Alerts, Warnings, and Notifications (AWN) Updates

Antwane Johnson, Director, Integrated Public Alert and Warning System (IPAWS) Program, Federal Emergency Management Agency (FEMA); Budge Currier, California Statewide Interoperability Coordinator (SWIC)

Mr. Johnson provided background information on the IPAWS program to include how it has evolved since 1951, and how it is used today to communicate public safety threats. Public safety organizations use AWN to communicate weather conditions, evacuations, Amber Alerts, and more to the public. Alerts can be sent in multiple languages and a variety of formats, including ring tones and text-to-speech. He discussed collaboration efforts with the Federal Communications Commission (FCC) to update IPAWS alerting rules. He highlighted new capabilities to improve the critical functions of AWN systems by this fall, such as enabling an organization to preview and publish more accurate messaging prior to dissemination, as well as cancel message dissemination, if needed. Mr. Johnson discussed the steps needed to increase the accuracy of messages through the new presidential alert, improvements to location capabilities to send messages to the polygon level, and additional measures to ensure organizations frequently update software for their systems. He also discussed plans to integrate IPAWS services to cloud-based platforms in September of 2019. Mr. Johnson highlighted efforts to engage with counties that currently do not use IPAWS and stated that SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC) can play a role in helping close the gap.

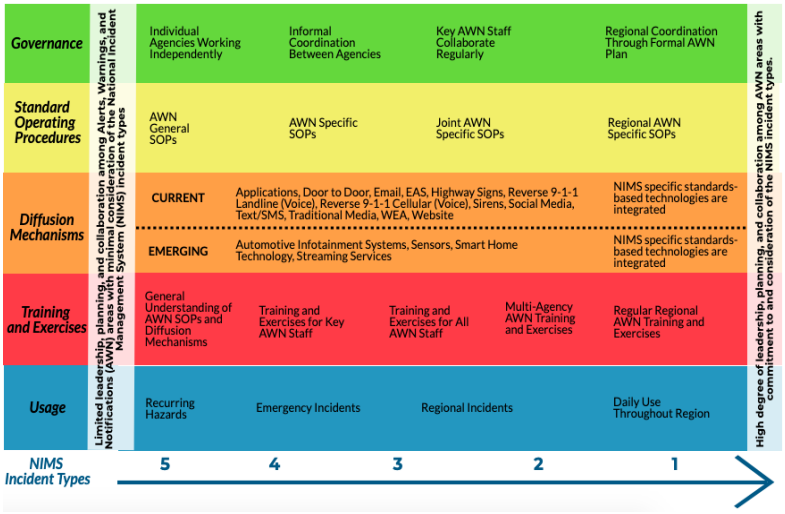

Figure 1: Maturity of AWN Systems as they relate to NIMS Incident Types

Mr. Currier provided examples of how California is integrating AWN into the state's Next Generation 911 (NG911) system and how it is being rolled out across the state. He discussed challenges with sending alerts during the 2017-2018 California wildfire season when they experienced cellular outages. Mr. Currier highlighted how the close partnership between the California Office of Emergency Services (CalOES) and cellular providers helped coordinate restoration activities and ensure coverage at evacuation centers, disaster recovery centers, incident command posts, and staging areas. He also provided an overview of AWN guidance recently developed by CalOES to provide best practices and training for jurisdictions and designated alerting authorities (AOs) in California.

During the discussion, members asked about requirements to update FCC emergency alert system (EAS) plans. Mr. Johnson stated that the requirement is to have a state EAS plan, but suggested those plans be more comprehensive to address AWN. Members also asked about engaging with businesses that send alerts. Mr. Johnson stated that FEMA engages with various businesses, such as Google, OnStar, and Microsoft. FEMA has plans to engage with the gaming community in the future to send alerts but noted vendor concerns about liability issues if a message is not delivered. Members discussed governance challenges associated with implementing an AWN system and encouraged collaboration between AOs and providers when sending alerts. Several members noted legislation in their respective states which addresses liabilities issues with phone companies. Mr. Johnson encouraged participants to reference CISA's *Public Safety Communications: Ten Keys to Enhancing Alerts, Warnings, and Notifications* document, citing that it includes excellent recommendations.

Panel and Working Session: SAFECOM's and NCSWIC's Roles Instituting a "Security First" Perspective to Mitigate the Cyber Threat

Dusty Rhoads, CISA; Michael Ogata, National Institute of Standards and Technology (NIST), Public Safety Communications Research Program (PSCR); Captain George Perera, SAFECOM (At-Large), Miami-Dade, Florida, Police Department; Mark Hogan, SAFECOM (At-Large), Director of Asset Management, City of Tulsa, Oklahoma; Richard Jackson, Information Security Manager, Asset Management, City of Tulsa, Oklahoma

Mr. Rhoads opened the session by discussing the importance of cybersecurity in the public safety community and the inclusion of cybersecurity initiatives in the National Emergency Communications Plan (NECP). Mr. Ogata discussed how to leverage the National Institute of Standards and Technology (NIST) Cybersecurity Framework for improving critical infrastructure and cybersecurity. The goal of the framework is to provide a common language for cybersecurity policies and initiatives, and guidance on how an organization can create their own cybersecurity initiatives. The framework empowers organizations to build or enhance an existing cybersecurity risk management program. Informed by industry, academics, and practitioners, the framework has five major functions: identify; protect; detect; respond; and recover. Implementing the actions and outcomes identified within the cybersecurity framework provides an organizational profile to inform executive decision makers, process managers, and business operations. The framework is designed with common and accessible language for customization and use across a broad spectrum of personnel. Its risk-based approach can be used in conjunction with existing documentation and the framework is intended to be a living document. The framework can be found at www.nist.gov/cyberframework, with additional cybersecurity resources available at http://csrc.nist.gov.

Figure 2: NIST Cybersecurity Framework v. 1.1

Mr. Perera, Mr. Hogan, and Mr. Jackson further highlighted the value of the NIST Cybersecurity Framework. Mr. Perera discussed the recent class-action lawsuit that has reached the Supreme Court regarding liability associated with an Amazon cybersecurity breach. As organizations are held more responsible and accountable for the consequences of cyber incidents, the need for proactive planning increases. Criminals are targeting Personally Identifiable Information (PII) information and data breaches are straining the resources of response organizations (e.g., Federal Bureau of Investigation). Additional agencies are being empowered as task force officers to investigate issues such as ransomware, as adversaries are targeting data beyond credit card information and seeking as much PII as possible. Mr. Perera reinforced the need to implement the NIST Cybersecurity Framework for threat protection. Mr. Perera also discussed the use of cloud-based technologies and architecture, and recommendations outlined in the 2014 International Association of Chiefs of Police (IACP) Technology Policy Framework available at https://www.theiacp.org/sites/default/files/all/i-j/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf.

Mr. Hogan reviewed recent cybersecurity incidents, including an impactful incident his organization experienced several years ago. He outlined the critical need for governance and responsive decision-making as well as cyber incident plans to augment response and recovery efforts. Since that time, the center has undergone penetration testing to discover vulnerabilities and enhanced IT policies, developed a Computer Security Incident Response Team (CSIRT) process, and made additional improvements to their cybersecurity posture.

Mr. Jackson stressed that a new paradigm exists where the IT mission is more foundational than the public safety mission for public safety organizations. The City of Tulsa used the NIST Cybersecurity Framework and assistance from the Department of Homeland Security to enhance their cybersecurity posture. Mr. Jackson stepped through the City of Tulsa's process of developing CSIRT procedures to support response/recovery and Information Technology/Information System (IT/IS) purchasing procedures to support risk mitigation. The key to the success of the CSIRT procedures is the collaboration of many parties. Mr. Jackson also mentioned upcoming federal legislation that will allow for cyber responses across organizations.

Next, participants engaged in guided discussions to answer questions focused on further scoping security concerns; identifying how existing resources are being used; current cybersecurity management strategies; and future program initiatives as they relate to objectives in the NECP. Mr. Rhoads closed the panel by reviewing activities within the 2019 NECP for both public safety organizations and SAFECOM/NCSWIC. These activities can improve the cybersecurity posture of the entire Emergency Communications Ecosystem.

A Proposal: Leveraging SAFECOM and NCSWIC to Address Information Interoperability

Chief Jonathan Lewin, SAFECOM (Major Cities Chiefs Association), Chicago Police Department; John Contestabile, Johns Hopkins University Applied Physics Laboratory; Rob Dew, CISA

Mr. Dew introduced Chief Lewin and discussed the Chicago Police Department's successes in technology adoption and integration. Chief Lewin reviewed the history and current state of Chicago's infrastructure, including the need for defined operational outcomes when collecting and integrating data. Taking a decentralized approach and pushing their fusion centers, known as Strategic Decision Support Centers (SDSCs), to the edge has enabled two-way data exchange through an Intelligence Action Cycle. Chicago is partnering with CISA to provide a data interoperability pilot. Chief Lewin reviewed some of the sources of input to their centers, including surveillance cameras, license plate readers, ShotSpotter, and location-based predictive tools. Chicago is using Citigraf™ to integrate computer-aided dispatch (CAD), ShotSpotter, Automatic License Plate Readers (ALPR), Geographic Information System (GIS), and other databases. Chief Lewin shared a video and statistics demonstrating the alignment of the various technologies and the real-world, positive operational outcomes of employing an integrated system. He also showed a video on GreenKey, an artificial intelligence tool intended to reduce administrative burden on law enforcement personnel.

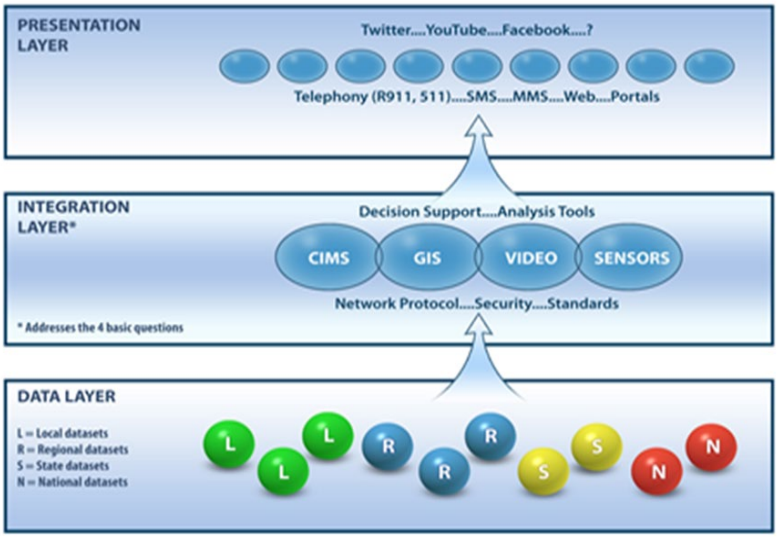

Figure 3: Conceptual Interoperability Model

Mr. Dew discussed a potential "data interoperability operational framework" to define rules and structure for achieving standards-based, two-way data exchange for public safety organizations. Mr. Contestabile reviewed the impact of an incident on data exchange with regard to sharing critical information, such as impacted jurisdiction, affiliation, and incident location. Data exchange is not just a technical issue, so the framework will need to account for people, processes, and technology. To advance development of the framework, the presenters proposed establishing a joint SAFECOM-NCSWIC subgroup for data interoperability (now termed the Information Sharing Framework Task Force). Mr. Dew provided a conceptual interoperability model, but stated the proposed subgroup would need to establish a more detailed model from a public safety perspective. The framework model would provide value to public safety organizations by helping them to define their own roadmaps. The subgroup would also address additional complexities, such as how to balance data access with security, handle the influx of Internet of Things (IoT) data, address the ability to create ad hoc networks, and address the need for overall process coordination.

Potential subgroup tasks include: ongoing engagement with peers to obtain community feedback and aggregate best practices/lessons learned; identification of the desired information flows between networks, applications/services, and devices;

development of recommendations to close interoperability gaps; and creation of a recommended roadmap of actions to be taken by SAFECOM-NCSWIC to solve interoperability challenges.

Mr. Dew solicited participants for the proposed data interoperability subgroup and Mr. Galvin also took an informal poll to determine the level of the interest among members. The majority of individuals were interested in establishing the group. Rob and John encouraged interested members to officially volunteer for the group by emailing SAFECOMgovernance@hq.dhs.gov or NCSWICgovernance@hq.dhs.gov.

A Proposal: Leveraging SAFECOM and NCSWIC to Address Information Interoperability Encryption for Storage Location Numbers (SLN)

Dusty Rhoads, CISA; Jim Downes, CISA

Mr. Rhoads discussed a recent concern expressed by multiple federal entities regarding the security of static encryption keys. The keys were distributed as part of the National SLN assignment plan, which the National Law Enforcement Communications Center (NLECC) and the Federal Partnership for Interoperable Communications (FPIC) created to establish a common configuration to enhance national encrypted interoperability. In June 2014, the FPIC approved a plan to reserve SLNs 1-20 to be used for national interoperability. By adopting this plan, public safety agencies at all levels can coordinate encrypted interoperability plans while minimizing SLN and key conflicts with other agencies.

However, given the reach and the now-outdated nature of the crypto keys, the consensus of federal entities is all current static encryption keys must be assumed compromised. Therefore, any agency that is currently utilizing static crypto keys should also consider them compromised. Mr. Rhoads urged state, local, tribal, territorial, and other users to work with CISA to develop a plan to rekey all Land Mobile Radio (LMR) subscriber units, which have been using the static encryption keys. He solicited support to stand up a task force to develop a plan that would be completed by the November 2019 Joint SAFECOM and NCSWIC meetings, to be presented for action in 2020. The task force would seek to minimize the time from start to finish, to focus work regionally, and to address any other programming issues or concern during the same timeframe. Jim Downes, CISA, was identified as the federal lead for this effort.

SAFECOM/NCSWIC Committees and Working Groups

- Joint Technology Policy Committee
  - Viewed a video demonstration of the NG911 Readiness Assessment Matrix and provided input
  - Received updates on the T-Band giveback legislation in U.S. Congress
  - Discussed information interoperability as it pertains to the Committee
  - Received updates about the status of the P25 User Needs Subcommittee and Compliance Assessment Program Advisory Panel
  - Discussed Committee work products and priorities for the remainder of the calendar year
  - Considered support for single-key encryption and Key Management Facility issues pursuant to changes in interoperability standards
  - Next Conference Call: Tuesday, May 21, 2019; 3:00 PM ET
- SAFECOM Governance Committee
  - Discussed documenting processes for reviewing SAFECOM membership composition for the Government Accountability Office Report and include in *SAFECOM Governance Charter* updates
  - Received SAFECOM membership updates
  - Discussed updating the SAFECOM product approval process to prepare for implementation
  - Next Conference Call: Wednesday, June 5, 2019; 1:00 PM ET
- Next Generation 911 Working Group

  - Reviewed and provided additional feedback on the *NG911 Maturity State Self-Assessment Tool* and accompanying resources (fact sheet and educational video) that provide background information and usage instructions
  - Reviewed and provided feedback on the *NG911 Executive Summaries* document which provides a high-level overview of resources and guidance available to assist public safety and emergency communications stakeholders during the transition to NG911
  - Continued developing the *GIS Best Practices* resource
  - Next Conference Call: Thursday, May 16, 2019
- NCSWIC Governance Committee
  - Brainstormed topics for the NCSWIC Academy, including discussing a proposed schedule and speakers
  - Proposed an edit to the NCSWIC Charter, allowing for non-Executive Committee (EC) members to Chair committees
    - NCSWIC EC Members approved a modified edit during the NCSWIC EC meeting on April 24
  - Discussed developing a series of NCSWIC Videos, the first of which will provide a SWIC 101 overview for external audiences
  - Next Conference Call: Thursday, May 23, 2019; 1:30 PM ET
- Joint Funding and Sustainment Committee
  - Continued developing the *Value Analysis Guide*
  - Discussed future updates to the *Funding Mechanisms Guide*
  - Next Conference Call: Wednesday, May 15, 2019; 3:00 PM ET
- SAFECOM Education and Outreach Committee
  - Continued developing the *Public Safety Communications Succession Planning Guide* and additional outreach and engagement tracking materials
  - Discussed potential future platforms for SAFECOM to engage social media
  - Next Conference Call: Wednesday, May 22, 2019; 2:00 PM ET
- NCSWIC Planning, Training, and Exercise (PTE) Committee
  - Discussed the PTE in-person meeting outcomes and action items
  - Reviewed the COMM-X Portal and discussed potential improvements
  - Next Conference Call: Tuesday, May 28, 2019; 3:00 PM ET
- Communications Section Task Force (CSTF)
  - Highlighted outcomes from the Incident Communications Advisory Council Meeting on March 19, 2019, in San Diego, California to include narrowing of options for changing the organization of the National Incident Management System Incident Command System including adding an Information Technology Unit to the Service Branch; adding a Communications Branch under the Logistics Section; or creating a Communications Section
  - Reviewed, provided feedback to, and granted provisional approval of the draft National Qualification System Position Task Book for the position of Auxiliary Communications pending incorporation of CSTF recommendations
  - Received an update on and provided input to CISA's Incident Communications Measures, which are a product of the CSTF Metrics Team, to include identification of future opportunities for CSTF members to engage with CISA to help inform incident communications metrics
  - Identified action items for the next CSTF conference call on May 13, 2019

Future Meetings

Meeting	Location	Date
SAFECOM and NCSWIC Public Safety Strategic Collaboration Meeting	Atlanta, Georgia	November 4-8, 2019