United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510–6275

June 12, 2015

VIA ELECTRONIC TRANSMISSION

The Honorable James B. Comey, Jr.
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535

Dear Director Comey:

I am writing in regard to the Federal Bureau of Investigation's ("FBI") use of spyware. According to press reports, spyware programs can be remotely deployed to a targeted computer to surreptitiously activate the computer's camera and microphone; collect passwords; search the computer's hard drive, random-access memory, and other storage media; generate latitude and longitude coordinates for the computer's location; and intercept phone calls, texts, and social media messages. Obviously, the use of such capabilities by the government can raise serious privacy concerns.

As you and I discussed at an oversight hearing in May of last year, the Department of Justice is currently seeking to amend Federal Rule of Criminal Procedure 41 ("Rule 41") to allow the Department to deploy spyware more easily. Rule 41 applies to search and seizure warrants, and under the current version of the rule, federal prosecutors generally must seek a warrant in the judicial district in which the target of the search is located.[1] This can be a difficult task in the context of cybercrime. The Justice Department's proposed changes would, under certain circumstances, allow judges to grant warrants for remote searches of computers located outside their district or when the location is unknown -- changes that would allow the FBI to more easily obtain approval to infiltrate computer networks to covertly install spyware.[2] The

[1] Fed. R. Crim. P. 41(b)(1), subject to exceptions in Fed. R. Crim. P. 41(b)(2)-(5).
[2] Dustin Volz, *FBI's Plan to Expand Hacking Power Advances Despite Privacy Fears*, NATIONAL JOURNAL, Mar. 16, 2015, available at http://www.nationaljournal.com/tech/fbi-s-plan-to-expand-hacking-power-advances-despite-privacy-fears-20150316.

proposed changes would not affect the requirement that, in order for the FBI to obtain a warrant under the rule, it must demonstrate probable cause that the targeted device contains evidence of a crime.

It is essential that law enforcement has the necessary technological tools and legal framework to keep the public safe. However, a number of organizations have raised concerns about the scope of the proposed rule change, including constitutional concerns, risks of forum-shopping, and potential extraterritorial use.[3] Despite these concerns, the U.S. Courts' Judicial Conference Advisory Committee on Criminal Rules voted in favor of the change in March of this year, as did the next group in the review process, the Courts' Standing Committee, on May 28.[4] In keeping with the process for modifying the rules, the proposed change will next be considered by the Judicial Conference, and if approved there, by the Supreme Court, with a Congressional review period to follow.

Although the uses of stealthy surveillance and deception to catch criminals are lawful and well-recognized investigative tactics under certain circumstances, and although the FBI's use of spyware in general has long been reported,[5] the Committee needs more specific information about the FBI's current use of spyware in order to fulfill its oversight responsibilities, including: the types of spyware programs used; their capabilities; the FBI's internal policies and procedures for using spyware; the legal processes used; the methods of deploying spyware; and the audit procedures used to ensure the spyware is used in compliance with both FBI policies and the law.

Publicly available information on the FBI's use of spyware is often inconsistent. It is unclear from public reporting which spyware programs the FBI currently uses and what their capabilities are. While some press reports have stated that FBI spyware merely logs a target's "IP address, MAC address, computer programs running, operating system details, browser details, and other identifying computer information,"[6] a 2013 court order denying an FBI warrant application stated that the "application request[ed] authorization to surreptitiously install data extraction software [that] has the capacity to search the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to FBI

---

[3] Dustin Volz, *Google Calls FBI's Plan to Expand Hacking Power a 'Monumental' Constitutional Threat*, NATIONAL JOURNAL, Feb. 18, 2015; Stan Schroeder, *Proposed Rule Would Give U.S. Power to Cybersnoop Worldwide, Google Warns*, MASHABLE, Feb. 19, 2015.

[4] Cory Bennett, *FBI Request to Expand Hacking Power Advances*, THE HILL, Mar. 17, 2015; Cory Bennett, *FBI Inches Closer to Expanded Search Powers*, THE HILL, May 29, 2015; Tim Cushing, *Judicial Committee Gives FBI The First OK It Needs To Hack Any Computer, Anywhere On The Planet*, TECHDIRT, Mar. 17, 2015.

[5] Craig Timberg and Ellen Nakashima, *FBI's Search for "Mo," Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, THE WASHINGTON POST, Dec. 6, 2013; *see* Kevin Poulsen, *Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years*, WIRED, Apr. 16, 2009.

[6] Kate Knibbs, *The FBI Has Its Own Secret Brand Of Malware*, GIZMODO, April 2, 2015; Kevin Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, WIRED, July 18, 2007.

agents."[7] A Washington Post article also reported that the FBI's spyware can "covertly download files, photographs[,] and stored e-mails, or even gather real-time images by activating cameras connected to computers[.]"[8] Similarly, while some press reports have described a spyware program developed in-house by the FBI,[9] others have noted that the U.S. government is now the largest purchaser of malware from the private sector,[10] and there are reports that another component of the Justice Department has purchased such private-sector spyware.[11]

The procedures used by the FBI to obtain approval to deploy spyware and the methods of such deployment also raise important issues. The Washington Post has reported that FBI agents "obtain warrants to search a suspect's computer but generally do not inform the judge of an intent to hack the computer to install the malware."[12] The Washington Post also reported that the most common delivery method for installing the spyware is phishing attacks, in which the FBI masquerades as a trustworthy source in order to trick the target into clicking on a link infected with the spyware.[13] In one publicly-reported case, FBI agents posed as the Associated Press and created a fake AP news article in a successful phishing effort to deploy spyware.[14] However, in the relevant search warrant application, the agents "did not alert the judge of their plan to mimic the media."[15] After learning of the ruse, the AP stated "[w]e find it unacceptable that the FBI misappropriated the name of the Associated Press and published a false story attributed to the AP. This ploy violated AP's name and undermined AP's credibility."[16] It is also unclear from public reporting whether the FBI uses other methods of spyware deployment in addition to phishing, such as zero-day exploits, which exploit vulnerabilities in legitimate software applications.

In short, the FBI's use of spyware and the DOJ's proposed changes to the legal framework through which the FBI receives judicial approval to do so raise several important

---

[7] *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753, 755 (S.D. Tex. 2013); *see* Jennifer Valentino-DeVries, *Judge Denies FBI Request to Hack Computer in Probe*, THE WALL STREET JOURNAL, Apr. 24, 2013.
[8] Craig Timberg and Ellen Nakashima, *FBI's Search for "Mo," Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, THE WASHINGTON POST, Dec. 6, 2013.
[9] *Supra* n. 6.
[10] Zack Whittaker, *U.S. Government Becomes the 'Biggest Buyer' of Malware*, ZDNET, May 13, 2013; *see* Joseph Menn, *Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback*, REUTERS, May 10, 2013.
[11] Lorenzo Franceschi-Bicchierai, *The DEA Has Secretly Been Buying Hacking Tools From An Italian Company*, MOTHERBOARD, April 15, 2015; Timothy J. Seppala, *The DEA's Using Powerful Spyware For Surveillance Too*, ENDGAGET, April 16, 2015.
[12] Ellen Nakashima and Paul Farhi, *FBI Lured Suspect With Fake Web Page, But May Have Leveraged Media Credibility*, THE WASHINGTON POST, Oct. 28, 2014.
[13] [13] Craig Timberg and Ellen Nakashima, *FBI's Search for "Mo," Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, THE WASHINGTON POST, Dec. 6, 2013.
[14] *Supra* n. 12; *see* James B. Comey, *To Catch a Crook: The FBI's Use of Deception*, Letter to the Editor, THE NEW YORK TIMES, Nov. 6, 2014.
[15] *Supra* n. 12.
[16] *Id*.

questions. The Committee needs additional information from the FBI in order to address them. Accordingly, please provide written responses to these questions by June 26, 2015:

1. Which spyware, related programs, and other network investigative techniques has the FBI used in the field since 2009? Please include both government-created programs and ones purchased externally, if any, from companies such as Hacking Team and Gamma Group International.

    a. What are each program's capabilities?

    b. How much has the FBI spent on each program?

    c. How many times has the FBI used each of these programs in the field, and in what capacity? How many times has the FBI used the programs to remotely activate the subject device's camera or microphone?

2. What are the internal FBI policies and procedures related to requesting, approving, deploying, and terminating the use of spyware and related programs? Please provide copies of all guidance documents.

3. Pursuant to what legal authorities does the FBI deploy spyware and related programs?

    a. Does the FBI always obtain a search warrant or other judicial approval prior to using such programs? If not, why not?

    b. Does the FBI use different legal authorities or processes based on the jurisdiction in which it determines the target to be located?

    c. Does the FBI use different legal authorities or processes if it cannot determine the jurisdiction in which the target is located?

4. Has the FBI deployed spyware on behalf of state or local law enforcement? If so, what are the internal FBI policies and procedures related to doing so?

5. When the FBI seeks a warrant to search a computer, does it always notify the judge when it intends to hack the targeted computer and surreptitiously install spyware? Does it specify in the warrant application the capabilities of the spyware it seeks to deploy? Does it specify the method of deployment to be used?

6. What methods does the FBI use to deploy spyware? Please list each method of deployment used in the field since 2009 and the number of times it has been used.

7. Does the FBI use zero-day exploits in conjunction with its use of spyware?

    a. If so, are these zero-day exploits developed by the government or purchased externally from private companies, such as Vupen Security?

    b. If so, how much has the FBI spent on developing or purchasing zero-day exploits? Please list both the cost for in-house development and external purchases.

    c. If so, does the FBI ever notify the company that owns the exploited software of the security breach? If it does, what policies guide the timing and content of this disclosure? If it does not, why not?

8. As noted above, the FBI has acknowledged using phishing to deploy spyware, and impersonating a real media outlet in doing so. Since 2009, how many times has the FBI impersonated personnel from legitimate companies, whether media or otherwise, in deploying spyware?

    a. Which companies has it impersonated?

    b. Does the FBI notify the companies it impersonates that it has done so? If so, what policies guide the timing and content of this disclosure? If not, why not?

9. For how long does the FBI retain any data obtained through spyware?

a. Who has access to the data while it is in the FBI's possession?

b. How, if at all, is the data destroyed?

10. What internal audit procedures does the FBI use to ensure that spyware and related programs are used in accordance with agency policies, procedures, and the law?

a. If they exist, have such internal audit procedures discovered any violations of FBI policies, procedures, or applicable law relating to the use of spyware or related programs? Has the FBI discovered any such violations through other means?

b. If so, please provide the details of each violation, as well as any remedial or punitive measures taken in response.

Please number your answers according to their corresponding questions. In addition, please arrange for FBI officials to provide a briefing to Judiciary Committee staff about these issues following the provision of your responses, but in any event no later than July 2, 2015. If you have any questions about this request, feel free to contact Patrick Davis of my Committee staff at (202) 224-5225. Thank you for your attention to these important matters.

Charles E. Grassley

Chairman
Senate Committee on the Judiciary