

Federal lawmakers highlight FirstNet's cybersecurity needs during hearing

Urgent Communications By Donny Jackson

February 7, 2016

[FirstNet](#) should take measures to ensure that its nationwide public-safety broadband network is not victimized by the kind of data breaches and cyberattacks that have plagued other federal-government entities, several members of a House subcommittee said during a hearing last week.

Rep. Anna Eshoo (D-Calif.) cited “massive security breaches” at the Office of Personnel Management (OPM) and the Internal Revenue Service (IRS) as incidents that must be avoided by FirstNet, which is designed to communicate a host of sensitive information about first-response entities and the people they are supposed to protect.

“In order to prevent the breach of sensitive FirstNet data, cybersecurity has to be a core focus,” Eshoo said during the hearing, which was webcast. “The continuation of the unraveling of the OPM, IRS and other agencies that have the massive security breaches should be instructive to FirstNet, because you’re going to have to utilize the most innovative security technologies available.

“I think that, in doing so, it will not only lessen the chance of a widespread breach and prevent disruption, but there is a word that is so operational in this, and that is ‘confidence’—confidence in the system by all of the users.

FirstNet President TJ Kennedy testified that the FirstNet RFP includes a section devoted to cybersecurity, reiterating the organization’s long-stated philosophy on the matter.

“We’ve always envisioned that we’re building in security from Day 1—we’re not just tacking it on at the end. We also want to leverage the best practices from the private sector, as well as within government ...”

At that point, Kennedy was interrupted by Rep. Marsha Blackburn (R-Tenn.), who indicated that she is not impressed with the results of federal-government cybersecurity efforts.

“Let’s stop right there, because government networks obviously—the OPM breach, NASA—they’re not secure,” Blackburn said. “Whether it is an encryption issue or whatever, we know there are some gaping holes—if you will—that are there, so I don’t think that is the standard that we want to hold up.”

Kennedy said [FirstNet](#) also plans to depend on cybersecurity expertise from the private sector.

“We’re really looking for industry, as part of their responses to this RFP, to bring forward private-sector best practices as part of their solutions that will be judged against our standards that we’ve put forward ... [in] the RFP,” Kennedy said. The RFP’s cybersecurity objectives are designed to “make sure that we ensure the security of all the data related to emergency medical services and law enforcement and the fact that we’re going to have all of this data operating across the FirstNet network.”

David Furth, deputy chief of the [FCC](#)’s public-safety and homeland-security bureau, notes that the FCC’s Task Force on Optimal [PSAP](#) Architecture (TFOPA) studying the transition of 911 centers to IP-based [next-generation 911](#) technology includes a working group dedicated to addressing cybersecurity.

“We recognize that this is a critical issue, and we’re concerned that many PSAPs—particularly smaller ones—around the country are not adequately prepared,” Furth said during the hearing. “That task force has just come back to us, as of last week, with a series of very detailed recommendations on how to move forward on cybersecurity for PSAPs in the [next-gen 911] world, and we’re working with FirstNet to make sure that those recommendations sync up with what FirstNet is doing, so that both ends of the communications chain are secure from cyberattack.”

[Link to Article](#)

[Link to Urgent Communications News Articles](#)