FBI says it won't disclose how it accessed locked iPhone

April 27 2016, by By Eric Tucker

In this Feb. 17, 2016 file photo, an iPhone is seen in Washington. The FBI said Wednesday, April 27, 2016, that it will not publicly disclose the method that allowed it to break into a locked iPhone used by one of the San Bernardino attackers, saying it lacks enough "technical information" about the software vulnerability that was exploited. (AP Photo/Carolyn Kaster, File)

The FBI said Wednesday that it will not publicly disclose the method that allowed it to access a locked iPhone used by one of the San

Bernardino attackers, saying it lacks enough "technical information" about the software vulnerability that was exploited.

The decision resolves one of the thorniest questions that had confronted the federal government since it revealed last month that an unidentified third party had come forward with a successful method for opening the phone. The FBI did not say how it had obtained access, leaving manufacturer Apple Inc. in the dark about how it was done.

The new announcement means that details of how the outside entity and the FBI managed to bypass the digital locks on the phone without help from Apple will remain secret, frustrating public efforts to understand the vulnerability that was detected and potentially complicating efforts to fix it.

Apple did not immediately respond to requests for comment.

In a statement Wednesday, FBI official Amy Hess said that although the FBI had purchased the method to access the phone—FBI Director James Comey suggested last week it had paid more than $1 million—the agency did not "purchase the rights to technical details about how the method functions, or the nature and extent of any vulnerability upon which the method may rely in order to operate."

The government has for years recommended that security researchers work cooperatively and confidentially with software manufacturers before revealing that a product might be susceptible to hackers. The White House has said that while disclosing a vulnerability can weaken an opportunity to gather intelligence, leaving unprotected Internet users vulnerable to intrusions is not ideal either.

An interagency federal government effort known as the vulnerabilities exploit process is responsible for reviewing such defects and weighing

the pros and cons of disclosing them, taking into account whether the vulnerability can be fixed, whether it poses a significant risk if left unpatched and how much harm it could cause.

Hess, the executive assistant director of the FBI's science and technology branch, said Wednesday the FBI did not have enough technical details about the vulnerability to submit it to that process.

"By necessity, that process requires significant technical insight into a vulnerability. The VEP cannot perform its function without sufficient detail about the nature and extent of a vulnerability," she said.

The revelation last month that the FBI had managed to access the work phone of Syed Farook—who along with his wife killed 14 people in the December attacks in San Bernardino—halted an extraordinary court fight that flared a month earlier when a federal magistrate in California directed Apple to help the FBI hack into the device. Since then, the government has not disclosed the entity or said anything about how the work was done.

At an appearance earlier this month at Kenyon College in Ohio, Comey said the FBI had not yet decided whether to disclose details to Apple but suggested that the agency had reservations about doing so.

"If we tell Apple, they're going to fix it and we're back where we started," Comey said. "As silly as it may sound, we may end up there. We just haven't decided yet."

The FBI director was correct, but that's exactly the way the process should work, said Joseph Lorenzo Hall, senior technologist at the Center for Democracy and Technology.

"If you're going to use flaws in the technology to gain access, then you

better be prepared to report it," he said. Given the imperfections inherent in software writing, and their ability to be exploited for access, "Those bugs need to be fixed as fast as we can because we have no clue about whether there are tons and tons of bugs—or just a few," he said.

Though one can imagine a scenario in which the FBI would hold onto its secret for "a little while," vulnerabilities generally should be reported to the company so they have an opportunity to patch them, said Susan Landau, a cybersecurity policy professor at Worcester Polytechnic Institute.

"To me, and I think the government would clearly agree, the default should be report," she said.