SEGURIDAD PÚBLICA

CAPÍTULO 16

LA SEGURIDAD ES ESENCIAL PARA LA PROSPERIDAD DE LOS ESTADOS UNIDOS La banda ancha puede ayudar al personal de seguridad pública a evitar emergencias y responder con rapidez cuando ocurran. La banda ancha también puede proporcionar al público nuevas formas para pedir ayuda y recibir información de emergencias.

Un sistema vanguardista de comunicaciones de seguridad pública usa tecnologías de banda ancha:

- Para permitir que las personas que sean las primeras en responder, en cualquier lugar del país, envíen y reciban datos de voz y video fundamentales para salvar vidas, reducir lesiones y evitar actos delictivos o terroristas.
- Para asegurar que todos los Estadounidenses puedan acceder a servicios de emergencia rápidamente y enviar y recibir información esencial, sin importar cómo se transmita.
- Para revolucionar la forma en que se informa a los norteamericanos sobre emergencias y desastres de forma tal que puedan recibir información esencial para su seguridad.
- Para reducir amenazas al comercio electrónico y otras aplicaciones basadas en el Internet garantizando la seguridad de las redes de banda ancha del país.

Desafortunadamente, los Estados Unidos todavía no ha realizado el potencial de la banda ancha para mejorar la seguridad pública. Hoy, personal de emergencia de las diferentes jurisdicciones y agencias no siempre se pueden comunicar durante emergencias. Los sistemas de emergencias 911 funcionan en redes de conmutación de circuitos. De la misma forma, los gobiernos locales, estatales, tribales y federales usan sistemas antiguos de alerta para informar al público durante las emergencias.

Los Estados Unidos también enfrenta amenazas a la resiliencia y la seguridad de sus redes. A medida que el mundo se traslada a la comunicación en línea, las fronteras digitales de los Estados Unidos tienen una seguridad muy inferior a la de las fronteras físicas.

El país debe mejorar en ese sentido. En un mundo con banda ancha, existe una oportunidad única para lograr una visión integral para mejorar la seguridad del pueblo estadounidense. La planificación cuidadosa y el compromiso firme pueden crear un sistema vanguardista de comunicaciones de seguridad pública para permitir que las personas que sean las primeras en responder, en cualquier parte del país, se comuniquen entre sí, envíen y reciban datos de voz y video para salvar vidas, reducir lesiones y evitar actos delictivos o terroristas.

La banda ancha también puede hacer que los sistemas de alerta de emergencia y del 911 sean más efectivos al permitir una mejor protección de vidas y bienes. Por ejemplo, con la banda ancha, los centros de llamada del 911 (también conocidos como puntos de respuesta de seguridad pública o PSAP [*public safety answering points*]) podrian recibir textos, imágenes y videos del público y proveerlos a las personas que sean las primeras en responder. De forma similar, el gobierno podría usar las redes de banda ancha para difundir información esencial en varios formatos e idiomas para el público durante emergencias en varios formatos e idiomas.

Finalmente, las redes de banda ancha con buenas estructura y seguridad podrían reducir las amenazas a los programas de aplicación basados en el Internet. La diseminación de comunicaciones basadas en protocolo de Internet (IP) requiere una seguridad cibernética más sólida. Los desastres y las pandemias pueden llevar a problemas repentinos en los flujos normales del tráfico IP. Como resultado, las redes de comunicación de banda ancha deben mantener estándares altos de confiabilidad, resiliencia y seguridad.

Las recomendaciones en este capítulo se concibieron para hacer posible esta visión.

RECOMENDACIONES

Promover comunicaciones de banda ancha inalámbrica para la seguridad pública

- Crear una red de comunicaciones interoperable de banda ancha inalámbrica para seguridad pública (red de banda ancha para seguridad pública).
- Identificar sobre dispositivos e infraestructura inalámbrica de banda ancha para seguridad pública.
- Asegurar que los servicios satelitales de banda ancha sean parte de cualquier programa para la preparación ante emergencias.
- Preservar las comunicaciones de banda ancha durante emergencias.

Promover la seguridad cibernética y la protección de infraestructura crítica de banda ancha.

- La Comisión Federal de Comunicaciones (FCC, *Federal Communications Commission*) debería emitir una guia de seguridad cibernética.
- La FCC debería expandir sus requisitos de informes sobre cortes de suministro para los proveedores de servicios de banda ancha.

- La FCC debería crear un sistema voluntario de certificación de seguridad cibernética.
- La FCC y el Departamento de Seguridad Nacional (DHS, *Department of Homeland Security*) deberían crear un sistema de reportes de información de seguridad cibernética (CIRS, *cybersecurity information reporting system*).
- La FCC debería expandir el alcance comunitario y participación internacional.
- La FCC debería explorar la preparación y la resiliencia de las redes.
- La FCC y el Sistema Nacional de Comunicaciones (NCS, *National Communications System*) deberían crear acceso a redes de prioridad y enrutamiento para comunicaciones de banda ancha.
- La FCC debería explorar la resiliencia y la confiabilidad de las comunicaciones de banda ancha.

Fomentar la innovación en el desarrollo y la implementación del 911 de última generación (NG 911) y de los sistemas de alerta de emergencia

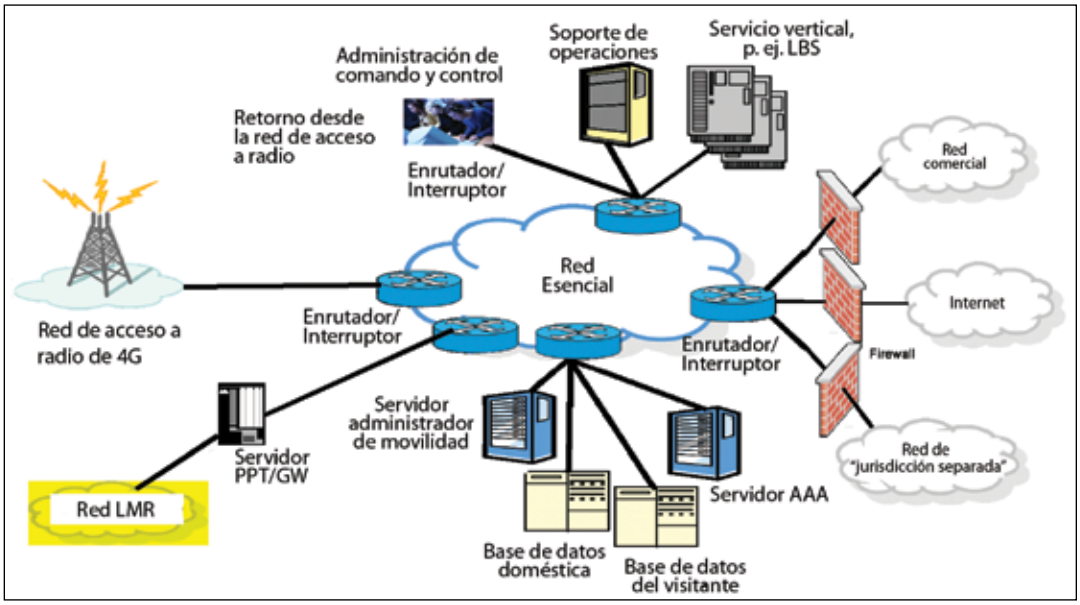
- La Administración Nacional de Seguridad de Tráfico por Autopistas (NHTSA, *National Highway Traffic Safety Administration*) debería preparar un informe para identificar el costo de implementación a nivel nacional del sistema NG911 y recomendarle al Congreso que considere proveer financiamiento público.
- El Congreso debería considerar promulgar un marco regulatorio federal.
- La FCC debería abordar servicios, aplicaciones y dispositivos de comunicaciones basados en IP.
- La FCC debería lanzar consultas del sistema de alerta integral de próxima generación.
- El Poder Ejecutivo debería aclarar los roles de las agencias en la implementación y el mantenimiento del sistema de próxima generación de advertencia y alerta.

16.1 PROMOCIÓN DE LA SEGURIDAD PÚBLICA EN LAS COMUNICACIONES DE BANDA ANCHA INALÁMBRICA

RECOMENDACIÓN 16.1: Crear una red de banda ancha para seguridad pública.

- **Crear un sistema administrativo que garantice el acceso a una capacidad suficiente en forma diaria y en casos de emergencia.**
- **Garantizar que haya un mecanismo implementado para promover la interoperabilidad y la operabilidad de la red.**
- **Establecer un mecanismo de financiamiento para garantizar que la red se implemente en todos los Estados Unidos y tenga la cobertura, la resiliencia y la redundancia necesarias.**
- **Alinearse con los programas existentes para funcionar con la red de banda ancha para seguridad pública.**

Exposición 16-A: Arquitectura de la red de banda ancha para la seguridad pública[3]



Hace tiempo el país reconoció el potencial que tienen las tecnologías de banda ancha para revolucionar las comunicaciones móviles inalámbricas de respuestas ante emergencias. Esta tecnología proveerá a las primeras personas en responder herramientas nuevas para salvar vidas en los Estados Unidos. El país necesita una red de banda ancha para seguridad pública que permita a las primeras personas en responder comunicarse entre sí. Un triple enfoque permitirá la implementación rápida, el funcionamiento y la evolución continua de dicha red.

En primer lugar, un sistema administrativo debe garantizar que los usuarios del espectro de banda ancha para seguridad pública tengan la capacidad y el servicio que necesitan para su red y puedan optimizar las tecnologías comerciales para capturar economías de escala y alcance. Existen beneficios significativos, incluso eficiencias a nivel de costo y avances tecnológicos mejorados, si la comunidad de seguridad pública puede usar cada vez más las aplicaciones y los dispositivos desarrollados para redes de banda ancha inalámbrica comercial. En última instancia, este sistema debe ser flexible y permitir que las entidades de seguridad pública puedan forjar sociedades basadas en incentivos con operadores comerciales y otros.[1]

Este sistema permitirá que la comunidad de seguridad pública materialice los beneficios de las tecnologías comerciales, las cuales reducirán los costos y asegurarán el desarrollo de la red. Sin embargo, la optimización de la banda ancha comercial no será suficiente para desarrollar una red nacional realmente interoperable que cumpla con los estándares de seguridad pública. Para garantizar la resiliencia, la capacidad y la redundancia necesarias, la comunidad de seguridad pública debería poder itinerar y obtener acceso prioritario a otras redes comerciales de banda ancha. Los operadores comerciales deberían ser compensados por este servicio a una tasa razonable.

Las iniciativas anteriores por crear una red de voz interoperable con banda estrecha para seguridad pública han fallado. Los datos sugieren que muchos sistemas de radio para seguridad pública carecen de la interoperabilidad básica. También sugieren que la mayoría de las jurisdicciones que mejoraron sus sistemas aún tienen un nivel "intermedio" de interoperabilidad, en el mejor de los casos, no el nivel avanzado de interoperabilidad que se requiere para comunicaciones verdaderamente integradas en caso de una emergencia seria.[2] La red de banda ancha para seguridad pública ofrece actualmente una nueva oportunidad para lograr interoperabilidad avanzada hoy.

Además de un sistema administrativo sólido, la FCC también debería crear un Centro de Interoperabilidad para Respuestas ante Emergencias (ERIC, *Emergency Response Interoperability Center*) para asegurar que estas aplicaciones, dispositivos y redes trabajen en forma conjunta para que las primeras personas en responder se puedan comunicar entre sí sin contratiempos. Además, la Agencia Federal de Administración de Emergencias (FEMA, *Federal Emergency Management Agency*) debería llevar a cabo una encuesta para hacer seguimiento del progreso de la interoperabilidad de la banda ancha para la comunidad de seguridad pública. El ERIC establecerá el curso de la interoperabilidad de inmediato y garantizará que se mantenga. Concentrarse en la interoperabilidad desde el principio debería ayudar a la red de banda ancha para seguridad pública a superar las dificultades enfrentadas por otras iniciativas de voz anteriores.

Finalmente, un programa de subvenciones será diseñado para proveer apoyo federal a las iniciativas locales a fin de financiar el capital y los costos continuos de la red de banda ancha para seguridad pública. El programa de subvenciones debe proveer a los operadores de la red de seguridad pública apoyar a largo plazo y flexibilidad suficiente para formar asociaciones adecuadas con los integradores de sistemas y otros proveedores para garantizar que la red de banda ancha para seguridad pública se implemente en forma adecuada.

Sistema administrativo

En 1997, el Congreso dictaminó que la FCC ofrece a las agencias de seguridad pública un espectro en la banda de 700 MHz, considerado espectro de primera calidad para la comunicación

CUADRO 16-1:

Materializar la promesa de la banda ancha para mejorar la respuesta médica ante emergencias.

El Cardiólogo Richard Katz conoce el potencial de la banda ancha para salvar vidas.

Durante una audiencia de campo de la FCC en el Centro médico de Georgetown University, el profesor universitario de medicina de George Washington University (GWU) detalló claramente cómo las tecnologías de banda ancha inalámbricas pueden ayudarlo a proveer atención médica ante emergencias.

Una "tirita inteligente" (smart band-aid) pegada al pecho o a la muñeca de una víctima de un accidente puede detectar los signos vitales y transmitir en forma inalámbrica esta información al Dr. Katz a través de la red mVisum de la GWU.

Puede recibir electrocardiogramas de calidad "inmaculada" en su teléfono celular.

Y puede usar su teléfono para acceder a los registros médicos del paciente y difundir mensajes de emergencia y alertas. En resumen, las tecnologías de banda ancha permiten al Dr. Katz integrar los aspectos de la atención médica y mejorar su capacidad de proveer asistencia durante una catástrofe u otra emergencia.

de seguridad pública. En 2007, la FCC adoptó normas para promover la construcción, implementación y funcionamiento de una red[4] nacional de banda ancha para seguridad pública de 700 MHz, inalámbrica e integrada, mediante la creación de una asociación obligatoria entre la comunidad de seguridad pública y el titular privado de una licencia con una asignación de un espectro comercial de 700 MHz, conocida como "Bloque D". Luego, la FCC llevó a cabo una subasta en la cual el espectro del Bloque D no logró conseguir la oferta mínima requerida. Existen varias razones posibles para este fracaso.[5]

La FCC debería superar los desafíos anteriores impulsando, sin exigencias, asociaciones basadas en incentivos para asegurar el éxito. La FCC debería impulsar soluciones de red que reduzcan costos y debería proveer opciones para la comunidad de seguridad pública a fin de optimizar las redes comerciales, las redes privadas o ambas.[6] Estas normas también deberían ofrecer a la comunidad de seguridad pública más alternativas competitivas entre los socios comerciales. Además, una vez que la red nueva pueda admitir comunicaciones de voz de "misión crítica", la FCC debería evaluar los requisitos necesarios del espectro para garantizar una capacidad adecuada para ese uso, tanto como para las redes existentes. Eventualmente, un conjunto de normas más flexible debería permitir un mejor equilibro entre las necesidades de la comunidad de seguridad pública y las compañías que se asociarán para construir esa red.

Con más detalle, el sistema administrativo debería incluir:

- *La oportunidad de ingresar a asociaciones flexibles de espectro compartido con operadores comerciales.* La comunidad de seguridad pública debe poder asociarse con operadores comerciales y demás (tales como integradores de sistemas) para reducir los costos de la construcción de la red e impulsar su evolución. A diferencia del enfoque anterior que se centralizó únicamente en el Bloque D, un modelo de asociación basada en incentivos que aborda no sólo al Bloque D, sino a un espectro comercial inalámbrico más amplio, ofrecerá una flexibilidad mejorada y los beneficios de las economías de escala. Estas asociaciones deberían estar sujetas a los requisitos de interoperabilidad establecidos por el ERIC. Los titulares de las licencias de seguridad pública también deberían permitir que los socios de seguridad no pública usen del espectro en forma secundaria, el cual pueden adquirir por medio del arrendamiento con opción de compra o mecanismos similares. Los socios podrían incluir usuarios de infraestructura crítica tales como la conexión de servicios públicos a una red inteligente.[7] Sin embargo, cualquier ingreso que reciba una entidad de seguridad pública por dicho uso debe utilizarse para construir o mejorar la red de banda ancha para seguridad pública.
- *Acceso de la seguridad pública a itinerancia y acceso prioritario a redes comerciales.* Para mejorar la capacidad de las redes de seguridad pública durante emergencias, la FCC debería iniciar una reglamentación para requerir a los proveedores de servicios comerciales móviles de radio que ofrecen a los usuarios de seguridad pública la posibilidad de itinerar en redes comerciales de 700 MHz y, potencialmente, con otras bandas. La comunidad de seguridad pública debería tener esta posibilidad tanto en áreas donde las redes inalámbricas de banda ancha para seguridad pública no están disponibles como en áreas donde actualmente hay una red para seguridad pública funcionando pero se requiere más capacidad para responder en forma efectiva ante una emergencia.

  La reglamentación también debería estipular que, cuando una red inalámbrica de banda ancha para seguridad pública está al límite de su capacidad o no funciona, los usuarios autorizados de seguridad pública deberían obtener acceso prioritario a redes comerciales, incluso todas las redes que usan la banda de 700 MHz y potencialmente a otras redes también. El o los titulares de licencias deberían poder obtener acceso prioritario bajo términos similares a aquellos requeridos actualmente en el Servicio Inalámbrico Prioritario (WPS, Wireless Priority Service). Pero, a diferencia del WPS, esta capacidad debería estar disponible para las personas que sean las primeras en responder a nivel local y estatal, tanto como para las comunicaciones de seguridad nacional/preparación ante emergencias (NS/EP). Además, el marco de acceso prioritario debería aprovechar el acceso adicional y las capacidades de priorización de tecnologías inalámbricas 4G. A diferencia de las redes celulares actuales de conmutación de circuitos, las redes inalámbricas 4G pueden darle prioridad inmediata a los datos de seguridad pública sin tener que esperar que se libere la capacidad comercial. Los operadores comerciales deberían recibir una compensación razonable por el acceso prioritario y las capacidades de itinerancia de la seguridad pública en sus redes.
- *Adjudicar licensias al Bloque D para uso comercial, con opciones para asociaciones de seguridad pública.* La FCC debería adjudicar rápidamente licencia al Bloque D para uso comercial mientras se implementan varios requisitos para el titular(es) de las licencias para maximizar las opciones para las asociaciones con seguridad pública. En primer lugar, la FCC debería solicitar que tanto el titular(es) de las licencias del Bloque D como el titular(es) de las licencias de la banda ancha para seguridad pública operen sus redes usando el mismo estándar de tecnología de interfaz por aire. El consenso que surge de la comunidad de seguridad pública y de los proveedores es que las redes de 700 MHz usarán los estándares del tipo Evolución a Largo Plazo (LTE, *Long Term Evolution*). La FCC debería considerar la designación de

este estándar.[8] Una interfaz por aire consistente genera una probabilidad mayor de interoperabilidad entre las redes de seguiridad pública y comericales del Bloque D. Facilitará el servicio itinerante entre redes para mejorar la cobertura y el acceso de los clientes para la seguridad pública y comercial. Además, una interfaz por aire consistente impulsará mas usuarios potenciales y permitirá a las entidades de seguridad pública beneficiarse con las economías comerciales de escala, que de otra forma no existirían. Antes que el Bloque D sea subastado, se deberá aclarar que se le puede exigir a cualquier titular de licencia del Bloque D que provee itinerancia y acceso prioritario del tipo WPS con una compensación razonable.

Segundo, el desarrollo de dispositivos comerciales que puedan funcionar en la totalidad de la Banda 14 de 3GPP es fundamental. (La Banda 14 en la banda de 700 MHz incluye el Bloque D y un espectro de banda ancha para seguridad pública). Por lo tanto, la FCC debería requerir al titular(es) de las licencias del Bloque D y, potencialmente, a otros titulares de licencias, que desarrollen y ofrezcan dispositivos capaces de proveer servicio usando todo el espectro de la Banda 14 de 700 MHz e identifiquen un recorrido hacia una producción a gran escala de dichos dispositivos. Los dispositivos comerciales deberían permitir a la comunidad de seguridad pública el acceso a alternativas mejores y menos costosas para el uso en el espectro de seguridad pública y facilitarán el acceso a bloques de espectro donde el titular de la licencia del Bloque D y el titular de la licencia de seguridad pública puedan formar una asociación de redes compartidas. La FCC debería investigar otros modos de impulsar la implementación de dispositivos de seguridad pública que transmitan a través de toda la porción de banda ancha de la banda de 700 MHz (es decir, Banda 12, Banda 13, Banda 14 y Banda 17).

- *Cobertura de responsabilidad civil para socios comerciales.* Una ley federal que provee servicios de Voz sobre el Protocolo de Internet (VoIP, *Voice over Internet Protocol*) inalámbricos y otras comunicaciones ante emergencias con cobertura de responsabilidad civil e inmunidad para el transporte de comunicaciones de seguridad pública que no sea inferior que la cobertura de responsabilidad civil e inmunidad otorgada a los proveedores de las centrales telefónicas locales.[9] Los titulares de la licencia comercial deberían tener la misma cobertura de responsabilidad civil para las comunicaciones de seguridad pública cuando, por ejemplo, los titulares de la licencia de seguridad pública itineran o usan el acceso prioritario en redes comerciales o en redes compartidas que dan soporte a comunicaciones de seguridad pública o comerciales.
- *Optimización del poder de compra.* La FCC, conjuntamente con otras agencias federales, debería investigar otras medidas de reducción de costos para la construcción de infraestructura de redes de banda ancha para seguridad pública. El ERIC y el DHS deberían trabajar con la Administración de Servicios Generales (GSA, *General Services Administration*) para ofrecer un programa de tarifas que las entidades de seguridad pública puedan usar para acceder a las redes de banda ancha nacionales comerciales y para obtener equipos para las redes. Esto generaría ahorros inmediatos y brindaría un importante criterio de referencia para costos. Además, los gobiernos, locales, tribales y estatales pueden ayudar a bajar los costos. El uso compartido de infraestructura también puede reforzar la confiabilidad de la red y la continuidad del servicio entre las redes comerciales, particularmente cuando los proveedores ingresan en asociaciones basadas en incentivos con organizaciones de seguridad pública.

ERIC

La FCC debería crear inmediatamente el ERIC bajo la Oficina de Seguridad Pública y Seguridad Nacional (*Public Safety and Homeland Security Bureau)*. El ERIC desarrollará estándares comunes para la interoperabilidad y procedimientos de funcionamiento para que sean usados en las entidades de seguridad pública con licencias para construir, operar y usar esta red a nivel nacional. Para establecer una visión común, el ERIC debe existir antes de que alguno de los titulares de licencias comience la construcción de esa red. Esto asegurará que el gobierno, la seguridad pública y la industria de las comunicaciones se alejen de la creación y del soporte a las redes fragmentadas de seguridad pública para comunicaciones inalámbricas de banda ancha.[10]

El ERIC establecerá una norma para un intercambio integral de comunicaciones inalámbricas para seguridad pública a nivel nacional, base interoperable desde el inicio del desarrollo de la red. Esto es crucial para permitir a quienes responden desde las diferentes jurisdicciones y disciplinas a comunicarse entre sí cuando convergen en una emergencia o cuando los incidentes abarcan varias jurisdicciones. De forma similar, las personas que son las primeras en responder deben tener acceso a programas de aplicación comunes en cualquier situación o ubicación.[11] Para asegurar el éxito y la optimización de la experiencia existente, el ERIC debería tener aprobación para trabajar de cerca con la Oficina de Comunicaciones de Emergencia (OEC, *Office of Emergency Communications*) del DHS. Una coordinación cuidadosa le permitirá al ERIC complementar la misión de la OEC de crear procedimientos estándares de funcionamiento y control para asegurar que comunicaciones para seguridad pública fluyan a través de una red integrada. El ERIC también

debería tener un cuerpo de asesores sobre seguridad pública para garantizar el asesoramiento adecuado.[12]

El presupuesto del año fiscal 2010 de la FCC propone fondos de $1.5 millones para establecer el ERIC y requisitos de personal inicial de soporte. A medida que el ERIC y las redes de banda ancha propuestas maduran, se necesitarán aproximadamente $5.5 millones por año a partir del año fiscal 2012 para que el ERIC funcione a pleno.[13] Estos fondos adicionales le permitirán a la FCC asociarse con el Instituto Nacional de Estándares y Tecnología (NIST, *National Institute of Standards and Technology*) para desarrollar los estándares adecuados y mantener la experiencia profesional del ERIC. Estos fondos también asegurarán que el personal adecuado aborde las tres funciones centrales del ERIC: ingeniería de redes, operaciones técnicas de redes y control de redes. Además, el Congreso debería considerar proveerle al DHS $1 millón en fondos públicos durante el año fiscal 2011, como está propuesto en su presupuesto, y de allí en más cada año. Los fondos ayudarán al DHS a coordinar el ERIC con la OEC y las entidades del DHS relevantes, y a mejorar el alcance de la OEC a agencias tribales, estatales y locales.

Como mínimo, el ERIC debería:

- Adoptar procedimientos y requisitos técnicos y operativos para asegurar un nivel nacional de interoperabilidad; esto debería implementarse y hacerse cumplir a través de las normas, licencias, condiciones de arrendamiento y condiciones de subvención de la FCC.
- Adoptar e implementar otros procedimientos y requisitos técnicos de interoperabilidad y operativos que puedan hacerse cumplir para abordar, como mínimo, operabilidad, itinerancia, acceso prioritario, funciones de puerta de entrada, interfaces e interconectividad de las redes de banda ancha para seguridad pública.
- Adoptar requisitos de autenticación y cifrado para los aplicaciones comunes de banda ancha para seguridad pública y el uso de red.
- Coordinar el marco de interoperabilidad de las regulaciones, los requisitos de licencias, las condiciones de subvención y los estándares técnicos con otras entidades (p. ej., quienes son titulares de licencias de banda ancha para seguridad pública, DHS, NIST y la Administración Nacional de Información y Telecomunicaciones).

El ERIC también debería trabajar con el DHS y la comunidad de seguridad pública para asegurar que la red de banda ancha para seguridad pública y las redes inalámbricas de banda estrecha para seguridad pública puedan comunicarse entre sí sin contratiempos. El comité de asesores de seguridad pública del ERIC[14] proporcionará datos de la comunidad de seguridad pública sobre las acciones propuestas del ERIC.

El ERIC debería trabajar con el Programa de Investigación de Seguridad Pública (*Public Safety Communications Research Program*) de NIST para asegurar que colabore en su trabajo sobre investigación, desarrollo, pruebas, evaluación y estándares tanto con la industria como con la comunidad de seguridad pública. No existe ninguna instalación de laboratorios federales para probar en forma independiente y demostrar las tecnologías de banda ancha de 700 MHz de seguridad pública. La creación de una instalación huésped neutral les permitirá a todos los interesados trabajar para desarrollar una red de banda ancha inalámbrica para seguridad pública y asegurar que los estándares de banda ancha comercial puedan cumplir con los requisitos específicos de seguridad pública. Esto ayudará a hacer que las redes y los equipos sean compatibles para el uso de seguridad pública.

El NIST ha anunciado que está avanzando con el desarrollo de una demostración de red de banda ancha para seguridad pública de 700 MHz en el año calendario 2010. El Congreso debería considerar asignar fondos públicos a largo plazo para continuar este y otros programas que apoyen la nueva red para seguridad pública.

Programa de subvenciones

El desarrollo de una red de banda ancha para seguridad pública en todo el país a través de asociaciones basadas en incentivos hará que los Estadounidenses estén más seguros.[15] Un programa de subvenciones le dará a la seguridad pública su red edurecida de acceso inalámbrico de banda ancha; asegurará que la mayoría de las áreas vulnerables de los Estados Unidos tengan la cobertura que necesitan; proporcionará seguridad pública con capacidad adicional y resiliencia a través del acceso al espectro comercial de los alrededores; asegurará que la comunidad que ofrecen respuestas ante emergencias tenga las herramientas que necesita; y optimizará el uso efectivo de recursos.

Como se muestra en la Exposición 16-B; un enfoque múltiple proporcionará seguridad pública con aumentados confiabilidad, capacidad y ahorros de costo. Primero, la red endurecida proporcionará un servicio confiable en un área amplia completa. Segundo, debido a que quienes responden ante emergencias podrán itinerar en redes comerciales, la capacidad y la resiliencia mejorarán a un costo razonable. Tercero, la cobertura localizada mejorará a través del uso de microcélulas fijas (como las que proporcionan cobertura interna en los rascacielos) y microcélulas móviles que pueden colocarse en autobombas, vehículos de policía y ambulancias. Cuarto, los equipos se pueden obtener de depósitos y usarse durante una catástrofe cuando la infraestructura está destruida o es insuficiente o no funciona. Las subvenciones para apoyar la red de banda ancha para seguridad pública deberían distribuirse a través de una

sola agencia para integrar las operaciones, reducir costos y asegurar que las subvenciones se dan en forma consistente. Las subvenciones deberían financiar solamente proyectos que cumplan con los requisitos del ERIC y deberían hacerse para los cuatro objetivos que se presentan a continuación:

- Construcción de una red de banda ancha de 700 MHz para seguridad pública que involucre asociaciones y usos de infraestructura comercial, infraestructura de seguridad pública o ambas a través de asociaciones basadas en incentivos.
- Cobertura de áreas rurales dentro de la geografía de la red.
- Fortalecimiento de la red comercial existente y los nuevos sitios que funcionarán como parte de la red para seguridad pública (incluso la cobertura de los costos de ingeniería no recurrentes para el acceso prioritario inalámbrico a la banda ancha).[16]
- Desarrollo de un inventario con capacidad para implementarse para la banda de 700 MHz para seguridad pública.

Una sola agencia que otorgue las subvenciones, en coordinación con el ERIC, debería estructurar los fondos para asegurar que la red se construya en forma eficiente. La agencia que otorgue las subvenciones debería tener flexibilidad para limitar el tiempo que tiene quien recibe la subvención para gastar los fondos subvencionados. También debería asegurar que el dinero gastado se justifique a través de requisitos de informes y de auditoría. La agencia que otorga las subvenciones debería instar a quienes las reciban a firmar acuerdos para compartir infraestructura, cuando corresponda, con entidades que implementen redes de banda ancha con apoyo de otros programas de subvenciones. Estos acuerdos deberían revisarse anualmente y cualquier ahorro que generen debe tenerse en cuenta al momento de asignar fondos para cada programa.

La red de banda ancha para seguridad pública requiere una inversión sustancial. Con el uso de un modelo que cubra a un 99% de la población,[17] la implementación de esta red requerirá tanto como $6.5 mil millones en gastos de capital en 2010 durante un período de 10 años, lo que pueda reducirse tomando medidas de eficiencia tales como programas estatales y locales y USF (Fondo del Servicio Universal, *Universal Service Fund*).[18] Los fondos públicos iniciales para los requisitos de capital deberían comenzar a tiempo para permitir que la red para seguridad pública se beneficie de las construcciones de infraestructura planificadas de las redes de banda ancha inalámbrica 4G privadas, que están programadas para que comiencen en 2010. El Congreso debería considerar proporcionar la mayoría de estos fondos entre el segundo y quinto año de la construcción de la red.

Se espera que suban los costos corrientes, incluso los gastos operativos y los costos adecuados de mejora de la red, de cero a comienzos del año fiscal 2011 y lleguen a un pico de $1.3 mil millones por año en 10 años del programa de construcción

Exposición 16-B: Soluciones y red para la seguridad pública

de capital y luego seguirá un curva ascendente sustancial que coincide con la expansión de la red.[19]

El valor total presente del gasto de capital y los costos corrientes durante los próximos 10 años es de aproximadamente $12–16 mil millones. Los gobiernos estatales y locales podrían contribuir con fondos para cubrir algunos de estos costos y podrían existir métodos adicionales de reducción de costos para disminuir esa estimación (tales como compartir infraestructura federal, trabajar con servicios públicos o usar torres estatales o locales para mejorar la cobertura). También se espera que este emprendimiento produzca una cantidad de empleos a largo plazo en los Estados Unidos.[20]

Es esencial que los Estados Unidos establezca un mecanismo de financiamiento adecuado, sustentable y a largo plazo para ayudar a pagar el funcionamiento, el mantenimiento y las actualizaciones de la red de banda ancha para seguridad pública. La seguridad de los Estados Unidos depende de ello. El Congreso debería considerar la creación de un mecanismo de financiamiento en el año fiscal 2011, pero no después del año fiscal 2012. El reconocimiento de que los Estadounidenses obtendrán beneficios sustanciales de la creación de esta red mediante la imposición de una tarifa de seguridad mínima en todos los usuarios de banda ancha de los Estados Unidos sería un mecanismo de financiamiento justo, sustentable y razonable. La tarifa sería suficiente para sustentar el funcionamiento y la evolución de la red de banda ancha para seguridad pública.

Es esencial que la comunidad de seguridad pública tenga los fondos para funcionar, mantener y mejorar la red. Todos los usuarios de banda ancha de los Estados Unidos se beneficiarán de esta red. La expansión de los costos nominales entre ellos asegurará que quienes responden ante emergencias en el país tengan acceso a capacidades de comunicaciones críticas cuando y donde lo necesiten.[21]

El Congreso deberá considerar autorizar a la FCC para imponer o requerir la imposición de dicha tarifa u otros medios de financiamiento. El Congreso también debería considerar permitir que la FCC implemente o autorice mecanismos para recaudar, administrar, auditar y apoyar el desembolso de estos fondos a través de la agencia que otorga las subvenciones. El dinero recibido financiaría el programa de la agencia que otorga subvenciones para las operaciones y evolución de la banda ancha para seguridad pública. Deben establecerse condiciones estrictas para prohibir cualquier desvío de esos fondos por parte de los gobiernos estatales y locales, y requerir que se cumplan los estándares desarrollados por el ERIC. La agencia que otorga, subvenciones debería tener autorización para determinar de qué forma es mejor asignar los fondos para asegurar un equilibro adecuado entre los usuarios urbanos, suburbanos y rurales, y requerir que quienes reciban las subvenciones justifiquen los fondos que reciben. Y debería distribuir los fondos en una forma que también permite la evolución de la red.

Programas existentes

En las emergencias, el gobierno federal usa un sistema desarrollado por la FCC llamado *Project Roll Call* para determinar el estado operativo de las comunicaciones inalámbricas y de transmisión (incluso las comunicaciones de seguridad pública) y para ayudar a los administradores ante emergencias a restaurar las operaciones cuando fuere necesario. Sin embargo, el sistema no está diseñado para funcionar en un entorno de espectro de banda ancha de 700 MHz. La implementación de una nueva red para seguridad

Exposición 16-C: Selección de aplicaciones y servicios de banda ancha propuestos para la red de banda ancha para la seguridad pública

Fidecomiso para el espectro de seguridad pública	• Acceso remoto a bases de datos de criminales • Descarga de archivos a alta velocidad • Distribución de señales de video de vigilancia para el personal que se encuentra en escena
Funcionarios de EMS de la Asociación Nacional de Estado	• Videos de calidad médica • Transmisión de diversas señales vitales • Seguimiento de recursos en tiempo real (p. ej., ambulancias) • Transmisión segura de registros médicos
Consejo Nacional de Telecomunicaciones para la Seguridad Pública	• Recopilación de información • Inspecciones automatizadas • Monitoreo ambiental • Gestión de tráfico
AT&T	• Servicios basados en la ubicación • Envío de mensajes • Red privada virtual
Telcordia	• Comando y control en tiempo real • Logística y apoyo de decisiones
Distrito de Columbia	• Administración de identidad y credenciales en tiempo real • Interoperabilidad con sistemas de despacho asistidos por computadora y sistemas de voz

pública de banda ancha requerirá volver a diseñar el *Project Roll Call* y las compras de nuevos equipos para que funcionen en el nuevo espectro. Estos esfuerzos le darán al gobierno federal la capacidad que necesita para restaurar rápidamente las comunicaciones de banda ancha para seguridad pública ante una catástrofe o una emergencia. Del mismo modo, el Congreso debería considerar proporcionar $6.9 millones adicionales en el año fiscal 2012 o antes (y $1.9 millones de fondos públicos en forma reiterada todos los años) para que la FCC diseñe y adquiera sistemas mejorados para el proyecto *Roll Call*.

RECOMENDACIÓN 16.2: Realizar encuestas sobre dispositivos e infraestructura móvil inalámbrica de banda ancha para seguridad pública.

Falta información detallada sobre las implementaciones estatales y locales de equipos, infraestructura y redes de banda ancha para seguridad pública. La FEMA, que trabaja con grupos de trabajo de Coordinación Regional de Comunicaciones de Emergencia, recoge datos periódicamente sobre los sistemas de banda estrecha. La documentación de la implementación y el uso de la banda ancha por las comunidades de seguridad pública estatal, tribal y local, incluso el estado de interoperabilidad, ayudará a evaluar los programas que admiten esta tecnología.

En consecuencia, el Congreso debería considerar proporcionar fondos públicos por $3.75 millones por año durante tres años (por un total de $11.3 millones) para permitir que la FEMA expanda la recopilación de datos y las iniciativas de encuestas con estados y territorios. Proporcionarle a los gobiernos federales, tribales y estatales información actualizada sobre capacidades de banda ancha para seguridad pública puede ayudar a dirigir las subvenciones para llenar las brechas de la banda ancha.[23]

RECOMENDACIÓN 16.3: Asegurar que los servicios satelitales de banda ancha sean parte de cualquier programa para la preparación ante emergencias.

Los factores técnicos pueden afectar el servicio de banda ancha durante catástrofes, pero es fundamental que las redes de banda ancha funcionen en forma confiable y tengan capacidades en una emergencia. Una forma de asegurar esto es mediante el uso de servicios satelitales fijos y móviles de banda ancha existentes en un área afectada en caso de una catástrofe o crisis. Los satélites pueden servir como una opción de comunicaciones y una fuente crítica de redundancia, particularmente cuando la infraestructura territorial no está disponible. Los servicios satelitales posiblemente sean más importantes como un método de comunicación en las primeras horas o días de una catástrofe, si los servicios con base terrestre están dañados o destruidos, lo que provea un valor único para objetivos de seguridad pública. Ya hay, varias agencias federales, locales y estatales que usan aplicaciones de servicios satelitales de banda ancha para la salud pública, la continuidad de los gobiernos y las actividades de preparación ante catástrofes.[24]

Las agencias federales deberían recomendar el uso de servicios satelitales de banda ancha fija y móvil para la preparación ante emergencias y las actividades de respuesta, como también seguridad nacional, seguridad interior, continuidad y negociación de crisis.[25] Estas recomendaciones deberían emitirse cuando las agencias ofrecen pautas de información de respuestas y preparación ante emergencias a la comunidad de respuesta ante emergencias o cuando desarrollan planes y programas sobre respuestas ante emergencias. La Oficina de Confiabilidad Gubernamental (GAO, *Government Accountability Office*) debería emitir un informe sobre las capacidades actuales y futuras de banda ancha satelital para proporcionar los servicios necesarios durante una emergencia.

RECOMENDACIÓN 16.4: Preservar las comunicaciones de banda ancha durante emergencias.

Las leyes actuales prohíben que las entidades con fines de lucro (tales como hospitales, emisoras y prestadores de servicio) reciban asistencia federal para mantener o restaurar comunicaciones inmediatamente después de una catástrofe, lo que incluye servicios de banda ancha y transmisión. Sin embargo, ciertas entidades de comunicaciones con fines de lucro proporcionan servicios fundamentales para asegurar la seguridad pública. Los hospitales, por ejemplo, proporcionan información sobre salud pública, mientras que las emisoras distribuyen información importante y advierten al público de peligros latentes. La incapacidad de mantener o restaurar los servicios de banda ancha puede evitar que los hospitales y empleados de la salud pública compartan información urgente. La falta de energía o conectividad de banda ancha puede evitar que las emisoras distribuyan información sobre la salud al público a tiempo.[26] Sin iniciativas federales para mantener y restaurar rápidamente los servicios de banda ancha y transmisión, los residentes más vulnerables podrían quedar sin los servicios esenciales como NG 911, alertas y advertencias, incluso los mensajes del Sistema de Alerta ante Emergencias (EAS, *Emergency Alert System*).

De la misma forma, el Congreso debería considerar reformar la Ley Stafford para permitir la ayuda federal durante una catástrofe a entidades privadas con fines de lucro, que incluyen a proveedores de atención de salud, emisoras y proveedore de servicios de comunicación, para mantener o restaurar los servicios de comunicaciones críticas relacionadas con la seguridad pública (p. ej., advertencias y alertas públicas, cumplimiento de la ley, incendio, medico, búsqueda y

rescate, PSAP y otros servicios de emergencia) durante una gran catástrofe. El Director Federal de Coordinación o el Coordinador de Recursos Federales en la Oficina local conjunta (JFO, *Joint Field Office*) o, antes la instauración de una JFO, el Jefe de Sección de Operaciones en el Centro de Coordinación de Respuestas, deben tener autorización para decidir si subvencionar pedidos de ese tipo de asistencia federal.[27] Para evitar abusos, los pedidos deben ser subvencionados sólo por los servicios relacionados a los problemas operativos y solo por un tiempo limitado, p. ej., 30 días.[28] Estos cambios legales y normativos deberían tener vigencia antes del inicio de la temporada de huracanes del 2010 en junio, debido a la posibilidad de catástrofes climáticas a gran escala.

16.2 PROMOCIÓN DE LA SEGURIDAD CIBERNÉTICA Y PROTECCIÓN DE LA INFRAESTRUCTURA CRÍTICA

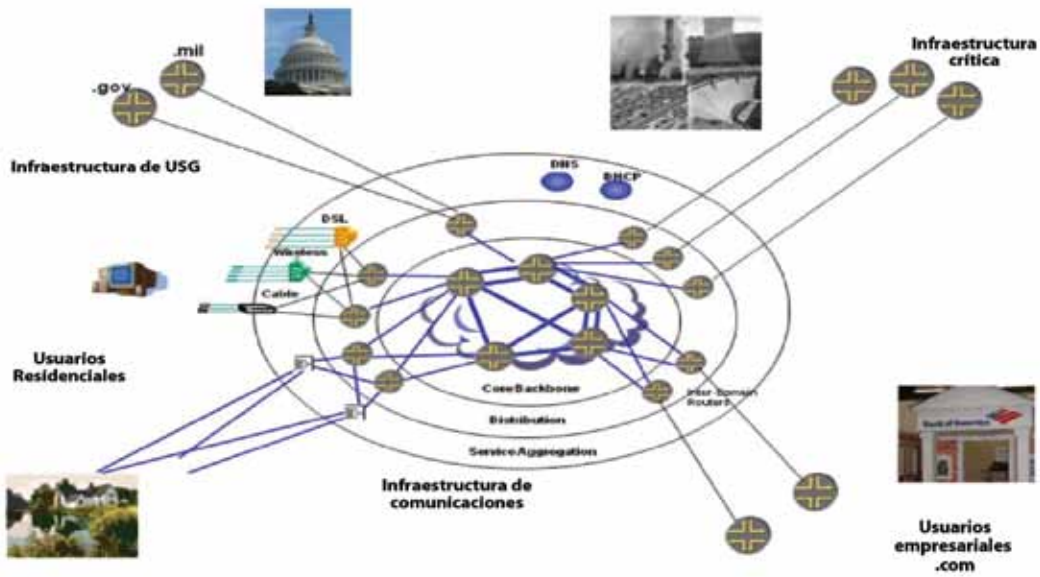
Mejora de la seguridad cibernética

Los proveedores de comunicaciones han experimentado ataques frecuentes en infraestructura crítica del Internet. Varias entidades estatales y no estatales han demostrado capacidad para robar, alterar y destruir datos y manipular o controlar sistemas diseñados para asegurar el funcionamiento de partes de nuestra infraestructura crítica. Posiblemente se necesiten protecciones adicionales para salvaguardar la infraestructura nacional de comunicaciones comerciales de los ataques cibernéticos. Estas protecciones podrían promover la confianza en la seguridad y la fiabilidad de comunicaciones de banda ancha y fomentar la adopción.

RECOMENDACIÓN 16.5: La FCC debería emitir un mapa de seguridad cibernética.

El almirante Mike McConnell, ex Director de Inteligencia Nacional, dijo recientemente que "en la actualidad, los Estados Unidos están luchando una guerra cibernética y estamos perdiendo".[29] Observó que "la economía expansiva de los Estados Unidos habita un espacio físico común y esos lugares son nuestras redes de comunicaciones."[30] El país necesita una estrategia clara para asegurar las redes de comunicaciones fundamentales sobre las cuales están basadas la infraestructura crítica y las comunicaciones de seguridad pública. Dentro de los 180 días posteriores a la aprobación de este plan, la FCC debería emitir, en coordinación con el Poder Ejecutivo, una guia para abordar la seguridad cibernética. La guia la FCC debería identificar las cinco amenazas más críticas de seguridad cibernética a la infraestructura de comunicaciones y a sus usuarios finales. La guia debería establecer un plan de dos años, que incluya hitos, para que la FCC aborde estas amenazas.

Exposición 16-D :
El mundo cibernético



RECOMENDACIÓN 16.6: La FCC debería expandir sus requisitos de informes sobre cortes de suministro de energía para los proveedores de servicios de banda ancha.

Actualmente, la FCC no recaba en forma habitual información sobre cortes cuando los proveedores de servicios de banda ancha experimentan cortes en la red. Esta falta de datos limita nuestra comprensión sobre operaciones de la red y sobre cómo evitar cortes de servicio. La FCC debería iniciar un procedimiento para ampliar las normas de informes sobre cortes de la Parte 4 de la FCC para los proveedores de servicios de Internet (ISP, *Internet service provider*) de banda ancha y proveedores de VoIP interconectados. Dichos informes le permitirán a la FCC, otras agencias federales y, según convenga, proveedores de servicio analizar información sobre cortes que afecten a redes basadas en IP. La información también ayudará a evitar cortes futuros y a asegurar una mejor respuesta a los cortes actuales.

Los informes disciplinados y a tiempo sobre los cortes de redes ayudarán a proteger las redes de comunicaciones de banda ancha de los ataques cibernéticos mediante la mejora de la comprensión de la FCC sobre las causas y cómo recuperarlos. Esto ayudará a mejorar la seguridad cibernética y a promover la confianza en la seguridad y la fiabilidad de las comunicaciones de banda ancha.[31]

RECOMENDACIÓN 16.7: La FCC debería crear un programa voluntario de certificación de seguridad cibernética.

Muchos usuarios de Internet aparentemente no consideran que la seguridad cibernética sea una prioridad. Casi la mitad de todas las empresas en el Estudio del Estado Global de Seguridad de la Información del 2009 informaron que están cortando presupuestos para iniciativas de seguridad de la información. Un informe de investigaciones sobre violaciones de datos de 2008 concluyó que el 87% de las violaciones cibernéticas podrían haber sido evitadas si hubiera habido controles de seguridad razonables.[32] La FCC debería explorar de qué forma instar las iniciativas voluntarias para mejorar la seguridad cibernética.

La FCC debería comenzar un procedimiento para establecer un sistema voluntario de certificación de seguridad cibernética que cree incentivos de mercado para proveedores de servicios de comunicaciones para mejorar su seguridad cibernética de redes. La FCC debería examinar los incentivos voluntarios adicionales que podrían mejorar la seguridad cibernética y mejorar la educación sobre problemas de seguridad cibernética e incluir aspectos internacionales de los problemas. Un programa de certificación voluntaria de seguridad cibernética podría promover más seguridad de red entre participantes del mercado, aumentar la seguridad de la infraestructura de comunicaciones de la nación y ofrecer a los usuarios finales información más completa sobre las prácticas de seguridad cibernética de los prestadores. En este procedimiento, la FCC debería considerar todas las medidas que promoverán la confianza en la seguridad y la fiabilidad de las comunicaciones de banda ancha.[33]

RECOMENDACIÓN 16.8: La FCC y el Departamento de Seguridad Nacional (DHS, *Department of Homeland Security*) deberían crear un sistema de reportes de información de seguridad cibernética (CIRS, *cybersecurity information reporting system*).

La FCC, otros socios del gobierno y los ISP carecen de una "concientización situacional" que les permita responder en forma decisiva y coordinada a los ataques cibernéticos en la infraestructura de comunicaciones. La FCC y la Oficina de Seguridad Cibernética y Comunicaciones (*Office of Cybersecurity and Communications*) del DHS deben desarrollar juntos un CIRS sobre redes IP para acompañar el Sistema de Reportes sobre Información ante Catástrofes. El CIRS será una herramienta invalorable para controlar la seguridad cibernética y proporcionar respuestas decisivas a los ataques cibernéticos.

El CIRS debería estar diseñado para difundir información rápidamente a proveedores participantes durante eventos cibernéticos importantes. El CIRS debería crearse como un sistema de control voluntario en tiempo real para eventos cibernéticos que afecten la infraestructura de comunicaciones. La FCC debería actuar como un facilitador confiable para asegurar que se comparta en forma recíproca y que el sistema esté estructurado para que la información patentada de ISP permanezca como confidencial.

RECOMENDACIÓN 16.9: La FCC debería expandir el alcance comunitario y participación internacional.

La FCC debería aumentar su participación en foros nacionales e internacionales que aborden las actividades y problemas de seguridad cibernética internacional. También debería involucrarse en diálogos y asociaciones con autoridades regulatorias que aborden los problemas de seguridad cibernética en otros países. Esto debería incluir alcance a organizaciones internacionales y entes reguladores de comunicaciones en el extranjero sobre elementos del Plan Nacional de Banda Ancha (Vea capítulo 4 donde se analiza el alcance internacional). La FCC debería también continuar revisando las actividades de seguridad cibernética de organizaciones y otras naciones para mejorar la concientización en estas actividades en la medida en que se relacionan con políticas internas de los Estados Unidos. Y debería continuar participando en iniciativas internas que se relacionen con las actividades de seguridad cibernética a nivel internacional.

Supervivencia de la infraestructura crítica

RECOMENDACIÓN 16.10: La FCC debería explorar la preparación y la resiliencia de las redes.

Las fallas simultáneas o daño a varios enrutadores o instalaciones de red de IP podrían afectar el tráfico entre las áreas metropolitanas más importantes o entre las oficinas de seguridad nacional y seguridad pública. Debido a que muchas compañías colocan equipos juntos, los daños a ciertos edificios podrían afectar una gran cantidad de tráfico de banda ancha, incluso las comunicaciones del NG911. La FCC debería comenzar una investigación sobre la resiliencia de las redes de banda ancha bajo un grupo de fallas físicas (intencionales o no) bajo carga intensa. Esto permitirá que la FCC evalúe la capacidad de los sistemas de comunicaciones de seguridad pública para resistir ataques directos y determinar si deberían tomarse acciones al respecto.

Este procedimiento también debería examinar la preparación de las redes comerciales para resistir sobrecargas que puedan ocurrir durante eventos extraordinarios, tales como ataques de bioterrorismo o pandemias. El DHS ha desarrollado prácticas recomendadas para preparación ante pandemias para proveedores de servicios de red, pero no se realiza seguimiento del cumplimiento de estos estándares voluntarios. Por ejemplo, un repentino aumento en el uso de la red de banda ancha residencial durante una pandemia u otra catástrofe podría dificultar el rendimiento de la red para usuarios críticos y programas computacionales porque dificulta el flujo de información de salud pública y médica urgente en las redes públicas. Este proceso judicial le dará a la FCC puntos de vista sobre la preparación ante pandemias en redes de banda ancha comercial. Además, generará información importante sobre la susceptibilidad de esas redes ante cargas intensas y de qué forma la congestión en las redes de acceso residencial (particularmente en la "última milla") puede debilitar las comunicaciones de seguridad pública y el acceso al 911 durante una pandemia u otro evento a gran escala.[34]

RECOMENDACIÓN 16.11: La FCC y el Sistema Nacional de Comunicaciones (NCS, *National Communications System*) deberían crear acceso a redes de prioridad y enrutamiento para comunicaciones de banda ancha.

Los usuarios de banda ancha en la comunidad de seguridad pública no tienen ningún sistema de acceso prioritario y enrutamiento en redes de banda ancha. Dicho sistema es crítico para proteger información urgente y de seguridad de vida para que no se pierda ni se retra debido a la congestión de la red. Mientras que el trabajo técnico está en camino para permitir la creación de un sistema, no existe un conjunto de normas de la FCC para apoyarlo. La FCC y el Sistema Nacional de Comunicaciones (*National Communications System*, NCS) deberían aprovechar sus experiencias con el Servicio de Telecomunicaciones de Emergencia del Gobierno (GETS, *Government Emergency Telecommunications Service*) y el WPS para desarrollar en forma conjunta un sistema de acceso prioritario de red y enrutamiento de tráfico para los usuarios de seguridad nacional/preparación ante emergencias (NS/EP) en redes de comunicaciones de banda ancha. El Poder Ejecutivo debería considerar clarificar una estructura para la implementación de agencias y delinear las responsabilidades e hitos clave; el orden debería ser consistente con las políticas nacionales en documentos presidenciales ya existentes. La FCC y la NCS deberían administrar este programa en forma conjunta.

RECOMENDACIÓN 16.12: La FCC debería explorar estándares para la resiliencia y la fiabilidad de las comunicaciones de banda ancha.

Durante años, las redes de comunicación se diseñaron y se implementaron para lograr la fiabilidad de "clase portadora" (*carrier-class*). A medida que la infraestructura de las comunicaciones migra de tecnologías viejas a tecnología de banda ancha, los servicios de comunicaciones críticas se realizarán en redes de comunicaciones que talvez no estén construidas de acuerdo con estos altos estándares. La caída posible en la fiabilidad del servicio es una preocupación para los sectores críticos, tales como energía y seguridad pública, y para los clientes en general. La FCC debería comenzar un procedimiento de investigación para obtener una mejor comprensión de los estándares de fiabilidad y resiliencia que se aplican a redes de banda ancha. El procedimiento debería examinar los estándares y las prácticas aplicados a la infraestructura de banda ancha en todas las capas, desde los programas computacionales a las instalaciones. El objetivo debería ser determinar qué acción, si corresponde, debería tomar la FCC para reforzar la fiabilidad de la infraestructura de banda ancha.

16.3 OPTIMIZACIÓN DE LAS TECNOLOGÍAS DE BANDA ANCHA PARA MEJORAR LAS COMUNICACIONES DE EMERGENCIA CON EL PÚBLICO

Paso a 911 de nueva generación (NG911, *Next Generation 911*)

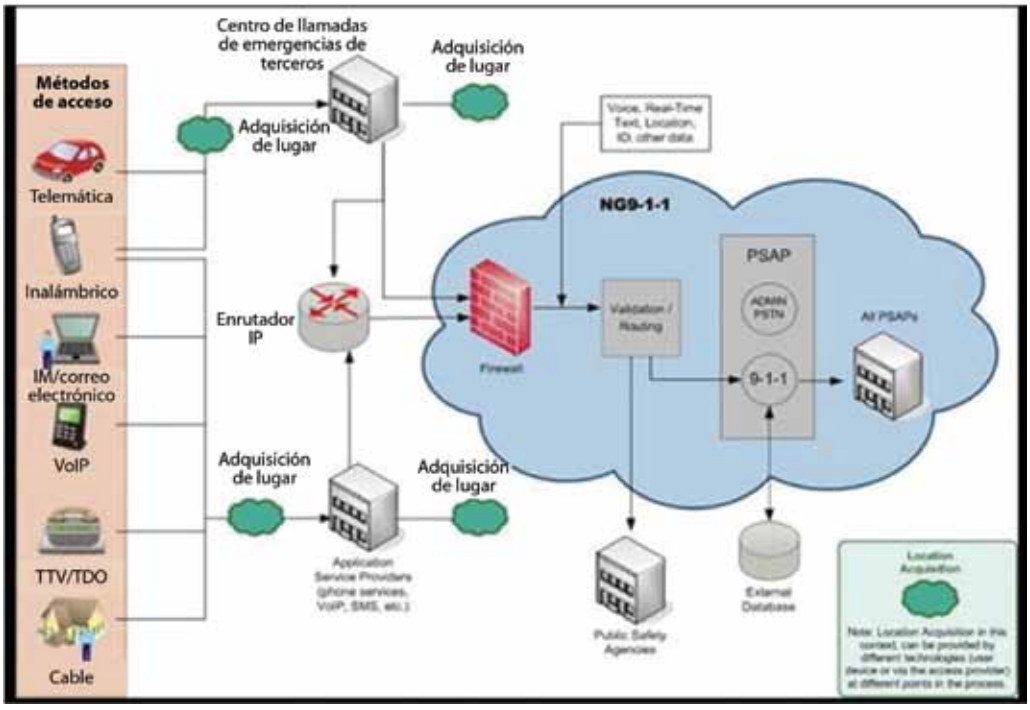
El sistema 911 del país está evolucionando para admitir NG911, el cual integrará las funciones y capacidades centrales de E911 (*Enhanced 911*, 911 mejorado) y al mismo tiempo agrega nuevas capacidades en formatos múltiples, tales como texto, fotos, video y correo electrónico. NG911 también integrará las entidades involucradas en respuestas ante emergencias más allá de los PSAP (ver Exposición 16-E). Esto mejorará ampliamente la calidad y la velocidad de respuesta, dándoles a las personas que llaman (incluso los discapacitados) un servicio igual. La posibilidad de enviar videos y fotografías a los PSAP trascenderá las barreras del idioma y proporcionará información de calidad de "testigo ocular" para dar a las personas que son las primeras en responder la información más relevante en una emergencia. NG911 proporcionará una capacidad de respuesta ante emergencias interoperable e integrada para los PSAP, las personas que son las primeras en responder, hospitales y otros profesionales de respuesta ante emergencias.

Los cuatro propósitos fundamentales de NG911 son:

- Reemplazar el sistema E911 manteniendo sus funciones centrales, tales como información automática de ubicación e identificación automática de número.
- Agregar capacidades para compatibilizar el acceso al 911 en formatos múltiples para todo tipo de proveedores de servicios de emisión, diseñadores de aplicaciones y fabricantes de dispositivos.
- Aumentar la flexibilidad del sistema, la redundancia y la eficiencia para los PSAP y las autoridades de control del 911.
- Agregar capacidades para integrar e interoperar con entidades involucradas en respuestas ante emergencias más allá de los PSAP.

La banda ancha hará que sea posible que los PSAP envíen y reciban imágenes de video, información médica, transmisiones del sensor ambiental y un sinfín de otros datos a través de redes y bases de datos compartidas. Esto facilitará que el público (incluso discapacitados) acceda a los servicios del 911. Los usuarios podrán transmitir voz, texto o imágenes a los PSAP desde una variedad de dispositivos compatibles con la banda ancha.

Exposición 16-E : Flujo de llamadas en NG911[35]



Uso de la banda ancha para unir la brecha hacia NG911

Muchos en las comunidades de seguridad pública no tienen acceso a servicios de banda ancha.[36] Algunos PSAP están ubicados en áreas donde las comunicaciones de banda ancha no están disponibles.[37] Muchos PSAP no se pueden permitir la conectividad a banda ancha y los programas de subvenciones existentes no están concentrados en actividades de financiamiento a largo plazo. Además, los límites normativos han dificultado la implementación de NG911. Es necesario desarrollar una transición más eficiente para sustentar estos servicios.

Ha comenzado la transición del sistema 911 antiguo a NG911. Las organizaciones de seguridad pública y de estándares industriales han llegado a un consenso sobre la arquitectura técnica de 911 para cumplir con las demandas planteadas por las nuevas formas de tecnología y métodos de comunicación. El Departamento de Transporte (DOT, *Department of Transportation*) de los Estados Unidos ha publicado un plan de transición para la migración a NG911.[38] Varios estados y localidades han comenzado a implementar NG911. Al menos una prueba en vivo de mensajes de texto de 911 está en marcha (ver Exposición 16-F).

Sin embargo, las barreras financieras y normativas dificultan la implementación de NG911. Los programas de subvenciones que apoyan NG911 carecen de coordinación y el alcance es limitado. Las normas federales y estatales inconsistentes, desactualizadas y que se superponen han retardado el desarrollo de NG911.

Es fundamental que el sistema NG911 se desarrolle en una forma que asegure de manera más efectiva que los Estadounidenses puedan acceder a los sistemas del 911 en cualquier momento y en cualquier lugar. (ver Exposición 16-G para obtener las diferencias entre la arquitectura del 911 antiguo actual y los sistemas NG911). Además, el sistema NG911 debe ser capaz de comunicar rápidamente información generada por quien llama a las personas que responden primero. La política de los Estados Unidos sobre NG911 debería concentrarse sobre la transición rápida de sistemas de comunicaciones de emergencia y del 911 analógico centrado en comunicación de voz a un modelo de servicios de emergencias basado en IP que sea posible a través de la banda ancha.

RECOMENDACIÓN 16.13: La Administración Nacional de Seguridad de Tráfico por Autopistas (NHTSA, *National Highway Traffic Safety Administration*) debería preparar un informe para identificar los costos de implementación a nivel nacional del sistema NG911 y recomendarle al Congreso que asigne fondos públicos.

La falta de fondos coordinados es una limitación importante para la implementación de NG911. Son varias las agencias que administran los programas de préstamos y subvenciones existentes sin ningún tipo de coordinación central o criterio uniforme.[40] Es más, la información que se ha desarrollado sobre el costo potencial de la implementación de NG911 es limitada. Si bien el DOT estimó a mediados del 2008 que el costo total de la implementación y funcionamiento del sistema NG911 a nivel nacional durante los próximos 20 años sería de $82 a $87 mil millones,[41] el país requiere un informe más detallado y enfocado para ayudar al Congreso a desarrollar un programa de subvenciones. Un análisis de la NHTSA debería determinar los costos detallados para los requisitos y especificaciones específicos del NG911 y especificar cómo los costos se detallan geográficamente o se asignan entre los PSAP, proveedores de servicios de banda ancha y proveedores subcontratados de servicios de NG911. El informe de la NHTSA debería además abordar el estado actual de preparación del NG911 entre los PSAP y cómo las diferencias en el acceso de los PSAP a la banda ancha en todo el país puede afectar los costos.

El Congreso debería considerar proporcionar fondos públicos para que la NHTSA analice los costos de implementar el sistema NG911 a nivel nacional. El informe debería estar terminado antes del 1 de diciembre de 2011. Debería incluir un análisis técnico y un estudio de costos de las diferentes plataformas de entrega (tales como, plataformas conectadas

CUADRO 16-2:

El centro de llamadas de 911 de Iowa se transforma en el primero en aceptar mensajes de texto[42]

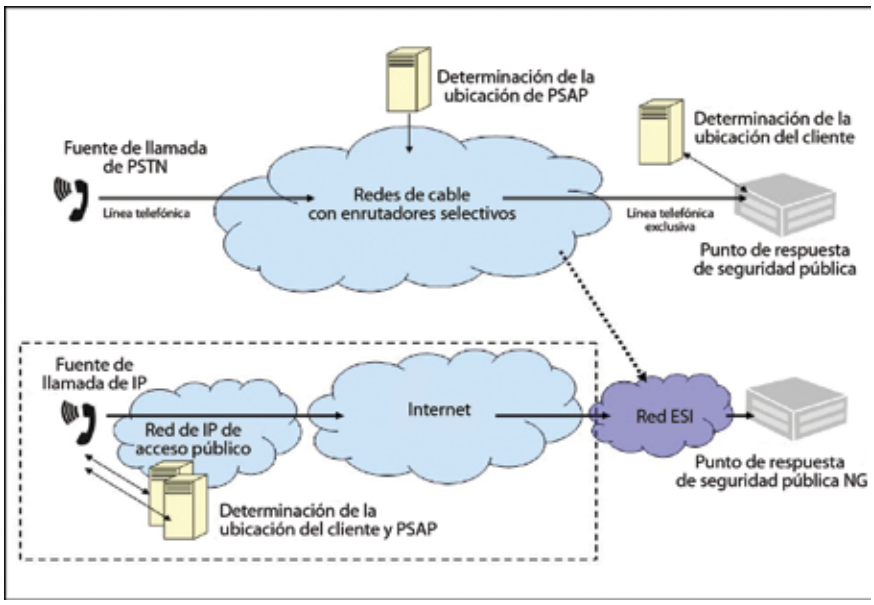
Un centro de llamadas de emergencia en el condado de Black Hawk, Iowa, se transformo en ser el primero en el país en aceptar mensajes de texto enviados al "911" en agosto del 2009. El jefe de policía del condado de Black Hawk, Thomas Jennings le dijo a La Prensa Asociada: "Creo que hay una necesidad de adelantarnos y hacer que esta tecnología esté disponible".

El sistema del condado de Black Hawk está diseñado para que las personas con discapacidades de habla y auditivas puedan enviar mensajes de texto al 911 para obtener servicios de emergencias. Elimina el proceso engorroso de hacer que una persona sorda tenga que usar un teclado para escribir un mensaje, que luego se envía a través de un centro de transmisión a un operador que responde la llamada. Una ventaja adicional es que los operadores del 911 pueden responder con mensajes de texto.

Si bien la comunicación por voz es el método principal de comunicación para las comunicaciones del 911, esta nueva onda de capacidad del NG911 es sólo un ejemplo de la forma en que el país está modernizando el sistema de 911 para mejorar el servicio al público.

Exposición 16-F :
NG911 permitirá que el público acceda al 911 a través los mensajes de texto (SMS) y otros formatos

Exposición 16-G :
Arquitecturas físicas del 911 actual y de la nueva generación



por cable, inalámbricas y satelitales) y una evaluación de las características de arquitectura, viabilidad y limitaciones de la entrega de NG911. El informe también debería incluir un análisis de las necesidades de las personas con discapacidades y debería identificar los estándares y protocolos para NG911 y para la incorporación de VoIP y estándares de "mensajes de texto en tiempo real".[43] El informe debería ser un recurso para el Congreso ya que considera la creación de un mecanismo de financiamiento coordinado y a largo plazo para implementación y funcionamiento, accesibilidad, desarrollo de aplicaciones, compra de equipos y capacitación para el NG911. Este análisis es esencial para identificar los requisitos de financiamiento para la implementación del NG911.

RECOMENDACIÓN 16.14: El Congreso debería considerar promulgar un marco normativo federal para el NG911.

Las normas federales y estatales que se centran en los sistemas 911 antiguos han dificultado la implementación del NG911.[44] Muchas de las normas se redactaron cuando las capacidades tecnológicas del NG911 no existían.[45] El Congreso debería considerar establecer un marco normativo y legal al nivel federal para la implementación del NG911 y la transición del 911 antiguo a las redes del NG911. Este marco debería eliminar las barreras jurisdiccionales y normativas antiguas inconsistentes, y proporcionar mecanismos legales para asegurar la transmisión exacta y eficiente de información de quien llama al 911 a agencias de respuesta ante emergencias. Sin un marco integral y un mecanismo de financiamiento es improbable que todos los estadounidenses reciban los beneficios del NG911 en el corto plazo.

La legislación debería reconocer una autoridad estatal existente sobre los servicios del 911 pero requerir que los estados quiten las limitaciones normativas al desarrollo del NG911. También debería darle a la FCC la autoridad para implementar un marco normativo federal para el NG911, eliminar normativas desactualizadas sobre el 911 a nivel federal y reemplazar normativas estatales inconsistentes. Esta legislación debería estar coordinada con el informe de la NHTSA para asegurar que la normativa federal de NG911 sea consistente.

El Congreso también debería considerar etapas para reducir el uso de fondos del 911 a nivel local, estatal y tribal para otros objetivos diferentes al 911. En el Informe al Congreso sobre los cobros y distribución de tarifas y gastos del 911 y E911 (*Report to Congress on State Collection and Distribution of 911 and Enhanced 911 Fees and Charges*) de la FCC del 31 de diciembre de 2008, algunos estados informaron que los fondos del 911/E911 cobrados a nivel estatal son o pueden ser usados, por lo menos parcialmente, para apoyar programas no relacionados con el 911 y el E911.

El Congreso también debería considerar reformar y volver a autorizar la Ley ENHANCE 911 y restaurar la Oficina de Coordinación de Implementación (ICO, *Implementation Coordination Office*) de E911 con fondos adecuados. La ICO puede construirse sobre el trabajo anterior con servicios del 911 inalámbricos que son posibles mediante IP y ayudar a asegurar que NG911 se implemente en una forma confiable e interoperable.

RECOMENDACIÓN 16.15: La FCC debería abordar servicios, aplicaciones y dispositivos de comunicaciones de NG911 basados en IP.

La FCC está considerando cambios en los requisitos de exactitud de ubicación y la posible extensión de los requisitos de Identificación Automática de ubicación (ALI, *Automatic Location Identification*) para interconectar los servicios VoIP.[46] La FCC debería expandir este procedimiento para explorar cómo el NG911 puede afectar la exactitud de ubicación y la ALI.

El sistema de 911 actual también necesitará volver a evaluarse a medida que las comunicaciones basadas en banda ancha continúan expandiéndose. El sistema 911 proporciona principalmente una plataforma de comunicaciones centradas en voz entre el público y los operadores del 911. Sin embargo, la implementación de diferentes tipos de comunicaciones, dispositivos, aplicaciones y servicios significa que los clientes están cambiando sus expectativas sobre cómo pueden acceder al 911. Muchos clientes, por ejemplo, ya esperan poder enviar comunicaciones que no sean de voz, tales como mensajes de texto cortos y mensajes multimedia a los PSAP. Pero por lo general los PSAP no pueden recibir ese tipo de comunicaciones. La estrategia nacional para la implementación del NG911 debería estar diseñada para cumplir con las expectativas futuras del consumidor.

CUADRO 16-3:

El sistema de alerta ante emergencias salva vidas en Samoa Americana[47]

El 29 de septiembre de 2009, un terremoto de una magnitud de 8.1 disparó un tsunami en Samoa Americana. Fue el mayor terremoto de ese año. KKHJ, la estación principal en el Sistema de Alerta ante Emergencias (EAS, *Emergency Alert System*) de Samoa Americana, emitió 2 alertas de EAS, una después del terremoto y una segunda cuando las aguas del puerto Pago Pago comenzaron a subir. Esta alerta de EAS advirtió a los residentes a evacuar el área. Luego de recibir la alerta, un pastor de la villa de Amanave hizo sonar las campañas de la iglesia, advirtiéndoles a la población local para que evacuara el área. Si bien murieron más de 180 personas en el terremoto y el tsunami, el sistema de advertencia temprana salvó vidas.

Los nuevas aplicaciones y dispositivos basados en banda ancha talvez no ofrezcan las funciones de "llamada" y voz tradicionales que los teléfonos inalámbricos o VoIP tienen hoy. Así, los clientes pueden asumir que pueden llegar a los PSAP a través de varios modos de comunicaciones basadas en IP. Los métodos de comunicación con el 911 que no son de voz tendrían el beneficio adicional de promover la accesibilidad al 911 para las personas que no hablan inglés o las personas discapacitadas. De esta forma, la FCC debería iniciar un procedimiento adicional para abordar la forma en que el NG911 puede acomodar a las tecnologías de comunicaciones, redes y arquitecturas más allá de los dispositivos centrados en voz. También debería explorar la forma en que las expectativas públicas pueden evolucionar en términos de plataformas de comunicaciones en las que el público puede confiar para solicitar servicios de emergencia.

Hacia alertas de nueva generación

La FEMA, basándose en la tecnología de alerta de emergencia de hoy, ha realizado acciones para desarrollar un Sistema Integrado de Advertencias y Alertas Públicas (IPAWS, *Integrated Public Alert and Warning System*) que llevará a un sistema público de advertencia y alerta de nueva generación.[48] La visión del IPAWS es construir y mantener un sistema completo, flexible, integrado y efectivo que les permita a los Estadounidenses recibir alertas e información de advertencias a través de la mayor cantidad de vías de comunicación posibles.[49] Pero en el informe de septiembre de 2009, la GAO identificó una cantidad de desafíos con la implementación de IPAWS, incluso algunos relacionados con la inclusión de las nuevas tecnologías,[50] coordinación de partes interesadas[51] y temas técnicos.[52] Los estados y las localidades necesitan recursos adicionales para actualizar las operaciones de alerta para acceder en forma efectiva al IPAWS. Además, el gobierno federal debería difundir información sobre el desarrollo y la implementación de IPAWS.

RECOMENDACIÓN 16.16: La FCC debería iniciar una investigación integral del sistema de alerta de nueva generación.

La FCC debería comenzar rápidamente un procedimiento que explore todos los temas para el desarrollo de un sistema de alerta de nueva generación redundante y de plataforma múltiple. La alerta de próxima generación debería incluir la emisión de alertas de emergencias en toda la nación a través de banda ancha. La investigación debería considerar desarrollos del Sistema de Alerta de Emergencia (EAS) y Servicio de Alerta Móvil Comercial (CMAS, *Commercial Mobile Alert Service*), como también el desarrollo del IPAWS de la FEMA. También debería considerar todas las tecnologías potenciales de plataformas múltiples cuales incluyan el uso de alertas ante emergencia a través de la programación de video en el Internet. La investigación debería determinar cómo sería mejor asegurar que todos los Estadounidenses puedan recibir alertas, advertencias e información crítica exactas y a tiempo sobre emergencias sin importar las tecnologías de comunicaciones usadas.

La FCC todavía no ha comenzado una investigación amplia sobre las alertas de nueva generación. Dicha investigación puede unir la brecha existente entre los sistemas de EAS y CMAS actuales con un sistema de alerta integral de nueva generación detallando una estrategia de implementación. Debería iniciarse ese procedimiento.

Las tecnologías de próxima generación transformarán las capacidades de entrega de información tanto del EAS como del CMAS. También pueden aumentar la efectividad de las alertas durante las emergencias. Los administradores de emergencias podrían proveer alertas a las comunidades que hoy tienen baja calidad de servicio (tales como las personas discapacitadas o que no hablan inglés) y proporcionar "seguimientos" de archivos de alerta mejorados que contengan información valiosa, tales como videos dinámicos y sistemas de seguimiento de tormentas mediante radar. Las alertas de emergencia en formato de video de Internet permitirían que los originadores de alertas de emergencias lleguen a personas que, en ese momento, no están escuchando la radio o la televisión u a otras fuentes actuales de alertas. Proporcionar métodos alternativos para la distribución de alertas de emergencias a todos los estadounidenses salvará vidas. Sin embargo, los sistemas que reúnen, administran y transmiten alertas necesitarán actualizaciones para acomodar a la banda ancha.

El sistema debería alertar al público sobre emergencias a través de todos los medios de comunicación posibles. En caso de un tornado, por ejemplo, las alertas se transmitirían en puntos de entrega de medio locales, se enviarían a teléfonos inalámbricos y con cable dentro del área afectada, se publicarían en fuentes de Internet y sitios Web y se emitirían a través de otros puntos de entrega de comunicación que presten servicios al área afectada. Eso aseguraría que el público esté informado de una emergencia y que tenga la información que necesita para protegerse. La investigación de la FCC debería concentrarse principalmente en cómo desarrollar ese sistema.

El desarrollo de la FEMA del IPAWS debería ayudar a asegurar que un sistema ubicuo de transmisión de alerta esté disponible para dar cabida a las plataformas múltiples de alerta y a la participación de todas las partes interesadas en alertas del sector privado, local, tribal, estatal y federal. También hay necesidad de una evaluación integral de la capacidad de los administradores de alertas para participar en IPAWS cuando se lance.

Una investigación integral permitirá que la FCC obtenga datos sobre el futuro del sistema de alertas y forme un marco normativo nuevo para las alertas de nueva generación. Esta

investigación debería concentrarse en las cuestiones políticas, legales y técnicas amplias asociadas con este sistema nuevo de plataformas múltiples. El procedimiento debería analizar la arquitectura del IPAWS en desarrollo para evaluar la capacidad del IPAWS para ser compatible con el sistema de alertas de nueva generación basado en banda ancha. La investigación también debería examinar las necesidades de los originadores de alertas de emergencia local, tribal y estatal sobre la utilización del sistema de alerta de nueva generación; qué asistencia, si fuera necesaria, la FCC y sus socios federales deberían proporcionar para abordar estas necesidades; y qué acciones la FCC y los socios federales deberían tomar para asegurar el desarrollo y la implementación a tiempo del sistema.

RECOMENDACIÓN 16.17: El Poder Ejecutivo debería aclarar los roles de las agencias en la implementación y el mantenimiento del sistema de próxima generación de advertencia y alerta.

El Poder Ejecutivo, a través de un concejo de política entre agencias o a través de un directivo, debería tomar acciones por orden presidencial, el comité de política entre agencias federales u otros medios formales para clarificar las responsabilidades de cada agencia federal en la implementación, mantenimiento y administración de los sistemas de alerta de nueva generación. Esta acción debería también establecer los hitos, criterios de referencia y acciones necesarias para la implementación y el establecimiento de un sistema de responsabilidad entre las agencias federales responsables de las alertas ante emergencias.

NOTAS AL FINAL DEL CAPÍTULO 16

1 Bajo este enfoque, por ejemplo, a los titulares de licencias de seguridad pública se les concede la flexibilidad de firmar acuerdos con socios comerciales para la construcción y funcionamiento de su red de 700 MHz.

2 En base a los resultados de la Encuesta nacional de referencia de interoperabilidad de 2006, los resultados de la interoperabilidad táctica de UASI de 2007 y la información de 2008/2009 proporcionada por cada estado con respecto a los Planes de interoperabilidad de comunicaciones a nivel estatal, es posible estimar que la mayoría de los UASI y los estados están aproximadamente a un nivel intermedio de interoperabilidad. *Consulte* Dep't of Homeland Sec., 2006 National Interoperability Baseline Survey (2006), *disponible en* http://www.safecomprogram.gov/NR/rdonlyres/40E2381C-5D30-4C9C-AB81-9CBC2A478028/0/2006NationalInteroperabilityBaselineSurvey.pdf; Dep't Homeland Sec., Tactical Interoperable Communications Scorecards Summary Report and Findings (2007), *disponible en* http://www.dhs.gov/xlibrary/assets/grants-scorecard-report-010207.pdf; Dep't Of Homeland Sec., National Summary of Statewide Communication Interoperability Plans (Scips) (2009), *disponible en* http://www.safecomprogram.gov/NR/rdonlyres/C6C0CD6A-0A15-4110-8BD4-B1D8545F0425/0/NationalSummaryofSCIPs_February2009.pdf. Según lo establecido en el Plan Nacional de Comunicaciones de Emergencia (*Goals of the National Emergency Communications Plan*), el DHS planifica evaluar la capacidad de cada una de las 60 mayores áreas urbanas del país para lograr claramente comunicaciones a nivel de respuesta al 30 de septiembre de 2010 y evaluará cada uno de los más de 3,000 condados en los Estados Unidos para el 30 de septiembre de 2011. *Consulte* Dep't of Homeland Sec., National Emergency Communications Plan 6–7 (2008), *disponible en* http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf.

3 Inst. de Estándares Europeos de Telecomunicaciones [ETSI], Proyecto MESA; *Technical Specification Group—System; System and Network Architecture*, en 20, ETSI TR 102 653 V3.1.1 (2007–2008), *disponible en* http://www.etsi.org/deliver/etsi_tr/102600_102699/102653/03.01.01_60/tr_102653v030101p.pdf.

4 *Consulte Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, PS Docket No. 06-229, Second Report and Order, 22 FCC Rcd 15289 (2007).

5 Los comentarios presentados en la procedimiento de Bloque D de 700 MHz de la Comisión sugieren una cantidad posible de explicaciones. *Consulte*, por ej., Association of Public Safety Communications Officials-International, Inc. (APCO) Comments in re 700 MHz Third Further Notice (*Service Rules for the 698–746, 747–762 and 777–792 Bands; Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band*, WT Docket No. 06-150, PS Docket No. 06-229, Third Further Notice of Proposed Rulemaking, 23 FCC Rcd 16661 (2008) (*700 MHz Third Further Notice*)), archivado el 20 de junio de 2008 en 3; Comentarios de Verizon Wireless en referencia a 700 MHz Third Further Notice, archivado el 20 de junio de 2008, en 2 .

6 El registro incluye propuestas, por ejemplo, para que las agencias de seguridad pública usen la infraestructura central existente mientras que se individualizan los dispositivos de usuarios finales y otros aspectos de la red perimetral para cumplir con los requisitos de seguridad pública y también para emplear tecnologías satelitales, aéreas y de otro tipo para ampliar la cobertura en áreas rurales. *Consulte, por ej.* La carta de Lucian Randolph, CEO de Planet TV Air-Tower Systems, a Marlene H. Dortch, Secretaria, FCC GN Docket No. 09-51, (12 de noviembre de 2009) (Planet TV , 12 de noviembre de *a instancia propia*) en 9; Space Data Reply en referencia al aviso de intención del Plan Nacional de Banda Ancha, archivado el 21 de julio de 2009, en 3; Comentarios de Iridium Satellite en referencia al aviso de intención del Plan Nacional de Banda Ancha, archivado el 8 de junio de 2009, en 4–5; Comentarios de MSS/ATC en referencia al aviso de intención del Plan Nacional de Banda Ancha, archivado el 8 de junio de 2009, en 5–6; Comentarios de Spacenet Inc. en referencia al aviso de intención del Plan Nacional de Banda Ancha, archivado el 8 de junio de 2009, en 9. La Comisión debe explorar también cómo cumplir mejor los requisitos de seguridad pública a través de varios medios, incluso el uso de infraestructura comercial que se adquirirá mediante los titulares de licencias de banda ancha para seguridad pública.

7 Esto sirve al propósito adicional de permitir que los titulares de licencias de seguridad pública aprovechen las infraestructuras que los servicios públicos pueden tener en la actualidad. Por lo tanto, el acceso a las torres de servicios públicos y otras estructuras puede ser parte de otro programa de uso secundario.

8 *Consulte, por ej.*, Comentarios de APCO Comments en referencia a NBP PN #8, (*Additional Comment Sought on Public Safety, Homeland Security, and Cybersecurity Elements of National Broadband Plan—NBP Public Notice #8*, GN Docket Nos. 09-47, 09-51, 09-137, PS Docket Nos. 06-229, 07-100, 07-114, WT Docket No. 06-150, CC Docket No. 94-102, WC Docket No. 05-196, Public Notice, 24 FCC Rcd 12136 (PSHSB 2009) (*NBP PN #8*)) archivado el 12 de noviembre de 2009, en 11; Comentarios de AT&T en referencia a NBP PN #8, archivado el 12 de noviembre de 2009, en 2; Comentarios de Verizon y Verizon Wireless en referencia a NBP PN #8, archivado el 12 de noviembre de 2009, en 6; Public Safety Spectrum Trust Comments en referencia a *700 MHz Public Safety Broadband Networks Waiver PN (Public Safety and Homeland Security Bureau Seeks Comment on Petitions for Waiver to Deploy 700 MHz Public Safety Broadband Networks*, PS Docket No. 06-229, aviso público, DA 09-1819 (emisión del 4 de agosto de 2009) (*700 MHz Public Safety Broadband Networks Waiver PN*) ee 11.

9 *Consulte* la Ley de Mejora de tecnologías nuevas y emergentes para el 911 (*New and Emerging Technologies 911 Improvement Act*) de 2008, Pub. L. No. 110-283, 122 Stat. 2620 (2008) (NET 911 Act) modifica la Ley de seguridad pública y comunicaciones inalámbricas (*Wireless Communications and Public Safety Act*) de 1999, Pub.L. No. 106-81, 113 Stat. 1286 (1999) (Ley 911 inalámbrica [*Wireless 911 Act*]).

10 Al punto que otros usuarios tienen permiso para ingresar a una red de seguridad pública, el ERIC también será responsable de trabajar para establecer prioridades comunes.

11 La misión del ERIC también puede extenderse en el tiempo para prestar otras funciones, tales como la coordinación del acceso de los PSAP a la red y la mejora de la interoperabilidad para comunicaciones de voz de misión crítica.

12 La FCC debería considerar miembros que comprendan representantes de agencias de seguridad pública locales y estatales, asociaciones de comercialización de seguridad pública, el Fideicomiso de Espectro de Seguridad Pública (*Public Safety Spectrum Trust*), grupos de usuarios federales y SAFECOM. La FCC debería considerar contar con representación adecuada de los representantes de la industria y representantes de proveedores de equipos y prestadores de servicios. La FCC también debería establecer un comité federal de coordinación de socios que incluya al DHS, al Departamento de Justicia, el NIST y la Administración Nacional de Información y Telecomunicaciones (NTIA) y que optimice el Centro de Preparación de Comunicación ante Emergencias (ECPC).

13 Esto incluye 20 nuevos empleados nuevos (ingenieros y técnicos), gastos de viaje y oficina, equipos de computación y simulación y contratación con el NIST para el desarrollo de estándares y pruebas. Omnibus Broadband Initiative, The Public Safety Broadband Wireless Network (Próximo) (OBI, The Public Safety Broadband Wireless Network).

14 Este comité de asesores debería quedar exento de la Ley de comité de asesores federales (*Federal Advisory Committee Act*). En segundo lugar, el Congreso debería asegurar el financiamiento adecuado para que el ERIC posibilite a la FCC pagar los gastos de viajes razonables de los miembros del comité de asesores de seguridad pública.

15 Bajo este modelo, las entidades de seguridad pública, según lo autorice la FCC, deberían poder seleccionar las entidades con quien quieren asociarse para construir y hacer funcionar sus redes, siempre que cumplan con los requisitos de la FCC, incluso del ERIC.

16 Muchas jurisdicciones estatales y locales han sancionado regulaciones que requieren la instalación de transmisores y otros equipos dentro de los edificios para mejorar la cobertura dentro de los edificios para redes de voz de banda estrecha de seguridad pública. Los gobiernos estatales y locales deberían considerar la implementación de requisitos de cobertura similares para las comunicaciones de banda ancha para seguridad pública.

17 Para lograr cobertura del 99% de la población, se asume que se usarán antenas montadas en el exterior en áreas rurales del país.

NOTAS AL FINAL DEL CAPÍTULO 16

18 La base de costos para esta solicitud de fondos se liberará luego en una OBI, The Public Safety Broadband Wireless Network. Estos costos de capital incluyen aprovechar aproximadamente 41,600 sitios ya implementados comercialmente, 3,200 sitios rurales (una mezcla de sitios nuevos y actualizados, con vehículos que se montan con antenas externas), fortalecimiento de todos los sitios y suministro de depósitos de equipos a nivel local y estatal.

19 Este número se basa en un tarifa RAN anual para servicios administrados, costos adicionales para servicios rurales y costos de funcionamiento, administración y mantenimiento anuales que incluyen tarifas de servicios administrados de transporte OBI, The Public Safety Broadband Wireless Network.

20 La mayoría de estos trabajos serán en servicios y operaciones, mientras que un pequeño porcentaje será en desarrollo y fabricación de productos. OBI, The Public Safety Broadband Wireless Network.

21 La tarifa debe ser baja. Los gastos operativos para los primeros 2 años de funcionamiento de la red se estiman en $500 millones.

22 *Consulte* 6 U.S.C. § 575. Este estatuto obliga la formación de grupos de trabajo de RECC (Cooperativa Eléctrica Rural, *Rural Electric Cooperative Corporation*), id. en § 575(a) y se les cobrará impuestos por, entre otras cosas, "evaluación de supervivencia, sustentabilidad y interoperabilidad de sistemas de comunicaciones locales ante emergencia". Id. en § 575(d)(1). Esta sección no dirige los grupos de trabajo para que se centralicen en infraestructura de banda ancha.

23 Estas encuestas deben incluir información para que se le entregue al ERIC sobre el estado actual de la interoperabilidad para la red de banda ancha para seguridad pública.

24 FCC, FCC Preparedness for Major Public Emergencies, Chairman's 30 Day Review (2009), *disponible en* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-293332A1.pdf.

25 *Consulte* la Carta de Diane Cornell, Vicepresidente de Asuntos Gubernamentales, Inmarsat, a Marlene H. Dortch, Secretary, FCC, GN Docket Nos. 09-47, 09-51, 09-137, WC Docket No. 02-60 (4 de diciembre de 2009) en 7.

26 *Consulte* 47 U.S.C. § 5172(a)(1)(B); Oficina de la Presidencia, Respuesta Federal Al Huracán Katrina: Lessons Learned 58–59 (2006), *disponible en* http://georgewbush-whitehouse.archives.gov/reports/katrina-lessons-learned.pdf.

27 Ann Arnold, Presidente, Tex. Ass'n of Broadcasters, declaración en la cubre de la FCC: Lessons Learned: Hurricane Seasons 2008 (11 de diciembre de 2008) *disponible en* http://www.fcc.gov/realaudio/mt121108.ram (1:00:35).

28 Las entidades con fines de lucro deberían ser consideradas elegibles para obtener asistencia sólo cuando la necesidad de servicios exceda las capacidades del sector privado y cualquier gobierno local, tribal y estatal relevante o en relación con la amenaza inmediata a la vida o los bienes, es fundamental para la respuesta ante catástrofes o seguridad de la comunidad o se relacione con las medidas de recuperación federales esenciales.

29 *Consulte* Mike McConnell, Op.-Ed., *Mike McConnell on How to Win the Cyber-War We're Losing*, Wash. Post, 28 de febrero de 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html. (McConnell, How to Win the Cyber-War).

30 McConnell, *How to Win the Cyber-War*.

31 Steven Chabinsky, Director asistente-División Cibernética, Agencia Fed. de Investigación (FBI), testimonio ante el Comité judicial del Senado de los Estados Unidos, Subcomité sobre Terrorismo y Seguridad Interna (17 de noviembre de 2009). El FBI considera que las amenazas cibernéticas contra la nación son "una de las mayores preocupaciones del siglo XXI". *Id.*

32 Verizon Business, 2008 Data Breach Investigations Report 2–3 (2008), *disponible en* http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

33 La comisión tendrá que asignar fondos para obtener un proveedor para desarrollar un criterio de auditoría y acreditar cuerpos de certificación de terceros. El Congreso debería considerar fondos públicos para la FCC en su próximo presupuesto en forma continua según se requiera.

34 En realidad, las estimaciones de capacidad de red de acceso residencial sugieren que las redes actuales pueden llevar entre 1/100 y 1/10 de su capacidad publicitada por usuario. *Ver también* Comentarios de AT&T en referencia al aviso de intención del Plan Nacional de Banda Ancha, archivado el 8 de junio de 2009, en 67–69; Comentarios de Telcordia en referencia al aviso de intención del Plan Nacional de Banda Ancha, archivado el 8 de junio de 2009, en 19.

35 Research and Innovative Tech. Admin., Next Generation 911 Concept of Operations, Fig. 4-2, http://www.its.dot.gov/ng911/pubs/concept_operations.htm (Última visita: 15 de febrero de 2010).

36 *Ver generalmente* Comentarios de NENA en referencia a NBP PN #8, archivado el 12 de noviembre de 2009.

37 Comentarios de PSST en referencia a NBP PN #8, archivado el 22 de noviembre de 2009, en 2.

38 U.S. Dep't of Transp., Next Generation 911 (Ng9-1-1) System Initiative, Final Analysis of Cost, Value, and Risk (5 de marzo de 2009) (DOT NG911 Cost Study).

39 Comentarios de Intrado en referencia a NBP PN #8, archivado el 12 de noviembre de 2009, en 11.

40 Por ejemplo, a través del Programa de Acceso al 911, el Servicio de Utilidades Rurales (*Rural Utilities Service*) proporciona préstamos a bajo interés a gobiernos estatales y locales, tribus indias y otras entidades para instalaciones y equipos para mejorar el acceso al 911 en áreas rurales. Ley de Energía, Conservación y Alimentos (*Food, Conservation, and Energy Act*) de 2008, Pub. L. No. 110-246, §6107, 122 Stat. 1651, 1959 (2008); *ver* E911 Grant Program, 74 Fed. Reg 29,967 (5 de junio de 2009).

41 U.S. Dep't of Transp., Next Generation 911 (Ng9-1-1) System Initiative, Final Analysis of Cost, Value, and Risk (5 de marzo de 2009) (DOT NG911 Cost Study).

42 *Consulte* Peter Svensson, *Iowa 911 Call Center Becomes First to Accept Texts*, ABC NEWS, 5 de agosto de 2009, http://abcnews.go.com/Technology/wireStory?id=8259735 .

43 El mensaje de texto en tiempo real es una función que permite que los usuarios vean el texto mientras lo escriben en una interfaz de texto.

44 Comentarios de NENA en referencia a NBP PN #8, archivado el 12 de noviembre de 2009, en 18–20.

45 *Consulte* Comentarios de NENA en referencia a NBP PN #8, archivado el 12 de noviembre de 2009, en 18–20.

46 *Consulte Wireless E911 Location Accuracy Requirements; Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems; 911 Requirements for IP-Enabled Service Providers*, PS Docket No. 07-114, CC Docket No. 94-102, WC Docket No. 05-196, Notice of Proposed Rulemaking, 22 FCC Rcd 10609 (2007).

47 *Consulte* Federal Emergency Management Agency, Integrated Public Alert and Warning System (IPAWS): Success Stories, http://www.fema.gov/emergency/ipaws/successstories.shtm (last visited Mar. 5, 2010) (IPAWS Success Stories).

48 *Consulte* Federal Emergency Management Agency, Integrated Public Alert and Warning System (IPAWS): http://www.fema.gov/emergency/ipaws/ (última visita:15 de febrero de 2010)

49 GAO, Emergency Preparedness: Improved Planning and Coordination Necessary for Modernization and Integration of Public Alert and Warning System 14 (2009) (GAO Emergency Preparedness Report), *disponible en* http://www.gao.gov/new.items/d09834.pdf (observe que las capacidades de distribuir alertas de emergencia y advertencias a través de correos electrónicos, teléfonos, dispositivos de mensaje de texto, teléfonos celulares, buscadores de personas y computadores de escritorio conectadas a Internet no se han implementado).

50 GAO Emergency Preparedness Report en 20–24.

51 GAO Emergency Preparedness Report en 24–26. Los desafíos identificados por la GAO incluyeron falta de redundancia, falta de cobertura en algunas zonas, integración de sistemas, desarrollo de estándares, desarrollo de alertas enfocadas según la geografía y alertas para personas con discapacidades y aquellas que no hablan inglés. En respuesta al informe, el DHS acordó con las recomendaciones para la GAO de abordar estas preocupaciones y ha comenzado a abordar muchos de estos desafíos. *Consulte* Declaración escrita de Damon Penn, Administrador Asistente, FEMA ante el Comité en Transporte e Infraestructura, Subcomité sobre desarrollo económico, edificios públicos y administración ante emergencias, Cámara de Diputados de los Estados Unidos (30 de septiembre de 2009), http://republicans.transportation.house.gov/Media/file/TestimonyEDPB/2009-09-30-Penn.pdf.

NOTAS AL FINAL DEL CAPÍTULO 16

52 *Consulte* Radio World, EAS Trigger salvó vidas en el Tsunami de Samoa (20 de septiembre de 2009), http://www.radioworld.com/article/87954; Bill Hoffman, *Lucky To Be Alive After Tsunami Destroys Dream Resort*, New Zealand Herald, Oct. 1, 2009, *disponible en* http://www.nzherald.co.nz/american-samoa/news/article.cfm?l_id=500605&objectid=10600668.