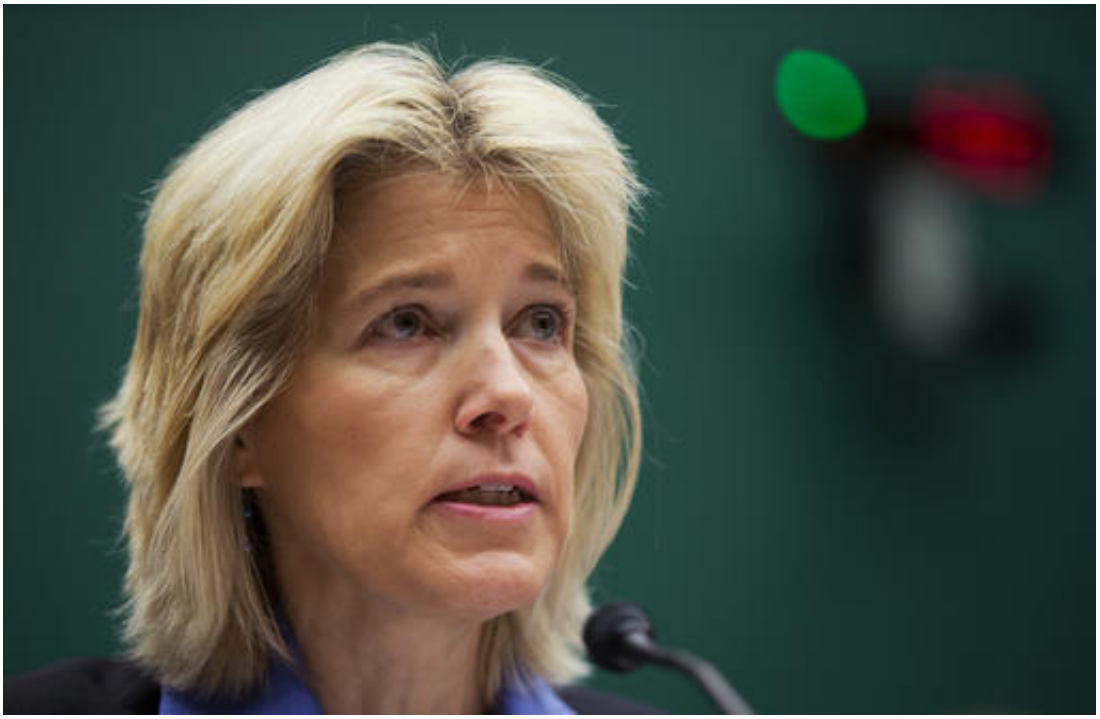
FBI: Using third parties to break encryption not only answer

April 19 2016, by By Eric Tucker



Federal Bureau of Investigation Executive Assistant Director for Science and Technology Amy Hess, testifies on Capitol Hill in Washington, Tuesday, April 19, 2016, before a House Oversight and Investigations subcommittee hearing on deciphering the debate over encryption. (AP Photo/Manuel Balce Ceneta)

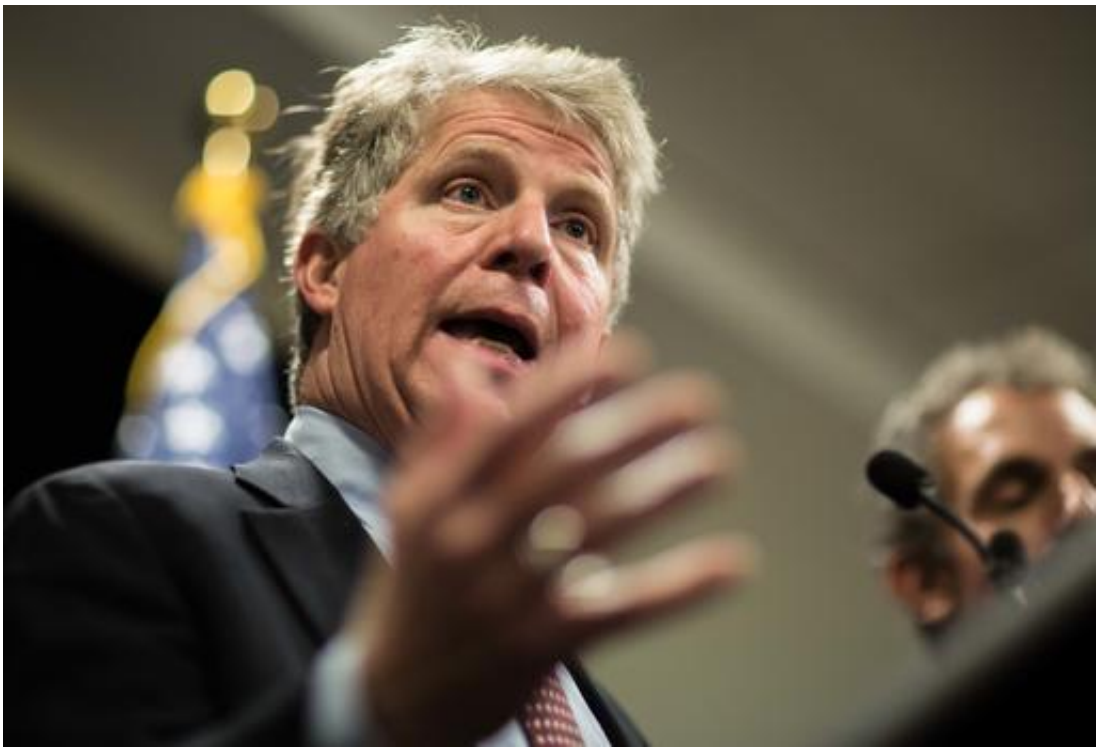
The FBI is facing an increasing struggle to access readable information and evidence from digital devices because of default encryption, a senior FBI official told members of Congress at a hearing Tuesday.

Amy Hess said that of the cell phones the FBI seized in the last six months as part of investigations, officials encountered passwords about 30 percent of the time and had "no capability" to access information "around 13 percent of that time."

"We have seen those numbers continue to increase, and clearly that presents us with a challenge," said Hess, the executive assistant director of the FBI's science and technology branch.

In her testimony to a subcommittee of the House Energy and Commerce Committee, Hess defended the Justice Department's use of a still-unidentified third party to break into the locked iPhone used by one of the two San Bernardino, California, attackers. But she said the reliance on an outside entity represented just "one potential solution" and that there's no one-size-fits-all approach for recovering evidence off a locked device. She said she did not think that path should be the sole solution for breaking open phones.

"These solutions are very case-by-case specific," she said. "They may not work in all instances. They're very dependent upon the fragility of the systems, the vulnerabilities we might find," she said, adding that cooperation between the government, academia and private industry was needed to come up with more solutions.



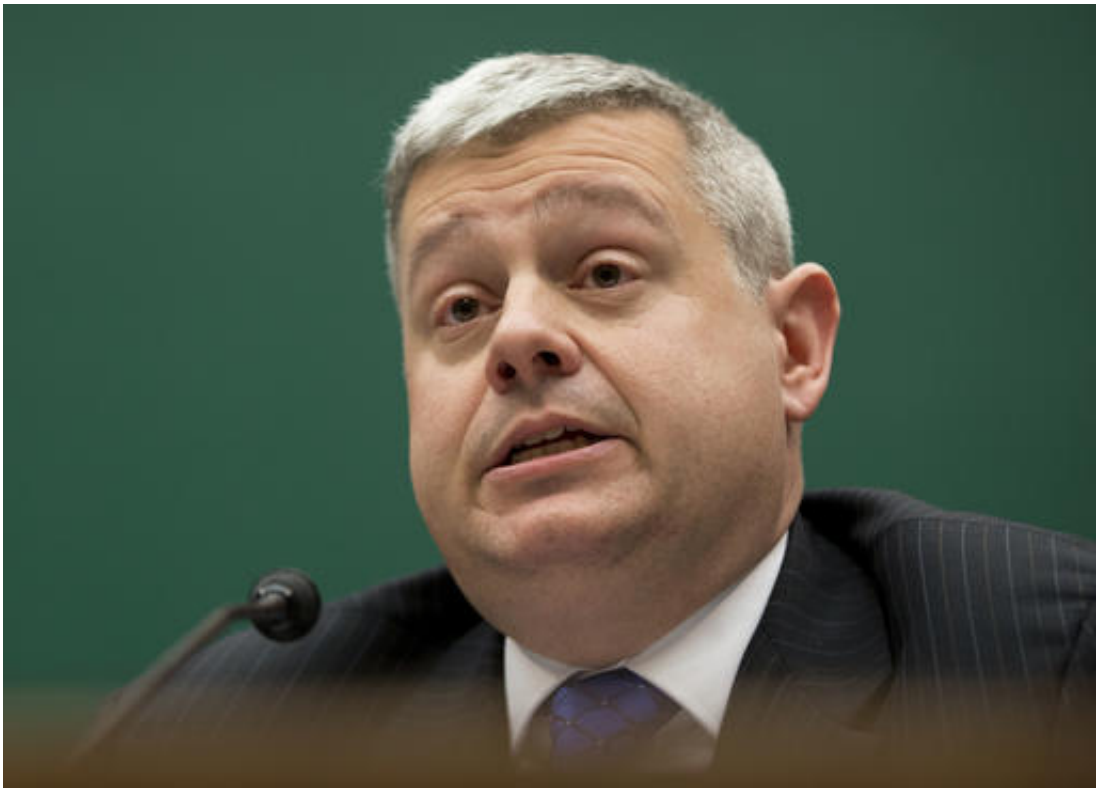
In this Tuesday, Oct. 21, 2014, file photo, Manhattan District Attorney Cyrus R. Vance Jr. speaks to the media during the inaugural National Prosecutorial Summit, in Atlanta. Calling it an issue of victims' rights, Vance, on the steps of New York's City Hall, urged Congress on Monday, April 18, 2016, to pass legislation that would require tech companies to give law enforcement a way to access information on encrypted phones and other devices. (AP Photo/Branden Camp, File)

Asked about the FBI's reliance on a third party to get into the phone, and its inability to access the device on its own, Hess said the work requires "a lot of highly skilled specialized resources that we may not have immediately available to us."

"We live in such an advanced age of technology development. And to keep up with that, we do require the services of specialized skills that we can only get through private industry," she said.

Representatives from local law enforcement agencies echoed Hess's concerns. Thomas Galati, chief of the intelligence bureau at the New York Police Department, said officials there have been unable to break open 67 Apple devices for investigations in 44 different violent crimes—including 10 homicide cases.

Still, despite anxieties over "going dark," a February report from the Berkman Center for Internet and Society at Harvard University said the situation was not as dire as law enforcement had been warning about and that investigators were not "headed to a future in which our ability to effectively surveil criminals and bad actors is impossible."



Indiana State Police, Office of Intelligence and Investigative Technologies Commander Capt. Charles Cohen, testifies on Capitol Hill in Washington, Tuesday, April 19, 2016, before a House Oversight and Investigations subcommittee hearing on deciphering the debate over encryption. (AP

Photo/Manuel Balce Ceneta)

The hearing comes amid an ongoing dispute between law enforcement and Silicon Valley about how to balance consumer privacy against the desire by police and federal agents to recover communications and eavesdrop on suspected terrorists and criminals. It also comes as the Senate considers a bill that would effectively prohibit unbreakable encryption and require companies to help the government access data on a computer or mobile device when a warrant is issued.

Bruce Sewell, Apple's general counsel who also testified, touted the importance of encryption particularly in light of devastating breaches of sensitive government information—including at the IRS and the Office of Personnel Management.

"The best way that we, and the technology industry, know how to protect your information is through the use of strong encryption. Strong encryption is a good thing, it is a necessary thing. And the government agrees," Sewell testified.

"Encryption today is the backbone of our cybersecurity infrastructure and provides the very best defense we have against increasingly hostile attacks," he added.

In response to questions raised at the hearing, Sewell said that the Chinese government had asked Apple for its source code within the last two years—and that Apple declined.

The long-simmering dispute escalated in February after a judge in California directed Apple to help the FBI break into the phone used by Syed Farook, who along with his wife killed 14 people in San

Bernardino on Dec. 2 before dying in a shootout with police. The Justice Department last month said a third party had approached it with a way into the phone, effectively ending that court case.

Another legal fight over a phone in a separate drug case is still pending in Brooklyn.