**NG 9-1-1 Interoperability Testing Program Phase 3**

Federal Award/Contract No.: 115295-19731/70RSAT21G00000012

Task 4.1 NG911 Functional Element cybersecurity assessment.

Part I – Threat Modeling and Cyber Risk Assessment

Revised: 30-April-2025

Version: 1.1

Contents

[1. References 2](#_Toc385279432)

[2. Acronyms and Abbreviations 4](#_Toc444950390)

[3. Definitions 6](#_Toc219285231)

[4. Executive Summary 14](#_Toc2114488979)

[5. Background and NG911 Overview 17](#_Toc1691134716)

[5.1 Overview of i3 System 17](#_Toc508260460)

[5.2 Overview of NG911 Functional Elements and Call Flow 18](#_Toc68326050)

[Call Flow 21](#_Toc193790953)

[5.3 Transition from E911 to NG911 22](#_Toc768013098)

[5.4 Assumptions For a Successful Transition to NG911 24](#_Toc1753526676)

[6. Threat Modeling and Risk Assessment of NG911 Functional Elements 24](#_Toc764541826)

[6.1 Foundations of Threat Modeling and Risk Assessment 25](#_Toc196892621)

[6.2 Threat Modeling and Risk Impact Analysis of NG911 Functional Elements 26](#_Toc632739149)

[6.2.1 Location Information Server (LIS) 26](#_Toc193100188)

[6.2.2 Location Validation Function (LVF) 28](#_Toc888456924)

[6.2.3 Border Control Function (BCF) 30](#_Toc1056034447)

[6.2.4 Emergency Call Routing Function (ECRF) 32](#_Toc1033867860)

[6.2.5 Policy Routing Function (PRF) 34](#_Toc173295524)

[6.2.6 Emergency Services Routing Proxy (ESRP) 36](#_Toc1638900411)

[6.2.7 Legacy Network Gateway (LNG) 37](#_Toc433672267)

[6.2.8 Legacy PSAP Gateway (LPG) 38](#_Toc122863293)

[6.2.9 Public Safety Answering Point (PSAP) 39](#_Toc1068575914)

[6.2.10 Security Considerations Across NG911 Components 41](#_Toc1809105669)

[7. Discussion and Conclusion 45](#_Toc1729928196)

[8. Bibliography 45](#_Toc984607006)

[Appendix: NG911 System Components and Interaction Flows 46](#_Toc2130094688)

[1. Location Information Server (LIS) 47](#_Toc1460443286)

[2. Location Validation Function (LVF) 51](#_Toc1108780607)

[3. Border Control Function (BCF) 53](#_Toc146396452)

[4. Emergency Call Routing Function (ECRF) 55](#_Toc1378665073)

[5. Policy-based Routing Function (PRF) 58](#_Toc1629620612)

[6. Emergency Services Routing Proxy (ESRP) 58](#_Toc1051712529)

[7. Legacy Network Gateway (LNG) 61](#_Toc764429817)

[8. Legacy PSAP Gateway (LPG) 62](#_Toc1929405997)

[9. Public Safety Answering Point (PSAP) 62](#_Toc398286993)

# 1. References

[1] National Emergency Number Association, NENA-STA-010.3d-2021: NENA i3 Standard for Next Generation 9-1-1 (i3), Oct. 2021. [Online]. Available: <https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/nena-sta-010.3d-2021_i3_stan.pdf>

[2] National Emergency Number Association, NENA STA-040.2-2024: Security for Next Generation 9-1-1 (NG-SEC), Apr. 2024. [Online]. Available: <https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/STA-040.2-2024_SecurityforNG.pdf>

[3] Cybersecurity and Infrastructure Security Agency, Cyber Risks to Next Generation 9-1-1: A Primer for Public Safety Agencies, Nov. 2022. [Online]. Available: <https://www.cisa.gov/sites/default/files/publications/NG911%20Cybersecurity%20Primer.pdf>

[4] California Governor’s Office of Emergency Services, Next Generation 9-1-1 Transition Plans, Mar. 2021. [Online]. Available: <https://www.caloes.ca.gov/wp-content/uploads/PSC/Documents/0001-NextGeneration9-1-1TransitionPlans.pdf>

[5] 911.gov, Cyber Risks to Next Generation 911, U.S. Department of Transportation and National 911 Program, 2021. [Online]. Available: <https://www.911.gov/assets/Cyber-Risks-to-Next-Generation-911.pdf>

[6] P. D. Moore, Denial-of-Service (DoS) Attacks Against the Availability of the Next Generation 911 (NG911) System, M.S. thesis, Utica University, 2022.

[7] National Emergency Number Association, NENA-INF-015.2-2016: NG-SEC Information Document, 2016. [Online]. Available: <https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/NENA-INF-015_NGSEC_INF_20161.pdf>

[8] IEEE Public Safety Technology Initiative, Cybersecurity Best Practices for Next Gen 911: Protecting Emergency Communication Networks, 2022. [Online]. Available: <https://publicsafety.ieee.org/topics/cybersecurity-best-practices-for-next-gen-911-protecting-emergency-communication-networks>

[9] E. Rescorla, HTTP Over TLS, RFC 2818, May 2000. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc2818>

[10] R. Fielding and J. Reschke, Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing, RFC 7230, Jun. 2014. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc7230>

[11] M. Belshe, R. Peon, and M. Thomson, Hypertext Transfer Protocol Version 2 (HTTP/2), RFC 7540, May 2015. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc7540>

[12] T. Dierks and E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246, Aug. 2008. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc5246>

[13] E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446, Aug. 2018. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc8446>

[14] T. Dierks and C. Allen, The TLS Protocol Version 1.0, RFC 2246, Jan. 1999. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc2246>

[15] T. Dierks and E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346, Apr. 2006. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc4346>

[16] M. Thomson and J. Winterbottom, HTTP-Enabled Location Delivery (HELD), RFC 5985, Sep. 2010. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc5985>

[17] R. Barnes, A Location-to-Service Translation Protocol (LoST) Usage for Emergency Calling, RFC 6753, Nov. 2012. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc6753>

[18] B. Rosen et al., A Presence Event Package for the Session Initiation Protocol (SIP), RFC 3856, Aug. 2004. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc3856>

[19] J. Rosenberg, XMPP Presence Document Format, RFC 5222, Sep. 2008. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc5222>

**[20]** J. Fischl, H. Tschofenig, and E. Rescorla, *Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)*, RFC 5763, May 2010. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc5763>

**[21]** D. McGrew and E. Rescorla, *Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)*, RFC 5764, May 2010. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc5764>

**[22]** H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, *RTP: A Transport Protocol for Real-Time Applications*, RFC 3550, July 2003. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc3550>

**[23]** T. Friedman, R. Caceres, and A. Clark, *RTP Control Protocol Extended Reports (RTCP XR)*, RFC 3611, November 2003. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc3611>

# 2. Acronyms and Abbreviations

The following acronyms and abbreviations are used in this report.

AES Advanced Encryption Standard

CHE Call Handling Equipment

DDoS Distributed-Denial-of-Service

DoS Denial of Service

DTLS Datagram Transport Layer Security

DTMF Dual-Tone Multi-Frequency

ESInet Emergency Services IP Network

FS Forward Secrecy

HELD HTTP-Enabled Location Delivery

HTTP Hypertext Transfer Protocol

IMS IP Multimedia Subsystem

IP Internet Protocol

IPsec Internet Protocol Security

LTE Long Term Evolution

MAC Message Authentication Code

MFA Multi-Factor Authentication

MitM Man-in-the-Middle

NDS Network Domain Security

NENA National Emergency Number Association

NGFW Next-Generation Firewall

NG911 Next Generation 911

PFS Perfect Forward Secrecy

PIDF-LO Presence Information Data Format - Location Object

PSAP Public Safety Answering Point

PSTN Public Switched Telephone Network

RFC Request for Comments

RTP Real-Time Transport Protocol

SBC Session Border Controller

SIP Session Initiation Protocol

SRTCP Secure Real-time Transport Control Protocol

SRTP Secure Real-time Transport Protocol

SSL Secure Sockets Layer

SWAT Special Weapons and Tactics

TDoS Telephony-Denial-of-Service

TLS Transport Layer Security

URI Uniform Resource Identifier

URL Uniform Resource Locator

URN Uniform Resource Name

VoIP Voice Over IP

XML Extensible Markup Language

# 3. Definitions

**Access Control:** Measures that restrict who or what can access a system or data.

**Alert Monitoring:** Automatic detection and reporting of suspicious events or system failures in real time.

**Audit Logging:** Recording system activity for monitoring, security reviews, and forensic investigation.

**Authentication:** Verifying that an entity (user, device, system) is who it claims to be.

**Authorization:** Deciding what actions an authenticated entity is allowed to perform (e.g., read, write, execute).

**Availability:** The property of being accessible and usable upon demand by an authorized entity. Availability encompasses the design and implementation of fault-tolerant systems, redundancy, and resilience against denial-of-service (DoS) attacks to ensure continuity of access to information and systems.

**Botnet:** A network of compromised devices (bots) controlled by an attacker, commonly used to launch distributed denial-of-service (DDoS) attacks, send spam, steal data, or carry out other malicious activities at scale.

**Call Queues Filled with Fake Calls:** In a TDoS (Telephony Denial-of-Service) attack, fake 911 calls flood the queue, preventing real emergencies from getting through.

**Call Redirection:** Calls are re-routed to unintended or incorrect destinations due to manipulation or misconfiguration.

**Certificate Validation:** Checking that a digital certificate is genuine, unexpired, and trusted.

**Checksum:** A simple form of integrity check that adds up values in data to detect errors or alterations.

**Collapse of Dynamic Routing Capabilities:** The system loses the ability to intelligently route calls based on real-time policies, forcing reliance on static or degraded methods.

**Confidentiality:** The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. It involves the use of cryptographic, access control, and data classification mechanisms to prevent unauthorized data exposure.

**Configuration Hardening:** Securing systems by disabling unnecessary features and enforcing strict, secure settings.

**Data Breach:** The unauthorized access, disclosure, or theft of sensitive information. In NG911, this could involve the exposure of caller location, personal identifiers, call metadata, or emergency response logs.

**Data Integrity Failure:** When data is modified, deleted, or corrupted, either accidentally or maliciously, making it unreliable or incorrect.

**Dependency Audits:** Reviewing third-party libraries or components for known vulnerabilities or unsupported versions.

**DDoS (Distributed Denial of Service):** A DDoS attack floods a target system or network with a massive amount of traffic from multiple sources (often compromised computers or bots), overwhelming its capacity to respond to legitimate requests. The goal is to make the service unavailable to its intended users.

**Digital Certificate:** A cryptographic document used to prove the identity of a system or service (issued by a trusted Certificate Authority).

**Digital Signature:** A cryptographic way to ensure that a message or file is authentic and has not been modified.

**DoS (Denial of Service):** A DoS attack is like a DDoS attack but typically originates from a single source. It aims to flood a target system or network with traffic, exhausting its resources and making services unavailable to legitimate users.

**DTMF (Dual-tone Multi-frequency):** A system where pressing a key on a phone produces two sounds. These sounds represent numbers or symbols, allowing the phone to send the input to a system like a voicemail or automated service.

**Eavesdropping:** Unauthorized interception of 911 call content or metadata, violating confidentiality.

**Egress:** The outbound flow of network traffic leaving a system, device, or network boundary.

**Encryption at Rest and in Transit:** Encrypting sensitive data when it's stored (at rest) and while it's being transmitted (in transit), to prevent unauthorized access.

**Endpoint Whitelisting:** Allowing only pre-approved systems or IPs to access a network or service interface.

**Exposure of Private Caller Location:** Unauthorized access to a 911 caller’s precise location (e.g., GPS or address), which is sensitive personal information.

**Fallback Routing:** The system uses a backup or default routing method when normal location-based routing fails, often less accurate.

**FS (Forward Secrecy):** A property of encryption protocols that ensures if one session’s encryption keys are compromised, past communications remain secure.

**Hardened SIP Stacks:** SIP protocol implementations designed to withstand malformed inputs and protocol-level attacks.

**Hash**: A fixed-length string generated by a mathematical function from input data, used to verify data integrity.

**Hashing:** The process of converting input data into a hash, even small changes to the input result in a different hash.

**Hash Algorithm:** A function that takes an input (or 'message') and returns a fixed-size string of bytes. The output, known as the hash, is typically a 'digest' that represents concisely the original input. Hash algorithm is designed to be one-way function; they can easily generate a hash from a message, but it's computationally infeasible to generate the original message from the hash.

**HTTP (Hypertext Transfer Protocol):** The foundation of data communication for the World Wide Web, HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

**IMS (IP Multimedia Subsystem):** An architectural framework for delivering IP multimedia services. It supports multiple types of access technologies, including GSM, WCDMA, LTE, and Wi-Fi. IMS is designed to facilitate the convergence of voice, video, data, and mobile network technology over an IP-based infrastructure.

**Ingress:** The point at which external traffic enters a system or network, typically monitored and filtered for threats.

**Input Validation:** Verifying that user or network input meets expected formats and values to prevent exploits.

**Insider:** A legitimate user (e.g., employee, contractor) who may misuse access intentionally or accidentally.

**Integrity:** The property of safeguarding the accuracy and completeness of assets. This includes ensuring that data has not been altered in an unauthorized manner, whether in storage, processing, or transit. Mechanisms such as cryptographic hash functions, checksums, and digital signatures are commonly employed to assure integrity.

**Integrity Check:** Verifying that data has remained unchanged (e.g., using hashes or checksums).

**Integrity Validation:** A broader process that includes integrity checks and confirmation against expected/authorized values. Note: (Integrity Check and Integrity Validation) are often used interchangeably, but "validation" implies a more formal or policy-driven check.

**Interactive Media Response System:** also known as IVR (Interactive Voice Response) system, is an automated system that allows computers to interact with humans through voice prompts and responses, often using DTMF tones or speech recognition.

**Intrusion Prevention:** A system that detects and actively blocks malicious activity before it affects the target.

**IP (Internet Protocol):** The principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking and essentially establishes the Internet.

**IP Filtering:** Controlling access to systems by allowing or denying traffic based on IP addresses.

**IPsec (Internet Protocol Security):** A suite of protocols for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.

**Jurisdictions:** Geographic or administrative areas used to determine emergency call routing and policy enforcement.

**Jurisdiction Inference:** Attackers determine the geographic boundaries or routing zones of PSAPs by probing the system, potentially for future misuse or attacks.

**Load Balancing:** Spreading workloads across servers to improve reliability and performance.

**Location:** The current physical location (i.e., co-ordinates plus estimated accuracy and timestamp) of the MCPTT UE that can be cross-referenced to a map.

**Location Metadata Leakage:** Information about a caller’s location is accessed or exfiltrated without authorization**.**

**Loss of Automated Location Delivery**: When the system fails to provide automatic caller location to PSAPs, forcing manual questioning or guesswork.

**Loss of Life:** The ultimate consequence of delayed, misrouted, or unhandled emergency calls, a worst-case scenario resulting from system failure or attack.

**MAC (Message Authentication Code):** A short piece of information used to authenticate and to provide integrity and authenticity assurances on the message. MACs are typically produced by combining a secret key with the message data via a process known as hashing. The resulting MAC is appended to the message such that it can be validated at the receiving end.

**Malformed SIP Messages:** SIP (Session Initiation Protocol) messages that are corrupted or intentionally crafted to crash or confuse the system.

**Malware:** Malicious software (e.g., viruses, trojans, spyware) designed to harm systems or steal information.

**Manual Delays / Manual Intervention:** Call takers must manually gather information or validate routing due to system failure, which slows response.

**MFA (Multi-Factor Authentication):** A security mechanism requiring more than one method of verification (e.g., password + phone code).

**Misrouted Calls:** 911 calls are sent to the wrong Public Safety Answering Point (PSAP), delaying emergency response.

**MitM (Man-in-the-Middle):** An attack where the adversary secretly intercepts or alters communication between two parties.

**Mutual Authentication:** Both sides (e.g., client and server) verify each other’s identities before communication.

**Network Segmentation:** Dividing a network into isolated zones to limit the spread of attacks or malware.

**NDS (Network Domain Security):** A framework for ensuring the security of data as it travels across a network by implementing protocols and policies designed to protect network traffic.

**NGFW (Next-Generation Firewall):** A security appliance that provides advanced traffic filtering beyond traditional firewalls. In NG911 systems, NGFWs are used to inspect SIP and HTTP traffic, prevent DDoS attacks, and enforce security policies at the ESInet perimeter.

**Null Targets:** Routing rules direct calls to non-existent or dead-end endpoints, resulting in dropping the call.

**Originating Networks:** Service providers who send calls to ESInets/NGCS.

**Overwhelming Call Takers:** Call center staff are flooded with calls beyond their capacity, often due to TDoS, preventing them from responding to real emergencies.

**Packet Inspection:** Analyzing network packets for malicious payloads, unauthorized protocols, or policy violations.

**PFS (Perfect Forward Secrecy):** Encryption property ensuring past communications can't be decrypted even if long-term keys are compromised.

**Phishing:** Fraudulent attempts to trick users into revealing credentials or downloading malware via fake emails or messages.

**PIDF-LO (Presence Information Data Format - Location Object):** An XML-based format used to represent a device's location information in Next Generation 911 (NG911) and other emergency services. It is an extension of PIDF (Presence Information Data Format) and includes geolocation data (latitude/longitude) and/or civic address information.

**Private Key:** A private key is a secret key that is used in asymmetric cryptography. It is kept confidential and used to decrypt data that has been encrypted with the corresponding public key or to sign data, proving the authenticity and integrity of the data and the identity of the signer.

**Protocol Hardening**: Strengthening network protocols by disabling weak features and enforcing strict standards compliance.

**Public Key:** A public key is used in asymmetric cryptography and is shared openly. It is used to encrypt data or verify a signature created with the corresponding private key. Public keys allow anyone to encrypt messages or verify signatures without compromising the security of the private key.

**Ransomware:** A type of malicious software that encrypts files or entire systems, making them inaccessible to users. Attackers demand payment (usually in cryptocurrency) in exchange for a decryption key.

**Rate Limiting:** A technique to control the number of requests a user/system can make, used to prevent abuse or flooding attacks.

**Request-URI:** is a specific field inside a SIP INVITE (or other SIP messages), It tells where the request should go (the target for the call). In a 911 call, The Request-URI MUST be **urn:service:sos or similar (e.g., urn:service:sos.police)**.

**RFC (Request for Comments):** A formal document from the Internet Engineering Task Force (IETF) that specifies the technical and organizational notes about the Internet, including protocols, procedures, and events.

**Role-Based Access Control:** Access is granted based on the user’s role (e.g., admin, operator), limiting exposure to sensitive functions or data.

**Rotating caller IDs:** Refers to a technique used by attackers, especially in Telephony Denial-of-Service (TDoS) attacks, where they rapidly change the caller ID number for each fake call they send to a 911 system or other voice service.

**RTP (Real-Time Transport Protocol):** A protocol used to deliver audio and video over IP networks in real-time. In NG911, RTP is used to transmit voice data from the caller to the PSAP. It operates alongside SIP and is critical for actual media delivery during a call.

**SBC (Session Border Controller):** A specialized network element that secures and manages real-time voice and video communications, especially SIP-based sessions. SBCs enforce signaling validation, conceal internal network topology, enable media encryption, and protect against malformed or malicious call setups. In NG911, SBCs are deployed at network borders to authenticate SIP messages, prevent spoofing, and support secure call handling.

**Secure Data Channels:** Communication paths (like HTTPS) that protect data in transit using encryption.

**Secure Media Gateways**: Devices that securely bridge media (voice, video) between different networks, enforcing encryption and policy controls.

**Service Crash:** The system stops functioning entirely due to overload, software faults, or attacks (e.g., DoS).

**Service Degradation:** System performance declines, such as slower responses or increased errors, even if it hasn't fully failed.

**Signature Algorithm:** A signature algorithm is a type of cryptographic algorithm used to implement digital signatures, which provides a way to verify the authenticity and integrity of data. The algorithm ensures that a signature generated by a private key can only be verified by its corresponding public key.

**SIP (Session Initiation Protocol):** signaling protocol used in NG911 to set up, manage, and terminate multimedia sessions such as emergency calls. SIP messages use methods like INVITE (to start a call), ACK (to confirm it), BYE (to end it), OPTIONS (to check capabilities), SUBSCRIBE (to request event notifications), and NOTIFY (to send updates). These messages carry headers and payloads that guide call routing, media negotiation, and emergency-specific behavior. Other methods like UPDATE, CANCEL, and MESSAGE may also be used depending on context.

**Spoofing:** Forging digital identity (e.g., IP address, SIP identity) to impersonate a trusted source.

**SRTP (Secure Real-time Transport Protocol):** Encrypted voice, video, and text transport protocol used to protect media in real-time IP communications.

**SRTCP (Secure Real-time Transport Control Protocol):** Secure protocol that protects control messages like call quality feedback in real-time media streams.

**SSL (Secure Sockets Layer):** The standard security technology for establishing an encrypted link between a web server and a browser, providing a mechanism for all data passed between them to be private and integral.

**STIR/SHAKEN:** A protocol suite that verifies the identity of callers in IP-based telephony, helping prevent call spoofing.

**Swatting**: A false emergency report is made to dispatch law enforcement or emergency services to a fake location, often as a prank or with malicious intent. In NG911, spoofed location data could enable this attack.

**System Compromise:** An attacker gains control over part of the system or its functions, allowing further manipulation or data theft.

**Tampered Call Metadata:** Critical data about the call (such as origin, timestamp, or location) is altered in transit, misleading PSAP systems or responders.

**TDoS (Telephony Denial of Service):** TDoS attacks target voice over IP (VoIP) systems or traditional phone systems. Attackers flood the target's phone lines with excessive call volumes, disrupting communication services.

**TLS (Transport Layer Security):** A protocol that ensures privacy between communicating applications and their users on the Internet. TLS prevents eavesdropping, tampering, and message forgery by encrypting the underlying communications.

**Unauthorized Network Entry:** An attacker gains access to NG911 internal systems by bypassing network access controls.

**Upgrade Planning:** Strategically managing software and hardware updates to ensure continuity and security.

**Upstream Systems:** External systems that feed into the current system (e.g., data providers or network sources).

**URI (Uniform Resource Identifier):** A standard way of identifying resources such as devices, services, or locations. Examples include SIP URIs (sip:user@domain), Telephone URIs (tel:+15551234567), and Service URNs (urn:service:sos).

**URL (Uniform Resource Locator):** An identifier that provides both the address and the access method for a resource. It tells you where the resource is located (e.g., a server) and how to retrieve it (e.g., using HTTP or HTTPS). For example, https://example.com/location/12345 points to a specific resource available on the web via HTTPS.

**URN (Uniform Resource Name):** A standardized identifier used to uniquely name a resource. Unlike URLs, which describe how and where to access something, URNs serve only as persistent, location-independent references. For example, “urn:location:12345” identifies a stored location in a Location Information Server (LIS) but must be dereferenced to retrieve the actual data.

**Version Lifecycle Monitoring**: Tracking support status of software/hardware versions to retire or upgrade insecure components.

**Version Management:** Keeping track of updates and changes to data, software, or configurations to detect unauthorized modifications.

**Vulnerability Assessment**: The process of scanning and evaluating systems for weaknesses that could be exploited.

**XML (Extensible Markup Language):** A structured, human-readable, and machine-readable format used to store and transport data. It allows for the organization and encoding of information in a hierarchical manner, making it useful for data exchange between different systems.

# 4. Executive Summary

As NG911 systems replace traditional emergency communication infrastructure, they bring enhanced capabilities but also increased cyber risk. This assessment identifies and prioritizes threats across core functional elements, evaluating their potential to disrupt emergency call routing, compromise location accuracy, or delay critical response services. Each threat scenario is mapped to its public safety impact and business consequence. The assessment demonstrates that NG911 systems, while technically advanced, require vigilant protection to prevent service outages, data breaches, or denial-of-service conditions that could endanger lives. The table below summarizes the most critical threat scenarios and risk ratings for each system element, providing a clear basis for prioritizing security controls and resilience planning.

Whenever “swatting” is referenced in this report, it encompasses serious public safety threats such as the wrongful dispatch of armed responders to fabricated emergencies, the potential injury or death of innocent individuals, public panic, and the diversion of emergency resources away from real incidents.

The table below summarizes some threat scenarios identified for each functional element, along with their corresponding business impacts and final risk ratings. For detailed threat reasoning, mitigation, and impact analysis, readers are encouraged to refer to Section 6 of this report.

Table 4. NG911 Functional Elements – Threat Scenarios and Risk Assessment Summary

|  |  |  |  |
| --- | --- | --- | --- |
| Functional Element | Threat Scenario | Business Impact | Risk Rating |
| LIS | **Impersonation of LIS (Spoofed Service):** An adversary spoofs the LIS service to send false location data, misleading responders and potentially misrouting emergency calls | Could reduce public confidence in 911 reliability, produce formal complaints or lead to emergency units being misdirected (i.e. “swatting”) | **High** |
| **Location Tampering:** An adversary modifies or corrupts legitimate location data in the LIS, causing responders to be sent to incorrect or fake addresses (e.g., swatting). | May lead to emergency units being misdirected (i.e. “swatting”) or causing response delays | **High** |
| **Unauthorized access or data breach:** An adversary gains unauthorized access to the LIS database to view, extract, or tamper with sensitive caller location data, leading to privacy violations and service disruptions. | Leaked location data may violate caller privacy and reduce trust in the 911 system. | **Medium** |
| **Denial of Service via query flooding:** An adversary floods the LIS with location requests or malformed queries, overwhelming the system and delaying accurate location resolution for 911 calls. | Slower responses could overwhelm call takers and disrupt call-handling operations | **High** |
| LVF | **GIS Data Tampering & Address Validation Corruption:** An adversary tampers with GIS data or the validation logic, causing the LVF to mis validate addresses and misroute emergency calls. | May cause dispatch routing errors, leading to emergency response delays or swatting-like incidents | **High** |
| **Uncontrolled Queries & Unauthorized Access to Validation Services:** An adversary abuses or gains access to the LVF interface to run mass queries or tamper with validation functions, exposing location patterns or degrading performance. | May slow validation services and expose address patterns, raising privacy concerns | **Medium** |
| **Address Validation Overload & Denial of Service:** An adversary floods the LVF with excessive or malformed queries, overwhelming the service and delaying call routing during active emergencies. | Could delay call routing and overwhelm PSAPs, reducing emergency response efficiency | **High** |
| BCF | **Network Access Bypass (Credential/IP Spoofing):** An adversary spoofs trusted IP addresses or uses stolen credentials to bypass BCF filters, gaining access to the ESInet and injecting fake calls or malicious traffic into emergency systems. | Fake or malicious calls might enter the system, putting emergency services at risk and damaging public trust | **Medium** |
| **Telephony DoS (TDoS) & Call Spoofing:** An adversary floods the call system with spoofed or fake 911 calls using bots or rotating caller IDs, saturating PSAP queues and blocking real emergencies from getting through. | Fake calls can disrupt the system, preventing real 911 calls from getting through and delaying emergency help | **High** |
| **Denial-of-Service (DoS) & Overload:** An adversary overwhelms the BCF with excessive or malformed network traffic, such as SIP floods or UDP bursts, causing the system to drop or delay legitimate 911 calls due to processing bottlenecks. | Too much traffic can block or slowdown 911 services, causing major service interruptions during emergencies | **High** |
| ECRF | **GIS Data Corruption & Routing Misdirection:** An adversary tampers with the ECRF’s geospatial routing data, causing emergency calls to be sent to the wrong PSAP or a non-existent location. | May cause calls to be misrouted, delaying emergency help and damaging reputation | **High** |
| **Unauthorized ECRF Access & Call Manipulation:** An adversary gains unauthorized access to the ECRF and uses it to view caller data or manipulate routing responses, undermining system trust and data confidentiality. | May expose caller data or alter call routing, reducing trust in emergency systems | **Medium** |
| **Routing Lookup Failure via Denial of Service:** An adversary floods the ECRF with excessive or malformed requests, crashing or stalling the system and forcing default routes. | May block emergency calls and overload backups, causing major service disruption | **Medium** |
| PRF | **Metadata Spoofing to Evade Policy Filters:** An adversary spoofs call metadata (e.g., priority flags, jurisdiction info) to make fake calls appear legitimate, bypassing PRF filters and overwhelming PSAPs with false traffic. | May allow fake calls to bypass filters and flood emergency lines, slowing real responses. | **High** |
| **Routing Policy Tampering & Rule Manipulation:** An adversary with admin access tampers with the PRF’s routing rules, misdirecting or dropping real 911 calls and potentially causing large-scale service failures. | Can result in real 911 calls being misrouted (i.e “swatting”) or dropped, leading to service failures. | **High** |
| **Routing Logic Overload & PRF Disruption:** An adversary floods the PRF or its associated ESRP with malformed SIP messages or exploits routing logic, overloading call routing systems and delaying emergency response. | May overwhelm routing systems, causing delays or outages in emergency call handling. | **High** |
| ESRP | **Signaling Spoofing & Call Interception:** An adversary impersonates a trusted network device or manipulates SIP signaling to misroute or intercept emergency calls, potentially altering or leaking sensitive call setup data. | May cause calls being misrouted (i.e “swatting”) or intercepted calls, leading to service failures, privacy concerns and loss of trust | **High** |
| **Call Flooding via SIP-Based DDoS:** An adversary floods the ESRP with a high volume of fake SIP call setup requests, exhausting processing capacity and disrupting the routing of legitimate 911 calls. | Could delay or block emergency calls, overwhelming services and impacting public safety | **High** |
| LNG | **Protocol Conversion Vulnerabilities:** An adversary sends malformed or ambiguous legacy call signals that are misinterpreted by the LNG, leading to dropped or misrouted 911 calls during protocol translation. | Misrouted or dropped 911 calls may disrupt emergency response operations. | **High** |
| **Legacy Traffic Injection via Insufficient Security Controls:** An adversary spoofs legacy call signals from untrusted TDM sources, injecting fake calls into the NG911 system and enabling TDoS or impersonation attacks. | Fake or spoofed calls can overload systems and reduce trust in emergency services. | **High** |
| LPG | **Unsecured RTP Bridging & Media Path Compromise:** An adversary intercepts or injects media (audio, text, video) into calls bridged between IP and analog systems, exploiting unsecured RTP relays to compromise call integrity or privacy. | Call media (text, audio, video) may be intercepted or altered, potentially leading to privacy issues or response delays. | **High** |
| **DoS-Induced Isolation of Legacy PSAPs:** An adversary launches a DoS attack or triggers a misconfiguration on the LPG, severing the connection between NG911 and legacy PSAPs and preventing emergency calls from reaching responders. | Legacy call centers may become unreachable, blocking emergency access in affected regions. | **High** |
| PSAP | **Unauthorized Access & Data Breaches:** An adversary or insider gains unauthorized access to PSAP systems, exfiltrating or tampering with sensitive emergency call data, harming privacy and trust. | May expose sensitive emergency data, leading to loss of public trust and legal risk | **High** |
| S**ystem Compromise via Malware or Ransomware:** An adversary delivers malware (e.g., via phishing emails or media files), compromising PSAP systems or locking them with ransomware, halting dispatch operations. | May halt 911 services and force costly downtime or manual operation | **High** |
| **Telephone Denial of Service (TDoS):** An adversary floods PSAP lines with spoofed or automated calls from multiple media types, preventing legitimate emergency callers from reaching assistance. | May prevent real 911 calls from going through, causing public safety consequences. | **High** |
| Any NG911 Functional Elements | **Exploitation of Software Vulnerabilities:** An adversary discovers and exploits a bug in core NG911 software (e.g., ESRP or LIS), crashing services or bypassing routing logic to misdirect or block emergency calls. | Software flaws could crash services or misroute 911 calls, risking delayed emergency response | **High** |
| **Misconfiguration or Human Error:** An administrator or staff member unintentionally misconfigures access controls or routing rules, disrupting 911 operations or exposing systems to external threats. | Configuration mistakes can disable routing or allow untrained users to cause major outages. | **Critical** |
| **Use of Insecure or End-of-Life Components:**  Legacy software or unsupported hardware—left unpatched—exposes NG911 systems to exploitation, service failure, or security breaches during critical operations. | Outdated components may open critical vulnerabilities or fail during high-demand situations | **High** |
| **Insecure or Deprecated Protocols (e.g., TLS 1.0/1.1, Telnet):** An adversary intercepts or manipulates emergency communications due to outdated encryption protocols that lack forward secrecy and are susceptible to downgrade attacks. | Weak protocols may let attackers eavesdrop, spoof, or bypass encryption entirely | **High** |

# 5. Background and NG911 Overview

## 5.1 Overview of i3 System

* What is i3?
  + **The i3 architecture** is the standard defined by NENA [1] to transition 911 services from analog/PSTN-based systems to an IP-based emergency services network (ESInet).
    - **ESInet** is a network of networks designed for emergency services that serves as the foundational transport infrastructure supporting Next Generation Core Services (NGCS).
    - It provides standardized functional elements, databases, network elements, and interfaces required for handling multimedia emergency calls (voice, text, video, and data).
  + The goal of **i3** is to ensure that **emergency calls can be handled using modern digital technologies**, including:
    - Voice over IP (VoIP)
    - Text messaging (SMS)
    - Real-time video
    - Multimedia data sharing (e.g., crash notifications, medical records, images, etc).

## 5.2 Overview of NG911 Functional Elements and Call Flow

The following diagram illustrates the key functional elements and call flow in a Next Generation 911 (NG911) environment, based on the NENA i3 architecture. It reflects the transition from legacy systems to IP-based emergency services.

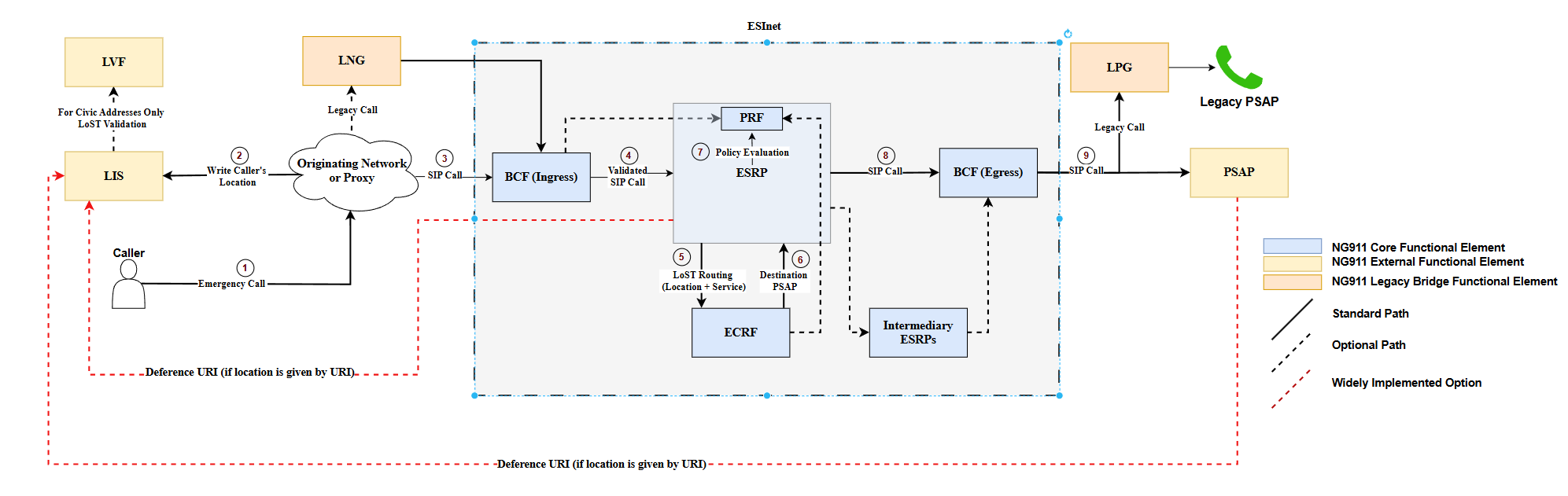


Figure 5.2. NG911 System Architecture and Call Flow

This section provides a high-level overview of the main functional elements defined in the NENA i3 architecture and their roles in supporting Next Generation 911 (NG911) operations. While this section outlines their purpose and placement within the system, further details for each element are addressed in Section 5.5, which walks through each functional element individually.

* **Ensures End-to-End IP Connectivity**.
* **Public Safety Answering Point (PSAP):** The emergency dispatch center responsible for answering and processing 911 calls.
* Types of PSAPs in NG911:
  + **Primary PSAP:** The first point of contact for emergency calls.
  + **Legacy PSAP:** A traditional PSAP that still operates on older PSTN-based technology.
  + **NG911 PSAP:** A modern, IP-based center that can handle multimedia (text, video, images, data).
* **Location Information Server (LIS): Supplies the geographic location of a caller.** 
  + Provides location data for VoIP, mobile, and IP-based devices.
  + Delivers Location-by-Value (latitude/longitude) or Location-by-Reference (URL or PIDF-LO format).
* **Location Validation Function (LVF):** Validates a caller’s location data before routing the call**.**
  + Ensures that **civic addresses** are correct and properly formatted**.**
    - A civic address refers to a standardized street address used for identifying locations in a structured format. Unlike geographic coordinates (latitude/longitude), a civic address is written in human-readable form and includes:
      * Street Number & Name (e.g., 123 Main St.)
      * City/Town (e.g., Springfield)
      * State/Province (e.g., California, TX)
      * Postal Code/ZIP Code (e.g., 90210)
      * Apartment/Suite/Floor (if applicable) (e.g., Apt. 5B, Floor 3)
    - Uses GIS-based databases to validate the caller's location in real time
* **Emergency Services IP Network (ESInet)**
  + Provides shared connectivity for all public safety agencies handling 911 calls.
  + Includes **NG911 Core Services (NGCS)** to process emergency communications.
    - **NG911 Core Services (NGCS)** refers to a set of essential backend services that help process, manage, and route emergency calls within the NG911 system.
    - These services operate within **ESInet (Emergency Services IP Network)** and ensure that emergency calls reach the correct **Public Safety Answering Point (PSAP)** with accurate location and caller data.
  + [1, B1] NGCS includes the following **Functional Elements**:
    - Border Control Functions (BCF): Manages security and interoperability between different networks.
      * Supplies a fixed entry point to ESInet for emergency calls (or exit point).
      * Provides firewall security and admission control.
      * Helps in Preventing unauthorized access and mitigating cyber threats.
    - **Emergency Call Routing Function (ECRF)**: Determines the correct PSAP to receive a 911 call.
      * Uses **GIS-based** routing to dynamically direct calls based on caller location.
      * Utilizes a **Location-to-Service Translation (LoST)** protocol with **Location Validation Function (LVF)** to ensure precise mapping.
      * The determined PSAP might be **further checked** **with other policies** to ensure correct routing (as discussed in further FEs).
    - **Policy Routing Function (PRF):** Ensures that calls follow **appropriate routing policies** set by public safety agencies.
      * Defines rules for prioritizing call routing (e.g., disaster scenarios, PSAP overflow).
      * Handling overflow calls when a PSAP is overwhelmed.
      * Rerouting based on jurisdiction-specific rules.
      * Directing calls to secondary PSAPs in case of failure.
    - **Emergency Services Routing Proxy (ESRP):** A SIP proxy server responsible for selecting the routing path within ESInet (main routing functional element).
      * Determines how emergency calls travel through the network.
      * Works with **ECRF** and **PRF** to ensure calls reach the right PSAP.
      * Routes calls dynamically based on **policy** and **caller location**.
      * ESRP uses **predefined fallback mechanisms**, such as routing to a default PSAP or employing static routing rules to maintain call availability **even if ECRF or PRF are not functioning.**
    - **Intermediary ESRP(s):** Used when multiple routing steps are required between the initial ESRP and the final PSAP.
    - **Legacy Network Gateway (LNG):** LNG provides the interface **between a legacy-originating network and NG911 core service-enabled network**.
      * Allow calls from older PSTN-based 911 systems to connect to NG911.
      * Ensures compatibility between legacy and modern emergency call systems.
    - **Legacy PSAP Gateway (LPG):** Ensures that calls can be transferred **between NG911 and Legacy PSAPs**.
      * Some PSAPs are not yet upgraded to NG911, so an interface is needed to bridge the gap.

While the Legacy Network Gateway (LNG) and Legacy PSAP Gateway (LPG) are defined as functional elements within the NG911 architecture, they are not part of the NG911 Core Services (NGCS) and do not contribute to core call routing or policy enforcement. As such, their internal behavior and signaling flows are not analyzed in this section. These elements serve primarily to support interoperability with legacy systems and are briefly introduced in Sections 5.5.7 and 5.5.8. Their relevance to system compatibility and associated cybersecurity risks is examined in greater detail in Section 6. Nonetheless, the general security principles discussed for PSAPs still apply for securing legacy systems (i.e. Legacy PSAPs) in a broader context.

For further details, refer to Appendix A: NG911 System Components and Interaction Flows.

### Call Flow

1. The originating network (service provider or Access network) or SIP proxy writes the caller location to the LIS. The location information, whether provided by value or by reference, is included in the SIP INVITE before the call enters the ESInet. If the location is provided by reference, such as a URI, which is common practice, the ESRP and the PSAP may periodically dereference the URI (for example, every 30 seconds) during the session to retrieve updated location information. The LVF is used to validate civic addresses against the authoritative GIS database (When the LIS is populated by the access network or provider).
2. The SIP INVITE is sent to the BCF (Ingress), which validates and normalizes the message, adds emergency- specific headers, and forwards it to the ESRP.
3. The ESRP queries:

* The ECRF with a LoST query, using the caller’s location and a service URN (e.g., urn:service:sos) to obtain the correct PSAP or intermediate hop.
* The PRF to apply policy-based routing, such as overflow handling or jurisdiction-specific rerouting.
* In some deployments, the BCF (Ingress) or ECRF may also invoke the PRF to apply early or supplemental policy checks before forwarding to the ESRP. This is typically optional and implementation- specific, allowing the system to enforce routing, security, or jurisdictional constraints.
* If ECRF or PRF is unreachable, the ESRP can fall back to default static routes to maintain call delivery.

1. The ESRP updates the Request-URI with the final destination SIP URI and forwards the call either
   1. directly to the BCF (Egress) and then to the PSAP, or
   2. Through Intermediary ESRPs if needed.
2. Legacy 911 Calls may enter through the LNG (e.g., from a TDM network) and Legacy PSAPs may be reached through the LPG.
3. After session establishment, media (RTP) is typically bidirectional but does not flow directly between the caller and the PSAP. Instead, RTP usually passes through the BCF and/or media relay components within the ESInet for security and network isolation.

## 5.3 Transition from E911 to NG911

The shift to NG911 requires transitioning **legacy wireline and wireless networks** and **PSAPs** to next-generation interconnections.

* **911 (Basic 911):** The original emergency calling system where all 911 calls were routed to a fixed PSAP (without location awareness).
  + **No location tracking:** Dispatchers had to rely on the caller to provide location details.
* **E911 (Enhanced 911):** E911 improved the basic 911 system by introducing Automatic Location Identification (ALI), Master Street Address Guide (MSAG) database and Selective Routing (SR) to enhance call routing accuracy.
  + **ALI (Automatic Location Identification):** A system that automatically provides the caller’s registered address to the 911 dispatcher when a landline call is made.
  + **MSAG (Master Street Address Guide):** A database that maps phone numbers to valid street addresses and emergency service zones to ensure accurate call routing.
  + Calls are routed based on the caller’s phone number and registered address (MSAG database).
  + Mobile phone support was added, but only with approximate location tracking (based on nearest tower).
* **NG911 (Next Generation 911):** NG911 is a modern, IP-based emergency communication system that replaces traditional 911 and E911.
  + Uses Geographic Information Systems (GIS) for real-time, location-based routing.
    - GIS-based routing allows calls to be directed to the nearest PSAP based on real-time location, rather than fixed, pre-assigned call routing areas.
  + Supports multimedia communications (text, video, images, sensor data).
  + Routes emergency calls dynamically based on **live** caller location.
* **Legacy System Components Being Phased Out**
  + **Circuit-switched telephone networks (TDM-based)**
    - **Traditional Time-Division Multiplexing (TDM)** networks were used to transmit 911 calls over circuit-switched technology.
    - Calls relied on **fixed infrastructure** like copper lines and dedicated circuits.
    - **NG911 Replacement:**
      * **ESInet (Emergency Services IP Network):** A fully IP-based transport system that supports all forms of emergency communication.
      * **Session Initiation Protocol (SIP) Routing:** Allows flexible call routing, multimedia transmission, and better failover protection.
  + **Selective Routers (SRs)**
    - **Selective Routers (SRs)** were used to route 911 calls based on the caller’s phone number (landline or cellular area code).
    - Calls were forwarded to the designated PSAP based on a **fixed mapping** of area codes and exchanges.
    - **NG911 Replacement:**
      * **Emergency Call Routing Function (ECRF):** Uses GIS-based routing for real-time, **dynamic** call handling instead of fixed area codes.
      * I**P-based ESInet and Next-Gen Core Services (NGCS):** Fully supports VoIP, video, and multimedia emergency calls.
  + **Automatic Location Identification (ALI) systems and Master Street Address Guide (MSAG) databases**
    - **ALI** systems stored a pre-registered address associated with a landline caller.
      * When a 911 call is placed, ALI would retrieve the pre-stored location from its database and send it to PSAP.
    - **MSAG databases were** used to validate street names and match addresses with emergency service zones.
    - An ALI database stores a person's address linked to their phone number, while an MSAG acts as a reference list of all valid street address ranges within a community, essentially verifying if an address provided in the ALI database is accurate and can be used to properly route an emergency call to the correct PSAP; so, if someone dials 911 from a phone number associated with "123 Main Street" in the ALI, the system would consult the MSAG to confirm that "123 Main Street" exists within the designated emergency service zone before sending the call to the appropriate dispatcher.
    - **NG911 Replacement:**
      * **Location Information Server (LIS) & HELD Protocol:** Enables VoIP devices to dynamically retrieve location before a 911 call**.**
      * **Location Validation Function (LVF):** Uses real-time GIS-based validation for accurate caller location.

## 5.4 Assumptions for a Successful Transition to NG911

As stated by NENA-STA-010.3d, Clause 1 [1], the following underlying assumptions should be mentioned for clear understanding:

* **All calls entering ESInet must be SIP-based.**
  + Non-SIP calls must be converted before entering the network.
* **Access Network Providers must provide location services.**
  + DSL, fiber, and mobile network providers need location tracking mechanisms.
* **Emergency calls must include location information.**
  + Every 911 call must provide a location, even if only approximate (e.g., cell tower ID, GPS, Wi-Fi positioning).
* **GIS-based validation of locations replaces MSAG.**
  + Master Street Address Guide (MSAG) databases used in legacy 911 are being replaced by GIS (Geographic Information System) data.
* **Continuous Location Validation.**
  + Access networks must validate the caller’s location before allowing an emergency call to be placed.
  + The Location Validation Function (LVF) ensures addresses are formatted correctly and exist in GIS databases before calls reach NG911.
* **Interoperability with legacy networks.**
  + Not all PSAPs will transition to NG911 at the same time, requiring Legacy Network Gateways (LNGs) to act as a bridge.
  + LNGs ensure compatibility between NG911 ESInet and older PSTN-based 911 systems.
* **Federal, State, and Local Laws Need Updating.**
  + Current 911 regulations were designed for landlines and MSAG-based routing.
  + New policies must align with IP-based call routing, GIS validation, and multimedia emergency calls (text, video, sensor data).
* **International Compatibility Challenges.**
  + While NG911 is based on global IP standards, interconnecting telecom networks outside North America may face compatibility issues.

# 6. Threat Modeling and Risk Assessment of NG911 Functional Elements

The transition to Next Generation 911 (NG911) introduces enhanced capabilities for emergency response, but it also exposes systems to new cybersecurity risks. As NG911 relies on IP-based networks, it becomes more vulnerable to cyberattacks such as denial-of-service, unauthorized access, and man-in-the-middle attacks. Threat modeling and risk assessment are essential to identify, prioritize, and mitigate these risks, ensuring the security and reliability of NG911 systems in protecting public safety [B2].

For the remainder of this section, when referring to standard clauses as specified in i3 Document [1] Terminology section, the following must be noted:

* **MUST, SHALL, REQUIRED:** These terms mean that the definition is a normative

(absolute) requirement of the specification.

* **“MUST NOT”:** This phrase, or the phrase "**SHALL NOT**", means that the definition is an absolute prohibition of the specification.
* “**SHOULD**” This word, or the adjective "**RECOMMENDED**", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
* “**SHOULD NOT**” This phrase, or the phrase "**NOT RECOMMENDED**" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
* “**MAY**” This word, or the adjective "**OPTIONAL**", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides).

## 6.1 Foundations of Threat Modeling and Risk Assessment

Understanding the security posture of NG911 systems requires analyzing both the threats they face and the risks those threats pose. This foundational section defines key terms and explains the methodology used in this assessment.

**Threat:** A threat is any potential event or actor, malicious or accidental, that could exploit a vulnerability in a system to cause harm. In NG911, this includes attackers attempting to misroute calls, access sensitive data, or disrupt services.

**Vulnerability:** A vulnerability is a weakness or flaw in the system, such as outdated software, weak access controls, or exposed interfaces, that could be exploited by a threat to cause harm.

**Risk:** Risk is the potential impact that arises when a **threat successfully exploits a vulnerability**. It is commonly expressed as a combination of:

* **Likelihood:** How probable it is that a threat will occur.
  + **Low:** Rare or highly improbable given existing controls.
  + **Medium:** Possible under certain conditions or with moderate effort.
  + **High:** Likely to occur or be attempted by common threat actors.
  + **Very High:** Almost certain to occur or frequently observed in similar systems.
* **Impact:** The severity of the consequences if it does.
  + **Low:** Minimal disruption, easily recoverable, limited to individual components.
  + **Medium:** Noticeable service degradation or data exposure, moderate recovery effort.
  + **High:** Major disruption to services or compromise of sensitive information.
  + **Critical:** Catastrophic outcomes including system-wide failure, public safety risk, or loss of life.

Thus, **Risk = Likelihood × Impact.**

**Threat Modeling: T**he process of identifying potential adversaries, their goals, and the attack vectors they might use. This helps anticipate how an attacker might try to compromise NG911 services.

**Risk Assessment:** Risk assessment evaluates each identified threat in terms of its likelihood and potential impact, prioritizing mitigation efforts accordingly. For NG911, this means protecting critical functions like call routing, location validation, and PSAP access.

**Risk Rating Levels:** In this assessment, likelihood refers to the expected frequency or feasibility of a threat, while impact measures the severity of its consequence on public safety and NG911 service continuity.

**Risks are categorized as:**

* **Low:** Unlikely or less severe risks.
* **Medium:** Possible but less frequent threats with moderate impact.
* **High:** Frequent or feasible attacks with serious consequences.
* **Critical**: Likely or targeted attacks that may lead to catastrophic consequences (e.g., public safety failure, loss of life, major service outage).

## 6.2 Threat Modeling and Risk Impact Analysis of NG911 Functional Elements

The following subsections combine threat modeling (identifying potential attack vectors and adversary actions) with risk assessment (evaluating their impact on public safety and NG911 system integrity).

This assessment focuses on evaluating risk based on the core objectives and operational roles of each NG911 functional element. It does not comprehensively account for all required or recommended security controls from the i3 standard (e.g., mutual TLS, SRTP, access control policies). Additionally, implementation-specific protections, deployment variations, and emerging threat vectors may further influence the true risk exposure. Therefore, actual risk may be higher or lower depending on the extent to which security best practices and NENA/NG-SEC guidelines are followed.

6.2.1 Location Information Server (LIS)

**Impersonation of LIS (Spoofed Service):** An attacker pretends to be the legitimate LIS and responds with fake location data. This could mislead call routing or send responders to the wrong place. Such spoofing may enable swatting attacks or erode trust in the system’s accuracy. If location data is falsified early in the call setup, the entire emergency response could be misdirected.

**Location Spoofing & Data Tampering:** An attacker may try to modify or insert false location data in the LIS, such as spoofing a location update or intercepting an unsecured LIS transaction (e.g., a man-in-the-middle attack) [B2]. This could lead to incorrect addresses or coordinates. Fake or altered location data can misroute emergency calls or mislead first responders. In extreme cases, it could enable "swatting" attacks, where responders are sent to the wrong address [3]. This manipulation compromises 911 data, wastes response time, and can put lives at risk by diverting resources to fake incidents.

**Unauthorized Access & Data Breach:** The LIS holds sensitive caller location data, making it a high-value target. Unauthorized users, whether external intruders or malicious insiders, could query, extract, alter, or delete records [3], compromising confidentiality and data integrity. A breach could expose private location details or disrupt emergency response by corrupting address data. NENA Security for Next Generation 911 Standard [2] mandates strict access controls for NG911 systems like the LIS: “persons not authorized to view or modify information SHALL be prohibited from viewing or modifying information.” Without these safeguards, attackers could manipulate or erase data, causing calls to be misrouted or ignored—potentially delaying emergency assistance with life-threatening consequences [B2].

**Query Flooding & Denial of LIS Availability:** Adversaries may launch network or application-layer DoS attacks to overload the LIS or block its connectivity. For instance, flooding the LIS with location queries or exploiting protocol weaknesses could make it unresponsive. If the LIS cannot deliver location information when 911 calls arrive, the system may fall back to less accurate methods or no location at all. Call takers would then have to spend precious time determining caller location manually. Any such loss of availability in NG911 infrastructure can “prevent urgent requests from reaching a PSAP” or impair emergency response [3]. In short, a disabled LIS means first responders might be dispatched late or to incorrect locations, elevating the risk of property damage or loss of life.

Table 6.2.1. Threat Analysis and Risk Assessment Summary – Location Information Server (LIS)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Threat Scenario | Likelihood | Impact | Risk Level | Business Impact | Mitigation |
| Impersonation of LIS (Spoofed Service): An adversary spoofs the LIS service to send false location data, misleading responders and potentially misrouting emergency calls | **Low** | **Critical** | **High** | Could reduce public confidence in 911 reliability, produce formal complaints or lead to emergency units being misdirected (i.e. “swatting”) | Enforce mutual TLS, validate endpoints with digital certificates |
| Location Tampering: An adversary modifies or corrupts legitimate location data in the LIS, causing responders to be sent to incorrect or fake addresses (e.g., swatting). | **Low** | **Critical** | **High** | May lead to emergency units being misdirected (i.e. “swatting”), causing response delays | Apply data integrity checks, secure data transmission with encryption, use digital signatures for location updates |
| Unauthorized access or data breach: An adversary gains unauthorized access to the LIS database to view, extract, or tamper with sensitive caller location data, leading to privacy violations and service disruptions. | **Low** | **High** | **Medium** | Leaked location data may violate caller privacy and reduce trust in the 911 system. | Enforce role-based access control (RBAC), encrypt data at rest and in transit, conduct regular security audits |
| Denial of Service via query flooding: An adversary floods the LIS with location requests or malformed queries, overwhelming the system and delaying accurate location resolution for 911 calls. | **Medium** | **High** | **High** | Slower responses could overwhelm call takers and disrupt call-handling operations | Implement rate limiting and network firewalls, validate input queries, deploy redundant LIS nodes for availability |

#### Risk Rating Reasoning

* **Service impersonation:** NG911 employs authentication and secure channels, so posing as the LIS is very difficult (**low likelihood**). If it were to happen, false location data from a spoofed LIS could send emergency resources to incorrect locations “swatting” (**Critical impact**).
  + **Business impact:** May cause loss of public trust, lead to complaints and might have same impact as location tampering.
* **Location tampering:** Compromising the LIS database requires overcoming strong security controls (**low likelihood**). However, any corruption of location information can misroute responders to the wrong place “swatting”, a potentially life-threatening outcome (**Critical impact**) [8].
  + **Business impact:** Could result in “swatting” and delays in service.
* **Unauthorized access:** While LIS interfaces are typically restricted, a determined attacker could target them via network or credential attacks (**low likelihood**). The exposure of precise caller location data is a serious privacy breach and could be misused (**high impact**) [8].
  + **Business impact:** May expose sensitive location data and lead to loss of confidence in emergency services.
* **DDoS on LIS:** While DDoS attacks can occur, NG911 systems are designed with increased resiliency, redundancy, and security measures to minimize the risk. That said, an attack on the LIS could still happen, especially if the system is not properly hardened or protected against such threats (**medium likelihood**) [8]. If the LIS is knocked offline, 911 call routing and response would be highly affected due to lack of reliable location info, but they can fallback to legacy location information systems or may have to rely on the caller to provide their location verbally (**high impact**).
  + **Business Impact:** May increase pressure on call centers and cause delays in service.

6.2.2 Location Validation Function (LVF)

**GIS Data Tampering & Address Validation Corruption:** The LVF relies on up-to-date GIS data (road networks, address points, etc.) to validate addresses. An attacker or insider could tamper with the underlying GIS data or the LVF’s configuration. If the validation data is poisoned (e.g. street names altered, address ranges incorrect), the LVF might reject legitimate addresses or approve wrong ones. This can result in misrouting calls, emergency calls might be routed to the wrong Public Safety Answering Point (PSAP) or not recognized at all.

**Uncontrolled Queries & Unauthorized Access to Validation Services:** The LVF, a critical query service for address validation, must be protected by strong access controls. If exposed, attackers could exploit it to run scripted queries, manipulate results, or overwhelm the service to disrupt availability. For instance, querying randomized addresses could let them harvest valid locations or infer jurisdictional boundaries. Even though address data is less sensitive than personal data, such misuse still poses security and privacy risks. Administrative access could allow attackers to alter or disable the LVF. NENA Security for Next Generation 911 and NG911 security best practices recommend proper authentication and query rate-limiting to ensure only trusted 911 systems can access it [2, 3].

**Address Validation Overload & Denial of Service:** LVF needs to validate addresses quickly to support real-time 911 call setup [4], making it vulnerable to performance issues. Attackers could flood it with queries or exploit protocol flaws (e.g., in HTTP/LoST), causing denial-of-service. An overwhelmed LVF can delay or prevent address validation, leading to fallback routing or manual verification—both of which slow emergency response. A DoS attack on components like the LVF could “disable PSAP operations” or significantly impair them [3] [B2]. Redundancy and strong input validation are essential to mitigate this risk.

Table 6.2.2. Threat Analysis and Risk Assessment Summary – Location Validation Function (LVF)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Threat Scenario | Likelihood | Impact | Risk Level | Business Impact | Mitigation |
| GIS Data Tampering & Address Validation Corruption: An adversary tampers with GIS data or the validation logic, causing the LVF to mis validate addresses and misroute emergency calls. | **Low** | **Critical** | **High** | May cause dispatch routing errors, leading to emergency response delays or swatting-like incidents | Control access to GIS data, enforce version management, perform periodic integrity validation |
| Uncontrolled Queries & Unauthorized Access to Validation Services: An adversary abuses or gains access to the LVF interface to run mass queries or tamper with validation functions, exposing location patterns or degrading performance. | **Medium** | **Medium** | **Medium** | May slow validation services and expose address patterns, raising privacy concerns | Implement authentication and logging, enable anomaly detection, restrict queries by source |
| Address Validation Overload & Denial of Service: An adversary floods the LVF with excessive or malformed queries, overwhelming the service and delaying call routing during active emergencies. | **Medium** | **High** | **High** | Could delay call routing and overwhelm PSAPs, reducing emergency response efficiency | Deploy redundant LVF servers with load balancing, harden protocols, sanitize inputs from upstream systems |

#### Risk Rating Reasoning

* **GIS Data Tampering & Address Validation Corruption:** The LVF relies on authoritative GIS data, which is usually tightly controlled, so malicious modifications are unlikely (**low likelihood**). If it did occur, some legitimate addresses might fail validation or false ones might pass, potentially delaying or misrouting calls for those locations “swatting” (**Critical impact**).
  + **Business impact:** Manipulated validation data could result in misrouted calls or swatting-like incidents and delaying response.
* **Uncontrolled Queries & Unauthorized Access to Validation Services:** An attacker with access to the LVF’s interface might try to enumerate the address database (**medium likelihood if access controls are weak**). While address data is not highly confidential, large-scale exposure could reveal sensitive location patterns or private facility information, though direct harm is limited (**medium impact**).
  + **Business impact:** May degrade validation service performance and expose internal address data patterns, leading to operational delays and privacy concerns.
* **Address Validation Overload & Denial of Service:** The LVF is an online service and could be subject to denial-of-service (e.g. excessive queries), especially in an IP environment (**medium likelihood**). If the LVF is unavailable, new or updated address validations cannot be performed, which could hinder call routing for unvalidated addresses, but existing validated addresses could still be used for routing, minimizing the disruption (**high impac**t).
  + **Business impact:** Call setup delays could overwhelm PSAP operations and reduce the ability to respond to real emergencies promptly.

6.2.3 Border Control Function (BCF)

**Network Access Bypass via Credential or IP Spoofing:** The BCF is designed to identify and block unauthorized sources, but attackers may bypass it by spoofing legitimate networks or exploiting misconfigurations. Techniques like using stolen credentials or mimicking valid carrier IPs can fool BCF admission controls, allowing entry into the system. Once inside, attackers may inject fraudulent 911 calls, launch TDoS attacks, or target internal components with malware. NENA’s NG-SEC information document states that all external connections must be protected by a BCF—there are no inherently “trusted” networks, and even interconnecting ESInets must each deploy their own BCFs [7]. If vulnerabilities exist, attackers may bypass screening mechanisms or falsely assign priority to malicious calls.

**Telephony Denial-of-Service (TDoS) & Call Spoofing Attacks:** A special category of DoS, TDoS involves flooding the call system with a high volume of fake call traffic rather than raw network packets. The BCF, often coupled with an intrusion detection system, is on the front line of detecting and mitigating TDoS. Attackers may cycle through source numbers or use bots to place thousands of fake 911 calls. Without mitigation, a TDoS can tie up all call takers, making it impossible for real 911 callers to get through – a direct threat to public safety. The BCF is designed to help by marking or filtering suspicious call traffic. NENA’s NG-SEC information document even allow the BCF to tag calls as suspicious so that the PRF/ESRP can route them differently (for example, to a secondary queue) [7]. Additionally, PSAPs can feed back information on “bad actor” callers to block repeat offenders at the border [7]. However, these defenses must be finely tuned: if too strict, they might drop legitimate calls; if too flexible, attack calls still flood in [7]. Attackers will try to exploit that balance, making their calls appear legitimate.

**Denial-of-Service (DoS) & Overload:** BCF is the first line of defense against malicious traffic such as DDoS attacks or floods of fake call setup requests. Attackers may overwhelm the BCF with excessive data, malformed packets, or rapid call attempts. A successful DoS on the BCF can mitigate or block 911 call handling across a region. Even with sufficient ESInet capacity, the BCF’s processing and filtering rules may become a bottleneck under attack, causing delays or call failures. Distributed attacks can be executed at scale against NG911 components [3] [B2].

Table 6.2.3. Threat Analysis and Risk Assessment Summary – Border Control Function (BCF)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Threat Scenario | Likelihood | Impact | Risk Level | Business Impact | Mitigation |
| Network Access Bypass (Credential/IP Spoofing): An adversary spoofs trusted IP addresses or uses stolen credentials to bypass BCF filters, gaining access to the ESInet and injecting fake calls or malicious traffic into emergency systems. | **Low** | **Critical** | **Medium** | Fake or malicious calls might enter the system, putting emergency services at risk and reducing public trust | Enforce mutual TLS, strict certificate validation, IP filtering, and role-based access enforcement |
| Telephony DoS (TDoS) & Call Spoofing: An adversary floods the call system with spoofed or fake 911 calls using bots or rotating caller IDs, saturating PSAP queues and blocking real emergencies from getting through. | **Medium** | **Critical** | **High** | Fake calls can disrupt the system, preventing real 911 calls from getting through and delaying emergency help | Use SIP-aware TDoS filtering, apply STIR/SHAKEN, enable suspicious call tagging and dynamic routing controls |
| Denial-of-Service (DoS) & Overload: An adversary overwhelms the BCF with excessive or malformed network traffic, such as SIP floods or UDP bursts, causing the system to drop or delay legitimate 911 calls due to processing bottlenecks. | **Medium** | **Critical** | **High** | Too much traffic can block or slow down 911 services, causing major service interruptions during emergencies | Rate Limiting, anomaly detection, deploy redundant BCF nodes with load balancing |

#### Risk Rating Reasoning

* **Network Access Bypass via Credential or IP Spoofing:** If a BCF is not configured to strictly authenticate upstream connections (e.g., via TLS mutual authentication and IP filtering), attackers can spoof legitimate entry points (**low likelihood**, especially with hardened systems). However, if exploited, adversaries could inject fake calls or malware into ESInet (**critica**l **impact**).
  + **Business Impact:** This could result in fake emergency calls or harmful content being allowed into the system, potentially putting real emergency services at risk and undermining public trust.
* **Telephony Denial-of-Service (TDoS) & Call Spoofing Attacks:** Unlike raw packet floods, TDoS uses valid-looking call setups with fake numbers or recycled identities. This makes detection harder. Attackers may spoof thousands of caller IDs using bots (**medium likelihood**). Call queues can be fully saturated, preventing real calls from reaching a PSAP (**critica**l **impact**). STIR/SHAKEN, dynamic filtering, and suspicious call tagging help mitigate this.
  + **Business Impact:** real 911 calls may not get through. This overwhelms call takers, causes delays, and can seriously affect public safety; possibly leading to missed or delayed responses.
* **Denial-of-Service (DoS) & Overload:** Attackers can send large volumes of traffic (e.g., malformed SIP messages, UDP floods) to overwhelm BCF capacity. NG911 networks are designed to be resilient, but a targeted flood may still succeed (**medium likelihood**). If BCF is unavailable, the entire ESInet entry point is affected, blocking or delaying emergency calls (**critica**l **impact**).
  + **Business Impact:** This can block, or slow down emergency calls on a regional scale, disrupting services and increasing operational pressure during critical moments.

### 6.2.4 Emergency Call Routing Function (ECRF)

**GIS Data Corruption & Routing Misdirection:** The ECRF relies on a geospatial database (maps of streets, address points, boundaries) to route 911 calls. An attacker might try to alter or poison this routing data, causing 911 calls to be misrouted to the wrong PSAP or location. Because emergency location records are valuable, attackers (even nation-states) could target ECRF databases to disrupt services or steal information [5]. Compromised routing data would delay or misdirect responders, so protecting the integrity of the ECRF’s GIS data is critical.

**Unauthorized ECRF Access & Call Manipulation:** The ECRF should only be queried by trusted systems, but a cyber intruder or malicious insider could try to access it directly. Unauthorized access might allow someone to reroute calls or harvest sensitive location data. For example, using digital certificates and encryption, as specified by NENA standards [1], helps ensure only valid 911 authorities can interact with the ECRF, reducing the risk of misuse or data breaches.

**Routing Lookup Failure via Denial of Service:** If the ECRF is overwhelmed or went offline, it cannot look up where to send incoming emergency calls. A DoS attack on the ECRF could prevent calls from being routed to any PSAP, effectively blocking callers from reaching help [5]. This risk to availability means NG911 systems must have redundant ECRF servers and network safeguards. In fact, a recent academic study was dedicated to analyzing DoS attacks against NG911, highlighting how serious this threat is [6].

Table 6.2.4. Threat Analysis and Risk Assessment Summary – Emergency Call Routing Function (ECRF)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Threat Scenario | Likelihood | Impact | Risk Level | Business Impact | Mitigation |
| GIS Data Corruption & Routing Misdirection: An adversary tampers with the ECRF’s geospatial routing data, causing emergency calls to be sent to the wrong PSAP or a non-existent location. | **Low** | **Critical** | **High** | May cause calls to be misrouted (i.e. “swatting”), delaying emergency help and damaging reputation | Apply strict access controls, use digital signatures for GIS data, enable audit logging for route changes |
| Unauthorized ECRF Access & Call Manipulation: An adversary gains unauthorized access to the ECRF and uses it to view caller data or manipulate routing responses, undermining system trust and data confidentiality. | **Low** | **High** | **Medium** | May expose caller data reducing trust in emergency systems | Enforce mutual TLS, restrict ECRF queries to authenticated systems, configure strict firewall rules |
| Routing Lookup Failure via Denial of Service: An adversary floods the ECRF with excessive or malformed requests, crashing or stalling the system and forcing default routes. | **Medium** | **Medium** | **Medium** | May block emergency calls and overload backups, causing major service disruption | Deploy redundant ECRF nodes, enable rate-limiting and anomaly detection on incoming queries |

#### Risk Rating Reasoning

* **GIS Data Corruption & Routing Misdirection:** Directly compromising the ECRF’s data store is difficult due to strong safeguards (**low likelihood**). If it happened, 911 calls could be routed to wrong or nonexistent PSAPs until detected, a critically dangerous situation (**critical impact**). Emergency calls might go unanswered or be sent to the wrong center, delaying help when every second counts.
  + **Business Impact:** May cause calls to be routed to the wrong PSAP, leading to critical delays and reputational damage.
* **Unauthorized ECRF Access & Call Manipulation:** ECRF queries contain caller location information and the corresponding PSAP route. It’s improbable for an outsider to tap into this traffic on a secured ESInet (**low likelihood**). If it did occur (for instance, on an unencrypted link), the attacker would obtain sensitive location data for ongoing emergencies [8], compromising caller privacy (**high impact**).
  + **Business Impact:** Could leak sensitive caller data or result in calls being tampered with, eroding trust in emergency services.
* **Routing Lookup Failure via Denial of Service:** Attackers could try to overwhelm the ECRF with excessive requests or exploit a vulnerability to crash it (**medium likelihood**). A downed ECRF means the system can’t determine where to send calls precisely; calls might default to backup routes (**medium impact**).
  + **Business Impact:** May block or delay 911 calls, fallback to default routes systems.

### 6.2.5 Policy Routing Function (PRF)

**Metadata Spoofing to Evade Policy Filters:** The PRF uses triggers like call origin, type, or time to make routing decisions, including filtering suspicious traffic. Attackers may attempt to bypass these controls by spoofing call metadata to appear legitimate or high priority. This tactic can allow malicious traffic to evade filters, effectively neutralizing policy-based defenses. If successful, such spoofing could enable a sustained telephony denial-of-service (TDoS) attack, overwhelming PSAPs despite mitigation rules. NENA’s NG-SEC information document [7] warns that “poor policy decisions, oversight, or technical implementation may have significant negative effects on the security of the ESInets”, while DHS has identified NG911 as susceptible to TDoS, where PSAPs are flooded with fake calls, disrupting emergency services [3].

**Routing Policy Tampering & Rule Manipulation:** The PRF draws on a policy store (a set of configured rules). An attacker who gets access to the NG911 core or an admin interface could attempt to change, add, or remove routing rules. Malicious changes to PRF rules could be catastrophic – calls might be re-routed to incorrect destinations or dropped entirely. For instance, an attacker could insert a rule that sends certain 911 calls to a dead-end or wrong number, causing those callers to never reach help. The integrity of the PRF is thus critical. NENA’s NG-SEC information document [7] would classify the policy store as a sensitive asset requiring tight access control and change management as stated “It is important that policies be securely stored, and mechanisms that control who can modify policies be secure”. Even unintentional misconfiguration (human error) is a risk here; therefore, robust authentication and oversight on any PRF rule changes are needed to prevent accidental or deliberate misrouting of emergencies. The consequence of policy tampering is misdirection of calls or outages in 911 service, directly putting lives and property at risk due to delayed response.

**Service Disruption via Routing Logic Overload:** Beyond data tampering, an adversary might simply attempt to crash or disable the PRF/ESRP function. This could be via flooding the ESRP with malformed SIP messages or exploiting a vulnerability in the policy processing engine (a form of protocol abuse). If the ESRP is overwhelmed or fails, NG911 call routing could revert to basic or static rules or stop entirely if the ESRP is down. As the PRF is “the primary routing component” of the ESRP [4], its failure can effectively bring down dynamic call routing in the region. Calls might not be properly distributed to backup centers during high load or could all pile onto a single center, causing call queues and dropped 911 calls. This single point of failure scenario is why NG911 best practices emphasize **resilience and redundancy** for core services [B2]. Any sustained disruption to the PRF undermines the smarter routing that NG911 promises, potentially resulting in slower responses especially during major incidents when policy-based routing (like overflow to other PSAPs) is most needed.

Table 6.2.5. Threat Analysis and Risk Assessment Summary – Policy Routing Function (PRF)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Threat Scenario | Likelihood | Impact | Risk Level | Business Impact | Mitigation |
| Metadata Spoofing to Evade Policy Filters: An adversary spoofs call metadata (e.g., priority flags, jurisdiction info) to make fake calls appear legitimate, bypassing PRF filters and overwhelming PSAPs with false traffic. | **Medium** | **High** | **High** | May allow fake calls to bypass filters and flood emergency lines, slowing real responses. | Validate call metadata, enforce STIR/SHAKEN, implement anomaly detection and logging |
| Routing Policy Tampering & Rule Manipulation: An adversary with admin access or an intentional/unintentional admin mistake tampers with the PRF’s routing rules, misdirecting or dropping real 911 calls and potentially causing large-scale service failures. | **Low** | **Critical** | **High** | Can result in real 911 calls being misrouted (i.e “swatting”) or dropped, leading to service failures. | Role-based access control, multi-factor admin authentication, policy change auditing |
| Routing Logic Overload & PRF Disruption: An adversary floods the PRF or its associated ESRP with malformed SIP messages or exploits routing logic, overloading call routing systems and delaying emergency response. | **Medium** | **Critical** | **High** | May overwhelm routing systems, causing delays or outages in emergency call handling. | Protocol hardening, input validation, redundant PRF nodes, load balancing |

#### Risk Rating Reasoning

* **Metadata Spoofing to Evade Policy Filters:** Attackers can craft calls that appear high priority (**medium likelihood**) by faking metadata (e.g., emergency flags, jurisdiction). This is moderately likely due to SIP flexibility. If successful, it bypasses PRF filtering and overwhelms call takers (**high impact**). STIR/SHAKEN can authenticate caller identity in SIP-based environments.
  + **Business Impact:** Could lead to fake emergency calls bypassing filters, overwhelming PSAPs and delaying real help.
* **Routing Policy Tampering & Rule Manipulation:** Tampering with routing logic (e.g., changing where emergency calls go) could be **catastrophic**. It requires admin-level access (**low likelihood**), but a single bad rule could drop or misroute all calls “swatting” (**critical impact**). This demands strong admin controls and audit trails.
  + **Business Impact:** A single misconfigured or malicious rule could result in real 911 calls never reaching responders.
* **Routing Logic Overload:** Unlike raw packet floods, TDoS uses valid-looking call setups with fake numbers or recycled identities. This makes detection harder. Attackers may spoof thousands of caller IDs using bots (**medium likelihood**). Call queues can be fully saturated, preventing real calls from reaching a PSAP (**critical impact**). STIR/SHAKEN, dynamic filtering, and suspicious call tagging help mitigate this.
  + **Business Impact:** May cause widespread delays in emergency call handling, reducing public trust and risking lives

### 6.2.6 Emergency Services Routing Proxy (ESRP)

**Signaling Spoofing & Call Interception:** The ESRP relies on IP protocols like SIP to manage calls, which exposes it to risks such as spoofing and man-in-the-middle attacks. An attacker could impersonate a trusted network or inject false signaling to misroute calls, intercept call setup messages, or alter caller data in transit. NG911 components are susceptible to such network-based attacks if not properly secured [B2].

**Call Flooding via SIP-Based DDoS:** The ESRP is the call-routing engine of NG911 – it decides which PSAP to send a 911 call to. Attackers can attempt to overload an ESRP by flooding it with a **huge number of fake call setup requests** (a distributed denial-of-service attack). This barrage could slow down or crash the routing function, delaying real emergency calls. DoS threats such as call flooding are well-recognized and considered a major risk to NG911 availability [6].

Table 6.2.6. Threat Analysis and Risk Assessment Summary – Emergency Services Routing Proxy (ESRP)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Threat Scenario | Likelihood | Impact | Risk Level | Business Impact | Mitigation |
| Signaling Spoofing & Call Interception: An adversary impersonates a trusted network device or manipulates SIP signaling to misroute or intercept emergency calls, potentially altering or leaking sensitive call setup data. | **Low** | **Critical** | **High** | May cause calls being misrouted (i.e “swatting”) or intercepted calls, leading to service failures, privacy concerns and loss of trust | Enforce TLS with mutual authentication, validate certificates, Enforce STIR/SHAKEN where applicable |
| Call Flooding via SIP-Based DDoS: An adversary floods the ESRP with a high volume of fake SIP call setup requests, exhausting processing capacity and disrupting the routing of legitimate 911 calls. | **Medium** | **Critical** | **High** | Could delay or block emergency calls, overwhelming services and impacting public safety | Enable SIP-aware rate-limiting and anomaly detection, deploy redundant ESRP nodes with load balancing |

#### Risk Rating Reasoning

* **Signaling Spoofing & Call Interception:** SIP and related signaling protocols can be spoofed unless protected by strong authentication. Attackers may impersonate trusted sources to inject or intercept call setup messages. While protections like TLS are increasingly mandated, weakly configured or legacy endpoints might still be vulnerable (**Low likelihood**). The potential consequences include call misrouting, metadata manipulation, or eavesdropping (**critical impact**). NG911 systems mitigate this with encryption, mutual TLS, and STIR/SHAKEN where voice identity spoofing is relevant, which verifies caller identity in SIP environments.
  + **Business Impact:** May lead to calls being routed incorrectly or intercepted, risking privacy breaches and loss of service trust.
* **Call Flooding via SIP-Based DDoS:** SIP signaling is inherently vulnerable to volume-based denial-of-service attacks, lightweight to send (e.g., flood with minimal bandwidth) but relatively expensive to process for servers parsing headers, managing state. While NG911 ESRPs are expected to implement load-balancing and backup proxy systems, a well-timed and distributed SIP flood can still degrade or halt routing decisions (**medium likelihood**). If real 911 calls are delayed or dropped due to overload, the impact is immediate and critical, delayed dispatch or no response at all (**critical impact**).
  + **Business Impact:** Could overwhelm routing functions, causing dropped or delayed 911 calls, with direct public safety and reputational consequences.

### 6.2.7 Legacy Network Gateway (LNG)

**Protocol Conversion Vulnerabilities:** The LNG bridges legacy TDM (Time-Division Multiplexing) systems with the IP-based NG911 core by translating legacy call signaling into SIP. Malformed legacy signals or improperly handled protocol conversions can disrupt call routing or introduce vulnerabilities into the ESInet. If the LNG processes signaling incorrectly, calls may be dropped or misrouted, and malformed inputs might lead to denial-of-service or SIP stack exploitation [1-3].

**Legacy Traffic Injection via Insufficient Security Controls:** Since LNGs handle traffic from older, non-IP networks, they often lack modern authentication and encryption. If not properly secured, attackers could spoof call signaling or inject fake calls from the legacy side. The LNG might pass spoofed or malicious traffic into the ESInet without proper validation, enabling Telephony Denial-of-Service (TDoS) or caller impersonation attacks. NENA Security for Next Generation 911 Standard [2] strictly enforces security controls even on gateway components to prevent legacy traffic from becoming an attack vector as stated “All NG911 entities SHALL deploy a Next Generation Firewall or SBC at all ingress and egress points not just in the ESInet”.

Table 6.2.7. Threat Analysis and Risk Assessment Summary – Legacy Network Gateway (LNG)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Threat Scenario | Likelihood | Impact | Risk Level | Business Impact | Mitigation |
| Protocol Conversion Vulnerabilities: An adversary sends malformed or ambiguous legacy call signals that are misinterpreted by the LNG, leading to dropped or misrouted 911 calls during protocol translation. | **Medium** | **Critical** | **High** | Misrouted or dropped 911 calls may disrupt emergency response operations. | Input validation, protocol conformance checks, hardened SIP stacks |
| Legacy Traffic Injection via Insufficient Security Controls: An adversary spoofs legacy call signals from untrusted TDM sources, injecting fake calls into the NG911 system and enabling TDoS or impersonation attacks. | **Medium** | **Critical** | **High** | Fake or spoofed calls can overload systems and reduce trust in emergency services. | Endpoint whitelisting, Enforce STIR/SHAKEN where applicable |

#### Risk Rating Reasoning

* **Protocol Conversion Vulnerabilities:** Malformed legacy signaling can crash SIP processing or result in misrouted calls (**medium likelihood**). While not trivial to exploit, protocol translation logic is complex and may fail with unexpected inputs. A failure here can drop or misdirect emergency traffic (**critical impact**).
  + **Business Impact:** May result in dropped or misrouted emergency calls, causing confusion, service delays, and potential public safety risks.
* **Legacy Traffic Injection via Insufficient Security Controls:** Legacy systems often lack authentication, allowing spoofed signaling from the TDM side (**medium likelihood**). Attackers could inject fake calls or impersonate real ones. If passed into the ESInet, this can enable TDoS or caller impersonation (**critical impact**).
  + **Business Impact:** Unchecked fake traffic from legacy systems could overwhelm call systems or mislead responders, harming response efficiency and public trust.

### 6.2.8 Legacy PSAP Gateway (LPG)

**Unsecured RTP Bridging & Media Path Compromise:** The LPG connects NG911 call flows to legacy PSAPs that cannot natively receive SIP/IP calls. It often bridges audio between RTP (real-time IP media) and analog voice. If not secured properly, this bridging point could be exploited for call interception or media injection. Attackers might exploit insecure media relays to eavesdrop or inject noise into calls. NENA Security for Next Generation 911 Standard [2] requires encryption and access controls to protect these interconnection points.

**DoS-Induced Isolation of Legacy PSAPs:** Because LPGs are transitional components, their failure can sever communication between modern NG911 services and PSAPs still operating on legacy systems. A DoS attack or misconfiguration at the LPG could isolate PSAP from all incoming NG calls. This would delay emergency response, especially in jurisdictions still completing NG911 migration.

Table 6.2.8. Threat Analysis and Risk Assessment Summary – Legacy PSAP Gateway (LPG)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Threat Scenario | Likelihood | Impact | Risk Level | Business Impact | Mitigation |
| Unsecured RTP Bridging & Media Path Compromise: An adversary intercepts or injects media (audio, text, video) into calls bridged between IP and analog systems, exploiting unsecured RTP relays to compromise call integrity or privacy. | **Medium** | **High** | **High** | Call media (text, audio, video) may be intercepted or altered, potentially leading to privacy issues or response delays. | TLS for SIP, Use SRTP and SRTCP for secure media transport, access controls, encryption in transit |
| DoS-Induced Isolation of Legacy PSAPs: An adversary launches a DoS attack or triggers a misconfiguration on the LPG, severing the connection between NG911 and legacy PSAPs and preventing emergency calls from reaching responders. | **Medium** | **Critical** | **High** | Legacy call centers may become unreachable, blocking emergency access in affected regions. | Redundant LPGs, traffic filtering |

#### Risk Rating Reasoning

* **Unsecured RTP Bridging & Media Path Compromise:** Legacy PSAP Gateways bridge IP and analog voice, often using RTP. If this path is not protected (e.g., lacks encryption or ACLs), attackers may intercept or inject audio streams (**medium likelihood**). This could result in eavesdropping or false information being inserted into emergency calls (**high impact**). Encryption of RTP streams and strong access control mitigate this risk.
  + **Business Impact:** Attackers could eavesdrop or inject false audio, leading to privacy concerns or misinformed response decisions
* **DoS-Induced Isolation of Legacy PSAPs:** Since some PSAPs still depend on LPGs to receive calls, disruption here could cut them off from NG911 entirely (**medium likelihood**). The impact is severe. 911 calls may not reach call takers at all (**critical** **impact**). Redundancy, secure configuration, and real-time monitoring help prevent or quickly recover from such outages.
  + **Business Impact:** Disruption could completely isolate legacy call centers, preventing emergency calls from reaching responders.

### 6.2.9 Public Safety Answering Point (PSAP)

**Unauthorized Access & Data Breaches:** PSAPs manage highly sensitive data, and unauthorized access—whether by hackers or insiders, can lead to theft or misuse. Due to NG911’s interconnected design, a breach in one area can impact others. The consequences include privacy violations, safety risks, and loss of public trust. To reduce these risks, best practices include strict authentication, role-based access, logging, and regular vulnerability assessments. Both NENA’s NG-SEC information document and the national NG911 program recommend such measures through self-assessment tools and checklists [7] [B5].

**System Compromise via Malware & Ransomware:** NG911 centers operate over IP networks like typical IT systems, making them vulnerable to common cyber threats. Malware can get into a PSAP’s network through phishing emails or infected files, such as images or videos sent by callers [B3]. Once inside, it could disrupt call-handling systems or leak sensitive information. Ransomware poses an even greater risk; it can lock down 911 and dispatch systems until payment is made. Real incidents, like the Suffolk County, NY attack, forced call-takers to revert to pen and paper [B4]. To protect against this, PSAPs must follow strong cybersecurity practices: updated antivirus software, segmented networks, regular data backups, and phishing awareness training. NG911 cybersecurity reports identify malware and ransomware as major threats to emergency services [B4].

**Telephone Denial of Service (TDoS):** Attackers can overwhelm 911 centers by flooding them with fake calls using auto-dialers or botnets. These false calls fill up the lines, preventing real emergency calls from getting through, which can delay help and put lives at risk [5]. Since NG911 supports multiple call types (like voice and text), attacks could come from several channels at once. To defend against this, PSAPs should work with phone carriers and use call-filtering tools to spot and block large volumes of fake calls.

Table 6.2.9. Threat Analysis and Risk Assessment Summary – Public Safety Answering Point (PSAP)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Threat Scenario | Likelihood | Impact | Risk Level | Business Impact | Mitigation |
| Unauthorized Access & Data Breaches: An adversary or insider gains unauthorized access to PSAP systems, exfiltrating or tampering with sensitive emergency call data, harming privacy and trust. | **Medium** | **High** | **High** | May expose sensitive emergency data, leading to loss of public trust and legal risk. | Role-based access, multi-factor authentication, audit logging, vulnerability assessments |
| System Compromise via Malware or Ransomware: An adversary delivers malware (e.g., via phishing emails or media files), compromising PSAP systems or locking them with ransomware, halting dispatch operations. | **Medium** | **Critical** | **High** | May halt 911 services and force costly downtime or manual operation. | Network segmentation, backups, staff training, antivirus, phishing prevention |
| Telephone Denial of Service (TDoS): An adversary floods PSAP lines with spoofed or automated calls from multiple media types, preventing legitimate emergency callers from reaching assistance. | **Medium** | **Critical** | **High** | May prevent real 911 calls from going through, causing public safety consequences. | Suspicious call tagging, Enforce STIR/SHAKEN where applicable, call filtering, dynamic rate-limiting |

#### Risk Rating Reasoning

* **Unauthorized Access & Data Breaches:** Attackers or insiders may access or exfiltrate sensitive caller or incident data through weak authentication or unmonitored accounts (**medium likelihood**). The breach of confidential public safety records leads to legal, ethical, and operational damage (**high impact**). Strong authentication, access control, and regular audits can significantly lower this risk.
  + **Business Impact:** Could compromise sensitive data and harm public confidence in PSAP security.
* **System Compromise via Malware & Ransomware:** PSAPs operate like standard IT environments, making them susceptible to malware via phishing, infected files, or lateral movement from connected systems (**medium likelihood**). Ransomware can lock down systems, call logs, or dispatch tools, completely halting emergency operations (**critical impact**). Segmentation, anti-malware defenses, and backup protocols are critical.
  + **Business Impact:** May force emergency services to operate manually, causing delays and resource strain.
* **Telephone Denial of Service (TDoS):** NG911 supports multiple media types (voice, SMS, video), making it vulnerable to coordinated TDoS attacks from botnets or spoofed caller IDs (**Medium likelihood**). If 911 lines are flooded with fake calls, real emergencies may be delayed or missed entirely (**critical impact**).
  + **Business Impact:** Can prevent critical calls from being answered on time or not answered at all.

### 6.2.10 Security Considerations Across NG911 Components

Like any software-based system, NG911 core components can have software bugs, misconfigurations, or outdated code that expose them to exploitation. An attacker who discovers a vulnerability in one of these components might exploit it to crash the service, disrupt routing logic, bypass security controls, or gain unauthorized access to sensitive data. For example, a compromised ESRP could misroute or drop calls. According to NENA’s NG-SEC information document [7], **all** **NG911 system software** **must** be kept up to date, hardened against attack, and subject to regular security testing to ensure resilience against both known and emerging exploits. Proper software patching and vulnerability management are essential to maintaining system integrity and availability across the entire NG911 architecture.

When someone makes an emergency call using voice, video, or real-time text, that media needs to travel securely over the network. In the NENA-STA-010.3d [1], this is done using a protocol called RTP, which carries the actual media content, and runs over a fast but connectionless method called UDP. However, RTP on its own does not provide security. To protect the call from eavesdropping or tampering, the NENA-STA-010.3d [1] requires that all media be encrypted using SRTP (Secure Real-Time Transport Protocol), with encryption keys exchanged securely using DTLS (Datagram TLS). Additionally, during a call, devices often send control messages that report on quality, like how many packets were lost or how much delay was observed. These control messages are sent using a related protocol called RTCP. To protect those messages, the secure version, SRTCP, is also required. While every system in the ESInet must be able to support RTCP and SRTCP, it's not strictly required that RTCP messages are always sent; the standard highly recommends that they are, since they help with call quality monitoring and troubleshooting. So, even if RTCP isn't always present in every call, systems must be prepared to handle it securely whenever it is.

To reduce these risks, NENA’s NG-SEC information document [7**]** requires all NG911 entities such that:

* **SHALL** maintain a documented backup plan and recovery procedures.
* **SHALL** test backup plans **annually at minimum.**
* Perform regular software updates, vulnerability checks, and replace insecure protocols (e.g., Telnet with SSH.
* Keep hardware and software up to date as part of ongoing maintenance
* Replace unsupported (end-of-life) devices.
* Conduct periodic security audits, including access control reviews and disabling unused ports.
* For legacy systems interoperability: NENA Security for Next Generation 911 Standard [2] advises enforcing security controls even on gateway components to prevent legacy traffic from becoming an attack vector as stated “All NG911 entities SHALL deploy a **Next Generation Firewall** or **SBC** at all ingress and egress points not just in the ESInet”.
* As specified in NENA-STA-010.3d [1], clause 2.8.1, 3.1.9 respectively:
  + "HTTP Transport i3 Services which use HTTP MUST support HTTP over TLS (HTTPS) (RFC 2818) [9]. The services, unless specified otherwise, MUST support HTTP/1.1 (RFC 7230) [10] and SHOULD support HTTP/2.0 (RFC 7540) [11]. Clients and servers MUST support TLS 1.2 [12], MAY support TLS 1.3 [13] or greater and MUST NOT offer or accept TLS 1.1 [15] or TLS 1.0 [14]. Perfect forward secrecy MUST be used within the ESInet."
  + “All call-handling components MUST use Secure Real-Time Protocol (SRTP) and Secure RTCP (SRTCP) for audio, video, and text. Media must run over RTP/UDP and use Datagram TLS (DTLS) for encryption.” This security requirement is explicitly reinforced in the NENA-STA-010.3d [1], clause 3.1.9, which states:
    - “Media streams for voice, video, and text MUST be carried on RTP over UDP (User Datagram Protocol). All endpoints in an ESInet MUST implement media security with Secure Real Time Protocol (SRTP) using Datagram Transport Layer Security (DTLS) as specified in RFC 5763 [20] and RFC 5764 [21]. SRTP Security MUST be requested in all calls originated within an ESInet. If a call is presented to the ESInet with SRTP, SRTP MUST be maintained through the ESInet. Since media are routinely logged, the Logging Service MUST maintain equivalent or better security on the logging (recording) session as that provided on the emergency call (communications) session. RTCP as defined in RFC 3550 [22] and Secure Real Time Control Protocol (SRTCP) as defined in RFC 5764 [21] MUST be supported within the ESInet, and it is highly RECOMMENDED that all calls presented to the ESInet provide RTCP. Within the ESInet, all User Agents MUST support RTCP Extended Reports (RTCP XR) [23]. SIP User Agents within the ESInet SHOULD label all media”.

Therefore, any mention of TLS in previous components (e.g., LIS, ESRP, BCF, PRF) is reinforced here as a baseline security requirement that all NG911 entities must comply with. Also, from a security architecture perspective, these requirements ensure that media confidentiality and integrity are enforced uniformly across the ESInet using SRTP and DTLS, and that control-plane encryption (via SRTCP) is not optional. While sending RTCP is highly RECOMMENDED, support for both RTCP and SRTCP is mandatory, ensuring that encrypted feedback channels are available to detect and respond to issues like packet loss or jitter. The mandate that logging systems provide security equal to or greater than the original media stream further prevents sensitive audio, video, or text from being exposed during recording or storage processes.

Table 6.2.10. Threat Analysis and Risk Assessment Summary – ALL NG911 Functional Elements

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Threat Scenario | Likelihood | Impact | Risk Level | Business Impact | Mitigation |
| Exploitation of Software Vulnerabilities: An adversary discovers and exploits a bug in core NG911 software (e.g., ESRP or LIS), crashing services or bypassing routing logic to misdirect or block emergency calls. | **Medium** | **Critical** | **High** | Software flaws could crash services or misroute 911 calls, risking delayed emergency response | Patch management, secure code reviews, software version control, vulnerability scanning |
| Misconfiguration or Human Error: An administrator or staff member unintentionally misconfigures access controls or routing rules, disrupting 911 operations or exposing systems to external threats. | **High** | **Critical** | **Critical** | Configuration mistakes can disable routing or allow untrained users to cause major outages. | Configuration hardening, role-based access control, logging & audit reviews, employee training |
| Use of Insecure or End-of-Life Components:  Legacy software or unsupported hardware—left unpatched—exposes NG911 systems to exploitation, service failure, or security breaches during critical operations. | **Medium** | **Critical** | **High** | Outdated components may open critical vulnerabilities or fail during high-demand situations | Version lifecycle monitoring, upgrade planning, dependency audits |
| Insecure or Deprecated Protocols (e.g., TLS 1.0/1.1, Telnet): An adversary intercepts or manipulates emergency communications due to outdated encryption protocols that lack forward secrecy and are susceptible to downgrade attacks. | **Medium** | **Critical** | **High** | Weak protocols may let attackers eavesdrop, spoof, or bypass encryption entirely | Enforce TLS 1.2+ with Perfect Forward Secrecy, deprecate legacy TLS/Telnet, use modern libraries with standards support |

#### Risk Rating Reasoning

* **Exploitation of Software Vulnerabilities:** Bugs in core services (like ESRP or LIS) can be exploited to crash the service, misroute calls, or access internal logic (**medium likelihood**). Since these are public safety-critical (**critical impact**). Best practices require secure coding, code audits, and fast patch deployment.
  + **Business Impact:** A flaw in core software could bring down key services, causing missed, delayed 911 responses or getting access to sensitive information.
* **Misconfiguration or Human Error:** Human error remains a top cause of outages and exposures. Mistakes in ACLs or routing logic can allow traffic misrouting or component isolation (**high likelihood**). Even minor configuration flaws can lead to major service degradation—or even crash the system, if the platform is not properly secured or if role-based access control (RBAC) is not enforced. For example, a misconfigured system or an unprivileged new employee with unintended access could inadvertently trigger failures (**critical impact**).
  + **Business Impact:** Misconfigured systems or permissions could result in outages, confusion, and overwhelmed call centers.
* **Use of Insecure or Unsupported Components:** Software that is outdated or unsupported (e.g., using OpenSSL versions with known CVEs, legacy Operating Systems) may lack modern TLS support or contain unresolved security holes (**medium likelihood**). Such problems may result in total loss of confidentiality or system compromise (**critical impact**).
  + **Business Impact:** Running old or insecure software can lead to data loss, call manipulation, or full-service outages.
* **Insecure or Deprecated Protocols (TLS 1.0/1.1, Telnet):**
  + Many historical vulnerabilities in TLS 1.0 and 1.1 make them unsuitable for any ESInet traffic. They are vulnerable to:
    - Weak cipher negotiation
      * When systems agree to use outdated or insecure encryption algorithms during TLS setup, exposing data to eavesdropping or tampering.
    - Downgrade attacks
      * **Downgrade Attacks:** An attack where an adversary tricks systems into using older, weaker protocols (like TLS 1.0), making it easier to exploit them.
    - Lack of forward secrecy
      * **Forward Secrecy:** A property of encryption that ensures past communications remain secure even if long-term keys are later compromised.
  + The NENA-STA-010.3d, clause 2.8.1 [1] mandates:
    - Mandatory support for **TLS 1.2**, **optional for 1.3**
    - **Perfect Forward Secrecy (PFS)**
    - Explicit **rejection of TLS 1.0/1.1**
  + Even TLS 1.2 must be correctly configured with modern cipher suites, certificate validation, and mutual authentication. Many older systems still permit fallback to insecure settings.
  + **Business impact:** Weak protocol settings can expose private data or allow attackers to intercept emergency traffic.
  + **Mitigation:** All NG911 systems must:
    - Use updated TLS stacks
      * Software libraries that implement TLS protocol standards to enable secure communication over networks (like OpenSSL).
    - Disable TLS 1.0/1.1 in all services
    - Enforce PFS, mutual authentication

Operational Security Practices for Resilience

In addition to standards-based security requirements, the following operational practices help maintain high availability and robustness in NG911 environments:

* To maintain both security and service availability, NG911 entities should adopt a phased patching strategy. This can include deploying updates to a limited test group (e.g., one call-taker and one dispatcher) within 12 hours of patch release, monitoring for stability or failure, and rolling out to the remaining workstations within 36 hours. This approach ensures systems remain protected while minimizing the risk of widespread outages from faulty patches.
* Isolate individual workstations or workstation groups to communicate only with authorized services such as NGCS or CHE (Call Handling Equipment). Effective implementation may involve VLANs, host-based ACLs, internal firewalls, or software-defined networking solutions like VMware NSX. These controls enforce least-privilege communication, preventing malware propagation and containing incidents to isolated zones in the event of a compromise.

# 7. Discussion and Conclusion

Although prior work has addressed general cybersecurity concerns for NG911, detailed modeling at the level of individual functional elements remains limited. This assessment advances the field by systematically evaluating threats and risks for each main NG911 component and proposing targeted mitigation strategies to enhance overall system resilience against evolving cyber threats.

By examining each functional element independently, including the LIS, LVF, BCF, ECRF, PRF, ESRP, LNG, LPG, and PSAP, the analysis identifies specific vulnerabilities that could impact call routing, location integrity, media security, and system availability. Although modeled individually, the findings demonstrate that vulnerabilities in one element, if left unaddressed, can cascade across interconnected systems.

This underscores the need for layered defenses (defense-in-depth), strict protocol compliance, up-to-date system configurations, and integration of cybersecurity into every phase of NG911 system design, procurement, deployment, and operation. As NG911 evolves and integrates with broader emergency networks, maintaining strong, individually secured components will be essential to protect public safety and uphold trust in emergency communications.

# 8. Bibliography

[B1] NGA 911, "NG9-1-1 Back to Basics: What are Next Generation Core Services," 2023. [Online]. Available: <https://nga911.com/blogs/post/ng9-1-1-back-basics-what-are-next-generation-core-services>

[B2] W. Schrier, "The Cybersecurity Needed for NG911 Systems," *StateTech Magazine*, Oct. 2019. [Online]. Available: <https://statetechmagazine.com/article/2019/10/cybersecurity-needed-ng911-systems>

[B3] New Jersey 9-1-1 Office, "NG911 Workshop Presentation," Jan. 2015. [Online]. Available: <https://www.nj.gov/911/home/highlights/NJ-ICTAP-NG911-Workshop-Presentation-Final-1-23-2015.pdf>

[B4] Fortinet, "Protecting Next-Gen 9-1-1 Systems," 2020. [Online]. Available: <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protecting-nextgen-911-systems.pdf>

[B5] S. Wirth, "Attention PSAPs: Test NG911 Readiness, Get Resources," *Gov1*, Feb. 2020. [Online]. Available: <https://www.gov1.com/emergency-management/articles/attention-psaps-test-ng911-readiness-get-resources-LXvpuUkI6A8BWc60/>

# Appendix A

## NG911 System Components and Interaction Flows

To support understanding of NG911 operations, this section presents conceptual representations of key functional elements and associated message flows based on the NENA-STA-010.3d-2021 [1] standard and related RFCs. These models are designed to clarify the roles and interactions of core components without prescribing implementation-specific details.

Figures and key elements (like fields in XML) included in this section are created based on the author's interpretation of the NENA-STA-010.3d-2021 [1] and related RFCs. While some representations may appear **close to real-world implementations**, they remain **conceptual and high-level**, serving to clarify interactions rather than to prescribe exact implementation details. **These examples should be independently validated against the official standards for accuracy in deployment**.

When presenting messages associated with functional elements, the most relevant headers to illustrate NG911-specific behavior will be included. While full messages contain many mandatory or optional headers, we intentionally focus on a minimal set that highlights the functional interaction. This approach helps maintain clarity while acknowledging that other headers, though present in actual signaling, are omitted here for simplicity and focus.

### 1. Location Information Server (LIS)

A Location Information Server (LIS) provides the caller’s location either as a PIDF-LO (XML location object – location-by-value) or as a URI that references a stored location; location-by-reference. The LIS is external to the NG911 Core Services (NGCS) and typically operated by the originating network or access provider.

The NG911 ESInet itself is not involved in the LIS’s location delivery transaction, instead, the location is obtained by the network provider then is stored in the LIS before or during call setup (whether location is civic or geodetic), and then includes that location (value or reference) in the SIP Geolocation header of the emergency call.

In a standard NG911 emergency call, **the originating device or originating network** is responsible for setting the **Request-URI to a Service URN**, such as “**urn:service:sos”**, during SIP INVITE creation, as required by NENA-STA-010.3d [1]. If the originating entity fails to include the Service URN, then the **Border Control Function (BCF)** or the **originating ESRP MUST insert** or correct the Request-URI to ensure the call is properly identified as an emergency session before further processing.

* **LIS and NG911 Interaction**
  + **Since LIS is external to NGCS**, its internal functioning is out of scope for i3 [1], but interactions with ESInet components must follow i3-defined interfaces.
  + **The LIS provides the following functions within i3 [1]:**
    - **Location Provisioning:** LIS provides location to devices, networks, and NG911 systems.
      * **Location can be supplied in two ways:**
        + **By Value:** Full PIDF-LO XML with **(latitude, longitude)** or **civic address**.

If NGCS receives a PIDF-LO, it must support location dereferencing via the SIP and HTTP Enabled Location Delivery (HELD) protocols (RFC 5985) [16].

* + - * + **By Reference:** Location URI (requires dereferencing to obtain actual location).

The LIS must also provide a way to dereference that URI to retrieve the actual PIDF-LO according to A Location Dereference Protocol Using HTTP-Enabled Location Delivery (HELD) (RFC 6753) [17].

* + - **Dereferencing Function:** Converts location references (URIs) into actual geographic or civic locations.
    - **Location Validation Function (LVF) Interaction:** LIS queries LVF to validate stored location data **(only for civic addresses)**.
  + LIS can be implemented as a **physical** or **logical** entity**.**
    - Some networks may not have a standalone LIS server but may integrate LIS functionality within other components.
* **Protocols Used by LIS** 
  + **HELD (RFC 5985)**: Enables IP-based devices to request their location from LIS
  + **HELD Dereferencing (RFC 6753):** Converts location URIs into precise geographic locations.
  + **SIP Presence Event Package (RFC 3856):** Allows real-time location updates using SIP messaging.
  + LIS **must** implement at least one of these protocols to comply with NG911 requirements.
* **Location Request Handling**
  + If NG911 system **request's** location:
    - If using SIP Location URI, the requestor must send a SIP SUBSCRIBE message (RFC 6665).
    - If using HELD Location URI, the requestor must perform HELD dereferencing (RFC 6753).
  + **NGCS Handling Rules:**
    - If NGCS receives a Location URI and forwards it to another system, it must pass the URI instead of resolving it itself.
    - Each entity must perform its own location dereferencing, using proper credentials.
* **Authentication and Security**
  + LIS must validate credentials using certificates issued by a PSAP Credentialing Agency (PCA).
  + Only authorized entities (e.g., PSAPs, NG911 Core Services) can access high-accuracy, dispatch-quality location data.
* **Handling Multiple Locations**
  + Multiple locations can be included in a SIP request, such as:
    - Device-determined location vs. Network-determined location (cross-validation).
    - Location by Value for fast routing, with Location by Reference for updates.
    - Geodetic (lat/long) and civic address included in the same request.
  + When multiple locations are sent:
    - The top entry in the Geolocation header should be the preferred location.
    - Downstream systems (e.g., ESRP) may use different locations for different purposes (e.g., routing vs. dispatching).
* **Constraints on Location Processing**
  + Location must not be altered along the NG911 path.
  + If new location data is acquired before reaching the PSAP, it must be included in call signaling.
  + If additional location data is obtained after the PSAP answers, it is included in an Emergency Incident Data Object (EIDO).
* **Error Handling in Location**
  + **Requests 200 OK:** Successful location retrieval.
  + **307 Temporary Redirect:** LIS redirects request to another LIS.
  + **454 Unspecified Error:** LIS encountered an internal failure.
  + **468 No Address Found:** The requested location could not be resolved.
  + **469 Unknown MCS/GCS:** LIS does not recognize the provided location reference.

#### HELD (RFC 5985) – IP-Based Device Requesting Location from LIS

HTTP-Enabled Location Delivery (HELD) – RFC 5985 [16] defines a protocol that allows a network entity (typically the originating service provider or SIP proxy) to retrieve the geographic location of a subscriber device from a Location Information Server (LIS). Although HELD supports direct device queries, in NG911 practice the LIS is deployed within the originating network and is accessed upstream before the call enters the ESInet. The following example illustrates a HELD (HTTP-Enabled Location Delivery) request issued by the **originating network or SIP proxy** on behalf of the device to a Location Information Server (LIS), as defined in RFC 5985 [16]. This example request asks the LIS to explicitly return to a geodetic location.

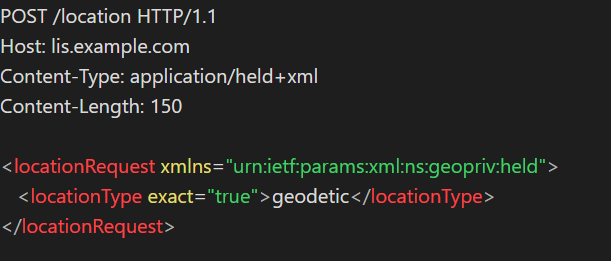


Figure A.1. Example of a HELD Request (XML format) sent to LIS

LIS responses (not necessarily tied to the previous request) may contain the caller’s location directly using the PIDF-LO (Presence Information Data Format – Location Object), which encapsulates either civic or geodetic coordinates as shown in Figure 3. Response formats depend on the request parameters (e.g., requested type, exact attribute) and LIS policy. Figures 3 and 4 are not strict responses to Figure 2.



Figure A.2. Example of a HELD Response with PIDF-LO Location (XML format)

The LIS may also return a Location URI instead of embedding the full location data in the response. This URI is typically inserted into the SIP INVITE and may later be dereferenced by downstream NG911 elements (e.g., ESRP or PSAP) to retrieve the actual location object, as demonstrated in Figure 4. It could also be explicitly requested in the HELD request to ask for URI instead of location by value by including the key element “<responseTime>locationURI</responseTime>”.

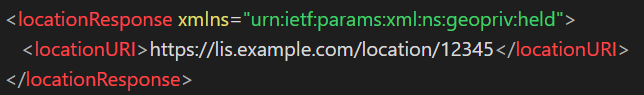


Figure A.3. Example of a HELD Response with Location URI (XML format)

#### HELD Dereferencing (RFC 6753) – Converting a Location URI to a Geographic Location

The LIS may return a Location URI, which the requester must dereference by querying the LIS again to obtain the location of the original device or caller, for example, a requester might send: “GET /location?uri=urn: location:12345 HTTP/1.1”. The LIS then returns the actual location data in PIDF-LO format, which may contain either a geodetic location (e.g., latitude/longitude such as 37.7749 -122.4194) or a civic address (e.g., country: US, state: California, city: San Francisco, street: Market Street, house number: 100).

The type of location returned depends on what was originally provisioned in the LIS, as well as the capabilities and policy preferences of both the LIS and the requesting system. Dereferencing allows location data to be retrieved on demand, enabling dynamic tracking or real-time updates of a caller’s location. This supports flexible, up-to-date use in NG911 call routing, transfers, and ongoing incident handling.

The frequency of such updates depends on the behavior of the requesting entity - for example, an Emergency Services Routing Proxy (ESRP), Border Control Function (BCF), or Public Safety Answering Point (PSAP) may periodically re-request the location at defined intervals to track a moving caller. However, to prevent excessive load on the LIS, location update requests are subject to rate control policies defined by the LIS.

#### SIP Presence Event Package (RFC 3856) – Real-Time Location Updates via SIP

The SIP Presence Event Package (RFC 3856) [18] enables **continuous location updates** (e.g., for a moving vehicle) uses a push model, where the LIS automatically sends location updates to the authorized NG911 elements (e.g., ESRP or PSAP). Instead of repeatedly polling the LIS, the requesting entity sends a **SUBSCRIBE** request to the caller’s Location URI (e.g., sip:urn:location:12345@lis.example.com) with the event type presence which tells the LIS that the requester is subscribing to presence information, which in this context includes the caller’s location as defined by the Presence Information Data Format (PIDF-LO). Once accepted, the LIS pushes updated location information via NOTIFY messages whenever the target's location changes. This mechanism enables real-time tracking of mobile callers during an active emergency session.

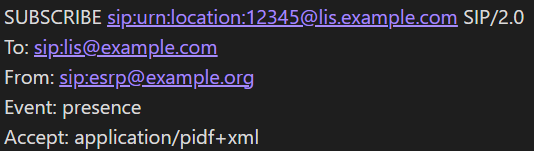


Figure A.4. Example of a SIP SUBSCRIBE Request to a LIS for Location Updates



Figure A.5. Example of a SIP NOTIFY Message from LIS Containing Updated Geodetic Location (PIDF-LO)

### 2. Location Validation Function (LVF)

The Location Validation Function (LVF) utilizes Location-to-Service Translation Protocol (LoST – RFC 5222) [19], an XML-based protocol used in NG911 to translate a location into a service destination. It can be used to **validate civic addresses** (via the LVF) or to **route emergency calls** (via the ECRF for example). In the context of the LVF, LoST is used specifically to **verify that a civic address is valid and recognized within the authoritative GIS database** before an emergency call occurs.

* Used during **provisioning**, meaning validation happens before an emergency occurs.
* Only validates civic addresses (not geodetic locations like latitude/longitude).

The LIS sends a validation request to the LVF using the LoST protocol (as defined in RFC 5222) [19], with a “findService” query and a civic address. The LVF then checks this address against the authoritative GIS database for the jurisdiction.

If the address is valid, the LVF returns a normalized version and confirms that it is routable. If not, the LVF responds with an error or suggestions for correction. This process helps prevent misrouted calls by ensuring the location is recognized before it reaches the ESInet.

**Note**: The LVF only supports validation of civic addresses, not raw geodetic coordinates (lat/long).

The following conceptual figures illustrate the core interaction between a Location Information Server (LIS) and the Location Validation Function (LVF) using the LoST protocol. This includes a civic address validation request and both a successful and unsuccessful response.



Figure A.6. Example of a LoST findService Request Sent from LIS to LVF for Civic Address Validation

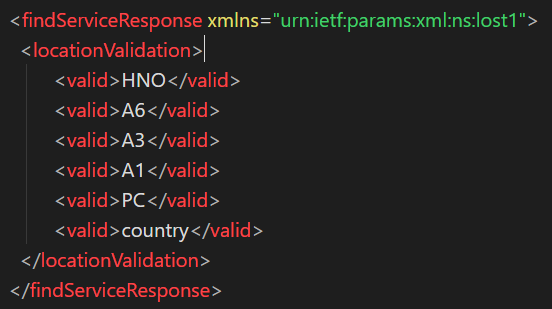


Figure A.7. Example of a LoST findServiceResponse from LVF Indicating a Valid Civic Address

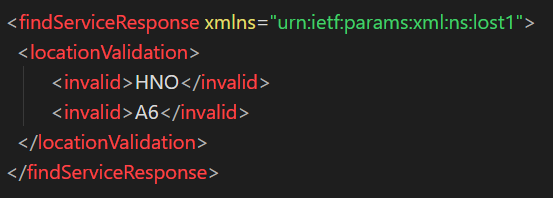


Figure A.8. Example of a LoST findServiceResponse from LVF Indicating an Invalid or Unrecognized Address

### 3. Border Control Function (BCF)

The Border Control Function (BCF) serves as the security and policy enforcement gateway at the edge of the Emergency Services IP Network (ESInet). It protects NG911 infrastructure from cyber threats, spoofed calls, malformed SIP messages, and unauthorized traffic, while enforcing protocol compliance and emergency call handling rules. According to NENA-STA-010.3d [1], “A BCF MUST be deployed between external networks and the ESInet/NGCS. A BCF SHOULD be deployed between the ESInet/NGCS and agency networks.”.

“A BCF MUST be deployed between external networks and the ESInet/NGCS. A BCF SHOULD be deployed between the ESInet/NGCS and agency networks." – NENA-STA-010.3d [1]

"The BCF, as the first active SIP element in the path of an emergency call, MUST add to the call the emergency-Call Identifier, emergency-Incident Tracking Identifier, and a SIP Resource-Priority header field.” – NENA-STA-010.3d [1]

"The BCF inserts a Call-Info header field with a purpose parameter of 'emergency-source' to allow downstream elements to identify the call source." – NENA-STA-010.3d [1]

* The BCF acts as a boundary between external networks and the ESInet.
* Site between the originating network (VoIP, cellular, PSTN) and the ESInet.
* Acts as the first point of security before emergency calls reach NG911 Core Services (NGCS).

BCF is a mandatory NG911 functional element, typically composed of two integrated components:

* A Next-Generation Firewall (NGFW) for network-layer filtering
* A Session Border Controller (SBC) for SIP-layer validation, normalization, and media control

**Note: downstream** refers to any functional element that comes *after* the BCF in the call processing flow (e.g ESRP).

The following table illustrates the process of Emergency Call Processing based on the standards mentioned above.

Table A.1. BCF Emergency Call Processing

|  |  |
| --- | --- |
| Step | What Happens? |
| BCF Receives SIP INVITE from Carrier. | A 911 call enters the ESInet via BCF. |
| BCF Inspects & Validates Traffic | The NGFW filters packets by IP, port, and protocol. The SBC validates SIP structure, certificates, and source trust. |
| BCF Normalizes SIP Message | The SBC corrects malformed headers, enforces compliance, and standardizes formats. |
| Header Insertion if not present (Mandatory) | If not present, BCF inserts the following SIP headers:  - Call-Info (with purpose=emergency-CallId)  - Call-Info (with purpose=emergency-IncidentId)  - Call-Info (with purpose=emergency-source)  - Resource-Priority: esnet.1 |
| BCF Applies Security Policies | Detects spoofing, overloads, or denial-of-service (DoS) indicators. Applies admission control. |
| BCF Forwards Call to ESRP | If validated and secure, the BCF forwards the call to the Emergency Services Routing Proxy (ESRP) for location-based routing. |

#### Headers Explanation

* **Call-Info: emergency-CallId:** A globally unique identifier for the individual emergency call. It allows consistent tracking of the same call across the ESInet.
* **Call-Info: emergency-IncidentId:** Used to associate multiple calls with the same emergency incident, enabling linkage of reestablished or related calls (e.g., callbacks, multi-party calls).
* **Call-Info: emergency-source:** Identifies the originating provider, gateway, or network source. This helps downstream systems recognize the call’s origin and flag malicious sources.
* **Resource-Priority: esnet.1:** Indicates that the call is an emergency and ensures it receives the correct priority treatment during network handling and routing.

#### What Happens if BCF Detects a Threat?

If the BCF identifies an attack (e.g., DDoS, spoofing, excessive failed calls), it can:

* Block the call and send a 403 Forbidden SIP response.
* Mark the source as a “Bad Actor” and prevent further attacks.
* Rate-limit traffic to reduce system overload.

As stated in NENA-STA-010.3d [1], "The BCF SHALL support an automated interface that allows a downstream element to mark a particular source as a 'bad actor' and notify the BCF." So, if one of these downstream elements detects a problem — for example, unusual call patterns, spoofing, or known abuse — it should be able to:

* Mark the call source (e.g., gateway, IP, provider)
* Report that back to the BCF
* The BCF can then block or rate-limit future traffic from that source

As explained earlier, **the originating device or network is responsible for setting the Service URN (e.g., urn:service:sos) during INVITE creation**. However, if the incoming SIP INVITE does not correctly include a Service URN, **the BCF MUST insert or correct the Request-URI to ensure proper emergency call identification before forwarding to downstream elements like the ESRP**.

### 4. Emergency Call Routing Function (ECRF)

Before introducing the Emergency Services Routing Proxy (ESRP), we first explain two essential backend functions, Emergency Call Routing Function (ECRF) and Policy Routing Function (PRF), that are triggered by the ESRP. These functions are critical for determining the appropriate PSAP destination and applying jurisdictional policies before the ESRP finalizes call routing.

The Emergency Call Routing Function (ECRF) **uses (LoST – RFC 5222) [19] to perform dynamic call routing based on the caller's location and the requested Service URN (e.g., urn:service:sos, urn:service:sos.fire)**. The ECRF accepts LoST queries from authenticated ESInet entities (such as ESRP), maps the supplied location and service URN to the correct **destination URI**, and returns it for call routing. If an exact service URN match is not found, the ECRF applies fallback logic to route based on the closest matching service URN.

#### a. ECRF Input

1. **Caller’s Location**:
   1. Either **geodetic coordinates (latitude/longitude)** or a **civic address,** provided through a **PIDF-LO** object (Fixed).
   2. **I**f a location is provided **by reference (URI)**, the entity making the LoST query (typically the ESRP) **must first dereference it to retrieve the full PIDF-LO object before querying the ECRF**.The ECRF expects a resolved location value, not a location URI (Dynamic like mobile or moving callers).
2. **Service URN**:
   1. **The ECRF requires the Service URN as an input to determine the appropriate emergency service destination (e.g., police, fire, medical). It combines this with the caller’s location to find the correct PSAP**, typically “urn:service:sos”, indicating an emergency call.
      1. **The Service URN (Uniform Resource Name)** follows a structured naming convention used in emergency services.
         1. Example URN Syntax:
            1. General Emergency: urn:service:sos
            2. Police Emergency: urn:service:sos.police
            3. Fire Emergency: urn:service:sos.fire
            4. Medical Emergency: urn:service:sos.ambulance
3. The system making the query (e.g., an **Emergency Services Routing Proxy (ESRP)**): If the LoST query was triggered by an ESRP (Emergency Services Routing Proxy), the source of the query is **implicitly** identified in the **SIP INVITE** request that **wraps the XML**.
4. **Policy and Rules (optional)**:
   1. The **Policy Routing Function (PRF)** **MAY** influence the final routing decision.
   2. **Jurisdiction-based rules** may override default PSAP assignments.
      1. **Jurisdictional boundaries in NG911:** refer to geographic areas that define the responsibility of Public Safety Answering Points (PSAPs) and emergency services. These boundaries ensure that each emergency call is routed to the correct PSAP based on the caller's location.
         1. Defined as polygon-based service areas in a Geographic Information System (GIS).
         2. Calls are routed based on the caller’s location relative to these boundaries.
         3. If a call is near a boundary, overlap resolution techniques are used to determine the most appropriate PSAP.

The following LoST findService requests show a query by civic address and by geodetic coordinate. These requests include the caller’s location and request Service URN.

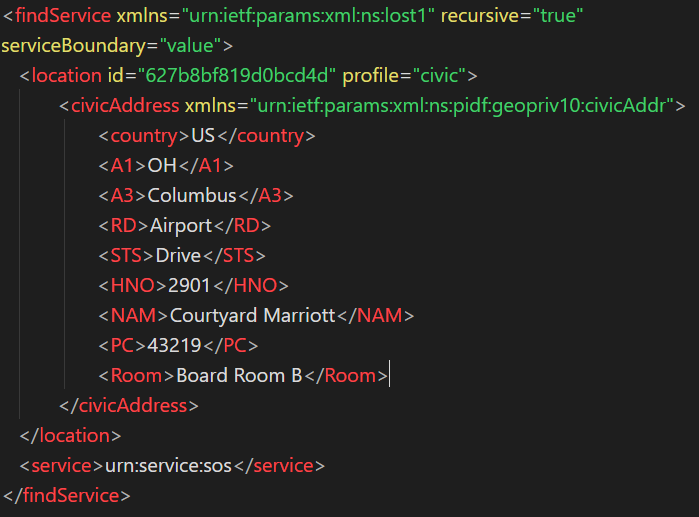


Figure A.9. Example of a LoST findService Request to the ECRF Using a Civic Address (profile=civic)



Figure A.10. Example of a LoST findService Request to the ECRF Using Geodetic Coordinates (profile=geodetic)

#### b. Processing by the ECRF

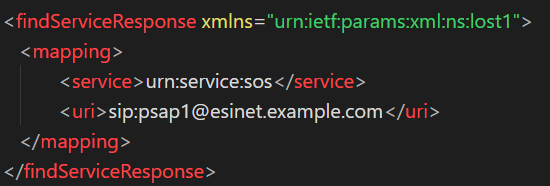
1. **Queries the Geographic Information System (GIS) Database**:
   1. Matches the caller’s location against **service boundaries**.
   2. Determines which PSAP is responsible for that location.
2. **Checks Routing Policies (optional)**:
   1. If the primary PSAP is **overloaded**, policy rules may route the call to a **backup PSAP**.
   2. Disaster scenarios may trigger **alternative routing**.
3. **Returns a SIP URI of the PSAP or intermediate ESRP as the destination to route the call to**:
   1. The response includes a **PSAP URI or an Emergency Services Routing Proxy (ESRP) URI**.
   2. At this point, the ESRP will replace the **Request-URI** in the SIP INVITE with the newly obtained **SIP URI** while **retaining the original Service-URN as a SIP header for downstream elements.**
   3. The call is then forwarded to this destination.
4. **The ECRF may also apply “serviceBoundary” constraints:** if recursive lookup is requested **(recursive=true**) as in the figures above, the ECRF must search across service areas if the location spans multiple jurisdictions (i.e. it contacts other ECRFs to complete the query and return a final routing URI if needed).

#### c. ECRF Output

After processing, the ECRF provides:

1. **A SIP URI of the Correct PSAP**:
   1. Example: [sip:psap1@esinet.example.com](mailto:sip:psap1@esinet.example.com)
2. **A SIP URI of an Intermediate ESRP** (if needed).
3. **Alternative Routing Information** (if the primary PSAP is unavailable).
4. **GIS-based Confirmation**:
   1. Ensures that the call is routed within jurisdictional boundaries.

The following figure illustrates a LoST findService response example.

  
Figure A.11. Example of a LoST findServiceResponse from the ECRF Providing a Routing SIP URI

### 5. Policy-based Routing Function (PRF)

The Policy-based or Policy Routing Function (PRF) is responsible for making dynamic, policy-based call routing decisions in the NG911 system. It operates **within** the ESRP (Emergency Services Routing Proxy) and applies predefined policies to determine the next hop for a call.

Where does this step take place?

* Inside the ESRP, after receiving a call and before sending it to the next destination.
* Works with the ECRF for location-based routing and policy rules from the Policy Store.
* Used for disaster handling, overflow routing, and jurisdiction-based call distribution.

The following two figures illustrate the process of the PRF.

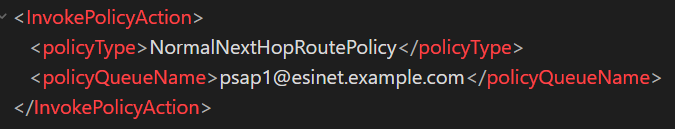


Figure A.12. ESRP Requests Routing from PRF

* The ESRP asks the PRF for the next hop routing policy.

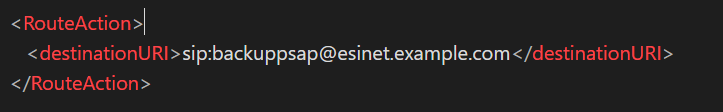


Figure A.13. PRF Determines Routing Outcome

* PRF decides to route the call to a backup PSAP due to overload at the primary PSAP.

### 6. Emergency Services Routing Proxy (ESRP)

The Emergency Services Routing Proxy (ESRP) is the core SIP-based call routing function within the Emergency Services IP Network (ESInet), responsible for directing emergency calls based on caller location, policy rules, and PSAP availability.

* Works alongside ECRF (for location-based routing) and PRF (for policy-based routing).
* Uses SIP protocol to process emergency calls and route them dynamically.
* Works with ECRF (for location-based routing) and PRF (for policy-based routing).
* The ESRP queries the **ECRF** and **PRF** to determine routing based on location, policy rules, and PSAP state.
* As the **primary dynamic routing element**, the ESRP may fall back to **static default routing policies (default routes)** if dynamic ECRF or PRF queries fail, ensuring call progression even during partial network outages or failures.

The ESRP can operate in different roles depending on where a call is in its routing journey through the ESInet. Table 5.5.6 summarizes these roles. Even though the following examples show a simple scenario with only one ESRP, in larger or multi-jurisdictional deployments, multiple ESRPs may work together to route calls between networks, states, or PSAPs.

Table A.2. ESRP Functional Roles and Types

|  |  |  |
| --- | --- | --- |
| **ESRP Type** | **Role** | **Where It Operates** |
| Originating ESRP | First ESRP that receives a call inside the ESInet. | Entry point for calls, routes to intermediate ESRPs or PSAPs. |
| Intermediate ESRP | Handles routing between multiple ESRPs in different jurisdictions. | Routes calls between counties, states, or regions. |
| Terminating ESRP | Routes calls to the final PSAP destination. | Last hop before the call reaches the PSAP. |

The following three figures illustrate the SIP signaling flow in NG911 when an emergency call enters the ESInet. The first figure shows the SIP INVITE sent by the originating network to the ESRP for dynamic routing. After location-based and policy-based routing is completed (via ECRF and PRF), the second figure shows the SIP INVITE generated by the ESRP to the correct PSAP destination, the third one shows the SIP 200 OK response received by the ESRP after routing to the PSAP. Each step ensures that the Service-URN, Geolocation information, and other headers are preserved for emergency handling.

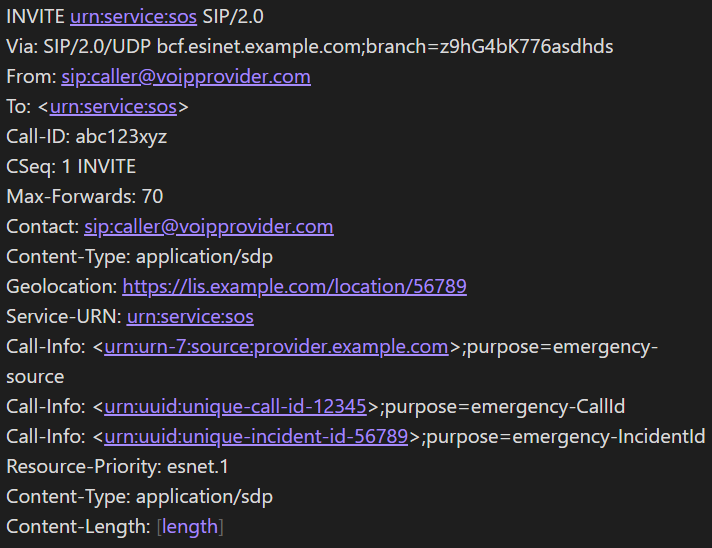


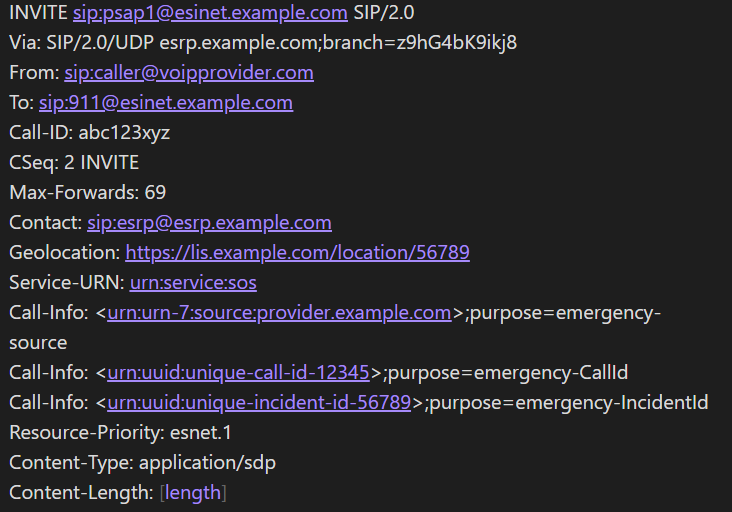
Figure A.14. Example of an Incoming SIP INVITE to ESRP After BCF Processing

The following table summarizes the major SIP headers included in an emergency call INVITE after passing through the Border Control Function (BCF) but before ESRP routing. These headers ensure call tracking, location reporting, emergency prioritization, and routing capabilities throughout the ESInet.

Table A.3. Key SIP Headers for Emergency Call INVITE after BCF Processing

|  |  |
| --- | --- |
| Field | Meaning |
| INVITE | SIP method to start a call session, and the **Request-URI** initially points to the “urn:service:sos”, because we still don't know yet which PSAP to route to. |
| Via | Identifies the last network element that forwarded the request |
| From | Caller (e.g., SIP user at VoIP provider). |
| To | Destination; 911 service “urn:service:sos”. |
| Call-ID | Unique call identifier across the session. |
| CSeq | SIP command sequence number (starts at 1). |
| Contact | Where the caller can be reached back. |
| Geolocation | Location URI pointing to where the caller is located (before dereferencing if needed). |
| Service-URN | Type of emergency service requested (urn:service:sos, urn:service:sos.fire, etc.). |
| Call-Info (emergency-CallId) | Unique ID to track this call across the ESInet. |
| Call-Info (emergency-IncidentId) | Unique incident ID for multiple related calls (e.g., re-calls). |
| Call-Info (emergency-source) | Originating network or provider name. |
| Resource-Priority: esnet.1 | Tells the network this is an emergency call, should be prioritized. |
| Content-Type | Type of payload, normally SDP (media negotiation). |
| Content-Length | Length of the body content (SDP). |

* Bring the emergency call into the ESInet (through BCF first, then ESRP).
* The ESRP will **analyze location**, **query ECRF**, **query PRF**, and **decide** the final PSAP or next intermediate ESRP (if needed).

  
Figure A.15. Example of SIP INVITE from ESRP to PSAP (Final Call Routing)

* ESRP **rewrites** the Request-URI after making the routing decision.
* **The INVITE now targets the final PSAP** (Public Safety Answering Point).
* But important SIP headers like **Service-URN** are still **preserved** to inform **PSAP** what type of emergency this is.

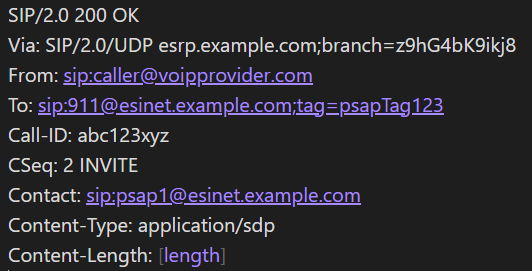


Figure A.16. Example of an Incoming SIP INVITE to ESRP After BCF Processing

* The ESRP has successfully routed the call to [psap1@esinet.example.com](mailto:psap1@esinet.example.com).

As previously noted, the originating device or BCF should ensure that the SIP INVITE includes a correct Service URN. If for any reason the INVITE reaches the ESRP without a valid Service URN, the originating ESRP is expected to insert or normalize the Request-URI to a proper emergency URN (e.g., urn:service:sos) before proceeding with location-based call routing.

### 7. Legacy Network Gateway (LNG)

A Legacy Network Gateway (LNG) is defined in NENA i3 as the interface between legacy originating networks (traditional wireline/wireless networks that send 911 calls via TDM trunks or non-SIP signaling) and the NG911 ESInet. In simpler terms, the LNG allows calls from legacy switches (end offices, MSCs) to enter the IP-based NG911 system.

### 8. Legacy PSAP Gateway (LPG)

The Legacy PSAP Gateway (LPG) is the mirror image of the LNG – it interfaces between the NG911 ESInet and a legacy PSAP that still uses old systems. NENA i3 defines the LPG as the element that “supports the delivery of an emergency call through the ESInet/NGCS to a legacy PSAP as well as the transfer of an emergency call between i3 PSAPs and legacy PSAPs. In essence, when an NG911 call needs to terminate at a PSAP that only has traditional 911 trunk lines, the LPG will convert the SIP call to analog/TDM signaling.

### 9. Public Safety Answering Point (PSAP)

An i3 PSAP is a Public Safety Answering Point fully capable of receiving IP-based emergency calls per the NENA i3 standard. The PSAP in NG911 is effectively a SIP user agent (or a cluster of them) that can handle voice, text, and video from the ESInet. The user’s description likely highlights the PSAP’s role as the call terminus that presents the call to a call-taker and possibly interacts back with NGCS for certain features.