RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate

WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

December 20, 2022

The Honorable Christopher A. Wray
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001

Dear Director Wray:

I write to request that the Federal Bureau of Investigation (FBI) publish basic information about its hacking operations against Americans, by making public the policies governing the agency's use of this technique and annual aggregate statistics.

The FBI has used hacking, which it calls a "remote search," as a law enforcement investigative technique for at least 20 years, but public details about the scope and policies governing FBI hacking remain scarce. The U.S. government's use of hacking to search and track individuals' computers was first revealed in 2007 by the government in court documents, with more significant details released in 2009, in response to a Freedom of Information Act request by *Wired* magazine. In a 2002 memo released in response to that FOIA request, the Department of Justice (DOJ) warned of abuse, writing, "we are seeing indications that [hacking tools are] being used needlessly by some agencies, unnecessarily raising difficult legal questions (and a risk of suppression) without any countervailing benefit." The heavily redacted documents identified several specific law enforcement investigations in which the FBI had used hacking software. However, even today no agency policy governing the use of hacking has been published, nor does the FBI publish statistics detailing how frequently the agency hacks Americans' phones and computers.

The handful of FBI hacking incidents that have come to public attention have raised troubling questions about the agency's use of this powerful surveillance technique. For example, in 2007, the FBI impersonated the Associated Press as part of an investigation into bomb threats made by a Seattle-area teenager. According to a report into the incident by the DOJ Inspector General, the FBI impersonated a journalist to "surreptitiously insert a computer program into the individual's computer that would identify his location."

In another case in 2013, the FBI obtained a court order allowing it to hack 300 users of an anonymous email service, who were suspected of serious criminal activity. However, according

to press reports, the FBI did not deliver its hacking software to these specific court-approved accounts, by identifying them after they had logged in. Instead, as reported by Wired in 2013, the home page of the TorMail service was replaced with a "Down for Maintenance" page that also included code that surreptitiously exploited a vulnerability in web browsers that visited the page.

If it is true that the FBI delivered its hacking software through TorMail's homepage, before users could login, that would mean that the FBI had no way of restricting the computers that were hacked to just those users authorized by the court-issued search warrant. It also would mean the FBI had no way of knowing which TorMail accounts were associated with the computers that the FBI successfully hacked. It remains unclear why the FBI's malware would have been deployed in this manner or, if these press accounts are true, whether the FBI disclosed to the judge that authorized the hacking operation that the government exceeded the scope of the court's order and seemingly botched the operation.

Most recently, the public learned that the FBI purchased hacking software from the NSO Group, a controversial surveillance company whose software has been used by authoritarian governments to hack human rights activists, political dissidents, and journalists. At an open hearing of the House Permanent Select Committee on Intelligence on March 8, 2022, you confirmed that the FBI purchased a license for the NSO Group's software, but testified that it had purchased a "limited license for testing and evaluation; so not used in any investigation of anyone." It was not until June 6, 2022, that you informed the public, in an unclassified letter to me, that one of the purposes of the license was to "explore potential future legal use of the NSO product." And it was not until November 2022, when the New York Times published internal FBI emails it obtained through a FOIA lawsuit, that the public learned the FBI only abandoned its efforts to use NSO Group tools in July 2021. FBI officials even developed draft guidelines for federal prosecutors, outlining how information about the use of this tool would need to be disclosed during criminal cases. It remains unclear what triggered the decision by FBI leadership to forgo operational use of the tool.

The FBI cannot continue to shroud in secrecy the rules that govern its hacking operations against Americans' phones and computers. The American people have a right to know the scale of the FBI's hacking activities and the rules that govern the use of this controversial surveillance technique. Judges must have the information they need to carefully review the FBI's remote search applications, particularly in cases where the FBI intends to engage in bulk remote searches against hundreds, or thousands of targets at a time. The FBI can and should provide much-needed transparency for both the courts and the public by releasing its internal policies governing its use of hacking tools, which it calls Network Investigative Techniques, and by publishing aggregate statistics on its remote search operations, similar to the reports that the government already publishes about other surveillance tools, such as wiretaps and pen registers.

Please also provide me with unclassified answers to the following questions by January 27, 2023:

1. In each of the last three years, in how many operations has the FBI used Network Investigative Techniques, how many were court-authorized, and how many individuals, devices, and accounts were searched remotely by the FBI?
2. After acquiring software from the NSO Group, did the FBI submit to the Vulnerabilities Equities Process the specific software exploits used by the NSO Group's software? If not, please explain why.
3. According to media reports, the NSO Group's software was discovered on devices used by State Department employees working overseas. Has the FBI ever alerted other U.S. government agencies about the specific vulnerabilities that the NSO Group's software exploits or provided those agencies with malware signatures for the NSO Group's software, so those agencies could defend their personnel from foreign government hacking? If not, please explain why.
4. Why did the FBI decide not to use the NSO Group's software to support its investigations?
5. Was a legal determination made that would preclude the FBI's future use of NSO or similar tools?
6. If the FBI determined that the NSO Group's software posed a national security threat, please explain how the FBI will assess other surveillance technology vendors to determine if they pose the same threat.
7. To date, has the FBI ever delivered Network Investigative Techniques to or otherwise conducted a remote search of the wrong person, account or device? If yes, what corrective action did the FBI take, including notifying the court that originally authorized the remote search operation?
8. The DOJ OIG's 2016 report on the FBI's impersonation of the Associated Press included three recommendations, and the FBI told the OIG it concurred with these recommendations. Please identify the specific outcomes of the FBI's implementation of these recommendations, including any changes the FBI made to its written policies.
9. The OIG's 2016 report stated that the FBI in June 2016 adopted an interim policy that provides guidance to FBI employees regarding their impersonation of members of the news media during undercover operations. Is this interim policy still in effect or has the FBI updated and finalized this policy? Please provide me with a copy of the policy currently in effect.
10. When the FBI conducts hacking operations against targets whose locations are then unknown and could possibly be located overseas, does the FBI coordinate its activities with the Department of State? If not, please explain why. Please also explain the steps the FBI takes to ensure that such operations are conducted in a manner consistent with

international law and, in particular, that the FBI is not unintentionally hacking computers that are used by organizations responsible for critical infrastructure.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,

Ron Wyden
United States Senator