U.S. Department of Justice

Federal Bureau of Investigation

Office of the Director

Washington, D.C. 20535-0001

July 21, 2023

[redacted]
United States Senate
Washington, DC 20510

Dear [redacted]

I write in response to Congress' concerns related to the FBI's compliance surrounding queries of FISA Section 702 information and to update the Committee on the FBI's compliance and accountability reforms, the impact of these reforms, and to provide some recently declassified examples that demonstrate how Section 702 is invaluable in protecting Americans and the homeland from malicious cyber actors, hostile nations, and international terrorists, among other foreign threats. I, my leadership team, and FBI personnel at headquarters and in the field are committed to providing Members of Congress and the American people with the information to demonstrate our role as good stewards of the important authorities entrusted to us under Section 702.

I. FBI's Substantial Compliance Efforts and Their Significant Impact

As I have said many times before, the FBI's pre-reform compliance related to Section 702 queries was unacceptable. Our analysis of the problem revealed that we needed to undertake foundational reforms focused on how FBI personnel used Section 702, including how they were trained and supervised. Accordingly, beginning in the summer of 2021 and continuing through 2022, the FBI instituted a series of reforms designed to address the root causes of FISA query compliance incidents.

The post-reform evaluations—including by the Foreign Intelligence Surveillance Court (FISC) and the Department of Justice (DOJ)—have revealed significant improvement in our Section 702 querying compliance.[1] In its April 2023 opinion, the FISC calculated its own rate of

[1] Over the past nine months, the Office of the Director of National Intelligence (ODNI) has declassified a number of FISC opinions and ODNI and DOJ joint assessments that discuss the FBI's **pre**-reform querying practices. The non-compliant practices described in these reports

FBI's compliance and found that FBI personnel complied with the query standard over 98 percent of the time. As the FISC succinctly put it, the FBI's reforms since 2021 "are having the desired effect."[2] DOJ's most recent Semi-Annual Report from March 2023 calculated that our compliance rate with the query standard rose to almost 99 percent. The high compliance rates detailed in the DOJ Report and the FISC's opinion match the findings from the FBI's independent Office of Internal Audit (OIA)—an office that I directed be created as part of our reforms. Following the implementation of the bulk of our reforms, OIA conducted an audit of the FBI's querying practices focused on the highest risk queries. OIA determined that FBI personnel had a 96 percent compliance rate with the query standard—a double-digit improvement from OIA's pre-reform audit.[3]

We have significantly lowered our incidents of non-compliance because of our focus on systemic issues, many of which were uncovered by DOJ and highlighted by the FISC. We changed FBI databases to address even inadvertent querying-related incidents. Personnel must now "Opt-In" and affirm that they intend to run their queries against our Section 702 collection. We also overhauled our training and now require FBI personnel re-take this training annually or else lose access to FISA databases. For higher-risk queries like sensitive and batch queries, we have also implemented and now require supervisory and/or legal approvals. As an example, sensitive queries require higher attorney level review, and in some cases, approval by the Deputy Director.

Along with substantially lowering incidents of Section 702 query non-compliance, these reforms have also significantly decreased the number of Section 702 queries conducted by FBI personnel, including lowering the number of U.S. person queries by over 93 percent.[4] Through our reforms, including the opt-in requirement and enhanced training, we have sought to cement in our personnel the need to take a surgical and judicious approach when conducting U.S. person queries of Section 702 intelligence—to use the least intrusive means to accomplish our mission of protecting Americans' lives, while protecting civil rights and liberties.

We are heartened by the measurable success documented by the FISC, DOJ, and OIA, but we recognize that we have more to do—that compliance is an ongoing endeavor. OIA's latest audit resulted in 11 recommendations.[5] I accepted all of OIA's recommendations and directed my leadership team to begin implementing them immediately. We are also regularly evaluating our reforms and looking for ways to strengthen them. For example, all queries using the FBI's batch job tool—which allows personnel to run multiple queries at the same time—will now require attorney review—removing the 100-query term threshold we originally instituted.

We have also heard loud and clear Congress' desire to ensure that the FBI has additional accountability measures where personnel run non-compliant queries in a negligent manner. To be

---

(including the 2022 FISC opinion declassified in April 2023) do not represent the FBI's current **post**-reform compliance practices. The 2023 opinion is the first **post**-reform opinion by the FISC.

[2] https://www.intel.gov/assets/documents/702%20Documents/declassified/2023/FISC_2023_FISA_702_Certifications_Opinion_April11_2023.pdf at 83.

[3] https://www.fbi.gov/file-repository/fisa-query-audit-051023.pdf at 6.

[4] https://www.dni.gov/files/CLPT/documents/2023_ASTR_for_CY2022.pdf at 24.

[5] https://www.fbi.gov/file-repository/fisa-query-audit-051023.pdf at 7.

clear, we have found very few instances of FBI personnel maliciously running non-compliant queries against our Section 702 collection—with the last identified instance occurring over four years ago. In each of those instances, they have resulted in referrals to our Inspection Division for investigation and disciplinary action, including severe employment consequences such as revocation of a clearance and termination. In June, we established a new policy with escalating consequences for performance incidents involving even negligent or careless querying, including centralized tracking of individual employee performance incidents over time. A first violation will result in immediate suspension of FISA access, requiring the employee to retake mandatory FISA training and be counseled by their field office attorney, along with a letter documenting the incident placed in their personnel file. Subsequent incidents will result in further measures, up to and including indefinite loss of FISA access, reassignment to a new role, and/or referral to FBI's Inspection Division. We have also instituted measures to hold FBI field leaders personally accountable for FISA compliance efforts in their offices, and performance against these measures will impact their eligibility for promotions, among other things.

We are committed to holding ourselves accountable and we are eager to discuss with Members how these reforms can be enshrined as part of Section 702's reauthorization. We also welcome discussing with Congress additional reforms and evaluating how these reforms can be implemented without diminishing Section 702's vital intelligence value.

II. The Value of Section 702 to Protect Americans and the Homeland

Section 702's critical importance to our national security has only grown with the evolution of technology and threats. Without Section 702 we would be unable to plug a critical intelligence gap—one that foreign threat actors regularly exploit as they traverse computer networks and electronic service providers to conduct cyberattacks, espionage campaigns, or coordinate with likeminded terrorists. To put it plainly, Section 702 is invaluable to our ability to know what our foreign adversaries are doing and how they are doing it—intelligence without which we could not protect Americans or the homeland.

For example, in the first half of this year, 97 percent of the FBI's raw technical reporting on malicious cyber actors, and 92 percent of our reporting on emerging technologies, such as artificial intelligence, came from Section 702. On average over the past 10 years, malicious cyber actors have accounted for more than half of our Section 702 targets. FBI's Cyber Division uses this intelligence to conduct strategic disruption activities against the malicious cyber actors, including taking down their infrastructure, seizing their money, and working with DOJ to bring charges against the hackers. Thanks to the intelligence we receive from Section 702, FBI's Cyber Division is able to work with our U.S. Intelligence Community (USIC) partners and warn victims when cyber criminals are prepositioning for attacks—so before the attack begins—and help the victims close backdoors and remove the hackers from their systems.

Section 702 has been pivotal for the FBI to detect and thwart Chinese hackers attempting to access U.S. critical infrastructure. The USIC has assessed that China is attempting to preposition on U.S. critical infrastructure—setting up backdoors to cripple critical infrastructure in the event China invades Taiwan and therefore limiting our ability to assist Taiwan. Accordingly, the FBI has seen China-based hackers access a variety of critical infrastructure in the United States.

Section 702 allows us to detect these hackers by monitoring them as they traverse the internet and determine when they access networks within the United States. Using U.S. person queries for the identifiers of potential victims—namely American businesses—we can see whether the hackers are merely researching a victim for future attacks or if they have already compromised the systems.

Using such techniques, the FBI identified Chinese hackers gaining access to computer networks of a major U.S. transportation hub. Through U.S. person queries, the FBI was able to identify the particular network infrastructure the Chinese hackers had successfully compromised. This allowed the FBI to quickly alert the network operators to the particular portion of their network that had been compromised and assist with fixing the vulnerabilities. Along with impeding our ability to assist Taiwan in case of an attack, such Chinese intrusions are meant to wreak havoc with the everyday lives of Americans, and they have the potential to cause millions (possibly billions) of dollars in damage to industry. Moreover, where we have seen foreign actors target critical infrastructure like hospitals, airports, and utilities such as power and water, such attacks would potentially jeopardize the physical safety of Americans. Without this intelligence, the FBI—which has the sole mandate in the USIC to act on the intelligence we get from Section 702 to protect the homeland—would be blinded to such malicious actions from China-based hackers and unable to counter them.

Iran has also been bolstering their cyber capabilities and have weaponized them against our critical infrastructure, including perpetrating a cyberattack on the Boston Children's Hospital in 2021. Iran, along with North Korea, is one of only two nation-states known to have conducted destructive cyberattacks within the United States. Iran has also sought to assassinate American citizens, including high-level government officials. Many of these covert and overt actions are planned from across the globe through the internet. Section 702 plays a crucial role to help us stay ahead of such threats and disrupt the attacks. For example, Iranian agents had targeted the former head of a U.S. federal department. In preparation, Iranian hackers conducted extensive research on their target. Our Section 702 collection and U.S. person queries helped us connect the dots. We were able to warn the victim and his former Department, and as a result they were able to take proactive steps to protect him. The intelligence provided by Section 702 is vital to our ability to help protect our government and legislative officials and mitigate potential attacks.

In the past five years, hostile foreign governments also have increasingly engaged in repressive activities against Americans to silence dissidents and minorities. This transnational repression is typically coordinated by agents in the foreign country using co-optees in the United States. Such repressive activities range from suppressing protests against their oppressive regimes to kidnapping Americans to even conducting assassinations in the United States. Using Section 702, the FBI has been able to identify the extent of transnational repression activities of countries like China and Iran, intercepting the foreign agents or their co-optees, and protecting victims.

The FBI needs Section 702 to keep countering the next five years of foreign threats—stopping international terrorists plotting with collaborators in the United States to launch terrorist attacks, disrupting foreign cyber actors trying to hold our government, our people, and our businesses hostage, and preparing to meet the new threats all of these adversaries constantly seek to bring to the homeland. The FBI looks forward to future engagements this year with Congress

The Honorable [redacted]

to highlight the value of this important authority to the American public and how we can become the best stewards of this vital source of foreign intelligence.

Sincerely,

Christopher A. Wray
Director

cc: [redacted]