Good morning, and thank you to Chair Franklin and the other members of the Board for the opportunity to contribute to this important discussion. As an FBI Agent who has investigated cyber and national security cases since before FISA Section 702 was created, I have personally used both it and "Traditional" FISA as a case agent, and in a wide variety of leadership roles. So, I have seen firsthand the value this authority brings to the FBI's mission: to protect the American people and uphold the Constitution.

From the FBI's perspective, the primary national security threats to the Homeland now reside outside of the United States, so we must collect outward to protect ourselves inward. There is no more agile or efficient tool to do so than Section 702.

This agility is particularly important in a technology environment where foreign threat actors can move to new communication accounts and infrastructure in a matter of hours, if not minutes. And Section 702's precision lets us home in on only the information necessary and relevant to investigating and countering threats.

To more concretely illustrate its value, let me tell you a few stories about how the FBI uses Section 702 to protect the Homeland. In particular, I'd like to focus on the importance of querying Section 702 data for terms related to U.S. persons, or USPER queries, a topic which I know has seen a lot of interest recently. While these are hypothetical scenarios, they are closely based on actual cases where we have used FISA 702, and USPER queries, to protect Americans from three of our biggest national security threats.

- First, terrorism: the FBI receives a tip that a foreign terrorist organization is targeting a particular U.S. person. So we regularly query Section 702 data for that potential victim's identifiers and, in one of those queries, find specific plans to target him through an unwitting associate. Because of those queries, we are able to give both U.S. individuals specific information to protect themselves, before the terrorists take action.
- Second, counterintelligence: the FBI finds a foreign spy possesses identifiers for dozens of U.S. persons. We query those identifiers against Section 702 data to determine which of those individuals might be actual or potential victims in need of defensive briefings or other protective measures, and which might be accomplices or co-optees in need of further investigation. The queries allow us to efficiently and selectively review foreign communications to answer that question, instead of using other, possibly more intrusive, techniques to accomplish the same end.
- Third, cyber: a U.S. company suffers a breach, and the FBI has reason to believe it may be the work of a foreign cyber actor. So we query identifiers related to the company, including employees whose accounts may have been targeted in the incident. In a situation where every passing minute could mean irreparable damage or loss of data, these queries allow us to quickly determine attribution, identify adversary footholds on the network, and share specific information about that cyber group with the company, allowing them to uncover the full extent of the breach and evict the bad actors.

As you can see, querying our lawfully acquired and held FISA information is crucial to finding threat intelligence in a targeted and efficient manner, so we can act on it quickly enough to prevent damage *before* it happens.

Now many of you may be tracking the FBI's compliance challenges related to USPER queries of Section 702 data, such as those noted by the Foreign Intelligence Surveillance Court in its since-declassified November 2020 opinion. While it is important to note that the Court did not find unlawful purpose or bad faith, the high rate of non-compliance found by the Court and other oversight bodies over the past couple of years is nevertheless unacceptable. As Director Wray has said publicly, he is "hell bent" on doing whatever it takes to fix our compliance, and that is a feeling all of us in FBI leadership share.

So what have we done about it? After a hard look at the types of errors we were seeing, the FBI implemented a series of major reforms throughout 2021 and 2022 to address their root causes. We made changes to our database systems to enhance understanding and compliance, including switching the default settings so users must affirmatively choose to have their queries run against FISA data. We instituted pre-approval for certain categories of queries, in some cases requiring the Deputy Director of the FBI to personally approve queries before they are run. We clarified our guidance to the workforce on query standards, and created new, improved, and mandatory training on those standards.

While initial indications from these reforms are promising, we are committed to continuing to take whatever steps we must to get it right. To that end, I would highlight one more important reform: the creation of a new Office of Internal Audit, solely focused on evaluating our FISA compliance and recommending reforms, on an ongoing basis.

Finally, I want to make sure we don't lose sight of the fact, as we contemplate renewal of this important authority, that we will need it not to counter the threats of the last 5 years, but those of the next 5 years and beyond. As foreign terrorist organizations reconstitute and pose a resurgent threat to the Homeland, as foreign cyber attacks continue to escalate in sophistication and frequency, and as we enter into an era of heightened strategic competition, the foreign intelligence we depend on Section 702 to collect will become even more crucial to protecting the United States and its interests. And loss of this vital authority would leave us vulnerable to all of those threats as they grow in intensity over the coming years.