incidents To Be Reported To SAMC****INCIDENTS TO BE REPORTED TO SAMC**

This list encompasses examples of situations that should be reported to SAMC. The list includes examples of incidents and/or threats (direct, indirect, implied), office closures, loss of ID media, disruptive/disgruntled taxpayers and personnel. This list does not encompass all incidents and can change as threats to the IRS change. **When there is doubt as to whether an incident should be reported to SAMC, the incident should be reported.**

INCIDENT

Active Shooter Incident (founded or unfounded)
Alarm activations (e.g., duress, fire and perimeter)
Arson or a fire with injury or a disruption of IRS operations
Attack on IRS infrastructure
Attack or assault against IRS employees
Attack or intentional destruction of an IRS facility or group of facilities
Attempted entry to a facility with a prohibited weapon
Bombing or explosion
Bomb threat (verbal, telephonic, by letter or email)
Burglary of IRS property
Civil disturbances resulting in aggression or violence on the part of the demonstrators
Continuity of Government Readiness Condition (COGCON) level change (1/2/3/4)
Counterfeit currency
Damage or destruction (inadvertent or accidental) to government property (includes graffiti)
Death of an employee or taxpayer while on IRS property
Delayed facility openings due to severe weather or utility/equipment failure
Demonstrations
DHS alert level activation
Disruptive or disgruntled taxpayer (e.g., yelling, uncooperative)
Employee altercation (e.g., verbal and/or physical)
Employee injury incident
Equipment failure
Exercises (e.g., fire drills, evacuation drills, Shelter-in-Place (SIP) drills, tabletop exercises)
Facility closures due to equipment failure (e.g., HVAC, water, electricity)
Facility closures due to severe weather (e.g., tornados, hurricane, snow)

Exhibit 10.2.8-1 (Cont. 1) (06-14-2023)
Incidents To Be Reported To SAMC

INCIDENTS TO BE REPORTED TO SAMC

Fire with or without injury/disruption of service

Found property (e.g., IRS assets)

Hazardous Material (HAZMAT) incidents (e.g., infectious disease) with no overt or implied threat or injury toward the safety of employees or IRS facility

Incidents resulting in injuries to taxpayers

Insider Threat

Intelligence threat advisory (e.g., threat assessment)

IRS scam complaint (non-IRS employee subject)

Loss of remittance with known PII disclosed data

Loss of remittance with no known PII disclosed data

Loss of perimeter, limited area and master keys, legacy ID card, Pocket Commissions, SMART ID, government property or equipment, sensitive data

Loss or theft of sensitive data (high impact and/or high risk)

Natural disaster (e.g., hurricane, tornado, severe snow, flooding, etc.)

Other - Employee reported incident when employee is acting as private citizen and there is no known nexus to their position with the IRS

Parasitic invasion (e.g., bed bugs, lice, tick, mice, etc.)

Partial day facility closure due to severe weather or equipment failure

Physical altercation (employee and/or taxpayer)

Possession (illegal)/discovery of a controlled substance

Power outages

Real world event (no impact to IRS employees or operations). Example: events that happen near an IRS location, but not related to the IRS.

Robbery of an employee and/or of a taxpayer on IRS property

Sick employee or taxpayer

Shelter-in-Place (not a drill)

Statements by individuals of support of violence to IRS employees and/or facilities

Statements by individuals of sympathy with radical groups. Example: a group favoring/ supporting/ representing a drastic political, economic, religious or social reforms by direct and often uncompromising methods.

Statements - Inappropriate. Example: statements of violence, sexual harassment or racism.

Suicide threats by employee or taxpayer with no nexus to an IRS facility or concern for the safety of IRS employees or facilities.
 (Suicide threats by a taxpayer must also be reported to PGLD.)

Exhibit 10.2.8-1 (Cont. 2) (06-14-2023)
Incidents To Be Reported To SAMC**INCIDENTS TO BE REPORTED TO SAMC**

Suicide threats nexus to an IRS facility (by employee or taxpayer when an overt or implied threat is made toward the safety of employees or an IRS facility, whether they can carry out the threat or not.

Suspicious activity (e.g., photographing or surveillances of IRS property; No-nexus related events/incidents at Federal Buildings or IRS shared locations)

Suspicious packages resulting in a disruption of IRS operations or negative finding.

Taxpayer complaint - Example: a complaint in regard to screening process or a guard complaint.

Theft of building access card, building or room keys, legacy ID card, pocket commissions, SMART ID, government property or equipment, sensitive data

Theft of government property, personal property, a lockbox, or tax remittance

Threat against IRS personnel

Threat against IRS infrastructure

Threat against government property (IT)

Threat on an IRS facility or group of facilities

Unauthorized entry to a facility and/or property (i.e., trespassing)

Unrecoverable building access card, building or room keys, legacy ID card, pocket commissions, and/or SMART ID

Unsecured property or facility

Vehicle accidents on government property (with or without injuries)

Verbal/written threat (involving an employee or taxpayer)

Weapon discharge

Workplace incident - disruptive/disgruntled employee (physical and/or verbal altercations)

Workplace incident - incident requiring minimal law enforcement, FMSS or senior IRS management mitigation

Workplace violence - Physical altercation between employees or between an employee and a taxpayer

