MEMORANDUM

DATE: **2/19/2020**
TO: **NPSTC Governing Board**
FROM: **Public Safety Internet of Things Working Group (PSIoT)**
RE: **Summary of Working Group Activities, Accomplishments and Recommendations for Future Work**

Dear NPSTC Governing Board,

In 2017, the Governing Board established the Public Safety Internet of Things (PSIoT) Working Group, under NPSTC's Technology and Broadband Committee. The PSIoT Working Group was charged by the Governing Board with accomplishing the following objectives:

- Examine the current state of IoT;
- Identify public safety-specific issues, focusing on the use of IoT devices and analytics;
- Identify issues and concerns for NPSTC Governing Board's review.

The Work Group has concluded these initial tasks and objectives assigned by the Governing Board. This Memo provides a brief status report on the activities, accomplishments and reports produced by the Working Group over the past three years.

We also have identified below several recommendations for PSIoT-related topics that merit additional research and study. We ask the Governing Board to review these recommendations and provide the PSIoT Working Group with guidance and direction for conducting additional work on any topics deemed by the Board to be worthy of investigation.

I. Activities and Accomplishments of the PSIoT Working Group

The PS IoT Working Group spent most of 2017 conducting research on the current state of IoT, by educating members about IoT technology, ecosystems, uses, benefits and other research being conducted. The Work Group hosted a series of presentations from federal government agencies, commercial vendors active in IoT technology development, wireless service providers and experts from law enforcement, fire, EMS and PSAP/dispatch centers.[1] We also held joint calls with other NPSTC Work Groups, such as the EMS Working Group and Video Technology Advisory Group (VTAG), to draw upon their expertise.

In 2018, the Group began to examine the specific value of IoT to public safety disciplines—law enforcement, fire, EMS, and PSAP/dispatch centers. The Group created eight use cases to highlight potential areas of interaction and benefits to public safety. The use cases were designed to identify how PSIoT might impact a variety of public safety responses, from basic to complex incidents, and escalating incidents involving multiple agencies and disciplines.

[1] The complete list of Work Group presentations is available in Appendix Two of the *PSIoT Outreach Report to Public Safety*.

In June 2019, the Working Group published its first report, *Public Safety Internet of Things (IoT) Use Case Report and Assessment Attributes*,[2] a compilation of the Group's discussion points for each use case. The *Use Case Report* also describes a list of 22 PSIoT Assessment Attributes—technical, governance and policy-based considerations that we used to focus use case discussions. These assessment attributes are a valuable guide, not only for public safety professionals considering PSIoT, but also for manufacturers and vendors wishing to develop PSIoT products and services for the public safety market.[3]

Building on the *Use Case Report*, the Working Group and NPSTC staff have developed a second report, the *Public Safety Internet of Things: Outreach Report to Public Safety*. The *Outreach Report* is designed to complement the *Use Case Report*, by providing a comprehensive overview of PSIoT and guidance to public safety agencies, Information Technology agency leaders and technical staff. This Report is now in the final stages of document formatting for submission to the Governing Board for final approval.

In addition to these formal reports, the Working Group developed comments from NPSTC to two important Interagency Reports developed by NIST, IR 8196, *Security Analysis of First Responder Mobile and Wearable Devices*[4], and Draft IR 8259, *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers*[5].

NIST IR 8196 analyzed the needs of public safety mobile devices and wearables from a cybersecurity perspective. NPSTC's Comments supported NIST's inclusion of local, state and Federal public safety entities in its process, and concurred with the overall conclusion that cybersecurity is a critical issue for public safety going forward.

In *Draft IR 8259*, NIST is proposing that manufacturers develop a "core baseline" of cybersecurity features for all IoT devices that makes devices at least minimally securable by the customers who acquire and use them. Although IR 8259 does not attempt to define specific baseline criteria—instead it references IR 8228 and recommends that IoT device manufacturers use the criteria established in IR 8228 to identify minimum cybersecurity features for devices.

NPSTC commented that NIST IR 8259 is an excellent starting point for manufacturers as they begin to define core baseline functions and develop transparent marketing materials describing those functions to their customers. However, device manufacturers need to recognize the importance of a specific "public safety vertical sector baseline," which would define IoT device cybersecurity and functionality features required by public safety. NPSTC suggested that the assessment attributes identified in the *Use Case Report* are a good starting point for IoT device manufacturers as they develop these necessary cybersecurity functionality baseline features for IoT devices that will be used during public safety incident operations.

---

[2] http://npstc.org/download.jsp?tableId=37&column=217&id=4195&file=NPSTC_PSIoT_Use_Cases_Report_190616.pdf

[3] The Use Case Report also captures the process used by the Work Group to develop the use cases, which can serve as a "roadmap" for NPSTC in the development of future use cases.

[4] http://npstc.org/download.jsp?tableId=37&column=217&id=4182&file=NPSTC_Comments_NIST_Cyber_190206.pdf.

[5] https://csrc.nist.gov/publications/detail/nistir/8259/draft.

Our work was also referenced in NIST IR 8255*, Interoperability of Real-Time Public Safety Data*, which provides recommendations for governance policies and procedures to help ensure effective data sharing among agencies, In addition, SAFECOM/NCSWIC's Information Sharing Framework Task Force (ISFTF) has proposed to use the NPSTC PSIoT use cases as a foundation for the development of functional and technical baseline requirements for an Information Sharing Framework (ISF).

II. Recommendations for Additional Research and Study

Based on this work, the Group has developed the following list of recommendations for additional research and study. We seek guidance as to which recommendations may fit best under NPSTC's mission, and ask for direction for what to include in the next phase of the Working Group's work. The list is not exclusive and includes only the most significant topics of the many areas that we discussed:

1) **Build on the NIST IR 8259 comments – to Outline and Develop a Public Safety Baseline for Cybersecurity Functionality (and for Other PSIoT Functionalities).** As we discovered in the development of NPSTC Comments to IR 8259, no one else in the public safety community is actively working on criteria for baseline functionality for PSIoT in the public safety vertical sector. Yet, there is a critical need to identify baseline functionality attributes as manufacturers develop secure, reliable and effective IoT systems for public safety. The Working Group can easily build on the 22 assessment attributes to propose a set of critical PSIoT functionalities to be considered by manufacturers as they develop PSIoT products and services. This baseline would be helpful to both the public safety community and to manufacturers serving the PSIoT market.

2) **Outline and Develop PSIoT Governance Best Practices.** Ideally, agencies should adopt PSIoT governance policies and procedures before the first PSIoT system is deployed. However, as we reviewed the many federal, state and local public safety governance documents and resources[6], we found that most are just beginning to address data, and none currently speak to governance policies and procedures for PSIoT. For example, while CISA's Incident Communications Advisory Council (ICAC) has made recommendations to enhance data communications and information management within the NIMS Incident Command Structure (ICS), these recommendations do not begin to address PSIoT. Likewise, although the *SAFECOM Interoperability Continuum* has been updated to include data communications, it does not specifically address PSIoT data sharing and interoperability.

[6] Sources reviewed included *SAFECOM Interoperability Continuum,* CISA's *National Emergency Communications Plan* (NECP) 2008, 2014 and 2019 revisions, Statewide Communications Interoperability Plans (SCIPs) and Tactical Interoperable Communications Plans (TICPs), the *Incident Command System* (ICS) recently updated to include a new role of Information Technology Service Unit Leader (ITSL), and state, local and regional standard operating procedures and operational plans. We also reviewed NIST-IR 8255*, Interoperability of Real-Time Public Safety Data*, which provides recommendations for governance policies and procedures to help ensure effective data sharing among agencies.

Although, this topic is very broad, we propose to focus the Working Group by building on the initial efforts of the ICAC and ISFTF. A starting point could be the development of a brief fact sheet with best practices for local agency PSIoT governance, policies and procedures. The fact sheet could also serve as a foundation for future revisions to ICS and SAFECOM/NCSWIC governance documents.

3) **Identify Local Needs and Opportunities for PSIoT.** As the Working group investigated the benefits of PSIoT, we discovered that implementation of new IoT technology will require collaboration between public safety agencies and other government departments, including Information Technology (IT) departments, transportation departments, public works departments and others. We identified two areas for collaboration that merit further study:
    a. **Define the Need and Requirements for Integrating PSIoT with Other Smart/Connected Community IoT Initiatives.** Areas to explore include cost-sharing, governance, security, data sharing and coordination of shared systems and facilities.
    b. **Define the Need and Requirements for Real-time Analytics Centers**. A real-time analytics center is a place where local or regional data (including PSIoT) is assimilated, analyzed and compared with other data to create actionable intelligence. As agencies begin to implement IoT and other technologies that generate vast amounts of data, some type of Real-Time Analytics Center will become necessary to manage and store this data. The Analytics Center can take one of several forms, depending upon the size of the community and relationship with regional partner agencies: Co-Located in the PSAP or Emergency Communications Center; Co-Located with a Smart City (or County) Operating Center; or developed in conjunction with a Public Safety Fusion Center.

As the Work Group develops additional resources and information, we believe that a comprehensive "Knowledge Book" of NPSTC Reports and other information on PSIoT topics would be beneficial to local agencies. Depending on the available NPSTC staffing and resources, this Knowledge Book could be an online repository of NPSTC PSIoT resources for both public safety agencies and manufacturers to provide information and answer questions on a wide range of PSIoT topics.

Conclusion

The Working Group wishes to expresses its thanks to the Board for allowing us to complete the work so far, which we believe to be of critical importance to public safety. We request that the Governing Board review the above recommendations and provide the PSIoT Working Group with guidance for conducting additional work on any topics deemed by the Board to be worthy of investigation. Please contact the Work Group Chair or Vice-Chair if you have any questions or feedback regarding any of our work.