

Briefcase

If this is the first time you access this guide please read the information below, otherwise [click here for the Table of contents](#).

CI has the ability to utilize a number of special investigative techniques that clearly enhance investigations and often provide the only means by which CI is able to obtain the evidence needed to make its recommendation for prosecution. Unfortunately, these techniques are often left on the shelf because agents either do not completely understand the procedures, or perceive them to be too laborious and fraught with red tape. As a result, the SIT Briefcase has been established to offer agents a special investigative technique instruction manual. Special agents will find this manual to be very easy to use and free from IRM-ease. Each section includes a brief definition along with a step by step instruction sequence for the initiation, maintenance and termination of the primary special investigative techniques administered by the Office of Operations Policy and Support, Special Investigative Techniques (SIT). The Briefcase also includes templates for the narratives and memorandums required for requesting these techniques. Go-bys are available from Undercover Program Managers (UPM) and in the SIT Community in CASE.

The SIT Briefcase is not designed to account for all situations and scenarios surrounding special investigative techniques, but rather to provide up to date guidance on the most common situations an agent in the field may encounter. Unusual or rare techniques are not discussed in detail in the briefcase and should be discussed with your UPM prior to initiation. Users who wish to print this document should be cautioned that the SIT Briefcase is a live document maintained on CASE, thus previously printed copies may not contain the most up to date information. Finally, if it has been a while since an agent has used a technique, or if it is the agent's first time to use a technique, it is highly recommended that the IRM sections referenced under each topic be read in their entirety.









SIT has oversight responsibilities for the authorization and implementation of a variety of special investigative techniques, including but not limited to:

- 1) Nonresponsive [REDACTED]
- 2) nonresponsive [REDACTED]
- 3) Non-Consensual Monitoring
- 4) Electronic surveillance,
- 5) Nonresponsi [REDACTED]
- 6) Nonresponsiv [REDACTED]
- 7) Nonresponsive [REDACTED]

SIT Senior Analysts and Undercover Program Managers are available for advice and guidance on these techniques. SIT staff is ready to be involved during the development and planning stages of all these techniques and will assist in the crafting of requests.

USING THE SIT BRIEFCASE

The SIT Briefcase is very easy to use. The table of contents is linked to the text for ease in navigating directly to the topics you are interested in. Throughout the guide you will see the symbols listed below that have been added to help the user quickly find the information he or she is seeking. Each special investigative technique begins with a brief definition followed by its step by step process from a special agent's standpoint. The steps in the process that are the agent's responsibility are marked with a green check mark. The other steps are listed for information purposes only. If a user encounters errors, or has any suggestions for improvement to this guide, please email Senior Analyst Shantelle P. Kitchen at shantelle.kitchen@ci.irs.gov

SYMBOLS		
	Definitions	 Link
	Process	 Reminders
	Special Agent's responsibility	 Suggested Reading
		 Authorization
		 Caution

➡ Remember, an excellent resource regarding special investigative techniques is your UPM. He/she has the background and experience to assist you in all SIT matters.

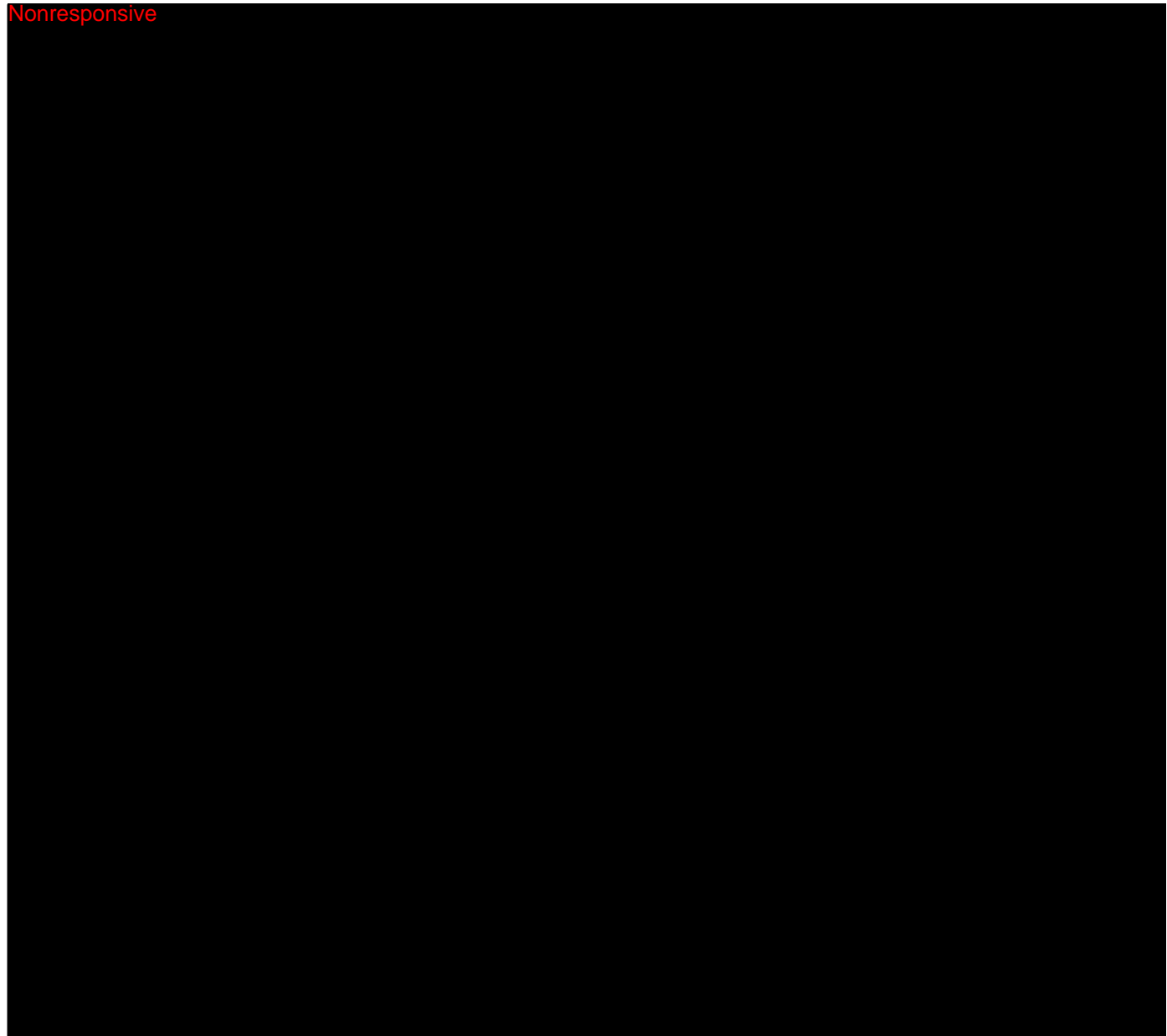


TABLE OF CONTENTS

USING THE SIT BRIEFCASE	2
Nonresponsive [REDACTED]	3
Nonresponsive [REDACTED]	6
☐ Nonresponsive [REDACTED]	7
☐ Nonresponsive [REDACTED]	7
☐ Nonresponsive [REDACTED]	7
Nonresponsive [REDACTED]	8
Nonresponsive [REDACTED]	8
Nonresponsive [REDACTED]	9
Nonresponsive [REDACTED]	9
☐ Nonresponsive [REDACTED]	10
☐ Nonresponsive [REDACTED]	10
Nonresponsive [REDACTED]	11
☐ Nonresponsive [REDACTED]	12
Nonresponsive [REDACTED]	13
☐ Nonresponsive [REDACTED]	13
Nonresponsive [REDACTED]	14
NON-CONSENSUAL MONITORING AND ELECTRONIC SURVEILLANCE	14
REAL TIME – INTERCEPTIONS OF COMMUNICATIONS (WIRETAP)	15
☐ <i>Real Time – Interceptions of Voice Communications</i>	15
☐ <i>Real Time – Interceptions of Electronic Communications</i>	16
STORED ELECTRONIC OR WIRE COMMUNICATIONS IRM 9.4.6.7.3.2	16
PEN REGISTERS IRM 9.4.6.7.4.1	17
TRAP AND TRACE IRM 9.4.6.7.4.5	18
Nonresponsive [REDACTED]	18
Nonresponsive [REDACTED]	19
Nonresponsive [REDACTED]	19
Nonresponsive [REDACTED]	20
☐ Nonresponsive [REDACTED]	21
☐ Nonresponsive [REDACTED]	22
Nonresponsive [REDACTED]	23
Nonresponsive [REDACTED]	23
Nonresponsive [REDACTED]	24
Nonresponsive [REDACTED]	25
Nonresponsive [REDACTED]	25

Nonresponsive

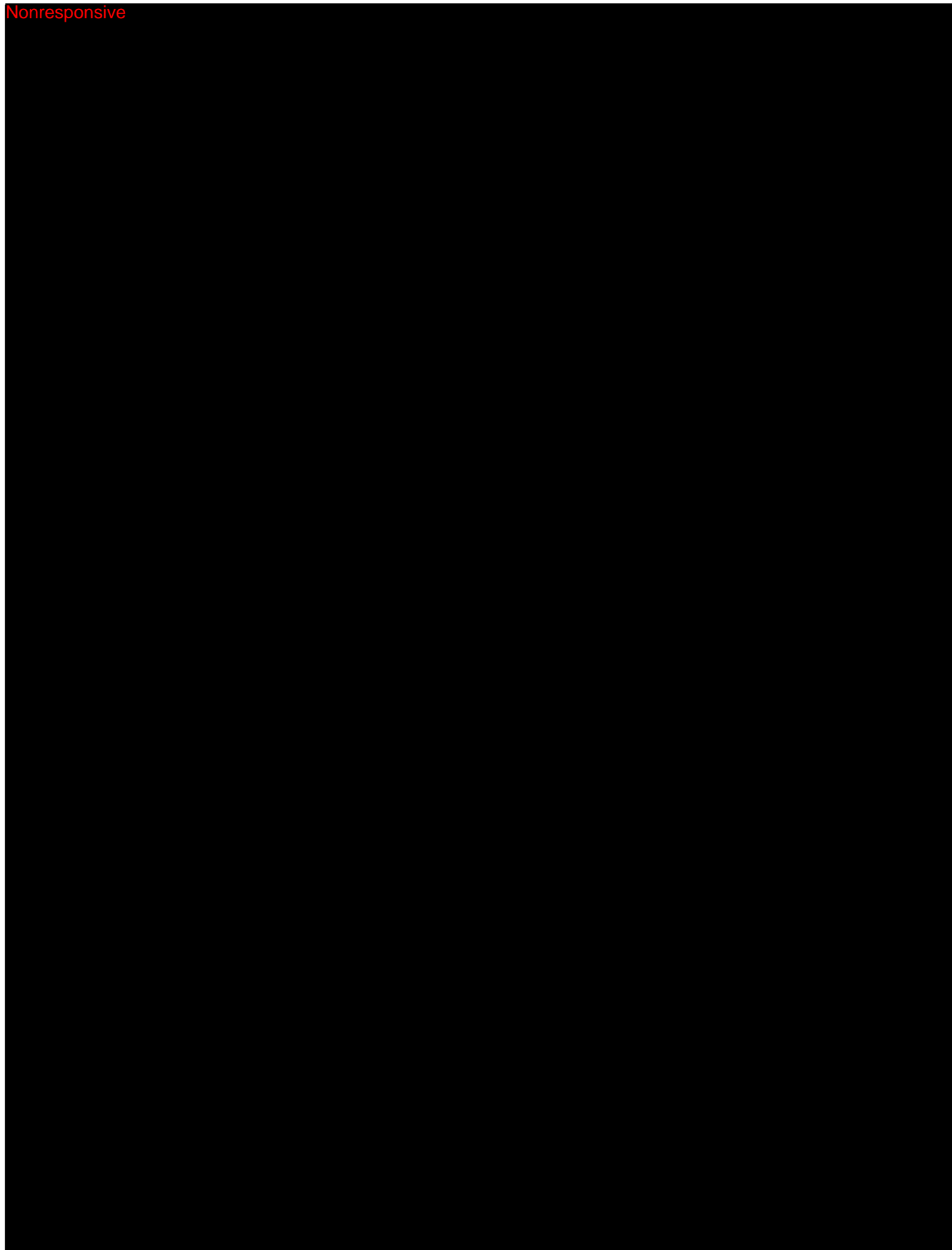
Nonresponsive

Nonresponsive



Nonresponsive

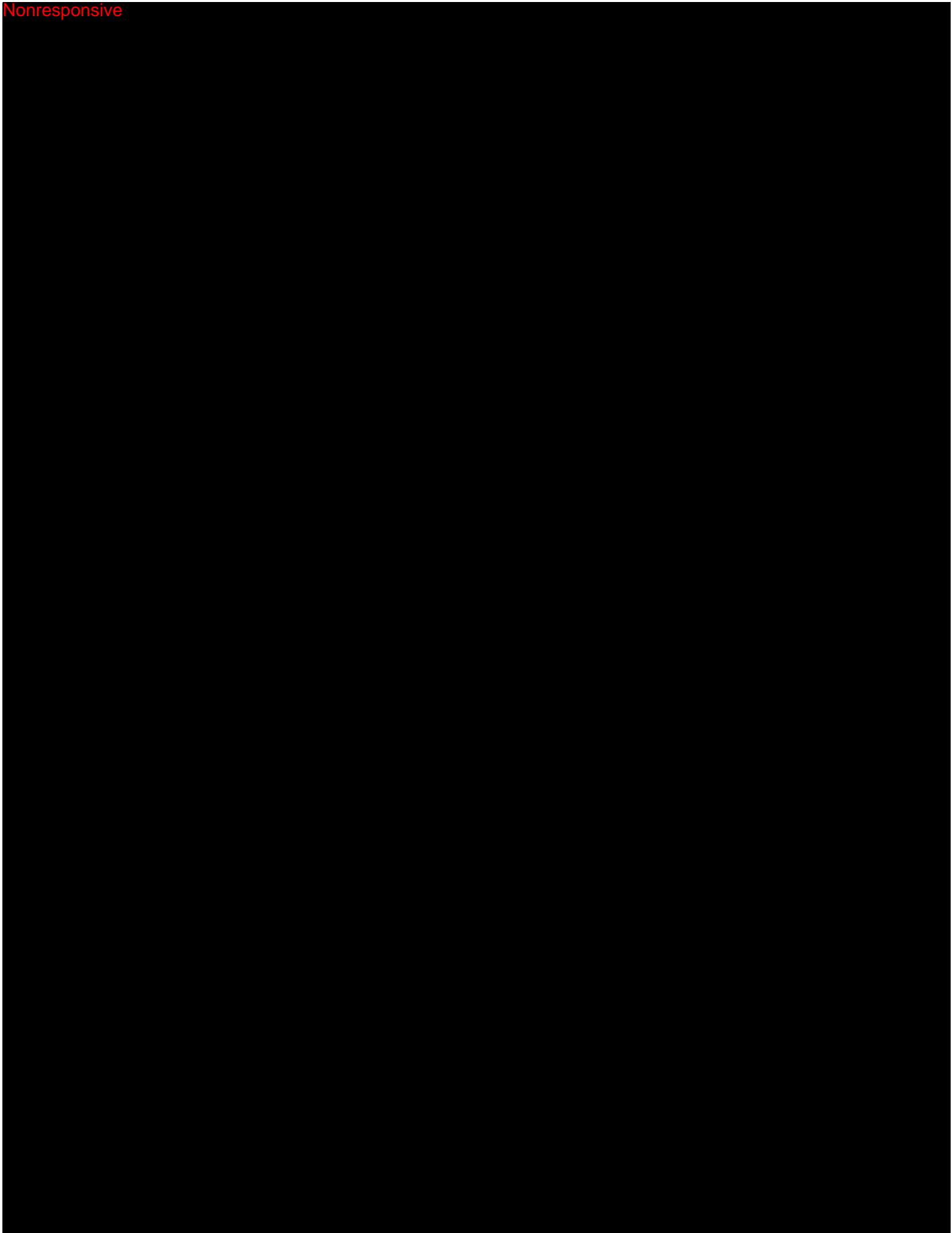
Nonresponsive



Nonresponsive



Nonresponsive



Nonresponsive



NON-CONSENSUAL MONITORING AND ELECTRONIC SURVEILLANCE


📖 Non-consensual monitoring is distinguished from consensual in that none of the parties being monitored has given his or her consent. Electronic Surveillance in the simplest of terms is the observance of an activity or individuals via an electronic, mechanical, or other device. When the two are married, various aspects of the wiretap statute (discussed in *IRM 9.4.6.7.1*) emerge, which are incorporated throughout this section in the definitions and processes outlined surrounding the following special investigative techniques:

- 1) Real Time – Interceptions of Oral, Wire, or Electronic Communications
- 2) Stored Wire and Electronic Communications
- 3) Pen Registers and Trap and Trace Devices

- 4) Nonresponsive
- 5) Nonresponsive



There are, however, restrictions on the use of these techniques. Most importantly, non-consensual interception of oral and wire communications (Wiretap, Title III) are restricted to Title 18 USC § 1956 and 1957 (money laundering) and 31 USC § 5322 (criminal penalties related to currency reporting offenses). In addition, IRS further limits its use to extremely limited situations and only in significant money laundering investigations. Non-consensual monitoring of electronic communications, electronic tracking devices, pen registers and trap and trace devices, however are not limited, therefore can be used to investigate any federal felony, including T26. Additional restrictions on the use of these techniques can be found in IRM 9.4.6.7.1.1.


Real Time – Interceptions of Communications (Wiretap)

 A real time interception or wiretap is the acquisition of the contents of any the following through the use of any electronic, mechanical, or other device where a reasonable expectation of privacy exists.


- 1) Wire - a communications that involves a human voice transmitted by a wire, cable, or similar method. The best example is a telephone call or voice pager.
- 2) Oral - any oral communication such as a conversation between two or more individuals who have a reasonable expectation of privacy.
- 3) Electronic communication - any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic, or photo optical system that affects interstate or foreign commerce that is real-time, point-to-point, transmission of, for example, digital display pager information, electronic mail, computer-to computer transmissions, facsimiles, transmissions, and private video transmissions (but not video surveillance).


Real Time – Interceptions of Voice Communications

- 1) Call your UPM before beginning any request surrounding this technique. Your UPM along with a SIT Analyst will assist you with this request.
- 2) Three situations exist where approval is required for IRS CI special agents' participation in investigations where the real time interception of voice communications occurs:
 - a) CI special agents are present in the wire room to review previously recorded real-time interceptions, issue surveillance assignments, other duties as assigned.
 - i)  SAC approval via memo required which includes: the significance of the investigation, need for CI resources, and any CI equipment being used (IRM 9.4.6.7.2.5.1).
 - b) CI special agent(s) are present in the wire room to monitor real-time interceptions, but are not the Affiant Agency.
 - i)  Chief, CI's concurrence and approval by Deputy Commissioner, IRS required via memo (See IRM 9.4.6.7.2.5.2 for details).
 - c) CI special agent(s) are present in the wire room to monitor real-time interceptions and are the Affiant Agency.


- i)  Chief, CI's concurrence and approval by Deputy Commissioner, IRS required via memo (See IRM 9.4.6.7.2.5.3 for details).

Real Time – Interceptions of Electronic Communications

 Remember, the interception of electronic communications is a valuable tool that CI special agents can use in the investigation surrounding any felony under CI's jurisdiction, including T26.

- 1) Call your UPM before beginning any request surrounding this technique.
- 2) Coordinate with SIT and Electronic Crimes to obtain proper approvals. Your UPM along with a SIT Analyst will assist you with this coordination and request.
- 3) If the technique can be used, the special agent will be required to prepare an affidavit and a memo per IRM 9.4.6.7.2.7.1
- 4)  This technique requires concurrence from the SAC, DFO, Electronic Crimes, SIT, and approval from the Director, Operations Policy and Support.

Stored Electronic or Wire Communications IRM 9.4.6.7.3.2

 Stored electronic communications includes those electronic messages temporarily stored by an electronic communication service provider prior to delivery to the intended recipient or stored as a backup. For example, display data stored in digital-display pagers and cell phones, stored electronic mail, stored computer-to-computer transmissions, stored telex transmissions, stored facsimile data and private video transmissions.

Service providers are prohibited from disclosing electronic communications to the government unless:

- 1) The subscriber/customer gives consent,
- 2) It is pursuant to a court order, search warrant, or subpoena, or
- 3) The information was obtained inadvertently and it refers to a crime.

The classes of information that can be obtained are:

- 1) The contents of electronic communication in electronic storage with an electronic communication service (such as unopened email) or with a remote computing service (such as records in off-site archives).
- 2) Transactional information, which includes all other records or information pertaining to a subscriber or customer that are not included in 1 and 2.
- 3) Basic subscriber information, including name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity (such as temporary assigned Internet Protocol (IP) addresses), length of service, and types of service the customer or subscriber utilized.

The information is obtained in the following manner:

- 1) Wire or electronic communication that has been in storage for 180 days or less must be obtained by search warrant.



- 2) Wire or electronic communication that has been in storage for more than 180 days may be obtained by:
 - a) Search Warrant,
 - b) Court order issued under 18 USC § 2703(d),
 - c) Grand Jury subpoena, or
 - d) Administrative Summons.
- 3) Transactional information and basic subscriber information may be obtained by:
 - a) Search Warrant,
 - b) Court order issued under 18 USC § 2703(d),
 - c) Consent from the customer or subscriber of the service,
 - d) Submission of a formal written request relevant to a law enforcement investigation concerning telemarketing fraud.
- 4) Basic subscriber information may be obtained by any of the means describe in (3) above or with a grand jury subpoena or administrative summons, without providing notice to the subscriber.

☛ Many electronic communication services keep store data for very short periods of time (two to three days in some cases). Special agents can issue a letter (called a preservation or 2703(f) letter) that is signed by either the special agent or AUSA. This letter requires providers of wire or electronic communication services to retain records for a period of 90 days, which can be extended for an additional 90 days with a renewed request. A Sample of a preservation letter can be found in the IRM Exhibit 9.4.6-2 or in the SIT Community in CASE under "Go-bys" titled "Letter: Title 18 Sec 2703(f) E-Communications Preservation".

Stored Electronic and Wire Communications IRM 9.4.6.7.3.4

- 1) Call your UPM before beginning any request surrounding this technique.
- 2) Coordinate with SIT and Electronic Crimes to obtain proper approvals. Your UPM along with a SIT Analyst will assist you with this coordination and request.
- 3) If the technique can be used, the special agent will be required to prepare Form 1101 (Request for Stored Electronic Communication/Transactional Information/Subscriber Information), prepare the appropriate legal request as discussed above, and secure the required concurrence and approval.
- 4) A copy of Form 1101 is forwarded to SIT for filing.

Pen Registers IRM 9.4.6.7.4.1

 A pen register (also called a "Dialed Number Recorder" (DNR)), is a mechanical instrument attached to a telephone line, usually at a central telephone office. A pen register may be used in both tax and non-tax investigations and to locate fugitives from justice who are the subject of a CI investigation regarding a felony violation.  SAC approval is required for this technique. Specifically, a pen register:

- 1) Records the outgoing numbers dialed on a particular telephone,
- 2) Registers incoming calls

- 3) Does not identify the telephone number from which the incoming call originated unless caller identification (ID) service is present, the service is on, and no one has blocked the caller ID service

🔗 Pen Register IRM 9.4.6.7.4.2

- 1) Seek the endorsement of the US Attorney to apply for a court order.
- 2) Prepare Form 9170 (Request for Pen Register and/or Trap and Trace Devices) and forward to SSA.
- 3) SSA will forward to ASAC/SAC for approval who will forward a copy to SIT for filing.
- 4) Upon approval, contact US Attorney for issuance of court order based on application by AUSA (See IRM Exhibit 9.4.6-3 Application for Pen Register and Exhibit 9.4.6-4, Court Order for Pen Register).
- 5) After approval by the magistrate or judge, make arrangement with a trained tech agent who will acquire and install the pen register(s) and accessory equipment.

🕒 Pen register devices are authorized to be used for a period not to exceed 60 days. Extensions for a period not exceeding 60 days are available upon application for another court order.

Trap and Trace IRM 9.4.6.7.4.5

📖 A trap and trace device (also called a "grabber") records the telephone numbers from incoming calls to a particular telephone. Like a pen register, no conversations are recorded. Call forwarding is part of the trap and trace procedure. It requires a telephone company to identify which facility or number telephone calls are being forwarded. ✍️ Trap and trace service requires SAC approval.

🕒 Whenever possible, before obtaining an order to trace incoming calls to a particular line, review the proposed trace with the local telephone company's security officer. The security officer should be able to advise of foreseeable problems in the execution of the proposed order.

🔗 Trap and Trace IRM 9.4.6.7.4.5(12)

- 1) Follow same procedures for pen registers.

Nonresponsive



Nonresponsive

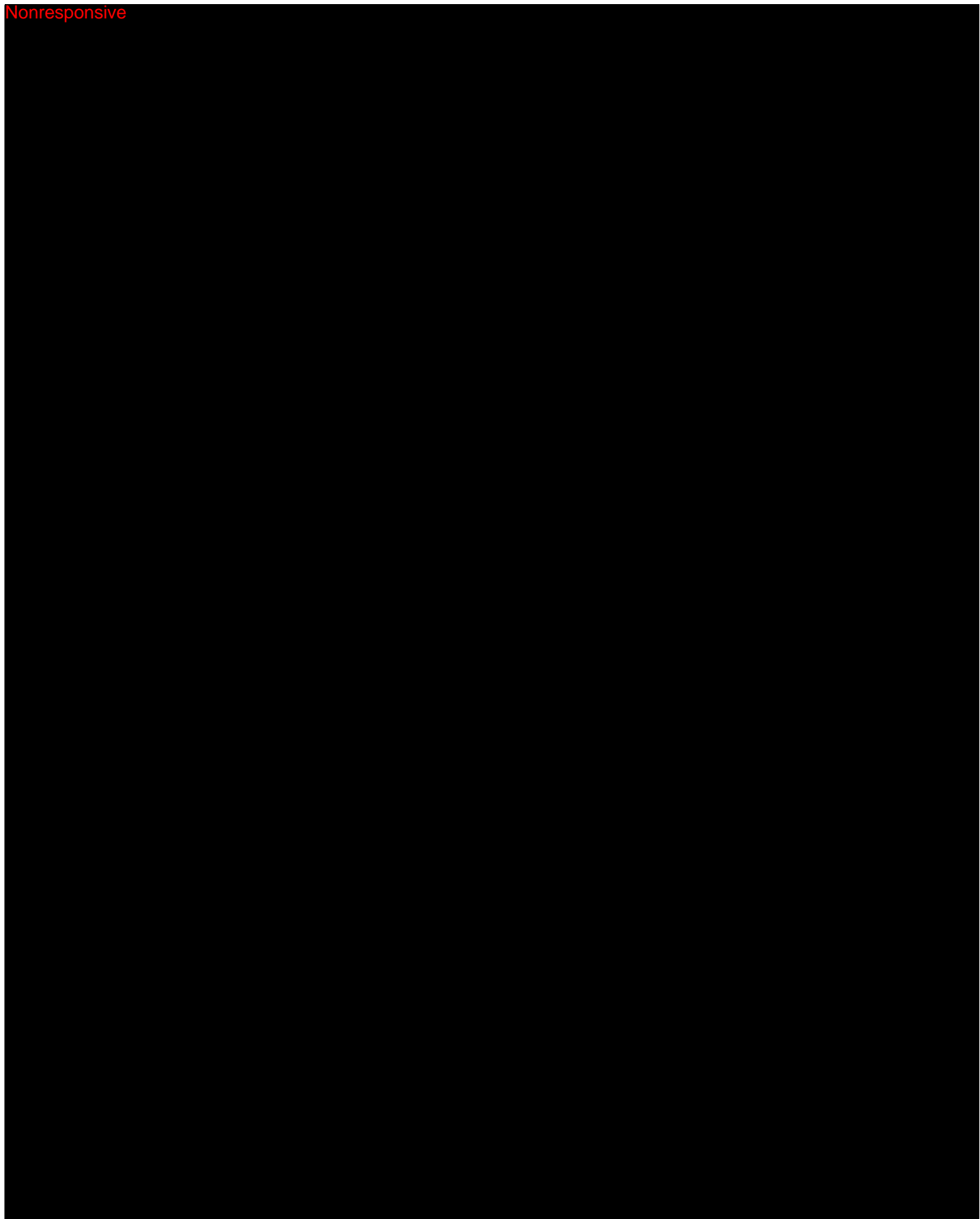


Nonresponsive

Nonresponsive



Nonresponsive



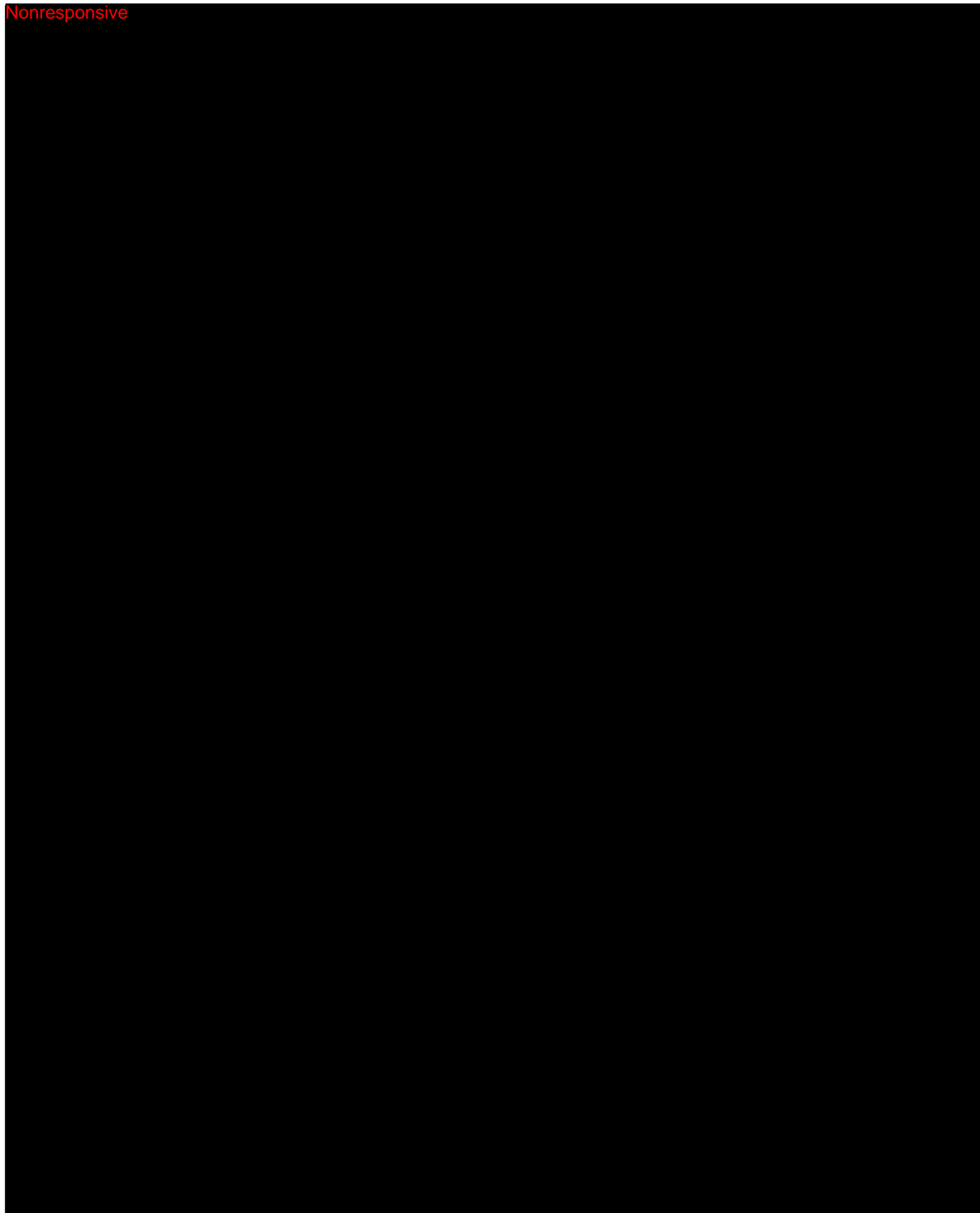
Nonresponsive



Nonresponsive



Nonresponsive



Nonresponsive

