Scientific Working Group on Digital Evidence

Best Practices for Historical Cell Site Analysis

SWGDE 17-F-001-5.0

Disclaimer Regarding Use of SWGDE Documents

SWGDE documents are developed by a consensus process that involves the best efforts of relevant subject matter experts, organizations, and input from other stakeholders to publish standards, requirements, best practices, guidelines, technical notes, positions, and considerations in the discipline of digital and multimedia forensics and related fields. No warranty or other representation as to SWGDE work product is made or intended.

SWGDE requests notification by email before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in such proceeding. The notification should include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; and 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in the proceeding please notify SWGDE as to the outcome of the matter. Notifications should be submitted via the SWGDE Notice of Use/Redistribution Form or sent to secretary@swgde.org.

From time to time, SWGDE documents may be revised, updated, deprecated, or sunsetted. Readers are advised to verify on the SWGDE website (https://www.swgde.org) they are utilizing the current version of this document. Prior versions of SWGDE documents are archived and available on the SWGDE website.

Redistribution Policy

SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain this SWGDE cover page containing the Disclaimer Regarding Use.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or creation date) of the document and also indicate if the document is in a draft status.

Requests for Modification

SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be submitted via the SWGDE Request for Modification Form or forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of any suggested modification:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address

d) Telephone number and email address
e) SWGDE Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for suggested modification

Intellectual Property

All images, tables, and figures in SWGDE documents are developed and owned by SWGDE, unless otherwise credited.

Unauthorized use of the SWGDE logo or document content, including images, tables, and figures, without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

Scientific Working Group on Digital Evidence

Best Practices for Historical Cell Site Analysis

Table of Contents

1. Purpose 3
2. Scope 3
3. Definitions 3
4. Considerations 6
5. Future Considerations 7
6. Call Detail Records Data Preservation, Procurement, Documentation, and Archiving 7
   - 6.1 Introduction 7
     - 6.1.1 Preservation Requests 7
     - 6.1.2 Customer Consent 8
     - 6.1.3 Lawful Emergencies and Exigent Requests 8
     - 6.1.4 Subpoenas, Search Warrants, and Court Orders 8
   - 6.2 Service of Legal Demands 8
   - 6.3 Obtaining Cell Site Lists, Reference Sheets, and Court Admission Issues 8
   - 6.4 Documentation 9
7. Data Interpretation 9
   - 7.1 Record Formats From Different Cellular Providers 9
     - 7.1.1 Evidence Hashing 9
   - 7.2 Cellular Service Provider versus Mobile Virtual Network Operators 9
   - 7.3 Differences in Time Zone Reporting 10
   - 7.4 Pen Registers/Traps and Traces 10
8. Processing the Data for Casework or Lead Purposes—Preliminary Reporting 11
9. Processing the Data for Court and Legal Proceedings—Final Reporting 11
10. Interpreting the Data 11
    - 10.1 Omni-Directional Cell Site vs. Sectorized Cell Site 11
    - 10.2 Sectors 12
    - 10.3 Azimuth and Orientation 13
    - 10.4 Horizontal Beamwidth 13
    - 10.5 Timing Advance (TA) 14

10.6 Proprietary Location Estimates 15
10.7 Ping 16
10.8 Data Sessions 16
11. Verification 17
12. Presenting the Data in Legal Proceedings 17
13. References 17
14. Additional Resources 17
15. History 18

1. Purpose

The purpose of this document is to provide recommendations on the use of Cell Site Location Information contained in Call Detail Records (CDR) when conducting Cell Site Analysis.

2. Scope

This document provides information and recommended guidelines for using Cell Site Location Information contained within CDRs to conduct Cell Site Analysis. The intended audience for this document is practitioners who have training, knowledge, and experience in using these investigative techniques, which may include investigators, analysts, and attorneys. This document is not intended to be a training manual or to replace standard organizational procedures. This document is not all-inclusive and does not account for every possible scenario related to Cell Site Analysis, and it should not be confused with mobile device forensics. Cell Site Location Information may be obtained through other means, including law enforcement surveillance activities such as pen register/trap and trace of devices with cell site information, mobile device forensics, and location data that may exist in cloud-based or remote locations. While obtaining the location information through other means can be invaluable, the focus of this document is limited to Cell Site Location Information contained within the CDRs, as maintained by the cellular service providers relative to Cell Site Analysis.

3. Definitions

The following definitions are provided to assist with interpreting this document. For further details, readers may refer to more technical resources defining these terms, such as Third Generation Partnership Project and European Telecommunications Standards Institute (see Additional Resources).

- 4G LTE: A standard for wireless communication of high-speed data for mobile devices; LTE is an abbreviation for Long Term Evolution.
- 5G NR: A cellular network technology, offering higher transmission speeds than 4G with lower latency; NR is an abbreviation for New Radio
- Addressing and Routing Data: Data that represents the transactional data of an electronic communications event. This data includes such items of data as the phone numbers dialed, durations of phone calls, phone numbers involved in text messages, Internet Protocol (IP) addresses involved in data transactions, etc. This data does not include the contents of any electronic communications.
- Antenna: An electrical device which converts electric power into radio waves, and vice versa. It is usually connected with a radio transmitter or radio receiver and can be mounted on various structures including poles, masts, towers, etc.
- Automated Cell Site Analysis Mapping Program: Software that automates the analysis and plotting of locations contained within the CDRs.

- Azimuth: A bearing, expressed in degrees (clockwise) from true north, which represents the orientation of a directional cellular antenna.
- Beamwidth: The angle between the two points on either side of the azimuth where the antenna's power drops to half its peak (-3 dB).
- Call Detail Record (CDR): Usage records (e.g. voice, text, data) maintained by the service provider capturing information typically needed to accurately bill a subscriber or, in the case of a prepaid service plan, debit the balance. This information typically includes the date, time, duration, source identifier, destination identifier, or the amount of data transmitted or received.
- Cell Site: A physical location that contains the equipment needed to receive and transmit radio signals for cellular voice and data transmission and may consist of equipment from one or more cellular telephone companies. Cell sites are designed to provide radio frequency to defined geographic areas.
- Cell Site Analysis: The analysis of historical records provided by the cellular companies, or other geographic data, in order to place a particular cellular device within an approximate geographic area during a specified date and time.
- Cell Site List: Also called a tower list, mast list, or cell site key, is a list of all cellular system antennas with sector information that is retained by a cell provider. Cell site lists typically contain the latitude and longitude of cell sites as well as specific sector information including the azimuths and beamwidths of sectors.
- Cell Site Location Information (CSLI): The historical data contained in records from cellular service providers, including Call Detail Records and Timing Advance Records.
- Cellular Service Provider: A wireless communications service provider that owns or controls all the elements necessary to sell and deliver services to an end user including radio spectrum allocation, wireless network infrastructure (antennas and switches), backhaul infrastructure, provisioning computer systems, and repair organizations. Examples of cellular network providers are AT&T, T-Mobile, and Verizon Wireless. This can also be known as cellular network operator, Mobile Network Operator (MNO), and wireless carrier.
- Code Division Multiple Access (CDMA): A spread spectrum technology for cellular networks based on the Interim Standard-95 (IS-95) from the Telecommunications Industry Association (TIA). Is a form of multiplexing a radio signal that allows multiple signals to occupy a single transmission channel.
- Distributed Antenna System (DAS): A network of relatively small antennas linked to a centralized base station within a geographic area or structure.
- Drive Scan Test: See Radio Frequency Propagation Survey.
- Global Positioning System (GPS): See GNSS.

- Global Navigation Satellite System (GNSS): A network of satellites to determine a location. Different systems are in operation around the world. Commonly referred to as GPS.
- Global System for Mobile Communications (GSM): A set of standards for second generation (2G) cellular networks currently maintained by the Third Generation Partnership Project (3GPP).
- Internet Protocol (IP): The principal communications protocol used to move data across the Internet, and most Intranets, via packets of data.
- Latitude and Longitude: A coordinate system, typically referenced to the WGS84 datum, enabling every location on the Earth to be specified by a set of numbers.
- Mobile Network Operator (MNO): see Cellular Service Provider.
- Mobile Virtual Network Operator (MVNO): A wireless communications services provider that does not own the wireless network infrastructure over which the MVNO provides services to its customers. An MVNO enters into a business agreement with a cellular network operator (MNO) to obtain bulk access to network services at wholesale rates, then sets retail prices independently.
- Neighboring Cell Sites: Cell sites that are in close proximity to the target cell site. Neighboring Cell Sites can affect the outer boundaries of a target cell site's serving coverage area.
- Omni-Directional Cell Site (AKA Omnipole): A cell site that contains only one sector with 360° of coverage.
- Pen Register / Trap and Trace (PRTT): A law enforcement surveillance technique that monitors and records, in real time or near real time, the outgoing and incoming identifiers (i.e., dialed phone numbers) of a target's phone calls, text messages, data transactions, or other electronic communications. Pursuant to appropriate legal authority, pen registers can also provide the cell site and sector and location data related to the device for these communication events.
- Ping: A real-time device location estimation method.
- Proprietary Location Estimate: Additional data that might be disclosed by a provider which may contain estimated mobile device location data derived from proprietary algorithms. This is distinct from Timing Advance Data.
- Radio Frequency (RF): Any of the electromagnetic wave frequencies that lie in the range extending from around 3 kHz to 300 GHz, which include those frequencies used for communications or radar signals.
- Radio Frequency Propagation Survey (RFPS): The process of measuring and illustrating the full cellular radio spectrum occupied by 2G through 5G cellular and Wi-Fi technologies in a given area. This method is used by all cellular providers for the

purpose of network optimization and can also be used by law enforcement to memorialize and forensically examine the characteristics of a cellular network in a given area.

- Radio Frequency Propagation Map: A geographical representation of RF coverage, not necessarily including signal strengths, which displays the approximate boundaries of a cell on the date and time that the survey was performed.
- Sector: The section of a cell site that covers a specific geographic area.
- Sector Angle: The planned coverage area of a sector (e.g.120°).
- Survey: See Radio Frequency Propagation Survey.
- Timing Advance (TA): The TA process is used within 2G GSM/4G LTE/5G NR cellular networks to synchronize the attached devices in the uplink direction towards the cell site. The cell site calculates the latency in the uplink direction between a device and the cell site. Timing Advance is the measure of delay (time), not distance, but it can be used to infer an approximate distance for geolocation purposes.
- Timing Advance (TA) Step: The units employed to measure delay in timing advance (e.g. 0.52**µ**s in LTE), which can be used to infer units of distance (e.g. approximately 78m in LTE).
- Technical Review: A qualified second party's evaluation of reports, notes, data and other documentation to ensure there is appropriate and sufficient support for the actions, results, conclusions, opinions, and interpretations. This may also be referred to as a Technical Review.
- Tower: See Cell Site.
- Trap and Trace (related Pen Register): See Pen Register / Trap and Trace (PRTT).

4. Considerations

There are limitations associated with Cell Site Analysis that should be understood.

Cell Site Analysis only demonstrates the specific cell site and sector (if applicable) used by a particular mobile device at a specific date and time. CDRs do not conclusively indicate who was using a device but can be used to establish patterns of use.

Furthermore, cell site and sector information in CDRs cannot be used to pinpoint the exact location of a device at a specific date and time (e.g., a specific intersection or address).

When available, timing advance records can assist in determining the geographic area of the device. Refer to Section 10.5.

An advanced method of Cell Site Analysis that is not detailed in this document includes the utilization of RF survey equipment to establish detailed cellular signal propagation estimates. These represent a sample of cellular coverage as it existed at the time the survey was undertaken and may or may not reflect the RF conditions that existed at the time of an event.

These more detailed RF estimates may be displayed on RF propagation maps. RF analysis requires specific experience, knowledge, training, and equipment and is not covered in this document. It should be noted these estimations are theoretical in nature and differ from a radio frequency propagation survey.

Cell Site Location Information (CSLI) may be obtained through other means, including law enforcement surveillance activities such as a ping, pen register and trap and trace of devices with cell site information, mobile device forensics, and location data which may exist in cloud-based or remote locations.

5. Future Considerations

This document was prepared with the resources available at the time of publication. As with all technology, Cell Site Analysis is a constantly evolving discipline, with frequent implementation of new features and innovations. As time progresses, the data available from cellular providers will change, as will the formats in which the available data is provided.

6. Call Detail Records Data Preservation, Procurement, Documentation, and Archiving

6.1 Introduction

Cellular service providers maintain records through the normal course of business or as required by law, which contain certain historical information, which may include CSLI. This information can be obtained through appropriate legal process. Additionally, data may also be available from other sources, including data from non-cellular providers which are considered official business records, from the forensic extraction of mobile devices, from law enforcement surveillance activities (e.g., pen registers), and potentially even from cloud-based or remote locations.

It is beyond the scope of this document to discuss, in detail, the various legal avenues a practitioner might pursue to preserve or obtain CSLI. Those seeking CSLI should consult with legal counsel for specific guidance in a particular investigation within their jurisdiction. Practitioners are encouraged to become familiar with the particulars of each of these possible legal channels. Federal, state, and local laws might also provide guidance. Practitioners should always be mindful to comply with their own organization's policies and procedures. In order to preserve or obtain CSLI, practitioners may make use of one or more of the following legal instruments, which may be applicable in certain jurisdictions.

6.1.1 Preservation Requests

Title 18 U.S. Code § 2703(f) [1] provides law enforcement officials with the ability to order the preservation of records and other evidence held by an electronic communications provider. Preservation requests allow law enforcement to order providers to preserve data. In doing so, data that may otherwise be perishable (e.g., deleted by the provider) is preserved for a specified period of time prior to obtaining the appropriate legal authority to secure the release of the preserved data.

6.1.2 Customer Consent

Electronic communications service providers may be able to release customer-related data to law enforcement officials with customer consent. Additional information relating to consent can be found in Title 18 U. S. Code § 2702(c)(2) [2].

6.1.3 Lawful Emergencies and Exigent Requests

Federal and some state laws allow for the immediate and voluntary release of records by providers in certain specific emergency situations. Consult Title 18 U.S. Code § 2702(b)(8) [2]. Providers may require submission of their "Exigent" form prior to providing records. Also, your jurisdiction may require you to follow your Exigent request with legal process.

6.1.4 Subpoenas, Search Warrants, and Court Orders

The most common method of obtaining CSLI through a criminal investigation is with a search warrant or, where permitted, other appropriate court orders.

In civil matters, civil court rules allow for the use of a subpoena or court order.

Legal issues change rapidly and are subject to interpretation, therefore always consult with your appropriate local legal counsel or prosecutor regarding all legal matters before acting.

6.2 Service of Legal Demands

In order to obtain CSLI data from cellular service providers, personnel requesting the data will typically need to serve legal demands to electronic communications providers. While service in person may be possible, legal demands are typically served electronically (e.g., email, website service) or via fax. It is important that both original and copies of legal demands be preserved and that the service of legal process be appropriately documented.

6.3 Obtaining Cell Site Lists, Reference Sheets, and Court Admission Issues

In addition to the specific CSLI, it is also important to obtain any applicable cell site lists from the time in question. This information will aid in indicating where cell site antennas are located and how they are configured in the associated geographic areas. In addition to the specific latitude and longitude references to the antenna used by a target device in a CDR, it may be useful to have the neighboring cell sites. This aids in conducting Cell Site Analysis more thoroughly. It is also important to compare the latitude and longitude coordinates listed in the CDRs to ensure they are consistent with the cell site list.

Other useful data includes any available reference sheets, instruction sheets, or legends that may be available to assist in properly interpreting the provided data. For example, time zones may be reported in various ways, and the appropriate time zone must be determined for the location of the device. It is also important to obtain a cell site list for the appropriate time period (e.g., not using a 2022 list when analyzing 2025 records).

Finally, if use of the records in court is anticipated, it is important to prepare to meet any applicable rules of evidence requirements. To ensure the admissibility of these business records in court, it is typically sufficient to obtain a business records affidavit for the CSLI, subscriber

information, any Proprietary Location Estimates, cell site list(s), and any applicable instruction pages or legend documentation. Practitioners should exercise caution, as records may have been purged from the provider's systems by the time these affidavits are requested.

6.4 Documentation

Practitioners should document the process and procedures used to conduct Cell Site Analysis. It is important to document where, how, when, and by whom the data was obtained. Additionally, documentation should include specifically what data was obtained and how the data was archived. Finally, those conducting Cell Site Analysis should also maintain current documentation, such as a detailed curriculum vitae (CV) that thoroughly details their qualifications to conduct Cell Site Analysis. The CV should include details of formal education, training, case experience, and relevant experience in the field of Cell Site Analysis.

7. Data Interpretation

CSLI used in Cell Site Analysis is typically obtained from historical CDRs sourced from the cell service providers. CSLI may also be obtained in real-time from legally authorized surveillance, namely, pen registers and trap and trace of devices. It may also be possible to obtain reliable location data from cellular devices utilizing mobile device forensics. Refer to *SWGDE 18-F-003-2.0 Best Practices for Mobile Devices Evidence Collection & Preservation Handling and Acquisition* for details of mobile device forensics best practices. Those conducting Cell Site Analysis should be familiar with the type of records produced by the various service providers and the intricacies, nuances, and limitations associated with each provider.

7.1 Record Formats From Different Cellular Providers

Cellular service providers produce records in various formats. While the CDRs from various cellular providers may look very different, they generally contain the same basic information, including the date and time of the event, the originating and terminating phone number, duration, and cell site and sector information. It is important to properly interpret this information and recognize the differences in key terms from the various cellular providers. A CDR reference document, also known as a "carrier key," should be requested from each cellular service provider when legal process is served.

7.1.1 Evidence Hashing

Many cellular service providers do not provide hash values for the respective files the company produces, and many times the files come in an uncompressed format. If hash values are provided by the company producing the records, the hash value should be retained for later discovery. Original electronic copies of records obtained through legal process should be retained as digital evidence and working copies of cellular records should be utilized during the analysis.

7.2 Cellular Service Provider versus Mobile Virtual Network Operators

A cellular service provider or Mobile Network Operator (MNO) is a wireless communications service provider that owns or controls all the elements necessary to sell and deliver services to an end user, including radio spectrum allocation, wireless network infrastructure (antennas and

switches), backhaul infrastructure, provisioning computer systems, and repair services. Examples of cellular service providers include but are not limited to AT&T, T-Mobile, and Verizon Wireless.

A MVNO is a wireless communications service provider that does not own the wireless network infrastructure over which the MVNO provides services to its customers. An MVNO enters into a business agreement with a cellular network service provider to obtain bulk access to network services at wholesale rates. The MVNO then resells network access to customers and sets retail prices independently. Examples of a MVNO are Straight Talk and TracFone.

It is important to note that in order to obtain usage records, data, or surveillance access on an MVNO cell phone, contact may also need to be made with the cellular network (MNO) providing service to the device, in addition to the MVNO.

7.3 Differences in Time Zone Reporting

Cellular service providers report CDRs in various time zones. For example, times could be reported in the time zone where the device is located, where the switch is located, a centralized location for the provider, or, commonly in Coordinated Universal Time (UTC).

Caution must be taken when analyzing CDRs in preparation for converting listed times to local times, if required. Additional caution should be exercised regarding Daylight Savings Time (DST), when applicable, as not all jurisdictions observe DST. In some circumstances, a switch may encompass multiple time zones, which could impact time adjustments for accurate analysis. A single CDR could also contain a mix of time zones based on different regions of the United States, as well as changes to or from DST.

7.4 Pen Registers/Traps and Traces

Pen registers/traps and traces are real-time, or near real-time, surveillance actions conducted by law enforcement. Pen registers and traps and traces provide real-time cell site and sector information for the target device, along with dialing, routing, addressing, and signaling data such as date, time, and sender and receiver identifiers. This data does not include the content of any communications.

As a result, Cell Site Analysis may be conducted with pen register or trap and trace data in addition to historical CDRs. However, practitioners should be aware that additional data may be available in CDRs than is available in pen register and trap and trace data.

Cell site records obtained during a pen register will likely contain more information in real time and therefore the volume of data may not be equal if historical records are also obtained for that time frame. This is due to historical and pen register information being obtained using two different methods. While still an accurate record of the phone's interaction, if one utilizes pen registers versus historical records, they should be aware of the differences which may be present in the volume and types of records.

8. Processing the Data for Casework or Lead Purposes—Preliminary Reporting

Practitioners frequently conduct preliminary analysis and mapping of CDR data to aid investigative efforts. Those conducting Cell Site Analysis for these purposes should exercise caution when placing too much confidence in Cell Site Analysis findings without additional verification. Practitioners will often conduct Cell Site Analysis under short time constraints. In doing so, various methods may be used to report preliminary results such as verbal reporting, quick hand-drawn maps, automated cell site analysis mapping program, etc. For example, images may be captured via screen capture utilities, sent in emails, or attached to other documents. While effective, those conducting Cell Site Analysis should always strive to accurately report the data and reduce confusion related to findings, especially with lay personnel. It is recommended that any preliminary reporting reflect a disclaimer representing that the product is in draft form and has not been fully verified.

9. Processing the Data for Court and Legal Proceedings—Final Reporting

When processing Cell Site Analysis data for court or legal proceedings, additional steps should be taken to ensure that the analysis was properly conducted and verified (including manual validation). Additionally, working with maps must be done with care so that presentations preserve aspect ratios (are not distorted) and include an accurate scale. Practitioners conducting Cell Site Analysis should follow their organization's quality standards, which may include technical review, to ensure the validity of the work product and provide assurance that the analysis of data contained in the CSLI is accurate and repeatable.

10. Interpreting the Data

10.1 Omni-Directional Cell Site vs. Sectorized Cell Site

Omni-directional cell sites transmit their RF signals in all directions from a single antenna. The single antenna provides 360° coverage from the site. Orientation cannot be determined from an omni-directional cell site. A sectorized cell site utilizes directional antennas oriented to provide coverage to a specific geographic area. The most common type of sectorized cell sites utilize three (3) antennas to provide complete 360° coverage around the cell site. See Figure 1 below for an example of Omni-Directional vs. Sectorized Cell Site.

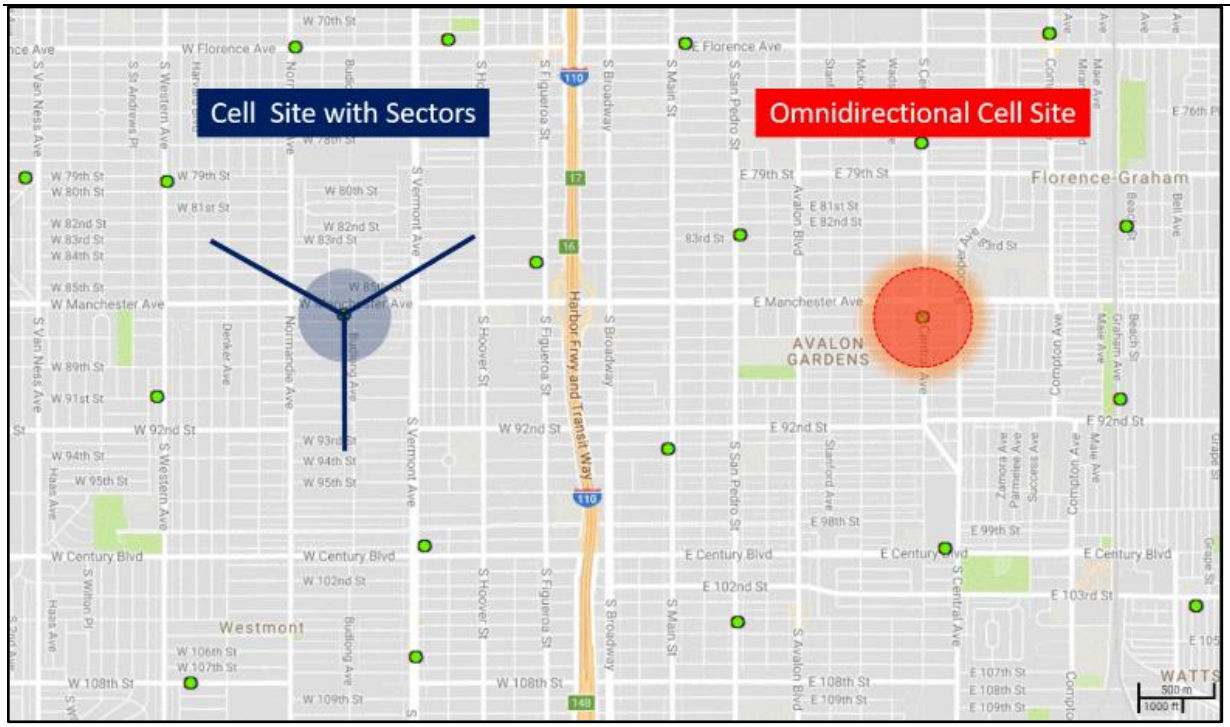

Figure 1. Omni-Directional vs. Sectorized Cell Site Example.
(Image Credit: SWGDE/Google Maps, 2017)

10.2 Sectors

Cell Sectors are utilized by service providers to increase coverage and capacity within a specific geographic area. Sectors are oriented in a specific direction to provide coverage and limit interference received from other sectors. The predominant configuration used by cellular service providers has three (3) separate sectors, each providing approximately 120° of coverage, and therefore collectively providing a 360° coverage around the cell site. The area over which a sector antenna transmits signals is commonly referred to as the Sector Angle (e.g. 120° coverage from one antenna on one sector). There are other configurations, with different numbers of sectors, or different sector angles, that may exist; for more information, consult the relevant cellular service provider's cell site list. Coverage is not always uniform across all sectors and can vary from cell site to cell site. A cell site may support more than one cell (transmitted on different radio frequencies) per sector to increase capacity. The sector angle should not be considered the absolute edge of the sector coverage.

For an example of a sector coverage area, see Figure 2 below. The depicted sector is one of three generated by the cell site and has a sector angle of 120°.

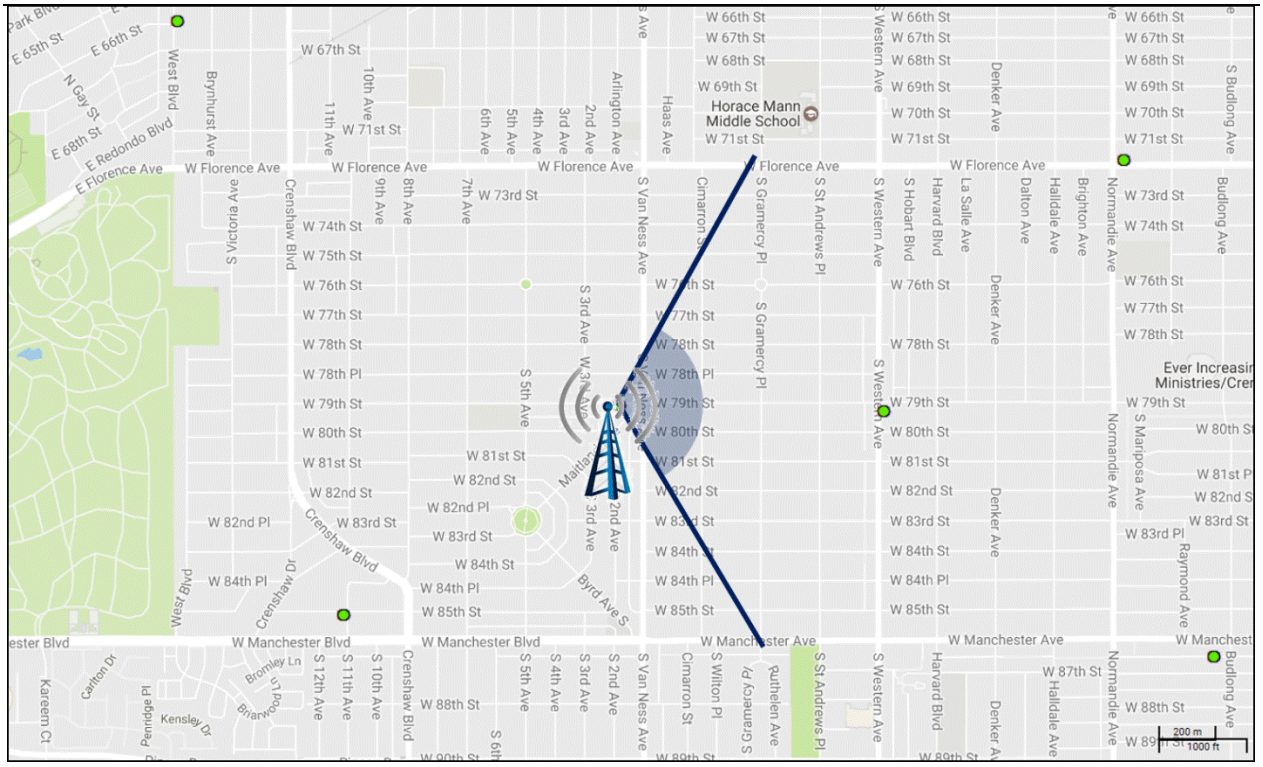

Figure 2. Example of a sector.
(Image Credit: SWGDE/Google Maps, 2017)

10.3 Azimuth and Orientation

The azimuth, also known as the cell orientation, is the direction representing the center of a sector angle and is reported in degrees measured clockwise from north. (Figure 3).

10.4 Horizontal Beamwidth

This is the measurement of transmitted radio signal power across the sector angle, represented in degrees. Peak transmit power is measured along the azimuth line of a sector, and power reduces radially out from the azimuth line to the edges of the sector angle on either side of the azimuth (Figure 3).

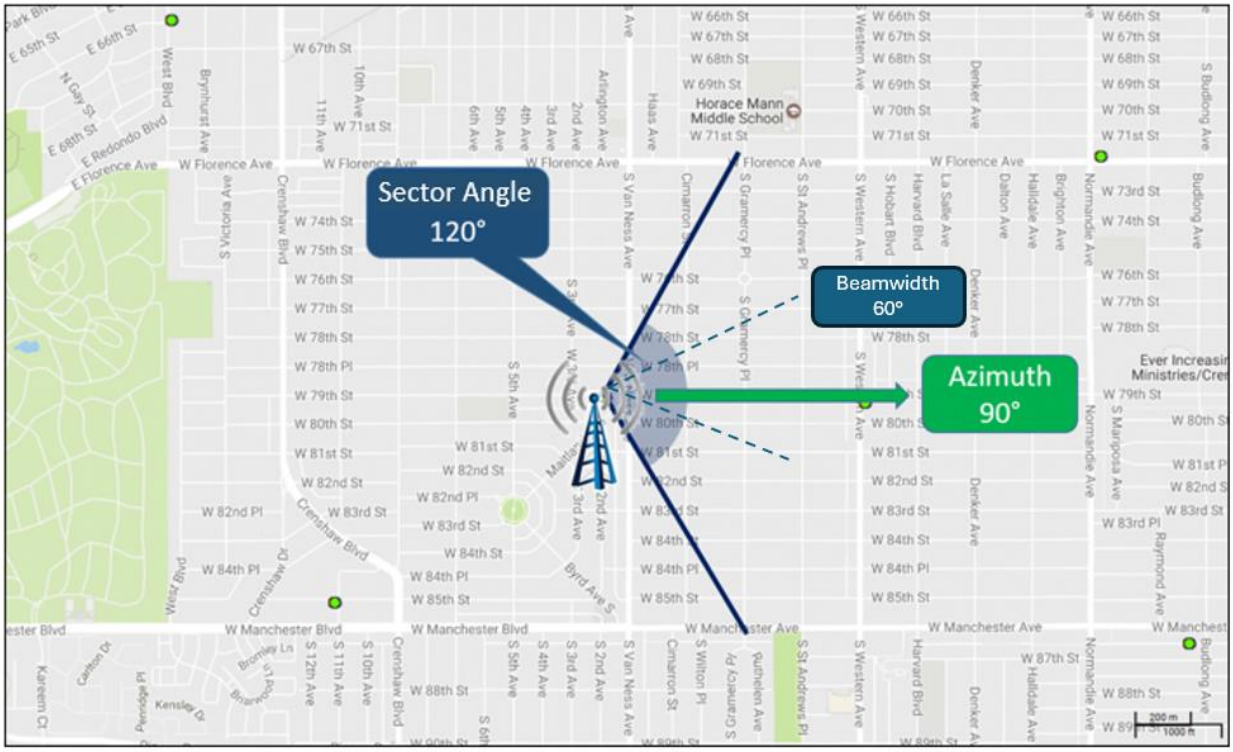

Figure 3. Example of Azimuth and Sector Angle measurements.
(Image Credit: SWGDE/Google Maps, 2017)

10.5 Timing Advance (TA)

Cellular service providers maintain Timing Advance (TA) records during the normal course of business. It is beyond the scope of this document to discuss, in detail, the various legal avenues a practitioner might pursue to preserve or obtain TA records. Timing Advance is the measure of delay (time), not distance, but it can be used to infer an approximate distance for geolocation purposes. The retention for these types of records can be relatively short, and requests to preserve the records should be made as soon as possible.

The TA process is used within 2G GSM/4G LTE/5G NR cellular networks to synchronize the attached devices in the uplink direction towards the cell site. The cell site calculates the latency in the uplink direction between a device and the cell site. The uplink synchronization is maintained through the application of TA. This is achieved through the cell site generating a calculated TA value which enables an attached device to advance or retard the timing of its transmissions towards the cell site in order to ensure synchronized uplink transmissions. This is an ongoing process which is periodically updated as a device moves around a network. The TA value issued by a cell site can be used to infer a device's physical distance from the cell site. The TA value actually represents a TA Step. The inferred distance is in the records from T-Mobile and Verizon. AT&T provides the TA step, which they refer to as a unitless integer. The physical

dimensions of a step depends on cellular technology. The TA Step should be displayed as an arc or ring on a map representing the dimensions of the step based on the specific cellular technology (Figure 4).

A complete explanation of TA is beyond the scope of this document.

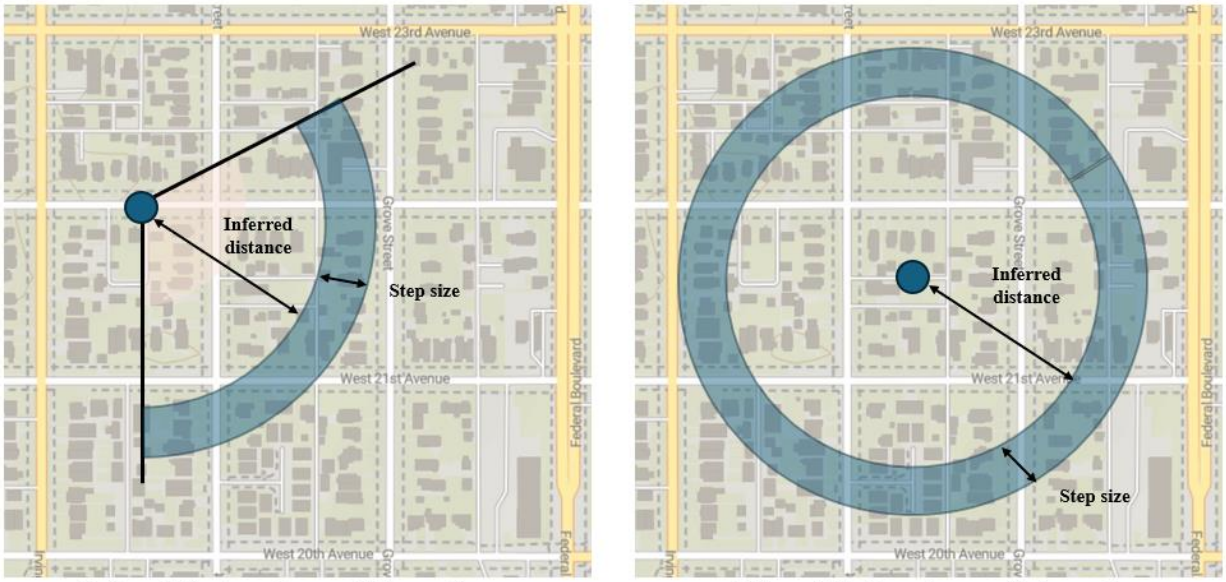

Figure 4. Example of Timing Advance Location Data as shown with cell site, sector, and approximate distance from cell site. (Image Credit: Forensic Analytics, 2025 [3])

10.6 Proprietary Location Estimates

Cellular service providers often maintain Proprietary Location Estimates for engineering and network optimization purposes through the normal course of business. The retention for these types of records can be relatively short, and requests to preserve the records should be made as soon as possible.

Proprietary Location Estimates provide a calculated location of the mobile device reported as latitude and longitude. Some providers include a confidence value with the calculated latitude and longitude. The coordinates provided in these types of records are derived from proprietary algorithms and are not intended to provide an exact location of a mobile device. Due to the proprietary nature of this data the locations cannot be independently validated. Caution should be used when analyzing this data. It should be emphasized that TA and Proprietary Location Estimates are two independent sources of data, often disclosed in the same dataset.

10.7 Ping

A ping will normally report an estimated real-time latitude and longitude of a mobile device along with an uncertainty factor or margin of error from that point. It is extremely important to map the uncertainty factor or radius reflected in the data. Simply mapping the latitude and longitude will not provide a valid result on its own. Because ping information is not kept in the normal course of business, it is not obtainable from the service provider as an historical official business record. Ping data should be retained in accordance with applicable law (Figure 5).

Those obtaining pings from cellular providers should be aware that many pings are calculated based on historical location information. This data is not GNSS from the mobile device. Some mobile device operating systems are known to obfuscate location precision, which may result in larger uncertainty radii for the received pings.

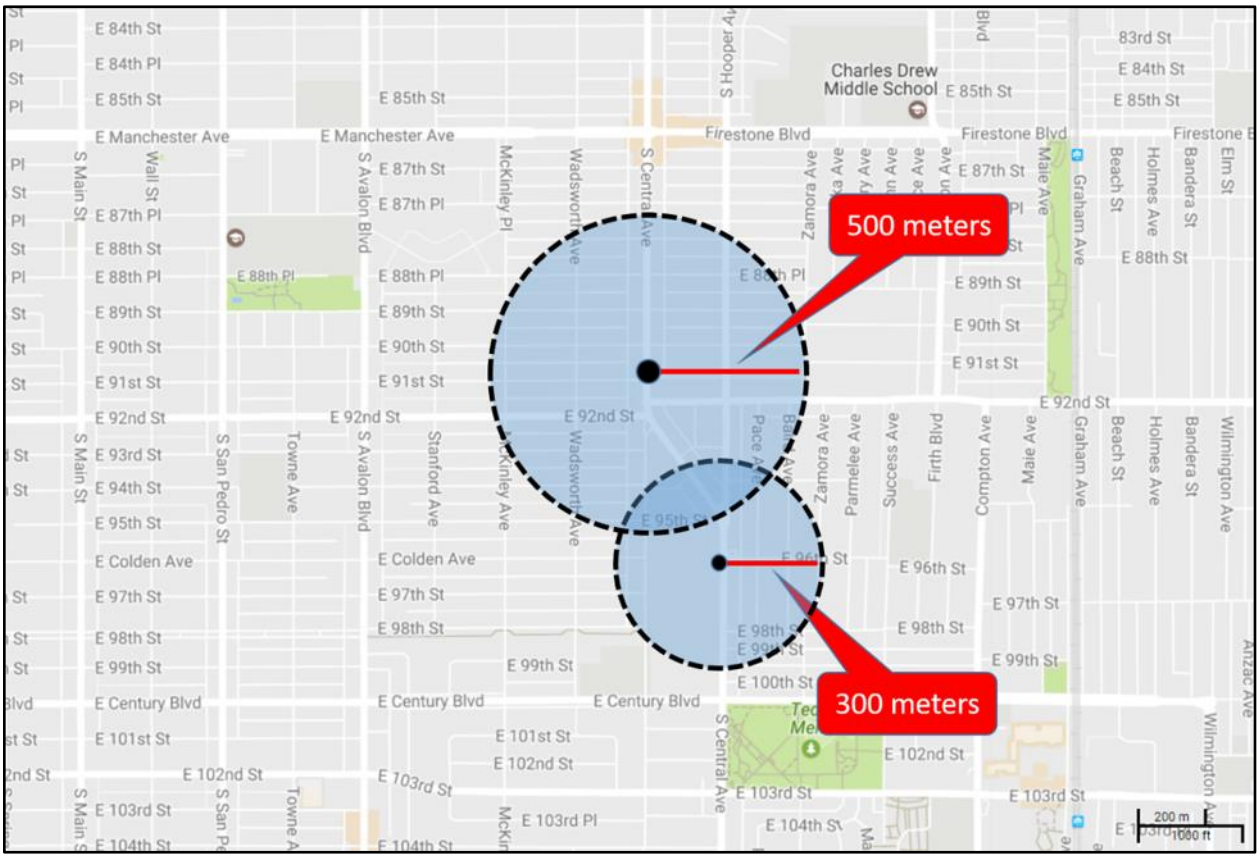

Figure 5. Example of Precision Geolocation Information ("Ping").
(Image Credit: SWGDE/Google Maps, 2017).

10.8 Data Sessions

Data session records are available from the cellular service providers for internet enabled devices. The records can include the date and time, bytes sent from the device to the cell site,

bytes sent from the cell site to the device, IP information, and may include location information. When using this data for geolocation, the records should be verified and validated because the correlation between the time stamps and cell site data associated with these records can vary.

11. Verification

Practitioners should be able to verify results by manual inspection or by using an alternate cell site analysis mapping solution. The completed analysis should undergo technical review to ensure an accurate result. Methodologies should be well documented and reproducible.

12. Presenting the Data in Legal Proceedings

Cell Site Analysis practitioners should properly represent map data by providing legends and distance scales that present proportionally accurate maps, and ensure all data incorporated in the analysis is referenced.

As a general rule, courts require the witness presenting CSLI to be admitted as an expert witness. The witness needs to have relevant knowledge, training, and experience of interpreting CDRs. Those conducting Cell Site Analysis should be prepared to present a thorough CV detailing this relevant knowledge, training, and experience. Legal considerations such as Daubert and Frye standards, or any other applicable expert witness legal requirements, may apply.

13. References

[1] United States, Congress, House. United States Code. Title 18, §2703 (f), Office of the Law Revision Counsel, 2011, https://uscode.house.gov/view.xhtml?req=(title:18%20section:2703%20edition:prelim)%20OR%20(granuleid:USC-prelim-title18-section2703)&f=treesort&edition=prelim&num=0&jumpTo=true.

[2] United States, Congress, House. United States Code. Title 18, §2702(c)/(b), Office of the Law Revision Counsel, 2011, https://uscode.house.gov/view.xhtml?req=(title:18%20section:2702%20edition:prelim)%20OR%20(granuleid:USC-prelim-title18-section2702)&f=treesort&edition=prelim&num=0&jumpTo=true.

[3] *Forensic Analytics*. https://www.forensicanalytics.io/uk/. Accessed 21 May 2025.

14. Additional Resources

- Chemello, Nicola. "Correlating CDR with other data sources," 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), 2016, Vancouver, BC, Canada, pp. 1-5, https://www.doi.org/10.1109/ICCCF.2016.7740425.
- European Telecommunications Standards Institute (ETSI), http://webapp.etsi.org/Teddi/. Accessed 14 Feb. 2026.

- Hoy, Joseph. Forensic Radio Survey Techniques for Cell Site Analysis 2nd Edition. United Kingdom, Wiley, 2023.
- Jovanovic, Vladen M., and Brian. T. Cummings. “Analysis of Mobile Phone Geolocation Methods Used in US Courts.” IEEE Access, vol. 10, 2022, pp. 28037-28052. https://ieeexplore.ieee.org/document/9729192. Accessed 14, Feb. 2026
- Kostanic, I., & Zec, J. (2023, July 10). Use of round-trip time (RTT) in estimation of the mobile location. Wireless Center of Excellence, Florida Institute of Technology. Retrieved from https://abmintel.com/wp-content/uploads/2025/10/Use-of-RTT-and-TA-for-CDR-Analysis.pdf
- Metcalf, Kevin. Cell Phones in Criminal Investigations: Basic Preparation, Analysis, and Mapping of Cellular Data. Amazon Digital Services LLC, 2016.
- Scientific Working Group on Digital Evidence. Best Practices for Mobile Devices Evidence Collection & Preservation Handling and Acquisition. SWGDE 18-F-003-2.0. SWGDE, 2025, https://www.swgde.org/documents/published-complete-listing/18-f-003-2/.
- Tart, Matthew, et al. "Historic cell site analysis – Overview of principles and survey methodologies." Digital Investigation, vol. 8, no. 3-4, 2012, pp. 185-193. https://www.sciencedirect.com/science/article/abs/pii/S1742287611000867?via%3Dihub#.
- Third Generation Partnership Project (3GPP), https://www.3gpp.org/. Accessed 14 Feb. 2026.

15. History

Revision	Issue Date	History
1.0 DRAFT	9/15/2016	Initial draft created and SWGDE voted to release as a Draft for Public Comment.
1.0 DRAFT	10/8/2016	Formatting and technical edit performed for release as a Draft for Public Comment.
1.0 DRAFT	1/12/2017	Full rewrite performed on the initial draft; title changed to remove “Forensic” before “Cell Site Analysis.” SWGDE voted to re-release as a Draft for Public Comment.

1.0 DRAFT	2/21/2017	Formatting and technical edit performed for re-release as a Draft for Public Comment.
1.0 DRAFT	6/22/2017	Additional revisions were made to all sections for finalization. SWGDE voted to re-release as a Draft for Public Comment.
1.0 DRAFT	7/11/2017	Formatting and technical edit performed for re-release as a Draft for Public Comment.
1.0	8/24/2017	SWGDE voted to publish as an Approved document (Version 1.0).
1.0	9/25/2017	Formatted and published as Approved Version 1.0.
2.0 DRAFT	9/21/2022	Formatting and technical edit performed for re-release as a Draft for Public Comment.
3.0 DRAFT	5/14/2024	Formatting and technical edit preformed for re-release as a Draft for Public Comment.
3.0 DRAFT	6/13/2024	SWGDE voted to approve as Draft for Public Comment. Formatted for release as a Draft for Public Comment.
3.0 DRAFT	9/19/2024	Formatting and technical edit performed for re-release as a Draft for Public Comment.
3.0	1/16/2025	No public comments received. SWGDE voted to approve as a Final Approved Document.
3.0	2/22/2025	Formatted for release as a Final Approved Document.
4.0 DRAFT	5/21/2025	Updated definitions. Reformatted and updated Specialized Historic Location Data, Timing Advance, pings, and Additional Resources.
4.0 DRAFT	6/29/2025	SWGDE voted to release as a Draft for Public Comment. Formatted for release for public comment.
4.0	11/21/2025	Formatted for release as a Final Approved Document.

5.0 DRAFT	1/15/2026	Substantive changes to align with other documents, title page changes, and definition changes. SWGDE voted to release as a Draft for Public Comment.
5.0 DRAFT	2/20/2026	Document formatted for release for Public Comment.
5.0 DRAFT	5/12/2026	Responses to public comment and non-substantive updates.
5.0	6/18/2026	SWGDE voted to approve as Final Approved Document.
5.0	7/9/2026	Document formatted for release as Final Approved Document.