

Suspicious Activity Reporting (SAR)

316.1 VERSION

Review Date	Effective Date	Approving Authority
12/04/2020	07/09/18	Gabriel Camacho, Interim Chief of Police

316.2 POLICY AND PURPOSE

This policy provides guidelines for reporting and investigating suspicious and criminal activity related to terrorism. The Harrisonburg Police Department recognizes the need to protect the public from criminal conduct and acts of terrorism and shall lawfully collect, maintain and disseminate information regarding suspicious activities, while safeguarding civil liberties and privacy protections.

316.3 ACCOUNTABILITY STATEMENT

All employees are expected to fully comply with the guidelines and timelines set forth in this policy. Responsibility rests with the supervisor to ensure that any violations of policy are investigated and appropriate training, counseling and/or disciplinary action is initiated. This directive is for internal use only, and does not enlarge an employee's civil liability in any way. It should not be construed as the creation of a higher standard of safety or care in an evidentiary sense, with respect to third party claims. Violation of this directive, if proven, can only form the basis of a complaint by this department, and then only in a non-judicial administrative setting.

316.4 DEFINITIONS

Involved party - An individual who has been observed engaging in suspicious activity, as defined in this policy, when no definitive criminal activity can be identified, thus precluding the person's identification as a suspect.

Suspicious activity - Any reported or observed activity that a member reasonably believes may have a nexus to any criminal act or attempted criminal act, or to foreign or domestic terrorism. Race, ethnicity, national origin or religious affiliation should not be considered as factors that create suspicion (although these factors may be used as specific suspect descriptions). Examples of suspicious activity may include, but are not limited to:

- Suspected pre-operational surveillance or intelligence gathering (e.g., photographing security features, asking questions about sensitive security-related subjects).
- Tests of security measures and response to incidents (e.g., "dry run," creating false alarms, attempts to enter secure areas without authorization).
- Suspicious purchases (e.g., purchasing large quantities of otherwise legal items, such as fertilizer, that could be used to create an explosive or other dangerous device).

Harrisonburg Police Department

Policy Manual

Suspicious Activity Reporting (SAR)

- An individual in possession of such things as a hoax explosive or dispersal device, sensitive materials (e.g., passwords, access codes, classified government information), or coded literature or correspondence.

Suspicious Activity Report (SAR) - A report used to document suspicious activity. The department receives SARS from banks, financial institutions, etc.

316.5 RESPONSIBILITIES

The Criminal Investigation Division Commander and the authorized designees will manage SAR activities. Authorized designees should include supervisors who are responsible for department participation in criminal intelligence systems.

The responsibilities of the Criminal Investigation Division Bureau include, but are not limited to:

- (a) Remaining familiar with those databases available to the department that would facilitate the purpose of this policy.
- (b) Maintaining adequate training in the area of intelligence gathering to ensure no information is being maintained that would violate the law or civil rights of any individual.
- (c) Ensuring a process is available that would allow members to report relevant information. The process should be designed to promote efficient and quick reporting, and should not be cumbersome, duplicative or complicated.
- (d) Ensuring that employees are made aware of the purpose and value of documenting information regarding suspicious activity, as well as the databases and other information resources that are available to the Department.
- (e) Ensuring that SAR information is appropriately disseminated to employees in accordance with their job responsibilities.
- (f) Coordinating investigative follow-up, if appropriate.
- (g) Coordinating with any appropriate agency or fusion center.
- (h) Ensuring that, as resources are available, the Department conducts outreach that is designed to encourage community members to report suspicious activity and that outlines what they should look for and how they should report it (e.g., website, public service announcements).

316.6 REPORTING AND INVESTIGATION

Any department employee receiving information regarding suspicious activity should take any necessary immediate and appropriate action, including a request for tactical response or immediate notification of specialized entities, when applicable. Any civilian employee who receives such information should ensure that it is passed on to an officer in a timely manner.

If the suspicious activity is not directly related to a reportable crime, the employee should document the suspicious activity including information about the involved parties and the circumstances of the incident. If, during any investigation an officer becomes aware of suspicious activity that is unrelated to the current investigation, the information should be documented.

Harrisonburg Police Department

Policy Manual

Suspicious Activity Reporting (SAR)

If an officer or other employee feels that there is an urgency involved, the on-duty patrol supervisor will be contacted for guidance as to whether a federal or state agency should be immediately notified and/or the Incident Command System be implemented to control a situation. If it is necessary to provide immediate information or evacuation of an area within the City of Harrisonburg, the reverse 911 system may be initiated by the Chief of Police or his designee.

316.6.1 TERRORISM AWARENESS

The Community Resources Unit will be responsible for incorporating information of the importance on reporting suspicious activity and terrorism awareness to both community and business groups through established crime prevention programs. Any release of information involving possible terrorist activity will be processed through the Public Information Commander in accordance with procedures established in the Media Relations Policy.

316.6.2 TYPES OF TERRORISM

- Chemical Incident - Occurs when chemical agents are intentionally released to produce death, injury or terror.
- Biological Incident - Involves the use of micro-organisms or toxins derived from living organisms to produce death or disease in humans, animals or plants.
- Radiological Incident - Involves the release of ionizing radiation into the atmosphere such as from a "dirty bomb" or other radiological dispersion device.
- Nuclear Incident - Involves the detonation of a nuclear device and results in an unrestrained fission reaction that causes blast damage.
- Explosive Incident - Occurs when the detonation of explosives causes death, injury, and/or terror.
- Hostage Taking Incident - Involves the taking of hostages to further terrorize the community and attempt to force government or private action.
- Incendiary Incident - Involves intentional ignition of combustible materials designed to start fires.

316.7 HANDLING INFORMATION

The Records Unit will forward copies of suspicious activity reports (SARs), in a timely manner, to:

- The Criminal Investigation Division supervisor.
- The Crime Analysis unit.
- Intelligence Unit
- Other authorized designees.

316.8 ALERT CODES

The Federal Homeland Security Advisory System provides a means to inform the citizens of the Commonwealth of the relative level of threat of a terrorist act. The National Terrorism Advisory

Harrisonburg Police Department

Policy Manual

Suspicious Activity Reporting (SAR)

System (NTAS) has replaced the color-coded threat scale and is comprised of the following threat conditions or levels:

- (a) Imminent Threat - Warns of a credible, specific, and impending terrorist threat against the United States.
- (b) Elevated Threat - Warns of a credible terrorist threat against the United States.

Additionally, the NTAS Alerts contain a “sunrise provision” indicating when a specific date when the alert expires. There will not be a constant NTAS alert or blanket warning that there is an OVERARCHING threat. If threat information changes for an alert, the Secretary of Homeland Security may announce an updated NTAS alert. All changes, including the announcement that cancels an NTAS alert, will be distributed the same way as the original alert. It may be extended if new information becomes available or the threat evolves.