SAFECOM INTEROPERABILITY CONTINUUM UPDATES FREQUENTLY ASKED QUESTIONS (FAQS)

INTRODUCTION

This Frequently Asked Questions (FAQs) document is designed to address commonly asked questions regarding the updates made to the *SAFECOM Interoperability Continuum*. To gain a full understanding of the Continuum, the *SAFECOM Interoperability Continuum Brochure* was developed to describe all aspects associated with the *Continuum.*

QUESTIONS AND ANSWERS

1) **Why was the *SAFECOM Interoperability Continuum* updated? Who updated it?**
   The *Interoperability Continuum* was updated to include additional guidance on public safety interoperability. The Continuum was updated with practitioner input from the SAFECOM program, federal partner agencies, and a cadre of public safety communications stakeholders under the auspices of the Cybersecurity and Infrastructure Security Agency (CISA).

2) **How is the updated version of the *SAFECOM Interoperability Continuum* different from the previous or orginal version?**
   The updated version does not render the original *Interoperability Continuum* obsolete, but rather expands the original's scope by including new sub-elements, success indicators, and language to address the dynamic Emergency Communications Ecosystem described in the *National Emergency Communications Plan*. Each critical success element (governance, standard operating procedures/guidelines [SOPs/SOGs] and field operations guides [FOGs], technology, training and exercises, and usage) has been updated in some capacity, as outlined below:
   - ***Governance:*** adds two new success indicators with accompanying language and new language regarding lifecycle funding
   - ***SOPs:*** element revised to *SOPs/SOGs and FOGs* and includes new language accompanying the addition of SOGs and FOGs
   - ***Technology:*** includes new sub-element, *Security & Continuity of Operations*, with accompanying success indicators and new language about the different types of security
   - ***Training and Exercises:*** includes new language describing the importance of evaluating/documenting performance and participating with personnel outside of individual organizations
   - ***Usage:*** revised fourth success indicator to include inter-jurisdictional and inter-disciplinary use

   Additionally, new language was added explaining the Emergency Communications Ecosystem and its relationship to the *Interoperability Continuum*.

   For full details on the changes listed, please refer to questions 4 – 8 or the updated SAFECOM Interoperability Continuum Brochure.

3) How should public safety agencies and jurisdictions use the *SAFECOM Interoperability Continuum*?

Interoperability is an evolving, multi-dimensional challenge. To gain a true picture of an agency's, jurisdiction's, and/or a region's interoperability, progress in each of the five inter-dependent elements must be evaluated. Optimal interoperability is contingent on an agency's and jurisdiction's public safety missions. The Continuum is designed to assist public safety disciplines, agencies, and jurisdictions pursuing interoperable solutions based on changing needs or additional resources.

4) Why is Governance the first lane in the *Interoperability Continuum*?

An effective governance structure supports valid and authorized decision-making, encourages collaboration, participation, and cooperation, fosters trust and understanding, and establishes policies and procedures. When working to establish and maintain interoperable communications across agencies, public safety disciplines, and all levels of government, it is essential to establish governance as the first step towards achieving success.

5) To what extent does the *Interoperability Continuum* provide guidance on security and cybersecurity? / How does security and continuity of operations interact with technology?

The original *Interoperability Continuum* focused on '*Security'* in the context of protecting voice and data communications from interception, disruption, and alteration. However, as federal, state, local, tribal, territorial, andpublic safety organizations increasingly collaborate and share information using advanced technologies (e.g., Internet Protocol [IP]-based and broadband equipment), the challenges of safeguarding technology and information now extends to cyberspace. As a result, across all levels of government, an integrated approach is required to address infrastructure and physical security, cybersecurity, and encryption in order to collectively strengthen the security posture of the Emergency Communications Ecosystem. This integrated approach addresses the security and authentication challenges that must be considered in all implementation decisions. Successful security risk management starts with strong governance and is highly integrated across all of the lanes of the Continuum.

Furthermore, cybersecurity crosses all lanes of the *Interoperability Continuum* as it affects service providers, end users, and both cyber and physical resources alike. The *Continuum Brochure* refers readers to the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Criminal Justice Information Services (CJIS) Guidelines for guidance on how to achieve their security and cybersecurity goals.

6) What is the difference between the Interoperability Continuum and the Ecosystem?

The Emergency Communications Ecosystem consists of the various functions and people that exchange information prior to, during, and after incidents and planned events. The Ecosystem encompasses traditional emergency response personnel, agencies, and stakeholders (e.g., medical facilities, public utilities, nongovernmental organizations) that share information as well as the media and private citizens.

As one of the evolving tools in the Ecosystem, the *Interoperability Continuum* is designed to assist emergency response personnel, agencies, and policy makers (e.g., Government-to-Government public safety communications) to plan and implement interoperability solutions for sharing data and voice

communications. Information sharing is critical for public safety personnel to make informed decisions and better protect themselves and the public.

7) How does lifecycle funding align with Governance?

Through the governance framework, public safety stakeholders make numerous important decisions to plan, fund, procure, implement, support, and maintain communications systems, and eventually replace and dispose of systems and components. A wide array of funding resources is available to support the acquisition and implementation of interoperable communications resources. Decisions as to which mechanisms to pursue are best handled at the governance level.

Funding decisions impact each of the five inter-dependent elements. For example, when a governance body purchases radios to work in chemical plants, firefighters and hazardous materials personnel require revised policies, procedures, training, and exercises to effectively use the new equipment. Funding this continuous system lifecycle planning can be daunting. To assist stakeholders, the 2011 *Emergency Communications Systems Lifecycle Planning Guide* and the 2018 *Compendium* are intended to provide considerations and recommended actions through easy-to-use checklists for each phase of the system lifecycle planning model.

8) What is the difference between Standard Operating Procedures (SOPs), Standard Operating Guidelines (SOGs), and Field Operating Guides (FOGs)?

Standard Operating Procedures (SOP) are formal written guidelines with specific instructions for incident response—typically with both operational and technical components. Established SOPs enable emergency responders to successfully coordinate an incident response across disciplines and jurisdictions. Clear and effective SOPs are essential in the development and deployment of any interoperable communications solution. End users may require justification to deviate from following an SOP.

Standard Operating Guidelines (SOG) provide a foundation of policies and procedures for how agencies operate during incidents. SOGs allow responders the flexibility to deviate from the guidance depending on situational or incident mitigation needs. Less prescriptive than an SOP, an SOG communicates a preferred but not necessarily required means of accomplishing a task.

Field Operating Guides (FOG) provide detailed interoperable communications resource information. FOGs can also include assets by location and technical assistance references to call upon additional skilled communications personnel. A FOG serves as a reference manual for delivering emergency communications services for incident management.

While an agency may have all three of these documents, agencies typically have either an SOP manual or an SOG manual rather than have both. A FOG may be used by an agency regardless of an accompanying SOP or SOG manual.