OVERSIGHT OF THE FEDERAL BUREAU OF INVESTIGATION
DIRECTOR CHRISTOPHER WRAY

JUNE 10, 2021

Questions for the Record
Submitted by Rep. Tom McClintock

1. How many persons on the Terrorist Watch List have been encountered this year crossing through our southern border and how many persons with criminal records or criminal warrants have been encountered this year crossing our southern border?

   Response: While it is a possibility that foreign terrorist organizations (FTOs) might use migrant travel routes into the U.S. to infiltrate our border crossing points, at this time, the FBI is not aware that we have information relating to a specific terrorist threat from current migrants heading into the U.S.

2. What is the current FBI estimate of how many terrorists, criminals, and gang members are among the hundreds of thousands of got-aways the Border Patrol was not able to intercept?

   Response: The Department of Homeland Security (DHS), and specifically U.S. Customs and Border Protection (CBP), is the lead federal agency for border security, and the FBI defers to CBP to address any questions about their border interception efforts.

3. On that point, House Republican Leader Kevin McCarthy sent you a letter in April requesting a briefing on this subject. Will you commit to providing all members of this committee with the briefing you provided to Mr. McCarthy to keep us fully informed on this issue?

   Response: On June 8, 2021, FBI Section Chief Michael Glasheen participated in a joint briefing with Department of Homeland Security and a member of the Intelligence Community for House and Senate Leadership. As the lead federal agency responsible for border security, DHS led the briefing, and the FBI defers to DHS for additional questions regarding that briefing.

4. With regards to announcement of the Joint Task Force Alpha to combat the human trafficking that the Biden open border policies made possible, how many agents will be assigned to this endeavor? How much money will back this task force?

   Response: Joint Task Force Alpha enhances U.S. enforcement efforts against both human smuggling and human trafficking groups. Since the announcement of Joint Task Force

Alpha, the FBI has partnered with DHS, CBP, the Drug Enforcement Administration (DEA), and other federal partners in combining investigative, prosecutorial, and capacity-building efforts to combat human smuggling and human trafficking. The number of personnel assigned and financial expenditures are still being determined. The FBI will continue to work closely with its national and international partners to identify, disrupt, and dismantle transnational criminal organizations engaged in human smuggling and human trafficking.

Questions for the Record
Submitted by Rep. Zoe Lofgren

5. Over the past year, there have been multiple press reports that government law enforcement and surveillance agencies, including the FBI, have bought large volumes of personal data and other information linked to individual persons in the United States – including information originally collected from and/or generated by the activities of individual users of electronic devices and online services – from private data brokers and other private sources. I have several related questions:
    a. Does the FBI purchase any products or services from private entities that give it either direct or indirect access to nonpublic information originally collected from and/or generated by the activities of individual users of electronic devices, software and/or online services? To be clear, this question would include services that allow the FBI to search or otherwise use databases of such privately collected data, even if the agency does not take immediate possession of databases or information itself.
    b. In what year did the FBI first start making such purchases?
    c. What types of such personal information (*i.e.*, that is linked or otherwise related to an identifiable individual) have been included in such purchases? In particular (and without limiting other categories identified in a complete response to the above question), which of the following have been included: geolocation data; photographic or video images of recognizable faces; information reflecting user activity on social media websites and services; information reflecting logs, histories, or equivalents of user activities in web browsers or other software applications?
    d. For what purposes does the FBI use personal information purchased from private entities (including any products and services giving either direct or indirect access to such information)?
    e. Has any such information purchased from private entities been used in the course of criminal investigations by the FBI? If so, are the defendants in any legal proceedings resulting from such investigations notified about these uses of purchased information?

Response: The FBI only obtains and utilizes data for its investigations where it is lawfully permitted to do so. The FBI adheres to the Attorney General's Guidelines for

Domestic FBI Operations (AGG-DOM), which lays out the rules the FBI must follow in collecting information. The AGG-DOM lists the "authorized methods" that the FBI may use at various stages of an investigation. Among those authorized methods are "obtain[ing] publicly available information" as well as "us[ing] online services and resources (whether nonprofit or commercial)." Certain information relating to the identification of specific data sources lawfully used by the FBI to further its investigations, including information relating to particular commercial entities, may be considered to be law enforcement sensitive, because it could reveal and thereby compromise the investigative techniques the FBI uses to detect and disrupt criminal activity. In national security investigations, this kind of information may also be classified. For these reasons, the FBI has and will continue to provide Congress with further information in closed settings, as appropriate. The FBI recognizes that the use of any of its authorized methods—including obtaining publicly available information or using online commercial services—can have an impact on the privacy of Americans, which is why the AGG-DOM additionally requires the FBI to employ the "least intrusive method" that is operationally sound and effective in a given situation. Further, the FBI is dedicated to supporting the Office of the Director of National Intelligence's efforts to provide more transparency to the American public about the circumstances and legal frameworks under which elements of the intelligence community—including the FBI—purchase and make use of commercially available information. The FBI will continue to do so.

6. Section 702 prohibits the FBI from "intentionally target[ing] a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States." Has the FBI used Section 702 to acquire information when targeting a particular, known person reasonably believed to be in the United States is **one of several** purposes of the acquisition? In other words, does the FBI understand Section 702 (as codified in 50 U.S.C. § 1881a(b)(2)) to prohibit an acquisition targeting a particular, known person reasonably believed to be in the United States only if that is the **sole** purpose of such targeting?

   Response: Acquisitions under Section 702 may not intentionally target a person reasonably believed to be located outside the U.S. if the purpose of the acquisition is to target a particular known person reasonably believed to be located in the U.S. In other words, reverse targeting is prohibited. Only non-U.S. persons reasonably believed to be located outside the United States who are reasonably expected to possess, receive and/or communicate the types of foreign intelligence information authorized for acquisition may be targeted under Section 702. To the extent a valid Section 702 target communicates with someone located in the United States or a U.S. person, applicable FISC-approved minimization and querying procedures regulate how such information may be accessed, retained, used, and disseminated.

7. Has the FBI purchased internet metadata, including "netflow" and Domain Name System (DNS) records?

   Response: (U//FOUO) The FBI has a contract with Argonne Ridge for Netflow, and purchases access to DomainTools, VirusTotal Enterprise, and Farsight Passive DNS. The National Cyber Investigative Joint Task Force (NCIJTF) also utilizes data from Shodan and Maxmind for enrichment.

8. Has the FBI purchased domestic internet communications (in which the sender and all recipients are associated with U.S. IP addresses)?

   Response: The FBI only obtains such content in support of its investigations consistent with applicable law and policy, such as through court-authorized criminal legal process pursuant to the Electronic Communications Privacy Act.

9. Has the FBI purchased internet communications in which one party is associated with a U.S. IP address and another party is associated with a non-U.S. IP address?

   Response: The FBI only obtains such content in support of its investigations consistent with applicable law and policy, such as through court-authorized criminal legal process pursuant to the Electronic Communications Privacy Act.

Questions for the Record
Submitted by Rep. Sheila Jackson Lee

On January 6th the domestic terrorists who beat law enforcement officers and breached the Citadel of democracy of the United States wore insignias of White Supremacist groups, waved confederate flags, hung a noose on the lawn, and they were shouting racial epithets. As indicated, NYPD sent a packet of raw intelligence concerning potential violence.

10. With all of that information, including an assessment at headquarters why did the FBI not issue a formal threat assessment that violence at the U.S. Capitol on January 6, 2021 was a foreseeable probability? Also, please explain in detail what other actions, if any, were taken by the FBI. Provide documentation.

    ***Response*:** In advance of January 6th, the FBI prioritized the collection, sharing, and dissemination of intelligence with federal, state, and local law enforcement partners through various channels.

    Throughout 2020, the FBI issued numerous external intelligence products to our partners specifically raising concerns about domestic violent extremism—including concerns about domestic violent extremism related to the election and related to domestic violent

extremism continuing past Election Day itself right up to the time of the certification and the Inauguration.

In the weeks leading up to the January 6, 2021, the FBI's Washington Field Office (WFO) participated in numerous coordination meetings and partner calls with other federal and local law enforcement agencies that focused on threat intelligence sharing and planning related to the election and the Inauguration. These discussions focused on each agency's operating posture in light of the planned events on the 6th, including the tactical assets that would be available in support of other agencies, as well as law enforcement partners' Inauguration briefs.

The FBI also activated a command post at FBI Headquarters and a command post at WFO to facilitate information sharing with our partners in advance of and on January 6th. Both command posts were connected virtually for briefings and other information sharing. On the morning of January 6th, the command posts instituted a regular briefing cycle for sharing threat intelligence and other pertinent information, with immediate threats being shared as they were received (outside of the existing, bi-hourly cadence).

The FBI Headquarters command post was comprised of multiple FBI Headquarters divisions, as well as representatives from the FBI's federal, state, and local partners. WFO's command post included representatives from U.S. Capitol Police, U.S. Park Police, the Washington Metropolitan Police Department (MPD), and U.S. Secret Service. In addition, WFO also embedded FBI intelligence personnel in MPD's Joint Operations Command Center (JOCC) on January 6th. WFO's command post and its presence in MPD's JOCC provided FBI situational awareness of our partners' operations related to the demonstrations, and prepared WFO to react quickly to any federal criminal activity.

The Norfolk FBI office issued a Situational Information Report (SIR) which contained the following message from extremist groups it had been monitoring:

"Be ready to fight, Congress needs to hear glass breaking, doors being kicked in, and blood from their BLM, Black Lives Matter, and ANTIFA slave soldiers being spilled. Get violent, stop calling this a march, or rally, or protest. Get ready for war."

11. Would you agree that these words clearly indicate racial bias and an attempt to use race and racism as a potential motive for violence?

Response: As part of all of its investigations, the FBI attempts to determine what mobilized a person to violence, but those motivators are highly personalized, varied, and complex, and build upon one another over time. Thus, it is often impossible to identify a single event or element as the one thing that motivated someone to act.

To date, the Department of Justice has charged nearly 840 defendants related to the events of January 6, 2021. Many of these cases remain ongoing, and additional investigations are also underway. Accordingly, it would be inappropriate to comment further at this time.

12. Was the FBI aware of online threats to the Vice President, Speaker of the House, and specific members of Congress connected with January 6th?

    Response: After the election, and in advance of January 6, the FBI performed standard preliminary open source analysis to identify any threats of violence or criminal activity related to potential protest activities in the National Capital Region (NCR). The FBI actively monitored threats related to January 6th and shared threat information with federal, state, and local partners. For example, in the weeks leading up to January 6, the FBI Counterterrorism Division engaged with all 56 Field Offices to collect information on threats to the NCR connected to January 6. The FBI also coordinated with federal, state, local, and private sector partners to determine whether any of those entities possessed information regarding potential threats. The FBI assessed there would be significant demonstrations at several key sites throughout the NCR, including the U.S. Capitol Complex. Additionally, there were online posts that mentioned possible violence; however, these posts were of limited specificity and unknown credibility.

    As detailed above, the FBI prioritized the collection, sharing, and dissemination of intelligence with federal, state, and local law enforcement partners through various channels in advance of January 6, 2021. This included the activation of two command posts to facilitate information sharing with our partners. Both command posts were connected virtually for briefings and other information sharing. On the morning of January 6th, the command posts instituted a regular briefing cycle for sharing threat intelligence and other pertinent information, with immediate threats being shared as they were received (outside of the existing, bi-hourly cadence).

13. On the day of, but in advance of the January 6 insurrection at the U.S. Capitol, did FBI Headquarters contact the Vice President? The Speaker of the House? Any member of Congress on the day of January 6th? Please copies documenting any such communications.

    Response: The FBI engaged in information sharing with federal, state, and local partners in the weeks leading up to January 6th through numerous partner calls, and culminating in the command posts that allowed for real-time sharing of information. As detailed above, the FBI had activated two command posts on January 6, 2021 for the express purpose of sharing information, and continuous communication, with our partner agencies, including U.S. Capitol Police. Throughout the course of the day, the FBI was in constant communication with federal, state, and local partners, including through the command posts. Prior to the breach of the U.S. Capitol, FBI and ATF bomb technicians and

explosives specialists responded to assist USCP with securing locations near the Capitol Complex where potential explosive devices had been discovered.

As a general matter, the FBI receives tips and intelligence from various sources and must assess the credibility and viability of the information it receives under the laws and policies that govern FBI investigations. Information of lead value is provided to the appropriate FBI field office and/or law enforcement agency for action.

Let us explore the connection of race and Donald Trump, who was President of the United States during the events in question, the president, former president of the United States. On December 19th, he tweeted: "Big protest in D.C on January 6th, be there, will be wild." At 12:15 p.m. on January 6th he said to the assembled multitude on the Ellipse: "You will never take back our country with weakness." Less than an hour later, at 1:10 p.m., he admonished the crowd: "We fight like hell, and if you don't fight like hell you will not have a country anymore." At 2:11 p.m. the Trump-incited mob breached police lines on the west side of the capitol.

14. Is it the position of the FBI that in the totality of the circumstances the words of Donald Trump cited above indicate that the former President knowingly motivated the domestic terrorist attack on January 6th. Have any of these words been reviewed to determine whether Donald Trump should be referred to the Department of Justice for investigation, arrest, and prosecution in connection with January 6, 2021 attack on the U.S. Capitol. Please provide documents supporting your response.

    Response: As discussed above, as part of all of its investigations, the FBI attempts to determine what mobilized a person to violence, but those motivators are highly personalized, varied, and complex, and build upon one another over time. Thus, it is often impossible to identify a single event or element as the one thing that motivated someone to act.

    In order to protect the integrity of all investigations, as a general practice, the FBI does not comment on the status or existence of any potential investigative matter. To date, the Department of Justice has charged nearly 840 defendants related to the events of January 6, 2021. Many of these cases remain ongoing, and additional investigations are also underway. Accordingly, it would be inappropriate to comment further at this time.

There are only 4.7% of African American in the FBI. Much has come to my attention of the lack of promotion, opportunities for leadership in the FBI, and the diversity office that you have does not report directly to the FBI director.

15. Please provide in writing a status update on the FBI's actions to ensure diversity and equality of opportunity within the Bureau, especially for racial and ethnic minorities, particularly African Americans?

***Response**:* The FBI values and leverages human differences, opinions, and perspectives to empower our FBI community to reach its greatest potential. The FBI's commitment to fostering diversity and inclusion is integrated into every facet of employment, including leadership and career development, recruitment, staffing, workforce planning and sustainability. The FBI has adopted aggressive recruiting goals to help us meet these objectives: to attain a 45% minority applicant rate. The FBI is making steady progress towards meeting—and exceeding—these goals. As of September 2021, 46.8 % of the FBI's special agent applicants and 26.7% of the FBI's workforce are minorities (10.66% Black/African American). Additionally, 32.2% of professional staff, 22.8% of intelligence analyst employees, and 19.4% of special agent employees are minorities. This includes 15.1% of the FBI's SES leaders.

The FBI has also recently partnered with Historically Black Colleges and Universities (HBCUs) through our "Beacon Project." The Beacon Project is an outreach collaboration with HBCUs to create pathways for their students to career opportunities with the FBI. In addition, FBI's Office of Diversity and Inclusion regularly hosts Diversity Agent Recruitment (DAR) events, which focus on increasing the number of minority and female applicants to the Special Agent position.
In FY21-to-date, the FBI has hosted six (6) DARs with 390 attendees, resulting in an additional 144 diverse applications to the Special Agent position. Special Agent basic training classes are becoming more diverse. The percentage of African American Special Agents is 4.8% and continues to trend upward.

In April 2021, the FBI appointed a Chief Diversity Officer (CDO) to ensure diversity and equality of opportunity occurs. The CDO position reports directly to the Associate Deputy Director. The CDO oversees the Office of Diversity and Inclusion, which has been elevated and expanded so it can meet its mission. The Office of Diversity and Inclusion established and now facilitates a Cross-Cultural Mentoring and Sponsorship (CCMS) program. CCMS pairs mentees and mentors of different races/genders. The CCMS program currently has 600 mentor-mentee matches, allowing for the development of networks across race and gender lines while connecting employees at different career stages for guidance, perspectives, support, and advice. Mentees are exposed to professional development and career advancement opportunities.

The FBI also has nine Diversity Advisory Committees (DACs). The DACs advocate for underrepresented groups within the workforce. The DACs also receive guidance and support from SES-level Diversity Executive Champions. The efforts of these groups have culminated in policy changes, innovative projects, and a deeper sense of community for minorities, women, and others within the FBI. For example, efforts led by our Black Affairs Diversity Committee resulted in permanent changes to the FBI Experience Museum to highlight diversity milestones in the FBI's history (including the hiring of the first African American Special Agent).

Questions for the Record
Submitted by Rep. Cliff Bentz

16. The Western United States is suffering from the impact of the greatest drought in modern history. Some 70 million people are affected, and almost the entire west half of the U.S. is at risk. One of the unfortunate impacts of the drought is to turn our beautiful usually green millions upon millions of acres of forest into tinder dry opportunities for massive and cataclysmic infernos capable of causing billions in damage, loss of thousands of homes, and destruction of human and animal life. Many communities are just a single match strike away from disaster. What is the FBI doing to anticipate the possibility of terrorists using our forests against us as a weapon of mass destruction?

    Response: The FBI is currently unaware of credible reporting indicating a threat targeting U.S. forests by foreign terrorist organizations, or homegrown or domestic violent extremists.
    The Weapons of Mass Destruction Directorate (WMDD) leads the FBI's effort to prevent and mitigate threats associated with the nefarious use of chemical, biological, radiological, nuclear, and explosive materials. The WMDD consistently engages with both internal, and external partners, including the Intelligence Community (IC) partners and local law enforcement authorities, to regularly share actionable intelligence on WMD-related activity.

17. In your opening remarks you mentioned the "attacks on minorities, Asians, Pacific Islanders, and Jewish people". These attacks appear to be prompted by the worst kind of racial bias. I also note that recently Attorney General Garland, in speaking about White Supremacy, described supremacists as "specifically those who advocate for the superiority of the white race." In this time of past due sensitivity toward challenges facing minorities in the United States, why is the FBI failing to bring its own demographics into some meaningful comparison to the percentages of minorities and women in our country? (To the point I note that only 4% of the Agency is black, and that the Agencies' "special agents" as of February of last year were 79.1% male. This is a problem of long duration apparently the result of means the Agency uses to select and then advance agents in the system.)

    Response: The FBI values and leverages human differences, opinions, and perspectives to empower our FBI community to reach its greatest potential. The FBI's commitment to fostering diversity and inclusion is integrated into every facet of employment, including leadership and career development, recruitment, staffing, workforce planning and sustainability. The FBI has adopted aggressive recruiting goals to help us meet these objectives: to attain a 45% minority applicant rate. The FBI is making steady progress towards meeting—and exceeding—these goals. As of September 2021, 46.8 % of the FBI's special agent applicants and 26.7% of the FBI's workforce are minorities (10.66% Black/African American). Additionally, 32.2% of professional staff, 22.8% of

intelligence analyst employees, and 19.4% of special agent employees are minorities. This includes 15.1% of the FBI's SES leaders.

18. I quote: "China's theft of technology is the biggest law enforcement threat to the United States". This is from a presentation you gave on February 6th, 2020. What is the Agency doing in this area and does it have the funding to adequately address this challenge?

Response: Investigating and preventing economic espionage and illegal technology transfer to the Government of China is a top priority for the FBI.

The FBI continues to work extensively with the interagency and National Security Council (NSC) on new policies to address the threat of China's economic espionage and technology transfer while allowing for the continued advancement of the U.S. scientific enterprise and international scientific collaboration.

For example, the FBI worked closely with the State Department and the NSC to create a new policy to address a large set of non-traditional collectors (NTCs) from China's People's Liberation Army (PLA) Military-Civil Fusion (MCF)-affiliated Universities.

On May 29, 2020, the President of the United States issued Proclamation 10043 (PP10043) suspending the issuance of visas to researchers from PLA MCF Universities in certain technology fields. This policy is the result of two years of interagency effort led by the FBI and, based on 2019 statistics, will prevent several thousand students a year, whose research was likely to benefit the PLA, from coming to U.S. universities.

Similarly, the FBI worked closely with the White House Office of Science and Technology Policy, federal grant funding agencies, and other agencies on National Security Presidential Memorandum 33 (NSPM-33), which strengthens protections on U.S. Government-funded research and development against foreign interference and exploitation.

<u>Talent Plans:</u>

Since 2015, the FBI has led a national initiative designed to mitigate and neutralize the technology transfer threat posed by the PRC's Talent Plans, a diverse group of recruitment programs controlled by the Chinese government to enhance their economic and military capabilities. Talent Plans represent one aspect of the PRC's multi-faceted, whole-of-government approach to technology transfer, along with other types of non-traditional collectors, cyber theft, collection by intelligence services, and other types of business and academic relationships that provide access to critical information, technology, or expertise.

The PRC has used Talent Plans to incentivize illegal activity from participants, including grant fraud, intellectual property theft, and export control violations. China's Talent Plans have for years exploited federal research grant funding provided by agencies like the National Institutes of Health, National Science Foundation, Department of Energy, and Department of Defense.

For example, the FBI's Operation Prime Weight was an effort to counter a sophisticated Chinese government scheme led by a Chinese military-affiliated university and Texas A&M professor, Shan Shi, who sought to steal critical U.S. syntactic foam technology. Shi was involved in a Chinese talent plan, where he pledged to "absorb" and "digest" the relevant technology from the United States. Syntactic foam is an export-controlled product used in submarines, naval ships, and oil platforms. Operation Prime Weight was the first economic espionage prosecution in the District of Columbia, yielding four guilty pleas and one trial conviction.

However, not all Talent Plan members are ethnic Chinese. In December, Charles Lieber, a Harvard University chemistry professor, who was a member of a Chinese talent plan was convicted of false statements and wire fraud. Lieber was allegedly accepting approximately $50,000 per month from the Chinese government without disclosing it to Harvard or NIH, from which he received millions of dollars in grant money from the American taxpayer.

NCITF:

In an effort to increase Counterintelligence engagement and partnership within the U.S. Government, the FBI created the National Counterintelligence Task Force (the NCITF), with Counterintelligence task forces in each of the 56 field offices.

The NCITF provides common goals and strategy, threat prioritization, training, analytic support, technical expertise, coordination, standardization, and information sharing and has created a whole-of-government approach to Counterintelligence Threats.

Outreach:

The FBI's Office of Private Sector continues to hold events for university presidents, including an annual academic summit, to provide clear guidance to universities on the threat posed by talent recruitment programs and the security obligations universities have.

Since June 2018, the Counterintelligence Division has been partnering with the three largest university associations: the American Council on Education, the Association of American Universities, and the Association of Public and Land-grant Universities. We have been doing this through a series of meetings and events.

FBI Field offices also engage on an almost daily basis with local academia, research institutions, and the private sector through personal outreach, executive-level engagement, and social media.

19. Cyber security and Artificial Intelligence are two of the greatest threats to America. Does your Agency have the technical expertise and staff needed to keep up with China, Russia and other countries engaged in these spaces?

    Response: The FBI is committed to leveraging artificial intelligence (AI) and other developing analytical techniques in ways that are equitable, legal, ethical, and well-managed. Thus, the FBI is developing appropriate governance for AI systems to meet these requirements, as well as pursuing an increase in technical capabilities and staff

expertise. This work is foundational to ensuring the FBI has the technical capabilities and staff to counter cyber and AI threats to the United States.

Adversaries are already implementing AI driven capabilities which will have a direct impact on FBI operational activities. The FBI must increase its expertise in understanding the weaknesses of AI capabilities to know how to exploit adversarial systems as well as counter those used against systems and assets. The FBI must also be able to defend its own use of AI technologies, consistent with democratic values, and conform to U.S. Government and industry recognized standards.

Mitigating AI and cyber threats relies on strong technical programs and experts in data science and computer science as well as foundational investments in the technical infrastructure used for innovation. AI is a fast-moving field and FBI is working towards increased ability to quickly design, develop, acquire, test, and use AI and related data science-based products. The required infrastructure includes tools similar to those used for developing innovative non-AI software along with specialized hardware and software components. Emerging technologies such as AI are still largely categorized under research and development spending, which is typically not well funded and can take time to be moved to programs of record which would offer additional resource opportunities. Thus, the current investment paradigm can be slow to match that of our adversaries.

Strategic partnerships with non-government companies and leveraging contract workforces can offer advantages. Nonetheless, the government staffing side requires upskilling and targeted recruitment in order to assess risks and opportunities of emerging technology developments such as AI, particularly in the areas of assessing the technical capabilities against policy and regulatory requirements, safeguards, and planning agency-specific adoption or mitigation. To that end, the FBI has established a Senior Level position as a subject matter expert in AI, with candidates for the position currently being assessed. This position will lead the FBI's AI efforts, enhanced by focused efforts to hire Data and Computer Scientists.

Finally, to ensure a coordinated government response and to facilitate collaboration in both the cyber and AI areas, the FBI and other National Security and Law Enforcement agencies must continue to expand participation in the domestic and international Standards Development Organizations to ensure awareness of adversary goals and objectives, and advocate for standards that protect current and enable future U.S. Government missions and interests.

Questions for the Record
Submitted by Rep. Scott Fitzgerald

20. According to the Department of Homeland Security, upwards of 80-90% of counterfeit goods globally originate in China, costing U.S. manufacturers and other businesses billions of dollars annually. Similarly, China is responsible for an enormous share of global piracy of American movies, music, sports broadcasts, and other content protected by intellectual property. There are criminal statutes in place to prosecute those responsible, and the Justice Department and FBI have an important role together with DHS to fight these criminals. As the head of the country's top law enforcement agency, what steps are you and the Biden Administration taking to prevent IP theft?

    Response: Investigating and preventing economic espionage and illegal technology transfer to the Government of China is a top priority for the FBI.

    The PRC government threatens our security through its concerted use of espionage, theft of trade secrets, malicious cyber activity, transnational repression, and other tactics to advance its interests — all to the detriment of the United States and other democratic nations and their citizens around the world.

    To that end, the Justice Department recently announced that, moving forward, we will be guided by the Department's Strategy for Countering Nation-State Threats and informed by three strategic imperatives. First, we must continue to defend core national security interests and protect our most sensitive information and resources. We will continue to aggressively investigate and prosecute espionage, export control and sanctions violations, and interference with our critical infrastructure.

    Second, we must protect our economic security and prosperity, including key technologies, private information about Americans, and supply chains and industry. We will bring all tools to bear, including the regulatory authorities of the Committee on Foreign Investment in the United States and Team Telecom — as well as criminal process where appropriate — to prevent and mitigate harms from economic espionage, hostile manipulation, and cyber-enabled malicious activity.

    Third, we must defend our democratic institutions and values to ensure that the promise of freedom remains a reality in the face of rising authoritarianism. We remain steadfast in our commitment to preventing malign influence inside our borders and to promoting freedom of expression and democracy against corrupt and repressive forces.

21. You and the FBI hold an important role in the Biden Administration in protecting American citizens and businesses from Chinese IP theft. But the Administration recently announced plans to support foreign adversaries, including China, in taking U.S. intellectual property relating to COVID-19 vaccines, including state-of-the-art new

mRNA drug development platforms. Have you or anyone else in the Administration, to your knowledge, advised the President that supporting foreign countries' waivers of this U.S. intellectual property essentially endorses IP theft?

Response: The FBI has been working to prevent the theft of intellectual property related to the COVID-19 vaccine. The FBI relies heavily on outreach efforts and private sector partnerships to achieve this. The FBI frequently pushes material to the public through the Internet Crime Complaint Center, ic3.gov, a tool to inform the public and where the public can report potential fraud like insurance and vaccine scams. Recently, the FBI released the 2020 Internet Crime Report, which includes information from nearly 800,000 complaints of suspected internet crime. The IC3 received over 28,500 complaints related to COVID-19, with fraudsters targeting both businesses and individuals.

In July 2020, the Department of Justice indicted two Chinese nationals, Li Xiaoyu and Dong Jiazhi, for stealing trade secrets and hacking into computer systems of firms working on the COVID-19 vaccine. The individuals allegedly conducted a global hacking campaign for more than a decade.

22. The crisis at the Southern border was caused by the radical immigration policies of the Biden Administration and raises serious national security risks. The FBI utilizes several programs that target fentanyl crimes, including the Prescription Drug Initiative, Safe Street Task Forces, J-CODE, and the Transnational Organized Crime Programs. I introduced the Stopping Overdoses of Fentanyl Analogues Act to keep fentanyl designated as a schedule I drug. Can you comment on the affect that designation, which was put in place in February 2018, has had on the flow of fentanyl and its derivatives into the United States?

Response*:* The FBI respectfully defers to U.S. Customs and Border Protection and the Drug Enforcement Administration for questions related to drug scheduling and data related to drug importation across the U.S. border.