NEAD Privacy and Security Plan

February 3, 2017

Wireless carriers take seriously the need to protect consumer information – including location information – throughout all elements of the services they provide, and this includes information related to the provision of 9-1-1 services. To that end, and as required by the Federal Communications Commission's (FCC) *Wireless E911 Location Accuracy Requirements Fourth Report and Order* (Order)[1], the NEAD LLC and national wireless carriers (AT&T, T-Mobile, Sprint and Verizon) submit this Privacy and Security Plan (Plan) for the National Emergency Address Database (NEAD), a key component of the new wireless 9-1-1 location accuracy framework.

As described in this Plan, the NEAD is designed and will be operated in a manner intended to protect individuals' private information and address cybersecurity, while enabling wireless carriers to provide public safety with a dispatchable location during a wireless call to 9-1-1.

Introduction

In 2015, the FCC adopted new rules that require wireless carriers to use innovative wireless technologies to provide location information for indoor wireless calls to 9-1-1. As part of those rules, the FCC recognized the nationwide wireless carriers' commitment to develop and utilize a location database of wireless access points (e.g., Wi-Fi) and beacons (e.g., Bluetooth Low Energy) that will enable wireless carriers to deliver a dispatchable location to help public safety quickly, efficiently and safely respond to indoor wireless 9-1-1 calls.

As described below, the NEAD Platform includes the NEAD itself as well as the National Emergency Address Manager (NEAM), which comprises systems to enable the input of accurate data records and to respond to requests for wireless access point and beacon location data as part of a wireless 9-1-1 call. NEAD LLC, a non-profit entity established by CTIA, will act as the NEAD Administrator to oversee the NEAD Platform's development and operation.

This Plan describes how privacy and security safeguards have been incorporated into the NEAD Platform "by design," with privacy and security considerations addressed on an end-to-end basis. In doing so, the Plan draws on the ATIS Standard for *Location Accuracy Improvements for Emergency Calls*[2] as well as applicable data privacy and security standards and frameworks. For example, it incorporates privacy protections based on the Fair Information Practice Principles initially developed by the Organization for Economic Cooperation and Development, such as a clear statement of purpose specification and use limitations. Leading cybersecurity methods such

[1] *Wireless E911 Location Accuracy Requirements*, PS Docket No. 07-114, Fourth Report and Order, 30 FCC Rcd 1259 ¶ 69 (2015).

[2] Alliance for Telecommunications Industry Solutions (ATIS), *Standard for Location Accuracy Improvements for Emergency Calls* (Oct. 2016) (ATIS-0700028) is available at https://www.atis.org/docstore/product.aspx?id=28273 (last visited Jan. 9, 2017).

as the NIST Cybersecurity Framework (v. 1.0) and the ISO 27001 Information Security Management Standard were used in the development of controls designed to maintain the confidentiality, availability, and integrity of the NEAD Platform's networks, systems, and data. The NEAD Platform's operations will be subject to a program of regular audits and assessments to enable ongoing governance, compliance, and risk management.

This Plan also reflects the review and input of a diverse array of stakeholders. In addition to the involvement of security, privacy, technical and other relevant personnel from the national wireless carriers and the NEAD Administrator, the Plan's development process included, for example, multiple formal consultation sessions with CTIA's 9-1-1 Location Accuracy Advisory Group.[3] The Plan was also reviewed with public interest, consumer, and privacy advocacy organizations.

What Is the NEAD Platform and How Does It Operate?

The NEAD is a database of the street address and additional location information (Street Address Information) of Wi-Fi and Bluetooth Low Energy Beacon access points (wireless access points). During a wireless 9-1-1 call, wireless carriers will interact with the NEAD Platform, using data from the NEAD to help provide to 9-1-1 call-takers a dispatchable location (i.e., street address, plus additional information such as suite, apartment or similar information necessary to adequately locate the caller).

How the NEAD Platform works. When someone calls 9-1-1 from their wireless handset equipped with Wi-Fi and/or Bluetooth radio(s), the wireless carrier network will automatically collect information from the wireless handset about wireless access points (i.e., any Media Access Control (MAC) addresses of Wi-Fi Access Points and any Bluetooth Public Device Addresses (BT-PDAs) of the Bluetooth beacons) within the vicinity of the wireless handset. The wireless carrier network will query the NEAD Platform to determine whether the MAC address or BT-PDA of any of these wireless access points is in the NEAD and is associated with a street address. If so, the wireless carrier network will determine which of the wireless access points' Street Address Information to provide as a dispatchable location for the 9-1-1 call.

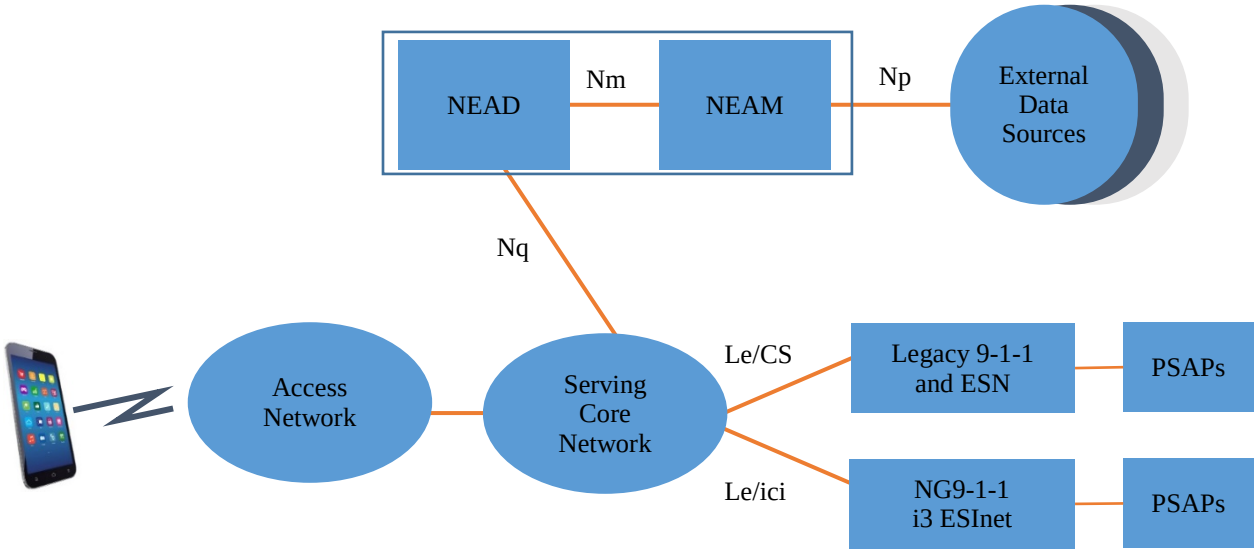
Components of the NEAD Platform. There are two main components of the NEAD Platform: the NEAD and the NEAM.

- As previously stated, the NEAD is the database of verified wireless access point Street Address Information. The NEAD will be designed to respond, only to 9-1-1 call-related requests from participating and authorized carriers.

[3] CTIA's 9-1-1 Location Accuracy Advisory Group is comprised of organizations representing public safety professionals, individuals with disabilities, privacy experts, state and local governments, and other industry stakeholders. See, *CTIA Announces Key Progress Toward Enhanced 9-1-1 Location Accuracy* (rel. June 5, 2015), available at http://www.ctia.org/industry-data/press-releases-details/press-releases/ctia-announces-key-progress-toward-enhanced-9-1-1-location-accuracy (last visited Jan. 9, 2017).

- The NEAM is the set of systems that will receive, process, and verify information on wireless access points that is submitted for inclusion in the NEAD. Such information will generally come from three sources: (i) service provider records of wireless access points, including MAC address, BT-PDA and location information, but no other customer-specific information; (ii) large enterprise system (e.g. hotels, restaurants, and retail stores) records of wireless access points, including MAC address, BT-PDA and location information, but no other customer-specific information; and (iii) eventually, individual consumers, who will be able voluntarily to input information about their wireless access points not otherwise provided to the NEAD along with information necessary for verification.

Figure 1. NEAD Platform & Wireless 9-1-1 System (Conceptual)



The reference model above (Figure 1) is an overview of the functional structure and the involved entities, interfaces and connections associated with the NEAD Platform.[4] ATIS-0700028 defines the architecture and requirements for the NEAD Platform, including:

1. **Nq** – Interface from the NEAD to a wireless carrier Serving Core Network.
2. **Np** – Interface from the NEAM to external data sources and authorized users.
3. **Nm** – Interface from the NEAD to NEAM within the NEAD Platform.

What Information Is Collected in the NEAD Platform and How Is Such Information Used and Shared?

As described above, during a 9-1-1 call made with a wireless handset, certain types of information will be collected, used, and shared to support the E911 services provided by the

[4] *See* High Level Architecture for Heightened Accuracy Location in ATIS-0700028.

NEAD Platform. During a 9-1-1 call, the only information that carriers will share with the NEAD Platform are the MAC addresses of detected Wi-Fi access points and the BT-PDA information of detected Bluetooth beacons. A 9-1-1 caller's name and telephone number will not be shared with the NEAD Platform.

In addition, the NEAD Platform must be populated with reliable and verified wireless access point information (Street Address Information and MAC address or BT-PDA) in order to enable wireless carriers to identify a dispatchable location. Such wireless access point information will be submitted to the NEAD Platform in the following ways:

- Service providers and entities that are responsible for large quantities of wireless access points (e.g. building managers, and other businesses) may submit information about wireless access points to the NEAD Platform via the NEAM. This information will not include information about any associated individual consumers, such as the 9-1-1 caller's name and telephone number.

- In the coming years, individual consumers also will be able voluntarily to submit wireless access point information to the NEAD Platform via the NEAM, improving location accuracy by increasing the number of detectable and verified access points. Individual consumers who voluntarily submit access point data may need to provide additional information such as their name for verification purposes. In those cases where individual consumers do voluntarily submit access point data and their personal information to the NEAD for verification purposes, the individual consumer's personal information will not be shared, except as otherwise required by law.

Consumer Privacy Protections Are Built Into How the NEAD Platform Will Operate

The NEAD Platform and its operations are designed to protect consumer privacy:

- The information submitted to populate the NEAD Platform will be used to support the provision of E911 services and will not be used for commercial purposes. Wireless carriers are required by the FCC's Order, before they access this information, to commit that they will limit its use to E911 purposes or as otherwise necessary to comply with law.
- Information transferred to or from the NEAD Platform during a 9-1-1 call will be the MAC address or BT-PDA and Street Address Information of wireless access points. The 9-1-1 caller's name and telephone number will not be transmitted to the NEAD Platform.
- A privacy notice will be posted on the public-facing portal of the NEAD Platform, so that individual consumers who interact with the NEAD Platform to upload wireless access point information can learn about, among other things, how personal information that may be collected (e.g. name for verification and access purposes) will be used.
- Except as may be required by applicable law, information contained in the NEAD Platform will not be disclosed to third parties, including government entities, other than

for E911 purposes. The NEAD Administrator will follow a defined procedure to assess and respond to valid governmental requests for information.

- Provisions will be made to provide consumers with the ability to access and submit updates and inquiries as to information that relates to them, that they have uploaded on the NEAD Platform.
- Information will be stored for a period of time necessary to enable the operation of the NEAD Platform.

Comprehensive Controls Will Support the NEAD Platform's Secure and Resilient Operation

The NEAD Administrator will utilize a comprehensive set of administrative, physical and technical controls to protect against the unauthorized access to, use of, and disclosure of information contained within, the NEAD Platform, and to maintain the availability and integrity of the NEAD Platform. The administrative, physical, and technical controls selected are drawn from the leading cybersecurity frameworks and standards, including the NIST Cybersecurity Framework, the ISO 27001 Information Security Management Standard, the CSRIC IV Working Group 4 Report, and CIS Critical Security Controls.

Administrative controls will include but not be limited to policies and procedures for personnel, such as background checks for all personnel with access to the NEAD Platform and enhanced background checks for those with higher levels of access to sensitive information; information security policy; and an acceptable use policy for information technology. Physical controls will include but not be limited to employee and personnel security procedures, badge access to facilities, biometric access to sensitive areas, various perimeter defenses and continuous physical security patrol and facility monitoring. Technical controls will include but not be limited to multiple layers of protection based on applicable industry practices and standards, from the host to the network edge, as well as vulnerability scanning and penetration testing.

It is planned that aspects of the NEAD Platform will obtain certification under the ISO 27001 Information Security Management Standard, which is a comprehensive and well-recognized management standard in this area.

Some of the specific key security controls to be implemented include the following:

a. **Inventory of IT Assets and Software:** An asset inventory of all NEAD Platform authorized devices will be maintained. Examples of NEAD Platform asset types include servers, routers, switches, and security devices such as firewalls, intrusion detection and intrusion prevention systems (IDS/IPS). All software installed on the NEAD Platform will exclusively come from the approved NEAD Platform software list.
b. **Secure Configurations for IT Assets and Network Devices:** Secure configurations (hardened versions of the underlying operating system and applications installed on the

system) of NEAD Platform systems will be maintained using configuration management tools including Active Directory Group Policy and third party management systems.

c. **Continuous Vulnerability Assessment and Management:** Continuous vulnerability scanning will be deployed to discover and scan for known, critical vulnerabilities. Asset information will be collected and assets will be assigned systems administration-level ownership. These processes will be supplemented by the registration of assets on the asset inventory as described above. In addition, periodic vulnerability assessments will be conducted, with results relayed to remediation teams for integration into the patch management lifecycle.

d. **Malware Defenses:** Anti-malware protections will be deployed in a layered model, including standard and heuristic advanced malware protections, both in-network and client-based. Known malicious command-and-control domains will be blacklisted.

e. **Access Controls, Segmentation and Separation:** The NEAD database will be neither connected nor visible to the Internet. The NEAD Platform will be segregated into specific security zones, based on the classification of the information stored on the system, with appropriate authentication processes for access. Web servers will be placed into an Internet-facing demilitarized zone (DMZ), and backend application/database servers will be controlled within a protected zone. Application firewalls will allow segmentation of trust zones by both port/protocol and application. Positive trust (default deny) will be the standard protection. Critical services will be operated on separate physical or logical host machines, such as Domain Name System (DNS), file, mail, web, and database servers. Development, test, and production systems will be managed as separate environments with only non-production data used in development and test environments and user access limited to either production or non-production roles. Production data will be maintained in segregated instances with further controls to limit access based on, for example, role, screen, and region, depending on user access requirements.

f. **Boundary Defenses:** Network design will require all inbound connections to traverse implemented security control frameworks and all outbound connections to traverse application-based firewalls. Web traffic will traverse internal proxy servers with dedicated diverse-vendor anti-virus protection. Applications and databases will run on independent systems with no production data stored in an externally accessible zone. Inbound and outbound communications will be monitored for unusual or unauthorized activities. Known malicious IP addresses will be blocked or blacklisted at the network perimeter.

g. **Encryption and Other Data Protection Measures:** The NEAD Platform will employ encryption for information contained in the NEAD Platform in transit and at rest, using no less than SHA-256 encryption with salts, and in transit using industry standard database encryption techniques, using the applicable encryption type such as IPSEC VPN or HTTPS using TLS 1.2 or higher. Advanced malware protection systems will also be put in place.

h. **Application Security:** Strict vendor controls will be deployed to maintain up-to-date and supported software. In-house and third party web applications will be tested in

internal/external penetration tests, as well as through application vulnerability management. Reverse proxies will be deployed to sanitize application traffic.

i. **Penetration Testing:** On a periodic basis, in-house penetration testing/red team exercises will be performed by trained staff, and external penetration testing will be done by expert vendor personnel.

j. **Sourcing and Supply Chain Restrictions:** A comprehensive approach to minimize vendor-related risk, involving risk assessment, screening, contractual obligations, and compliance monitoring, has been used and will be required. Strict controls will be implemented to ensure that the design, development, operation and maintenance of the NEAD Platform will be performed exclusively in the United States, and that the NEAD Administrator must specifically authorize the use of any vendor or sub-vendor to perform such activities. Further, all personnel involved in such activities will be confirmed by background check to be authorized to reside and work in the United States and to otherwise be eligible for such employment. Contractually imposed representations and warranties, compliance with which is subject to review and audit by the NEAD Administrator, establish that the software purpose-built for the NEAD Platform will be free of malicious code and that similar assurances will be sought with respect to any commercial software used within the NEAD Platform.

k. **Business Continuity and Disaster Recovery:** The NEAD Platform will be supported by multiple data centers across the country. This redundant and geographically diverse approach to hosting the NEAD Platform is intended to avoid any single point of failure. The NEAD Platform systems will be co-located in geographically diverse Public Safety class data centers. The NEAD is designed to deliver 99.999% availability. Real-time systems will be deployed and operated in a fault tolerant/fail safe/geo-redundant configuration. In the event of total destruction or catastrophic failure of the core site, other core sites will provide necessary processing until restoration is achieved.

l. **Incident Management and Response Plan:** Documented incident response procedures and role definitions will be maintained. These include resolution, documentation of any incident, communications, and post-event analysis. Incident Management processes and procedures will be in place and designed to handle various severity levels during the course of an event. Security incident response vendor retainers will also be put in place.

Personnel Management and Training

This Plan will be implemented with the support of experienced and credentialed personnel. In addition, at least annually, privacy and security training will be provided to all of the NEAD Administrator's personnel involved in the operation of the NEAD Platform. Security and privacy risks will be further mitigated by a combination of role-based training of personnel; as well as by pre-employment, on-boarding, and off-boarding procedures. Finally, certain personnel involved in the administration of IT assets that directly connect to the NEAD Platform will be restricted in their use of certain electronic and other information resources during the performance of their

NEAD Platform duties, including via the outright prohibition of certain actions and uses of technology that do not serve the NEAD Platform's 9-1-1 call response purposes.

Assessments, Audits and Compliance

The NEAD Platform will operate subject to ongoing processes to assess, audit and determine compliance with applicable security and privacy requirements. An operational committee formed and chaired by the NEAD Administrator for this purpose will meet regularly regarding privacy and data security developments and issues. Policies and procedures are subject to yearly reviews. Privacy and cybersecurity risk assessments will be conducted at least annually. In addition, the sufficiency of any safeguards in place to control those risks will also be assessed at least annually. Gaps and lessons learned will be incorporated into the procedures in an on-going process of continual improvement.

******

The NEAD LLC and the national wireless carriers are committed to supporting and advancing public safety while protecting consumer privacy and the security, integrity and availability of the NEAD Platform. In addition to the NEAD Platform's privacy-conscious design, which acts to limit significantly the personally identifiable information that may be collected as part of its operation, this Privacy and Security Plan documents a comprehensive set of processes and other controls. Taken together, the implementation of these measures is intended to safeguard consumer privacy and lay the foundation for the secure operation of the NEAD Platform as it launches and develops.