

SAFECOM Executive Summary

Welcome and New Member Introductions

SAFECOM Chair, Chief Gerald Reardon, SAFECOM At-Large (City of Cambridge, Massachusetts, Fire Department), welcomed SAFECOM members and announced new members who recently joined SAFECOM, including Chief Greg Rubin, International Association of Fire Chiefs, and Harriet Rennie Brown, National Association of State 9-1-1 Administrators (Alternate).

Cybersecurity and Infrastructure Security Agency (CISA) Acting Assistant Director (AAD) for Emergency Communications, Vincent DeLaurentis thanked SAFECOM for its outstanding work in communities across the country. He noted how in-person meetings provide an opportunity to exchange ideas to advance national level emergency communications missions, highlighting SAFECOM's recent endorsement of the updated National Emergency Communications Plan (NECP), released by CISA on September 25, 2019. The updated NECP addresses current gaps within emergency communications, reflects new and emerging technological advancements, and provides guidance to drive the Nation towards a common end-state of emergency communications. AAD DeLaurentis thanked members for their continued support as SAFECOM and CISA work together to implement the Plan.

SAFECOM Election

Over the past several months, SAFECOM conducted elections for open committee chair and vice chair positions, as well as the new Board Member positions and culminated in the re-election of Chief Chris Lombard as SAFECOM First Vice Chair. These elections filled the seats on the newly-established SAFECOM Executive Board, which serves as SAFECOM's leadership group and the primary resource for access to public safety stakeholders and policymakers.



Photo: 2020 SAFECOM Executive Board (left to right): Charlie Sasser (Board Member), Sheriff Paul Fitzgerald (Board Member), Anthony Catalanotto (Board Member), Chief Douglas M. Aiken (Board Member), Michael Murphy (SAFECOM Second Vice Chair), Chief Gerald Reardon (SAFECOM Chair), Chief Chris Lombard (SAFECOM First Vice Chair), Captain George Perera (Governance Committee Chair), Phil Mann (Technology Policy Committee Chair), Lloyd Mitchell (Funding & Sustainment Committee Chair), Michael Davis (Education & Outreach Committee Chair)

SAFECOM Strategic Priorities

Governance Committee: The Governance Committee discussed recent updates to SAFECOM membership, including discussions around further expanding SAFECOM's membership and will continue its membership recruiting efforts into 2020. With the establishment of the SAFECOM Executive Board, the Committee stood up a working group to review and update existing SAFECOM products and materials to reference the new Board. The Committee also discussed its 2020 strategic priorities which focus on providing guidance for elevating emerging communications issues and strategies for updating governance membership. The

SAFECOM Executive Summary

Committee will close out 2019 with the development of the *2019 SAFECOM Annual Summary* and the *2020 SAFECOM Strategic Plan*, both of which will incorporate feedback from across the SAFECOM committees. In 2020, the Committee will continue to revise the *SAFECOM Governance Charter*, incorporating the new Executive Board structure, and further clarifying the processes and procedures for operating SAFECOM.

Education and Outreach Committee: The Education and Outreach Committee addressed several administrative items, including electing Michael Davis, SAFECOM At-Large, and Sean Fensterwald, SAFECOM At-Large, to the Committee's Chair and Vice Chair positions, respectively; setting SAFECOM outreach goals using the SAFECOM Outreach and Engagement Form; and reviewing the status of the SAFECOM Membership Questionnaire and the SAFECOM Succession Planning Toolkit. The Committee also reviewed and updated their strategic priorities, charging the Committee with creating and implementing a broad engagement strategy heavily focused on digital media, such as social media and podcasts. The Committee will continue to promote all SAFECOM tools and resources for 2020 through the maintenance of the SAFECOM website and stakeholder engagement activities.

Funding and Sustainment Committee: The Funding and Sustainment Committee reviewed and finalized the *Value Analysis Guide* and *Value Analysis Guide Brochure* and plans to create a blog and elevator speech to accompany the products in the coming months. For the rest of 2019 and beginning of 2020, the Committee will continue to update the *Funding Mechanisms Guide*, providing an overview of various methods of funding emergency communications systems. Later in 2020, the Committee will begin to develop the *Funding Life Cycle Planning Guide Appendix: Continuity of Operations Planning (COOP)*. The appendix will show COOP best practices, models, and checklists to be considered during lifecycle planning.

Technology Policy Committee: The Technology Policy Committee resolved to develop several work products in 2020, including guidance on the following topics: dependencies on non-agency infrastructure or services, interoperability using messaging platforms, unmanned aircrafts systems (UAS), and specific radio frequency interferences reported by the user community. The Committee also approved the *Public Safety Communications: Essentials of Alerts, Warnings & Notifications* ("AWN Essentials") document.

Communications Section Task Force: The Communications Section Task Force discussed their 2020 priorities; NECP implementation activities; the Incident Communications Advisory Council's (ICAC) recommendation to FEMA; and developed a proposed Communications Branch structure. The group highlighted the need to share recent updates with incident communications personnel and will focus on developing an outreach plan as a top priority. The outreach plan will address recommendations to enhance information communications technology within National Incident Management System (NIMS) Incident Command System (ICS), such as the ICAC's proposal to develop a Communications Branch. CISA has collected 31 letters of support for the Communications Branch thus far, and two letters expressing reservations. As the CISA Interoperable Communications Technical Assistance Program (ICTAP) further develops the Information Technology Service Unit Leader (ITSL) and related positions, the Task Force developed a notional Communications Branch structure, defining the functions under the ITSL, and how cybersecurity and help desk functions should be organized.

Information Sharing Framework Task Force: Established in April 2019, the Information Sharing Framework Task Force was established to develop a framework to allow for public safety during a multi-jurisdictional, multi-agency incident to share information. The Task Force is developing a survey to consider who needs access to data; where is data located; and how to transport data. The Task Force will also utilize use case scenarios to help the public safety community understand the structure of the framework and how to apply it. Next year, the Task Force plans to conduct pilots for the framework and develop strategies for engaging industry partners like First Responder Network Authority (FirstNet Authority) and standards bodies to develop grant guidance so public safety entities can apply for funding to implement the framework. The Task Force will also seek to coordinate through ICTAP for training so that first responders and public safety agencies understand how to customize the framework.

SAFECOM Executive Summary

Project 25 Compliance Assessment Program Task Force: The Project 25 (P25) Compliance Assessment Program Task Force (CAPTF) met to discuss the transition from the Department of Homeland Security’s (DHS) Science and Technology (S&T) Compliance Assessment Program Advisory Panel meeting structure to the SAFECOM structure. During the meeting, participants discussed membership, meeting cadence, and the product approval process. The Task Force also discussed 2020 strategic planning during the meeting. The group proposed coordinating with S&T on the Inter-RF Subsystem Interface/Console Subsystem Interface conformance and interoperability compliance testing, developing a recommendation for a minimum set of standards for Mission Critical Push to Talk and Interworking Functions for action by the P25 Steering Committee and P25 manufacturers, and engaging with the P25 User Needs Working Group to develop interoperability and compliance testing for developed standards supporting new user needs requirements.



Photo: SAFECOM Members, November 2019

Member Spotlight: National Sheriffs’ Association



Photo: Sheriff Paul H. Fitzgerald

Sheriff Paul H. Fitzgerald, National Sheriffs’ Association, highlighted the International Criminal Police Organization ([INTERPOL](#)) and the use of federation—an indispensable tool for law enforcement that provides the ability to query two databases simultaneously. The nature of law enforcement has changed significantly over the past several decades, in large part because of the threats faced today—terrorism, organized narcotics trafficking, human trafficking and human smuggling operations, and transnational criminal organizations. These threats and threat-actors are present today both *physically* and *virtually*—in communities of all sizes. When dealing with transnational crime, agencies need access to actionable criminal investigative intelligence and information from our international law enforcement partners, which is where INTERPOL comes into play.

INTERPOL is the largest international police organization in the world; however, it is an *organization*, not an *agency*, and has no law enforcement authority of its own. Instead, it provides an inter-governmental platform upon which law enforcement agencies from 194-member countries can work together to combat transnational crime and terrorism. Under INTERPOL’s constitution, each member country is required to establish a National Central Bureau, which serves as the executive agent and primary point of contact for all INTERPOL matters within that country. In the United States, INTERPOL Washington is the U.S. National Central Bureau. A component of the U.S. Department of Justice, it is co-managed by DHS under an agreement whose purpose is to ensure that its international criminal investigative information and resources are available not only across the federal interagency, but across all state, local, tribal, and territorial law enforcement agencies.

SAFECOM Executive Summary

INTERPOL Washington is exclusively authorized to access INTERPOL’s system of investigative and analytical databases for purposes that include criminal investigation, law enforcement, border security screening, and humanitarian assistance. To ensure these systems provide the widest possible benefit, each National Central Bureau is also authorized to extend query access to any law enforcement agency within its own country, something that INTERPOL Washington has accomplished by integrating access to INTERPOL data into national law enforcement information sharing environments such as the National Law Enforcement Telecommunications System (Nlets). As a result, any law enforcement official with Nlets access can query INTERPOL data. To enhance the availability and use of this information, INTERPOL has worked with Nlets to develop a federated query capability. Federation gives law enforcement the ability to query two databases simultaneously—in this case, the Federal Bureau of Investigation’s National Crime Information Center (NCIC) system, and INTERPOL’s

Automated Search Facility: a single query that produces results from these two premier criminal justice indices. This capability is critically important for all law enforcement users in part because of a common misunderstanding that if you query NCIC on a

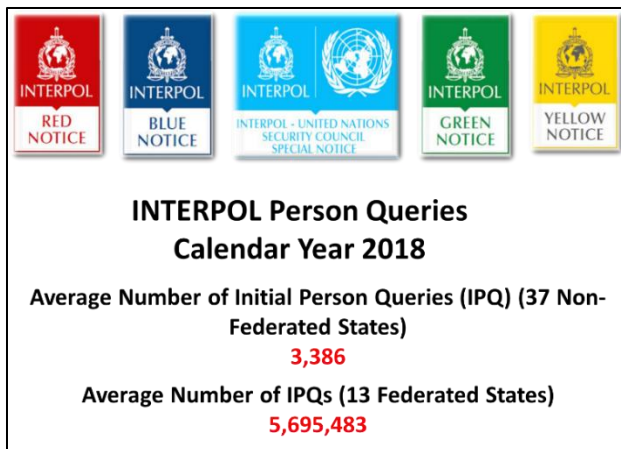


Image: Difference in amount of processing activity between states with federated queries and those without.

person, you obtain all INTERPOL information. In fact, because of certain NCIC entry criteria, this query results in only a fraction of INTERPOL’s information. The difference in the amount of processing activity between the states that have federated their queries and those that have not is extreme. In 2018, the 37 states who were not at that time federated, processed an average of 3,386 INTERPOL person queries. At the same time, the 13 states that had federated their systems processed nearly 5.7 million queries. This disparity leaves a potentially serious gap in law enforcement agencies’ ability to identify and detect persons who may pose a potentially serious threat to officer safety and public safety. Today, only 15 of the 50 states are known to have federated their systems, including only 4 border states. In an age in which transnational crime and terrorism are a growing threat, federated queries provide a critical capability—the ability to immediately and concurrently determine both the domestic *and* international law enforcement interest in, or threat posed by, a subject whom they encounter during their official duties.

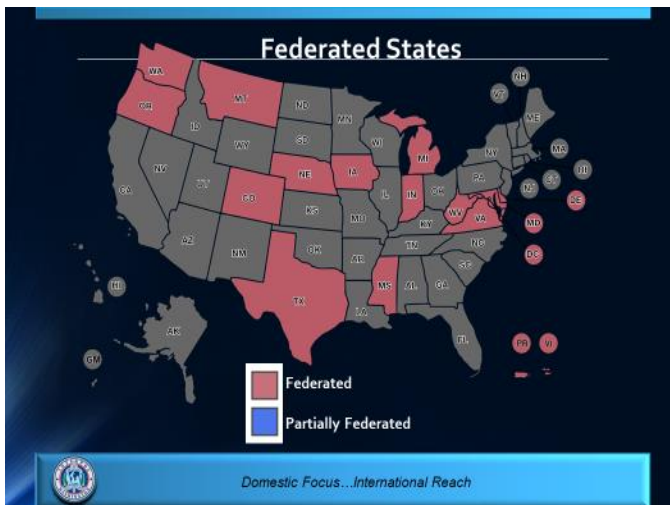


Image: Today, only 15 of the 50 states are known to have federated their systems, including 4 border states.

What can your agency do? First, recognize that crime is increasingly transnational and is present in communities of all sizes. Next—whether federated or not—ensure that INTERPOL data is being routinely queried in connection with all criminal investigation, law enforcement, and humanitarian assistance operations, where applicable. If your state is *not* federated, request that federation be made a strategic goal in its law enforcement and homeland security planning. Finally, contact INTERPOL Washington for additional information and technical assistance regarding federation at 202-616-9000 or USNCBFrontOffice@usdoj.gov.

SAFECOM Executive Summary

DHS S&T Updates

Sridhar Kowdley, S&T, provided an overview of the revitalized S&T organizational structure, including updates to the Office for Interoperability and Compatibility (OIC). OIC, now designated as a technology center, remains focused on emergency communications research and development (R&D) for public safety. However, there is a renewed focus on conducting enduring R&D activities which may have a three to five-year horizon. Mr. Kowdley detailed S&T's process for obtaining state and local first responder capability gaps, including discussion about the First Responder Resource Group (FRRG). FRRG is the representative stakeholder group through which S&T obtains its requirements for this customer segment. The presentation also focused on S&T's Small Business Innovation Research Program (SBIR) which provides an opportunity for S&T to partner with innovative small businesses on a variety of public safety related R&D topics. The SBIR program consists of three distinct phases: (1) proof of concept, (2) prototype demonstration, and (3) commercialization. Mr. Kowdley highlighted a select number of existing SBIR projects from the emergency communications and information sharing domain including a Wearable Fentanyl Badge Sensor, Social Media Extraction Tool, and a low-cost Internet of Things flood sensor. New topics are regularly chosen; the newly selected list of Fiscal Year 2020 topics were just [released](#). Mr. Kowdley highlighted S&T's recent Shaken Fury Operational Experimentation event that took place in Birmingham, Alabama, in coordination with state and local public safety agencies. The goal of the event was to evaluate how selected DHS-developed and commercial technologies integrate with existing public safety systems using open standards, and how those integrated capabilities enhance operational communications, increase operational coordination, improve responder safety, and augment situational awareness. Finally, Mr. Kowdley reminded SAFECOM members of S&T's planned presence at the [International Wireless Communications Expo \(IWCE\) 2020](#) in Las Vegas, Nevada, where S&T and CISA plan to once again share an exhibit booth. During the Expo, S&T will hold a demonstration of a Land Mobile Radio and Long-Term Evolution interworking solution from one of its SBIR efforts.

T-Band Update

Chief Reardon emphasized the need for SAFECOM members to support passage of [H.R. 451](#): "Don't Break Up the T-Band Act of 2019." Auctioning the T-Band spectrum would endanger crucial public safety communications and cost billions of dollars. For decades, in eleven major metropolitan areas around the country, the T-Band has supported vital public safety radio communications for first responders. A section of the *Middle-Class Tax Relief and Job Creation Act of 2012*, requires the Federal Communications Commission (FCC) to reallocate and auction the T-Band spectrum by 2021. Options for replacement spectrum are extremely limited. There is no alternative spectrum available for these public safety users. The Government Accountability Office (GAO) completed a 2019 study which found that auctioning off the T-band radio spectrum without the availability of alternative spectrum would jeopardize public safety in major metropolitan areas around the country. The GAO also concluded that even if alternative available spectrum were available, public safety users are likely to bear significant costs associated with relocating and reestablishing interoperability. In early 2019, the FCC placed the total cost between \$5-6 billion. GAO concluded that Congress should pass legislation allowing first responders to continue using the T-Band radio spectrum. The "Don't Break Up the T-Band Act" would repeal the FCC reallocation and auction requirement and allow law enforcement, fire officials, and EMS to continue using the T-Band spectrum.¹

¹ Based on excerpts of delivered remarks by Congressman Eliot Engel to the House Energy and Commerce Committee, Tuesday, July 16, 2019. <https://engel.house.gov/index.cfm?sectionid=61&itemid=4777>