

The Call

THE OFFICIAL PUBLICATION OF NENA:
THE 9-1-1 ASSOCIATION

ISSUE NO. 52

CAD DOWN

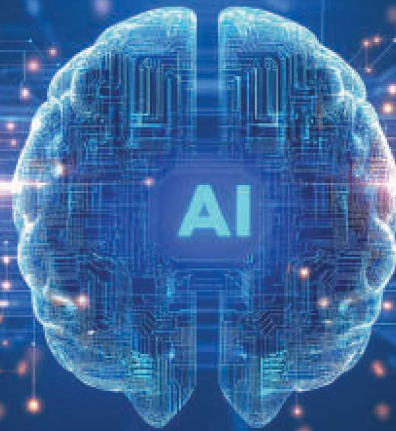
LESSONS LEARNED DURING A CYBER INCIDENT

HOW A CYBER INCIDENT AFFECTING
COMPUTER AIDED DISPATCH CAUSED
CHAOS, THEN BECAME AN INVALUABLE
LEARNING TOOL FOR THE ANNE
ARUNDEL COUNTY POLICE

ALERT

ADOPTING ARTIFICIAL INTELLIGENCE IN THE 9-1-1 CENTER

By William Doolittle, ENP



A sampling of recent literature reveals that the rate of adoption for the use of Artificial Intelligence (AI) is still increasing:

- 2 out of 3 people use AI tools for personal, work, or study purposes
- 65% of organizations use generative AI in at least one business function
- Almost 80% of smart devices feature AI technology
- Nearly 60% of businesses use AI for customer service

These are exciting times for the advancing use of this new technology, but as with all mission-critical platforms they must be planned and implemented with methodologies that control risk and provide a positive cost-benefit.

Artificial intelligence can be categorized by technology and purpose:

Machine Learning	Systems that learn from data using supervised, unsupervised, or reinforcement learning.
Deep Learning	A component of Machine Learning that uses multi-layered neural networks for tasks like machine vision, image, and speech recognition.
Natural Language Processing	Enables machines to understand and generate human language; includes translation services.
Robotics	Integrates AI with mechanical systems for physical task execution.
Expert Systems	Rule-based systems mimicking human decision-making in specialized domains.
Generative AI	Creates new content such as text, audio, images, and video or animation.
Predictive Analytics	Forecasts future outcomes based on analysis and extrapolation of data.
Conversational AI	Facilitates human-like interactions through dialogue (sometimes also referred to as <i>Agentic AI</i>).

This article will provide a structured approach to bringing AI tools into dispatch operations that balance technological innovation with operational reliability and ethical safeguards.

Needs Assessment and Strategic Plan

A **Needs Assessment** is the beginning of the business case for systems improvements. This contains the predictive statement

of where and how AI will improve operational capability. This could include:

- Identifying 'pain points' in current operations (e.g., accommodating surges in demand, delays in translation services, diverting lower-priority calls, etc.) where AI can add value.
- Scrutinizing discrete workflows to identify volumes, workload, measurement, and feedback parameters. Contemporary business analyst practices have a variety of means that improve upon previous methods of analyzing desk procedures with stopwatches.
- Defining clear objectives, such as: automating quality assurance reviews, reducing response times, improving resource allocation, or automating non-emergency call taking.

A **Strategic Plan** is typically the document that captures the operational needs, resource requirements, cost-benefit analysis, schedule, and action plan. This is also the communicating document to your stakeholders to secure buy-in and support from dispatchers, first responders, customers, and policymakers.

Data and Infrastructure Preparation

It is important to recognize that AI platforms will not only *consume* data from your daily operations but will also *create* new data. This is the time to consider how to store and manage these new warehouses of information; in particular, understanding how it impacts responses to public information requests. Specific steps could include:

- Aggregating and cleaning historical dispatch data (e.g., call logs, unit response information, incident cataloging, etc.) that would be used to train AI models.
- Reconcile and normalize numerous real-time data sources (e.g., GPS location, incident classifications, records management reporting, etc.) with an eye toward enhancing decision-making.
- Ensure interoperability with existing systems such as audio and multimedia recording, voice and text communications, quality assurance, computer aided dispatch, and records management systems.
- Evaluate the impacts on existing summary reporting, ad-hoc searching, and real-time display dashboards as well as secure storage and retention requirements.

Technology Selection and Customization

This is the stage where agencies gain the most knowledge about available products and services. While there may be no-cost platforms, the capabilities as well as the terms and conditions of use will vary substantially from paid versions. It is important to completely understand a provider's fee basis, as several have escalating costs based on the permanent storage of data regardless of statutory retention requirements.

Another important categorization of AI models is whether they are *public* or *private*, a distinction that expands on the design, control, security, and intended uses. In general, a public model is open to numerous users; is hosted over the Internet by third-party providers; system and training improvements are shared; and ownership, control, and governance reside with the provider. A private model is architected for a specific organization, with controlled access over the data and the model's learning; it may be provided as a dedicated cloud architecture or hosted in servers on-premise.

A summary of these and some other differences are provided below:

Feature	Public AI	Private AI
Accessibility	Open	Controlled
Data Security	Data processed externally	Data stays internal/private
Customization	Limited	Highly customizable
Compliance & Transparency	Provider-dependent	Improved clarity and accountability
Pricing	Lower up-front costs, typically subscription fees	Higher initial and recurring costs
Use Cases	Broad, general purpose	Specialized, proprietary, sensitive information

Typically, a formal solicitation (such as a request for proposals) begins substantive discussion with providers that elicits features, systems architectures, and total cost of ownership. While the number of AI models and tools increases daily, a platform should be selected that is tailored to emergency communications and dispatch needs; for instance:

- **Natural Language Processing (NLP)** for analyzing callers' speech, transcribing, and analyzing critical information.
- **Large Language Models (LLM)** for predictive analytics and optimizing resource deployment.
- **Geographic Information Systems (GIS) Integration** (such as geocoding addresses and boundary geofencing) for location-based requirements.

Ownership rights of the products from your new AI tools should also be carefully considered. In addition to the technical

fit for purpose evaluation, the entirety of provider license agreements must be understood. For example:

Intellectual Property	• What are the terms and conditions for receiving (and understanding) the provider's proprietary technology? • What are the specific non-disclosure terms and subsequent impacts on transparency and publicity regarding use of the products?
Model Training	• What data was used in preparing the AI model before it was acquired? • Who controls and has license to use the outputs of AI-processed transactions?
Use Restrictions	• Does the provider have specific restrictions or indemnification requirements on the use of the model (e.g., where lives are at risk)? • Does the provider allow or prohibit the development of proprietary product extensions and/or enhancements?
Responsibility for Output	• What is the understanding for resolution of flawed outputs such as 'hallucinations' or 'memorization' in offered products? • What tools are available for determining whether the model or the data is responsible for specific outputs?

A key set of concerns relates to the ownership, use and storage of agency-provided data. Much of the raw data that public safety agencies accumulate will include personal information, but location and incident data are increasingly being used by the private sector to develop correlations that impact an individual's privacy and which has financial and other implications.

In the past, many application provider's terms and conditions have been accepted at face value because they represented a reasonable protection of intellectual property. Some terms may now be negotiable, but others represent an unacceptable limitation or risk to a purchaser or the public they serve.

Pilot Testing and Validation

Testing and quality assurance of the platform are well established routines in information technology management. A team of experienced individuals from your stakeholders will assist in developing test cases, but you should also task a dedicated testing or project professional to track issues and resolution. Test plans and success criteria should consider:

- Conducting controlled trials for specific types of 'use cases' (e.g., various non-emergency calls, escalation, referral, etc.)
- Validate AI recommendations against existing policies, procedures, and human decisions to ensure accuracy.
- Implement fail-safes, such as automatic escalation to human operators or supervisory personnel for high-risk calls.
- Re-testing the resolution of specific reported issues as well as with each platform patch or upgrade.

Staff Training and Workflow Integration

Once you have confidence in your platform, implementation planning will guide training and roll-out. During this period, you should consider additional resources to focus on real-time evaluation and monitoring to correct critical issues. Don't forget the public relations component where you advise your public that they will observe changes in their access to services. In addition:

- Redesign workflows to blend AI automation (e.g., note-taking, translation) with human expertise.
- Train dispatchers to interpret AI outputs and override recommendations when necessary; have a system in place to capture these exceptions for follow-up.

Ethical and Legal Compliance

This phase of work is the culmination of your information technology governance, privacy, transparency, legal, and risk management oversight. Before deploying AI tools, you should have formal guidance and policy statements regarding the acquisition and use of artificial intelligence means and methods. Key guidance include:

- Adopting privacy-preservation practices to protect personally identifiable information (e.g., data minimization/ blurring, encryption, etc.).
- Periodic cataloging and audit of AI systems (especially for bias) and ensuring training data represents diverse demographics and current customer needs.
- Establishing specific accountability frameworks for reviewing and modifying AI-driven decision parameters.

Full Deployment and Continuous Monitoring

The last phase of implementation would represent the fulfillment of your strategic plan and the establishment of ongoing performance measurements. If your requirements are complex or impact multiple agencies, you may roll out AI incrementally starting with low-risk functions like call routing. Don't be discouraged if this is a multi-year project, but be sure to have interim milestones that represent affirmative checkpoints of value-added functions and features within a one-year time frame.

The core of quality is continuous learning, so monitor performance metrics and refine your measurement models (e.g., response time reduction, dispatcher workload). One of the great

benefits of AI tools is that measurement is done continuously, so there is no need to wait for periodic reporting cycles. Change can happen immediately (given appropriate reviews and approvals).

Final Considerations

In closing, the following key issues must be kept foremost in the planning and implementation of artificial intelligence capabilities in dispatch operations:

- **Human Oversight:** Maintain human-in-the-loop protocols to review AI decisions, especially in life-threatening scenarios.
- **Bias Mitigation:** Regularly update training datasets to address underrepresented groups and avoid discriminatory outcomes.
- **Cybersecurity/Data Protection:** Fortify systems against data breaches given the sensitivity of emergency call data to ensure criminal justice (CJIS) and personally identifiable (PII) information are not inadvertently "leaked" into an AI model.
- **Public Trust:** Communicate transparently with communities about AI's role to avoid perceptions of reduced accountability, loss of privacy, discrimination, or unequal treatment.
- **Regulatory Alignment:** Collaborate with state and local elected officials to establish standards for AI use in call taking and emergency response.

By following these steps and by addressing issues and concerns proactively, public safety dispatch centers can harness AI to improve operational capability, enhance efficiency, and maintain the public's confidence. ●

Bill Doolittle is the President of **911Insight®**, an independent management consulting practice specializing in public safety and emergency communications. He has over 20 years of experience supporting hundreds of public safety agencies nationally with information systems planning and implementation engagements. Doolittle is a certified professional in numerous disciplines, including change management, quality assurance, agile development, audit, and information technology service management.

This article is an original work and was authored using first-hand knowledge, substantial research, and market analysis by the author, but was also supplemented with the assistance of artificial intelligence tools.