EXECUTIVE SUMMARY

These are the proceedings of a workshop held on 2 March 2016 in San Antonio, Texas to address "Big Data and Fire Protection Systems." The goal of this workshop was to identify and prioritize the opportunities for big data to inform decision making for ITM (Inspection, Testing and Maintenance) used for built-in fire protection systems.

The on-going reliability of built-in fire protection systems is related to inspection, testing and maintenance (ITM) of these systems. This is addressed by multiple NFPA codes and standards, including NFPA 4, *Standard for Integrated Fire Protection and Life Safety System Testing*, NFPA 25, *Standard for the Inspection, Testing, and Maintenance of Water-Based Fire Protection Systems*, NFPA 72, *National Fire Alarm and Signaling Code*, and NFPA 2001, *Standard on Clean Agent Fire Extinguishing Systems*. Requirements for ITM have evolved over time, but often do not have a solid scientific basis.

A new activity at NFPA that directly relates to this topic is the proposed development of a Data Analytics Sandbox. NFPA is uniquely positioned to coordinate the next generation of data and data analytics in support of the built environment and safety infrastructure. Going forward, the NFPA Data Analytics Sandbox is anticipated as serving as an important collective resource, and serving as a next generation test bed in support of our rapidly evolving world of cyber physical systems and the internet of everything. The collection and coordination of ITM data, which will ultimately support the technical activities addressed by NFPA 4, 25, 72, 2001, etc., is considered a prime candidate activity for the NFPA Data Analytics Sandbox.

This workshop has gathered applicable stakeholder input and clarified certain information through roundtable discussions. Using Breakout Groups and through a series of structured questions, this information includes discussing how data can inform ITM decisions, identifying the key data needed and potential sources of data, and clarifying how NFPA can help. Key findings from this effort support five concept categories of recommendations: (1) *general*; *(2) data collection methods*; *(3) documentation*; *(4) stakeholder benefits/concerns*; and *(5) standardization*. Specifically, these include the following:

(1) General

- **Prioritize Occupancy Focus**: For start-up efforts, first focus on certain specific occupancies such as commercial properties.
- **Support Legislative Initiatives**: Identify, clarify and support legislatively-oriented initiatives that promote the sharing of data for the public good (e.g., the State of Georgia is working on data sharing legislation).
- **NFPA's Attributes**: NFPA, as a trusted 3rd party, is an ideal organization to serve as a central data collector.
- **Stakeholder Value Added**: NFPA can develop a clear consensus of the most important data based on stakeholder needs and explain to stakeholders the value of their own data collection.

 Code Requirement Validation: Analysis of collected data will verify whether or not recent code updates are successful or unsuccessful.

(2) Data Collection Methods

- **Novel Collection Methods**: Consider novel approaches such as indoor drone inspection.
- **Promote Automated Approaches**: Automate the data collection process to improve efficiency and effectiveness (e.g., automated impairment detection program to flag impaired systems).

Enable External Data Sets: Enable external unrelated data sets that can provide value-added to the overall pool of data (e.g., external real estate permitting data is presently available).

- **Data and Data Analytics Focus:** Focus on data and data analytics, and avoid any mandates of software, hardware, or similar details.
- **Positive Data Usage**: Data is often only collected if there is a negative issue, but there is also positive data available that shows the systems are functioning properly.
- **Enable User Friendly Data Collection**: Explore the aspect of user friendly data collection methods such as using mobile apps.
- **(3) Documentation**
- **Prioritize Essential Data**: Focus on data that is essential, and do not collect unnecessary data.
- **Focus on Data Needs**: Make sure the needed data drives the data collection process and not the forms and/or format.
- **Support Confidentiality Agreements**: Address confidentiality agreements between inspectors and property owners/manufacturers as a means of obtaining data that would otherwise be unavailable.
- **Manage Evolution**: Set performance characteristics, and allow the format to naturally evolve based on usage.
- **Establish Common Terminology**: Develop standard terminology to address the language and terminology differences between different regions or companies.

(4) Stakeholder Benefits/Concerns

- **Establish Data Safeguards**: Provide safeguards for user access so that all data and data analytics is used securely and wisely (e.g., by AHJs, end-users, researchers, etc.).
- **Address Data Breach Implications**: Consider liability implications due to data breaches (e.g., consider parallel case studies).
- **Identify Unrealized Data Analytics**: Demonstrate value-added for end-users by enabling analytics they would otherwise not have, including for their own proprietary data.
- **Promote User Benefits**: Continually emphasize end user benefits and value added.
- **Address Ultimate End-User Needs**: Identify and summarize end user problems to guide data analytic efforts (e.g., using collected thermostat data to develop residential profiles for addressing smoke detector performance in extreme temperatures)

(5) Standardization

- **Utilize Existing Standards**: Consider using existing standards that address the processing and handling of confidential data (e.g., existing ISO or IEEE standards on data confidentiality)
- **Clarify Data Types**: Distinguish between mandated data collection vs. voluntary.
- **Promote Automated Data Collection**: Promote automated data collection vs. manual data collection (e.g., establish minimum standardized data stream, with flexible data format)
- **Standardize Common Baseline Data**: Standardized baseline cross-sectional common data that is necessary for all ITM systems (e.g., limited location information, system age, commissioning details, etc.).
- **Support Risk Based Data Analytics**: Create code requirements customized for specific risks rather than system types. Systems vary based on occupancy type but there will always be a level of risk (which can be determined by analyzing collected data).