Senate Committee on the Judiciary Hearing
"Oversight of the Federal Bureau of Investigation: The January 6 Insurrection, Domestic Terrorism, and Other Threats"
Questions for the Record
March 2, 2021

QUESTIONS FROM CHAIRMAN DURBIN

1. In your written statement, you stated that FBI investigators "have identified hundreds of individuals involved in the siege of the Capitol Complex and already charged well over 300 of them." At a separate hearing, Assistant Director Sanborn testified that she could "only recall from [her] memory one of the individuals that was under investigation prior" to January 6.

    a. How many charged individuals were under investigation before the attack? Of the individuals subject to prior investigation, how many were the subject of a full investigation, how many were the subject of a preliminary investigation, and how many were subject to an assessment?

    b. How many of the individuals charged in connection with the January 6 attack on the Capitol were listed on the Terrorist Screening Data Base (TSDB) prior to January 6?

Response: As of April 2022, of the approximately 775 subjects charged to date related to the attack on the U.S. Capitol Complex on January 6, 2021, the Federal Bureau of Investigation (FBI) has identified two individuals who were predicated subjects prior to January 6th. It is important to note there are still several individuals who entered the Capitol that have yet to be identified. It is FBI policy to nominate all subjects of domestic and international terrorism investigations to the Terrorist Screening Database for watchlisting. The Terrorist Screening Center determines who is added to the watchlist.

2. In your written statement, you affirmed that the "top threat from DVEs continues to be those" you call "Racially or Ethnically Motivated Violent Extremists" (RMVEs)—"specifically[,] those who advocate for the superiority of the white race." You further testified that, with respect to the January 6 attack on the Capitol, the FBI is "seeing quite a number" of militia violent extremists as well as "a couple of instances" of RMVEs "who advocate for what you would call white supremacy."

    a. What is the difference between a white supremacist and an individual "who advocate[s] for the superiority of the white race"? If there is no difference, why does the FBI avoid using the terms "white supremacist" and "white supremacy"?

Response: The FBI uses the term "Racially or Ethnically Motivated Violent Extremism," (RMVE) because it focuses on the violence, not First Amendment-protected ideology or belief, as a way to label this threat. The FBI uses the description "RMVEs who advocate for the superiority of the white race" because it encompasses many sub-ideologies that draw from religious, cultural, and political themes. For example, the description RMVE captures the sub-

ideologies of neo-Nazi, white nationalist, racist Odinist, racist skinhead, Klan, Christian Identity extremists, and other expressions of white superiority.

b. What, if any, threat does the FBI assess is posed by RMVEs other than those who advocate for the superiority of the white race? What is the extent of this threat, particularly in comparison to "those who advocate for the superiority of the white race"? Please be specific.

Response: The large majority of the FBI's RMVE investigations involve RMVEs who advocate for the superiority of the white race; but the FBI has also seen some RMVE threat actors use political reasons – including racism or injustice in American society, the desire for a separate Black homeland or starting a "race war," or draw on aspects of religion, including elements of Christianity, Islam, and Judaism – as justification for their use or threat of force or violence. Between 2015 and 2020, at least 19 attacks and 72 deaths were the result of RMVEs. Of those, 11 attacks and 52 deaths were the result of attacks perpetrated by RMVEs who advocate for the superiority of the white race; and 8 attacks and 20 deaths were the result of attacks perpetrated by RMVEs motivated by racism and injustice in American society, the desire for a separate Black homeland, or religion-themed reasons.

3. You testified at the hearing that there were roughly three groups of people involved in the January 6 attack on the Capitol: "rowdy protesters" who didn't violate the law; individuals who had intended to participate in a peaceful protest, but who were "swept up" in the riot and engaged in "low-level criminal behavior"; and a group consisting of those who "attempted to disrupt the members of Congress and the conduct of their constitutional responsibilities," a subset of which "came to Washington . . . with plans and intentions to engage in in the worst kind of violence."

    a. Of the individuals facing charges in connection with the January 6 attack on the Capitol, how many fall into the subset of defendants who allegedly "came to Washington . . . with plans and intentions to engage in the worst kind of violence"?

    b. Of this subset of defendants, how many of them allegedly are members of or affiliated with the Oath Keepers, the Three Percenters, the Proud Boys, or similar groups, and how many are not? Were there any other white supremacist or violent right-wing militia extremist groups whose members or affiliates were charged in connection with the attack?

Response: According to publicly available court documents, the Department of Justice has charged a number of defendants involved in the attack on the U.S. Capitol with conspiracy, either to obstruct a Congressional proceeding, to obstruct law enforcement during a civil disorder, and/or to injure an officer. These investigations are on-going, but the FBI has seen indications of some small cells of individuals alleged to have been conspiring and communicating with each other prior to their involvement in the attack. For example:

- In February 2021, six individuals associated with the Proud Boys were indicted with conspiring to obstruct or impede an official proceeding and to impede or interfere

with law enforcement during the commission of a civil disorder, among other charges. The indictment alleges that the defendants planned with each other, and with others known and unknown, to enter the Capitol forcibly on January 6, and to stop, delay, and hinder the Congressional proceeding occurring that day. The defendants brought and wore paramilitary gear and supplies – including camouflaged combat uniforms, tactical vests with plates, helmets, eye protection, and radio equipment – and affixed orange tape to their clothing and tactical gear to identify each other.

- In February 2021, six individuals associated with the Oath Keepers, some of whose members were among those who forcibly entered the U.S. Capitol on January 6, were arrested for conspiring to obstruct Congress' certification of the result of the 2020 U.S. Presidential Election, among other charges. According to the indictment, one individual allegedly arranged, for himself and others, training by a Florida company that provides firearms and combat training. The indictment also alleges that in the lead-up to the attack on the U.S. Capitol, one individual allegedly communicated extensively with another about potentially joining her militia and combining forces for the events of January 6.

- In April 2021, two individuals associated with the Oath Keepers were indicted in federal court in the District of Columbia for conspiring to obstruct Congress, among other charges. According to the charging documents, they communicated with co-conspirators in advance of the January 6 incursion on the U.S. Capitol. The indictment alleges frequent and consistent communication leading up to the attack, such as in reserving hotel rooms and making phone calls to co-conspirators the morning of the breach.

Additional information related to the defendants charged in federal court in the District of Columbia related to crimes committed at the U.S. Capitol on January 6, 2021, as well as links to the court documents referenced above and, *inter alia*, related superseding indictments, are available at: www.justice.gov/usao-dc/capitol-breach-cases. 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. Given that this question relates to hundreds of ongoing investigations and pending prosecutions, it would be inappropriate to provide further information at this time.

4. With respect to the causes of domestic terrorism, you stated at the hearing that you are concerned about "any source that stimulates or motivates violent extremism." Both before and after the 2020 election, including at the hearing, you have repeatedly confirmed that the FBI has not seen any evidence of a national voter fraud effort.

    a. How do continued false claims of a stolen election impact the FBI's efforts to combat domestic terrorism?

b. Does disinformation or misinformation, including with respect to voter fraud, gain more credibility with individuals susceptible to radicalization to violence when it is amplified by prominent individuals, such as current or former elected officials?

c. Do false claims of a stolen election elevate the risk of a domestic terrorist threat when they are amplified by current or former elected officials? Is this a "source that stimulates or motivates violent extremism"?

Response: Although the FBI is not in a position to comment on any specific individual's speech or rhetoric, amplified perceptions of fraud surrounding the outcome of the 2020 General Election, when combined with long-standing Domestic Violent Extremist (DVE) drivers such as perceived government or law enforcement overreach, could lead some individuals to adopt the belief that there is no political solution to address their grievances and violent action is necessary. However, radicalization of DVEs most often occurs through self-radicalization to violence online, which presents mitigation difficulties. Social media has increased the speed and accessibility of violent extremist content, while also facilitating greater decentralized connectivity among violent extremist supporters. Trends continue to evolve, but long-standing DVE drivers, including racism, anti-Semitism, perceived government or law enforcement over-reach, socio-political conditions, legislation, and other world events, combined with personal grievances, remain constant. The FBI assesses some DVEs will continue to personalize their own ideology in an attempt to justify their violent acts.

d. Without confirming or denying the existence of any specific investigation, is the FBI investigating whether the mob that attacked the Capitol on January 6 was incited or encouraged to attack Congress? If not, why not?

Response: As part of all 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. Although groups may share a common purpose or objective, it is not always the case that a single event or element motivated someone to act on that purpose.

5. You've stated many times to Congress and the public that the FBI is concerned with violence, not ideology. You also stated at the hearing that "more and more, the ideologies . . . that are motivating these violent extremists are less and less coherent, less and less linear, and less easy to kind of pin down." Yet the FBI continues to categorize domestic terrorists as either "Racially or Ethnically Motivated Violent Extremism," "Anti-Government or Anti-Authority Violent Extremism," "Animal Rights/Environmental Violent Extremism," "Abortion-Related Violent Extremism," and "Other Domestic Terrorism Threats." The point of differentiation for each category appears to be the extremists' motivations for violence—i.e., their ideologies.

   a. If the FBI is concerned only with violence regardless of ideology, and if violent extremists' ideologies are getting less coherent, less linear, and harder to pin down, why does it categorize domestic terrorists according to their ideologies?

i. Do disparate groups within each of the categories used by the FBI have common (or, at least, more common) practices, methods, tactics, techniques, and procedures as between them? For example, does an Anti-Government or Anti-Authority Violent Extremist who supports male chauvinist causes (e.g., a Proud Boy) have more in common in terms of behavior, associations, and lethality with another Anti-Authority Violent Extremist who supports Antifa than they would with a Racially or Ethnically Motivated Violent Extremist who advocates for the superiority of the white race?

ii. What is the analytic value in having a category for "Other Domestic Terrorism Threats"? What can be generalized about a class of violent extremists that are defined solely by the fact that they don't fit into other categories?

Response: Classifications, or categories, help the FBI better understand the criminal actors it pursues, but actors' motivations vary, are nuanced, and sometimes are derived from a blend of socio-political goals or personal grievances.

Across all threat categories, the greatest domestic terrorism threat to the Homeland is posed by lone offenders, often radicalized to violence online, who look to attack soft targets with easily accessible weapons. Although there are key differences between the threat categories, there is some overlap in terms of targets and tactics. For example, although the underlying motivations differ, law enforcement personnel and facilities are a common target of Militia Violent Extremists (MVEs), Sovereign Citizen Violent Extremists (SCVEs), and Anarchist Violent Extremists (AVEs), all of which are categorized as Anti-Government or Anti-Authority Violent Extremists (AGAAVEs). Similarly, RMVEs and MVEs have both targeted ethnic and religious minorities based on different motivations. Arson and vandalism are shared tactics among AVEs, Abortion-Related Violent Extremists, and Animal Rights/Environmental Violent Extremists; whereas firearms and edged weapons have typically been used by RMVEs, MVEs, and Involuntary Celibate Violent Extremists, which is part of the "All Other DT Threats" category.

The "All Other DT Threats" category encompasses threats involving the potentially unlawful use or threat of force or violence in furtherance of ideological agendas that are not otherwise defined under or primarily motivated by one of the other DT threat categories. Such agendas could flow from, but are not limited to, a combination of personal grievances and beliefs, including those described in the other DT threat categories. Some actors in this category may also carry bias related to religion, gender, or sexual orientation.

b. Why did the FBI abandon the separate category used to track white supremacist incidents in favor of its current taxonomy if not to obscure the fact that the vast majority of domestic terrorist attacks—and the most lethal attacks—are being conducted by violent right-wing extremists?

i. Why has the FBI broken up right-wing violent extremist movements, many of whose members appeared to have acted in concert on January 6, across three separate categories?

ii. Doesn't this make it harder to understand the connections between these groups and movements, many of which share common values (e.g., racism, misogyny, homophobia, transphobia, anti-Semitism, Islamophobia, and xenophobia) and, at times, memberships?

Response: The FBI uses the term "Racially or Ethnically Motivated Violent Extremism," (RMVE) because it focuses on the violence and motivation, not First Amendment-protected activity, no matter how abhorrent. Integrating all types of racially or ethnically motivated violence into one threat category allows FBI Field Offices the latitude to collect intelligence and allocate resources to combat all RMVE threats, regardless of ideological motivation. More importantly, the FBI's internal threat-naming conventions do not dictate what domestic terrorism agents investigate; instead, the intelligence and violent criminal conduct dictate what is investigated.

The FBI does not view or describe violence as left- or right-wing. The FBI protects First Amendment rights, including the freedoms of association and assembly, and the right to coalesce with like-minded individuals. The FBI does not investigate or collect based on sheer ideology or assembly. As with all the threats, the FBI continually assesses and evaluates trends in the motivations and targets of like-minded threat actors. The FBI's priority is to stay agile in its efforts to confront domestic violent extremism and prevent the next attack.

6. In a recently-published report, the George Washington University (GWU) Project on Extremism concluded that "[t]he events at the Capitol on January 6th also evidence the reach of the QAnon conspiracy theory," noting that it had "identified over a dozen individuals at the Capitol with an overt QAnon affiliation." GWU PROJECT ON EXTREMISM, *"This Is Our House!": A Preliminary Assessment of the Capitol Hill Siege Participants* at 38 (March 2021), *available at* https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/This-Is-Our-House.pdf. When asked about the threat posed by the QAnon conspiracy theory at the hearing, you responded that you were "concerned" about it.

    a. Do you agree with the GWU Project on Extremism that QAnon adherents appear to have played a significant role in the January 6 attack on the Capitol?

    b. What are the domestic terrorism threats posed by QAnon?

    c. Are those threats exacerbated when prominent current or former elected officials endorse or amplify the QAnon theory, thereby lending it more credibility?

Response: It is important to note, though some individuals who commit violence may reference QAnon, the FBI does not investigate, collect, or maintain information based solely on First Amendment-protected activities. The FBI understands "QAnon" as a reference to a complex and constantly evolving conspiracy theory that is promoted by a decentralized online community that has morphed into a real-world movement. Of the hundreds of individuals the FBI has arrested for their participation in the Capitol attack on January 6, 2021, several were self-identified QAnon adherents. The participation of some DVEs who are self-identified QAnon adherents in

the Capitol attack underscores how the current environment likely will continue to act as a catalyst for some to begin accepting the legitimacy of violent action.

The FBI assesses some DVE adherents of QAnon likely will begin to believe they can no longer "trust the plan" referenced in QAnon posts and that they have an obligation to change from serving as "digital soldiers" towards engaging in real world violence – including harming perceived members of the "cabal" such as Democrats and other political opposition – instead of continually awaiting Q's promised actions, which have not occurred. Other QAnon adherents likely will disengage from the movement or reduce their involvement since the Administration changed. This disengagement may be spurred by the large mainstream social media de-platforming of QAnon content based on social media companies' own determinations that users have violated terms of service, and the failure of long-promised QAnon-linked events to materialize. Some DVEs have discussed how to radicalize new users to violence through niche social media platforms following QAnon adherents' migration to these platforms after large scale removals of QAnon content from other platforms. Adherence to QAnon by some DVEs likely will be affected by factors such as the severity of the COVID-19 pandemic, the level of societal polarization in the United States, social media companies' willingness to host QAnon-related content on their sites, and the frequency and content of pro-QAnon statements by public individuals who feature prominently in core QAnon narratives.

7. The FBI's annual hate crimes incident reports suggest a significant increase in the numbers of hate crimes across the country over the past five years, including an approximately twenty-five percent increase between 2015 and 2019. You acknowledged at the hearing that hate crimes are historically underreported. Even where victims report these incidents, they are often not reflected in the FBI's statistics. For example, the Arab American Institute (AAI) has found that there are often significant discrepancies between state-level statistics on hate crimes and the federal data. ARAB AMERICAN INSTITUTE FOUNDATION, *Underreported, Under Threat: Hate Crime Data in the United States and the Targeting of Arab-Americans* (July 2018).

    a. Why do we continue to see discrepancies between hate crimes as reported by the states in their own statistics and as reflected in the federal data?

Response: Each year, the FBI Uniform Crime Reporting (UCR) Program sets a submission deadline to the states for providing data. The hate crime totals reported annually by the FBI UCR Program and the state UCR programs differ because the submission deadlines between the FBI and the states do not always correlate. The annual *Hate Crime Statistics* publication is a snapshot in time. The numbers depicted in the annual publication are those reported voluntarily to the FBI UCR Program, by state law enforcement agencies, to meet the publication deadline.

    b. What is the FBI doing to address the significant reporting concerns surrounding federal hate crimes data?

Response: The FBI Uniform Crime Reporting (UCR) Program has been a member of the Department of Justice's Hate Crime Prevention and Enforcement Initiative, since 2017. On October 29, 2018, this initiative hosted a Law Enforcement Roundtable meeting with various law

enforcement practitioners and officers from around the country. The breakout sessions held during the roundtable provided insight into the reporting issues experienced at the agency levels across the country. In collaboration with the members, the FBI UCR Program staff identified the following obstacles to law enforcement's hate crime submissions to the FBI UCR Program:

- variations in federal, state, and local laws or definitions of hate crimes that make it difficult to know whether and when to classify incidents as hate crimes for FBI UCR purposes;
- miscoding of offenses and the need to update records as more evidence is gathered;
- gaps in training and investigation;
- obtaining leadership support at local levels regarding prioritization of treatment of hate crime reporting;
- cost of improving record management systems to make reporting easier; and
- lack of resources.

To address the reporting concerns surrounding the FBI UCR Program's Hate Crime Statistics Collection, FBI employees offer a training program for the law enforcement community via webinars. During these training sessions, the FBI provides an overview of the hate crime statistics collection and hate crime scenarios, the two-tiered decision-making process, bias motivation indicators, and the importance and benefits of reporting hate crime incident data (*i.e.*, increases understanding, supports long-range planning, promotes transparency, improves information sharing, and addresses threats). These instructional opportunities allow FBI personnel to meet with the law enforcement community from reporting agencies to address questions concerning records management. The training emphasizes the need and benefits of the Hate Crime Statistics Collection, as well as identifies gaps in training and determining bias indicators. This training encourages participants to discuss this important topic with law enforcement leadership and colleagues within their local agencies and communities. The free webinars allow the FBI UCR Program to continue outreach strategies and trainings with state UCR program agencies and the local agencies facing traveling constraints due to budgetary issues and the Coronavirus Pandemic.

The FBI UCR Program transitioned all federal, state, local, college/university, and tribal law enforcement agencies nationwide to the National Incident-Based Reporting System (NIBRS) on January 1, 2021. This transition will ease the ability for agencies to submit hate crime data as NIBRS includes a designated field for law enforcement agencies to report hate crimes. Therefore, reporting via NIBRS will improve the quality, reliability, and accuracy of hate crime data.

To support federal and tribal reporting, the FBI deployed the NIBRS Collection Application (NCA). The FBI developed the NCA, which is available on the Law Enforcement Enterprise Portal, to provide a no-cost solution for federal and tribal agency users to submit

NIBRS data to the FBI UCR Program and to comply with the Uniform Federal Crime Reporting Act of 1988. As the NCA's functionality became more robust, the NCA became a viable option for non-transitioned state and local agencies to submit NIBRS data. The NCA is an extension of the UCR system and enables users to directly enter and submit NIBRS crime data to the UCR Program for processing, retention, and publication.

The *Hate Crime Guidelines and Training Manual* was developed to assist law enforcement agencies in establishing a hate crime training program to allow personnel to collect and submit hate crime data to the FBI UCR Program. The manual provides suggested model reporting procedures and training aids for capturing the bias-motivated incident data reported to the FBI. The FBI UCR Program is currently revising this document to remove all Summary Reporting System (SRS) verbiage and adding all federal and tribal law enforcement offenses. The SRS collected hate crime data on 13 offenses versus the 70 offenses collected in the NIBRS. The manual is located on the FBI.gov website at: https://www.fbi.gov/file-repository/ucr/ucr-hate-crime-data-collection-guidelines-training-manual-02272015.pdf/view.

In 2021, the FBI UCR Program also published a hate crime article titled, *Hate Crime Data Helps Law Enforcement Address Threat.* This article was published in the *CJIS Link* on the FBI.gov website at: https://www.fbi.gov/services/cjis/cjis-link/hate-crime-data-helps-law-enforcement-address-threat. The *CJIS Link* article informs readers of the serious nature of hate crimes across the United States.

In addition, the FBI UCR Program developed a hate crime flyer containing the bias motivation categories for law enforcement officers to reference while investigating bias-related incidents. The flyer is provided to stakeholders during FBI Criminal Justice Information Services Division conferences, DOJ Civil Rights Division trainings, and FBI UCR Program hate crime trainings.

The FBI UCR Program finalized a 2021 Hate Crime Outreach and Communications Plan with a focus on most-in-population law enforcement agencies (over 100,000 inhabitants) and college/university law enforcement agencies. Through the NIBRS transition, the FBI UCR Program anticipates hate crime participation to improve over the next few years as agencies continue to transition to incident-based reporting.

8. You also pointed out at the hearing that you created the Domestic Terrorism-Hate Crimes Fusion Cell to ensure the FBI "didn't have a left-hand, right-hand problem" where hate crimes and domestic terrorism investigations weren't properly coordinated "because a lot of these crimes could fit either into a domestic terrorism bucket or a hate crimes bucket." These concerns, and the related concern that domestic terrorism crimes are too often labeled hate crimes and then deprioritized for investigative purposes—persist despite the fact that under its Civil Rights Program Policy Implementation Guide, the FBI requires that hate crimes investigations must also be opened as domestic terrorism investigations if the subject of the investigation has any connection to a white supremacist group.

    a. How confident are you that the Civil Rights Program Policy Implementation Guide is always being followed in practice? If it is, why did the FBI characterize the

investigation of the murder of Heather Heyer in Charlottesville as a civil rights investigation rather than a domestic terrorism investigation?

Response: The 2017 attack that resulted in the murder of Heather Heyer was included as an FBI-designated significant domestic terrorism incident in the May 2021 joint FBI, Department of Homeland Security, and National Counterterrorism Center report, titled "Strategic Intelligence Assessment and Data on Domestic Terrorism."

Hate crimes and domestic terrorism (DT) incidents are often not mutually exclusive. A hate crime is targeted violence motivated by the offender's bias against a person's actual or perceived characteristics, while a DT incident as a criminal act, including threats or acts of violence made to specific victims, is made in furtherance of a domestic socio-political goal.

To address the intersection of the FBI counterterrorism and criminal investigative missions to combat DT and provide justice to those who are victims of hate crimes, the FBI formally created the Domestic Terrorism-Hate Crimes Fusion Cell in April 2019. The Hate Crime Statistics Program of the FBI's Uniform Crime Reporting (UCR) Program collects data regarding criminal offenses that were motivated, in whole or in part, by the offender's bias against a person's actual or perceived race/ethnicity/ancestry, national origin, gender, gender identity, religion, disability, or sexual orientation, and were committed against persons, property, or society. As noted above, the FBI publishes an annual report of hate crime statistics, and in 2019, law enforcement agencies participating in the UCR Program reported 7,314 hate crime incidents. While the FBI collects and reports hate crime statistics, there is no mandatory reporting requirement for state and local law enforcement agencies to identify hate crime incidents that would also be considered criminal activity that appears to be motivated by a socio-political goal consistent with the DT threat categories. Therefore, the FBI does not have the data to be able to determine numbers of DT assessments and investigations that were opened as a result of a hate crime.

The FBI's understanding of domestic violent extremism continues to evolve, just as the domestic terrorism threat has evolved. Many of the domestic violent extremists who have committed attacks in the United States appear to have been motivated and inspired by a mix of ideological, sociopolitical, and personal grievances against their targets. The FBI is seeing more and more that the combination of violent extremist ideologies, individualized grievances toward a particular target, and personal factors all contribute to the mobilization to violence process. In short, the motivations behind acts of domestic terrorism are complex and nuanced, and often very personalized to the perpetrator.

b. Does the policy of opening domestic terrorism investigations for certain hate crimes also apply to hate crimes committed by members of other domestic violent extremist groups that are considered "Anti-Government/Anti-Authority Violent Extremists" or "Other Domestic Terrorism Threats"? If not, shouldn't it?

Response: The FBI opens a full investigation predicated on an "articulable factual basis" that reasonably indicates the existence of federal criminal activity or a threat to national security, or to protect against such activity or threat. The same policy applies across all DT threat categories.

9. In your written statement, you said that "the FBI does not investigate First Amendment-protected speech or association, peaceful protests or political activity." Associate Director Sanborn testified at a separate hearing that the FBI "cannot collect First Amendment-protected activities without sort of the next step, which is the intent. And so we'd need to have an already predicated investigation that allowed us access to those [communications] and/or a lead or a tip or a report from a community citizen or a fellow law-enforcement partner for us to gather than information."

    a. Under what circumstances may the FBI access, monitor, collect, retain, analyze, or disseminate speech protected by the First Amendment, and how are these actions consistent with applicable law and policy? Please be specific, including the relevant provisions of the Constitution, statute, executive order or other presidential directive or memorandum, regulation, departmental or agency policy or procedure, or case law interpreting those authorities that justify such activities?

    b. With respect to publicly available social or other open source media in particular, what kind of predicate is required for the FBI to monitor this media? Is it sufficient for the FBI to have a lawful purpose in monitoring the media? If not, what is required for it to do so? Can it monitor media related to an assessment, a preliminary investigation, or a full investigation?

Response: The *Attorney General's Guidelines for Domestic FBI Activities* (AGG-DOM) establish a set of basic principles that serve as the foundation for all FBI mission-related activities, including online investigation. The AGG-DOM prohibits the FBI from "investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States."

In accordance with those guidelines, the FBI may review, observe, and collect information from open sources as long as the FBI activities are done for a valid law enforcement or national security purpose and in a manner that does not unduly infringe upon the speaker's or author's ability to deliver his or her message. The FBI does not have the authority to persistently and passively examine the World Wide Web, Internet traffic, and social media conversations. The core requirement is that the authorized purpose must specifically be tied to federal criminal or national security purposes, usually to further an FBI assessment or predicated investigation, with due regard to the First Amendment.

With regard to predication, assessments require an authorized purpose but not any particular factual predication. Preliminary investigations may be initiated on the basis of any allegation or information indicative of possible criminal or national security-threatening activity, and full investigations require more substantial factual predication. The significance of the distinction between an assessment and preliminary and full investigations is in the availability of investigative tools and methods. A full investigation, which is based on the more robust factual predicate, permits the full range of legally available investigative tools and methods, whereas assessments and preliminary investigations are more limited in the available tools and methods.

10. You noted at one point in your testimony that DVEs and homegrown violent extremists (HVEs) "have a lot in common with each other" and cited the case of two Boogaloo Bois in Minnesota charged with allegedly providing material support to Hamas. Like HVEs, many DVEs are affiliated with or inspired by terrorist groups that operate at least in part outside the United States. These groups could be designated as foreign terrorist organizations under existing laws. Last year, the Department of State designated a foreign violent right-wing extremist group, the Russian Identity Movement (RIM), as a Specially Designated Global Terrorist organization, but it still has not designated the RIM as a Foreign Terrorist Organization.

    a. Would it advance the law enforcement and counterterrorism missions of the FBI if the RIM was designated as a Foreign Terrorist Organization?

    b. Would it advance the law enforcement and counterterrorism missions of the FBI if other violent extremist groups with international presences, such as the neo-Nazi accelerationist groups The Base and Atomwaffen Division, were designated as Specially Designated Global Terrorists or Foreign Terrorist Organizations?

Response: The FBI does not have the authority to designate a group as a terrorist organization. Regardless of a designation, the FBI investigates violent, criminal acts committed by individuals intending to intimidate, influence, or coerce a civilian population or a government. However, the FBI will use all tools and resources lawfully available to us to combat terrorism.

QESTIONS FROM SENATOR LEAHY

11. Currently there is no statutory authority for the FBI or Department of Justice to maintain a list of domestic terrorist groups comparable to the State Department's list of Foreign Terrorist Organization (FTOs) authorized by Section 219 of the Immigration and Nationality Act (INA). It is easy to see the potential First Amendment issues related to freedom of association and freedom of speech that a domestic terror group list could generate. It is also easy to see how this type of list could become overly politicized.

    a. Please describe how an official list of domestic terrorist organizations would aid the FBI in stopping domestic terrorist attacks in the future and lowering the overall threat level.

    b. What specifically would a list like this accomplish that cannot be accomplished by raising or decreasing threat levels as the FBI does currently?

    c. Would such a list be compatible with the FBI's policy of investigating violence and not ideology?

    d. In your opinion, how do the benefits of such a list weigh against the foreseeable costs?

    e. On Tuesday you noted that one of the largest threats we face from domestic terrorists in the racially motivated violent extremist group is "inspired" lone actors. How would a list of domestic terrorist organizations help prevent these attacks?

Response: The FBI does not have the authority to designate a group as a terrorist organization. Regardless of a designation, the FBI investigates violent, criminal acts committed by individuals intending to intimidate, influence, or coerce a civilian population or a government. When combatting terrorism, the FBI looks at individuals who commit or intend to commit violence and criminal activity that constitutes a federal crime or poses a threat to national security.

The FBI has the dual mission of protecting the American people and upholding the Constitution of the United States. Accordingly, the FBI protects First Amendment rights, including the freedoms of association and assembly, and the right to coalesce with like-minded individuals. Many groups in America form for the sole purpose of exercising their rights, and that is not a crime. However, separate and apart from protected assembly, the FBI works to determine whether multiple individuals worked together, or conspired together, to commit criminal acts in violation of federal law.

12. As you mentioned at the hearing and in past appearances before Congress, there is no crime of domestic terrorism or a domestic terrorism charge. There are, however, many tools available to both prosecute and investigate domestic terrorism. The FBI demonstrated this by disrupting the plot to kidnap Governor Gretchen Whitmer and the prosecution of those involved. Further, at least prior to the elevation of the domestic

terrorism threat level, the FBI in practice has deprioritized certain domestic terrorism related investigations by classifying them as hate crimes and passing them off to state and local law enforcement.

a. Given the link between the current domestic terror threat and racially motivated violent extremists, if the FBI and Department of Justice continue to exercise their investigative and prosecutorial authorities creatively and proactively—like in the case of Governor Whitmer or by expanding the investigation and prosecution of hate crimes—then does the FBI have the legal tools it needs to meet the current threat?

Response: Combatting terrorism is the FBI's top priority. Last year, the White House completed a comprehensive review of domestic terrorism (DT) and issued a report, titled "National Strategy for Countering Domestic Terrorism." The FBI was an active participant in that effort. It is important to send a strong message to hate-motivated perpetrators of violence and federal criminal activity, and the Department of Justice is still considering whether one way to convey that message is with additional legal tools. The FBI currently has a number of federal and state statutes available to use to investigate federal offenses involving DT incidents. The FBI will continue to use every single tool at its disposal to bring to justice those who engage in violence, regardless of their motivation. The FBI will do this through its Domestic Terrorism Operations Section (DTOS) and through Joint Terrorism Task Forces (JTTFs) across the country. The FBI is willing to work with Congress, the Department of Justice, and the Administration to consider thoughtful legislative efforts that seek to support and enhance law enforcement's ability to combat this threat.

b. The hate crimes and domestic terrorism "fusion cell" we briefly discussed during the hearing seems like an excellent example of the FBI acting creatively to maximize the legal tools at its disposal. If appropriate for this setting, please provide more details on how this program works, such as (i) specific examples of the types of cases the fusion cell has helped with; (ii) other relevant procedural or legal details; and (iii) how the fusion cells cooperate and share information with other federal, state, and local law enforcement agencies.

Response: To address the intersection of the FBI counterterrorism and criminal investigative missions to combat DT and provide justice to those who are victims of hate crimes, the FBI formally created the Domestic Terrorism-Hate Crimes Fusion Cell in April 2019. This Fusion Cell creates more opportunities for investigative creativity, provides multi-program coordination, helps ensure information sharing, and enhances investigative resources to combat the DT threat. The Fusion Cell has had significant successes. For example, in November 2019, the work of the Fusion Cell resulted in the arrest of Richard Holzer, a Colorado man who ultimately pleaded guilty and was sentenced to over 19 years in prison for federal hate crime and explosives charges for plotting to blow up a synagogue in Pueblo, Colorado. This was the first time in recent history that the FBI made a proactive arrest on a federal hate crimes charge.

13. The events of January 6th, the rise of domestic terrorism and hate crimes, and the increase in political violence highlight the need for cooperation across federal law enforcement—

including both the FBI and DHS—and state and local law enforcement. I thank you for providing clarity on the communication relayed from the FBI Norfolk Field Office to the relevant law enforcement authorities on January 5th. While I appreciate that it can be difficult to distinguish credible from aspirational threats, I share my colleagues' concern that this message was not acted on and worry that it highlights a gap across law enforcement cooperation.

a. Please describe the specific law enforcement and intelligence breakdowns as you see them that culminated in the events of January 6th. If the FBI were given raw intelligence from an information sharing law enforcement agency that the cooperating agency had deemed actionable—like the Norfolk Field Office Communication—but only had a few hours to process and act, what specific actions would the FBI take?

Response: Any time there is an attack, the FBI will ask itself what could be done differently and what can be improved in collecting, analyzing, and disseminating information. As the FBI continues to examine the events of January 6th, and what led up to that day, the FBI welcomes the opportunity to learn from its collective experiences and work to prevent such an attack from ever happening again.

Regarding information sharing, the FBI routinely shares intelligence products with its federal, state, and local partners. For example, throughout 2020, the FBI issued multiple external intelligence products to federal, state, and local partners with an assessment and warning of credible threats of violence from DVEs related to the election and the transition process, the elevated threats posed by AGAAVEs, and the potential for DVEs to exploit First Amendment-protected activities. The Situational Information Report (SIR) from the Norfolk Field Office is an example of how the FBI quickly shares raw, unevaluated intelligence quickly. On January 5, 2021, the FBI Norfolk Field Office received information from an online discussion thread, not linked to any specific person, calling for violence to begin on January 6th in Washington, DC. FBI Norfolk determined that information warranted dissemination and released the SIR to raise law enforcement awareness regarding the potential for violence in the Washington, DC, area. Upon receiving the report, the FBI Washington Field Office immediately: shared it by email with all partners on the JTTF; shared it during a briefing in the Washington Field Office interagency Command Post at which the U.S. Capitol Police, the Metropolitan Police Department, the U.S. Park Police, the U.S. Secret Service, and others partners were present; and distributed it to Virginia state and local law enforcement partners, as well as to certain federal law enforcement partners, through the Virginia Fusion Center.

b. While the Norfolk Field Office's threat assessment was not deemed serious enough to alert senior Congressional officials, what is the process for notifying such officials if a domestic threat is serious enough to require a coordinated full government response?

Response: The FBI takes seriously its duty to warn, and the FBI *Domestic Investigations Operations Guide* (DIOG) mandates that the FBI notify persons of threats to their life or threats that may result in serious bodily injury and to notify other law enforcement agencies of such

threats. If the FBI becomes aware of threats to life or threats of potential bodily injury that involve government officials, it may coordinate with the U.S. Capitol Police or the U.S. Secret Service, as the law enforcement agencies that have protective jurisdiction of the threatened person. Specific to Congressional officials, the FBI works with the U.S. Capitol Police via the Washington Field Office Joint Terrorism Task Force (JTTF) to issue "duty to warn" notifications. The practice is for the U.S. Capitol Police to then provide confirmations to the FBI once they have issued the notifications.

c. Do you believe the current level of cooperation, both generally and specific to domestic terror, is adequate and, if not, what changes need to be made to improve law enforcement cooperation?

Response: The front line of the counterterrorism mission in the United States are the approximately 200 FBI-led JTTFs in all of the FBI's 56 Field Offices and in many satellite Resident Agencies. The JTTFs have the participation of over 50 federal and over 500 state, local, tribal, and territorial agencies. These relationships are critical to effective information sharing and leveraging local expertise and experience in terrorism investigations, both domestic and international. Prior to January 6th, the effective coordination with law enforcement partners resulted in the disruption of subjects of predicated investigations who were planning to travel to Washington, DC for events on January 6, 2021. Those efforts may have reduced the number and type of individuals who breached the U.S. Capitol and may have kept at bay persons with even more malicious intent or capabilities.

d. During the hearing, you mentioned training efforts to assist state and local law enforcement with investigating active duty officers who may be racially motivated violent extremists or militia violent extremist group members. Recognizing that this does not apply to the overwhelming majority of law enforcement, please provide more details on your coordination with state and local law enforcement on this issue.

Response: The FBI continues to work with state and local law enforcement agency partners to detect, identify, and disrupt any and all DT threats, especially those that may stem from trusted communities and positions of authority within government entities at any level. One way the FBI does this is by providing regular training on DT matters to partners through FBI Field Office partnerships, as well as through established entities, such as the JTTF and the National Academy. Topics of training include mobilization indicators, iconography, and symbology for the violent extremism threats investigated by the FBI.

14. In your oral and written testimony, you mentioned that end-to-end encryption across devices and social media platforms threatens the FBI's ability to manage threats. You suggested that you believed that this was a policy judgement Congress should make but that instead it was being made by private companies.

a. Please describe, as specifically as possible, the biggest issues related to end-to-end encryption from the FBI's perspective that you believe this Committee should

be aware of when considering the balancing of civil liberties with law enforcement surveillance.

Response: The online, encrypted nature of radicalization to violence, along with the insular nature of most of today's attack plotters, leaves investigators with fewer dots to connect. These encrypted communications applications can make it difficult, if not impossible, for the FBI and its partners to track and disrupt threats before they proceed to violence or other criminal actions. Resources are an issue in a number of ways, but simply providing additional resources will not solve this problem. First, encryption vastly increases the cost of investigations by prolonging investigations and causing law enforcement to deploy more intrusive investigative efforts typically consuming other investigative resources. Second, even if methods to gain access to encrypted information are available, the advanced and technical resources necessary to access a single encrypted device or encrypted chat session are so significant that it requires significant triage.

When encryption is a barrier in an investigation, many resources are leveraged for an extended period. Those resources are then unavailable to assist in mitigation of future threats. Additionally, these delays create unnecessary risk to life and property from the lack of lawful access to critical data. This is all the more true for state and local law enforcement partners who have an infinitely greater number of serious criminal investigations, a growing number of which, they report, are now being significantly inhibited by encryption.

15. During the hearing you received many questions about the National Guard's role leading up to January 6th and during the attack on the Capitol. I understand from your responses that you were not involved in any decisions related to activating the Guard and have no such power to do so.

    a. Given the National Guard's prominent role protecting the Capitol today and their visual presence at the protests throughout the summer, do you believe there are adequate channels of communication open between National Guard leadership and the FBI, both in Washington, D.C. and throughout the country, to address and respond to domestic terror threats in the future?

Response: The FBI works in close coordination with federal, state, and local partners to combat terrorism, collaborate on operational activity, and share intelligence. The FBI works closely with the Department of Defense (DoD) through the FBI's Military Operations Support Team (MOST), which is assigned to the National Joint Terrorism Task Force (NJTTF). Leading up to events, the FBI reviews intelligence to identify potential threats to public safety and mitigate them before they become violent acts and federal crimes. The FBI also shares various intelligence products with federal, state, and local partners – including the DoD – through, for example, JTTFs and joint interagency Command Posts.

16. As discussed at the hearing, there has been a dramatic increase in firearm background checks during the pandemic. The FBI operates the National Instant Criminal Background Checks System (NICS), which conducts these background checks of buyers. Last year, the FBI processed nearly 40 million firearm background checks – the highest year on

record. And the numbers are only increasing. In January of this year, the FBI set another record for the highest number of background checks run in one month: 4.3 million. Notably, this was the same month as the deadly attack on the Capitol. As you well know, it's imperative that the FBI efficiently process these background checks to make sure that guns don't end up in the hands of those who are legally barred from owning them.

a. Congress provided the FBI $179 million in emergency funding to help address the increased workload of gun background checks. Has the FBI received this critical funding from OMB and if not, when do you expect to be able to access this funding?

Response: Yes, $179M in two-year supplemental funding was provided by Congress. This two-year funding was appropriated to the FBI for three purposes: NICS improvements; User Fee shortfall; and Coronavirus relief. In coordination with the Department of Justice and the Office of Management and Budget, the FBI has budgeted most of this funding to personnel and non-personnel NICS expenses to improve the timeliness and effectiveness of processing gun background checks.

b. Please describe how the funding will help improve the efficiency of the background check system and ensure that guns don't end up in the wrong hands.

Response: This supplemental funding continues to be instrumental in adding much needed personnel resources, augmenting information technology (IT) development staff, and enhancing the productivity of NICS through an improved telework posture. The ongoing system improvements being performed with the supplemental funding will help improve the efficiency of processing gun background checks.

Additional personnel resources will improve the NICS program by providing timely and accurate determinations of each individual's eligibility to possess firearms and/or explosives in accordance with federal law. An increase in resources will allow the staff assigned to important support functions to perform that function throughout the year and not be reassigned to process firearm transactions when the volume dictates. The increased personnel resources will allow for processing additional firearm background checks from the NICS Delay Queue and additional firearm background checks from the E-Check workbasket; thereby reducing the amount of firearm background checks that are not processed until the third business day. The ability to process background checks more efficiently will help to minimize the number of firearm sales to prohibited persons and decrease the workload for the Bureau of Alcohol, Tobacco, Firearms and Explosives, the federal agency tasked with retrieving firearms from prohibited persons who are in possession of a firearm due to delays in a NICS final determination.

All of the system development efforts that the NICS Section is focused on with this funding will be toward automation and efficiencies through increased development capacity. The NICS development effort utilizes an agile development methodology that prioritizes requirements to resolve known or discovered operational system defects. The prioritization is reevaluated upon identification of new system requirements during program increment planning

sessions. The exact requirements will change as priorities change. Priority changes are driven by newly identified system vulnerabilities or defects and changes in the operational environment such as changes in gun laws, new Congressional mandates, and new Executive Orders.

Some of the high-priority items that also have software and hardware costs in the development plan are:

- Robotic Process Automation (RPA) – The ability to search external state websites and pull back that information to the transaction.

- Computer Telephone Integration (CTI) – This will assist the NICS Section with processing the phone calls received from the call center and gain efficiencies on the call back functionality.

- Movement to the cloud – This will help the NICS Section with system stability and flexibility as well as future cost savings.

- Enhanced test tools – This will help the NICS Section to have a higher quality product when enhancements are deployed to the NICS system and provide stability and agility in
the future.

- Future technologies – The NICS Section will be prepared to implement future technologies and inputs if regulation changes occur in the near term.

c. What resources does the FBI need to keep pace with firearm background checks if this level of demand continues?

Response: The NICS Section's mission statement is: seeking to enhance national security and public safety by conducting background checks to determine a person's eligibility to possess firearms or explosives in accordance with federal and state laws. In order to meet this mission, the NICS Section must provide excellent service in several operational functions, such as the NICS E-Check and the NICS Delay Queue. These functions are the highest priority for the Section. The FBI has identified a need for additional personnel resources to increase its capacity to perform NICS background checks for firearm purchases. The additional personnel resources will provide an enhanced ability for the section to complete transactions within three business days, meet service levels of the NICS E-Check and telephone responses, and effectively address additional services provided to the law enforcement community and its customers. Since the beginning of calendar year (CY) 2020, the NICS Section saw a considerable increase to incoming federal firearm background checks, and in the beginning of CY 2021, the NICS set records for transaction volume with multiple days, weeks, and months ranking in the top ten. The increase has severely pressured the NICS Section to complete firearm transactions within three business days.

The President's 2023 Budget fully annualizes the personnel costs associated with the supplemental resources provided in 2021 and requests additional resources to support NICS.

17. In 2020, the National Center for Missing and Exploited Children's (NCMEC) CyberTipline received more than 21.7 million reports regarding online exploitation of children – almost 4 million more reports than in 2019. NCMEC also received almost twice as many reports in 2020 of online enticement of children than it did in 2019.

    a. Please describe, in as much detail as possible, the steps the FBI is taking to combat this disturbing rise in the exploitation of children online, particularly on social media and online gaming platforms.

Response: The FBI continues to work with its federal, state, and local counterparts to address child exploitation online. The FBI runs 85 Child Exploitation Human Trafficking Task Forces (CEHTTFs) around the country, which focus their efforts on the worst offenders – those who kidnap, produce or manufacture child sexual abuse material (CSAM), engage in sextortion, or travel to exploit children. Additionally, the FBI works with the DOJ-funded Internet Crimes Against Children (ICAC) Task Forces around the country to ensure we use all of the tools available to us, whether they be federal, state, or local charges, to hold these offenders accountable.

As it has for many years, the FBI continues to work closely with NCMEC to identify child victims and educate the community about crimes against children and how children, parents, and caregivers can protect themselves from child sexual exploitation. FBI personnel assigned to NCMEC review the tips received there and forward pertinent information to FBI field offices for investigation. Recently, the FBI partnered with NCMEC and the anti-human trafficking organization "Thorn" for a Twitter chat to educate the public about online child sexual exploitation as part of its efforts for National Child Abuse Prevention Month.

The FBI continues to develop and acquire innovative tools, technologies, methodologies, and external relationships that increase the efficiency and effectiveness of Violent Crimes Against Children (VCAC) investigations and operations. The FBI focuses these efforts on tools that assist in the identification of important data from within larger sets, reduce the burden of review for investigators, enhance or expand automation to identify newly produced CSAM, and indicate links or correlation between the activities or identities of threat actors across platforms.

Finally, since January 2020, FBI Agents around the country have conducted more than 4,300 training and outreach sessions with state, local, and community partners, which focused specifically on crimes against children and human trafficking.

    b. Please describe the resources the FBI is providing to educate parents about the issue and to help prevent their children from online exploitation, particularly with more children online during the pandemic.

Response: The FBI's Victim Services Division provides sextortion victims in FBI investigations with numerous services through its Child Pornography Victim Assistance Program. The FBI also has many resources available online for parents to learn about sextortion, solicitation, and enticement of a minor. There are brochures, cyber alerts for parents and children, news

regarding adjudicated child exploitation cases, and valuable data and resources collected by the National Center for Missing and Exploited Children (NCMEC).

c. Does the FBI have all of the resources it needs as part of this program to meet this growing challenge?

Response: Technological developments and encrypted messaging applications have made investigations of crimes against children more difficult and complex. The subjects of VCAC investigations are more likely to use sophisticated encryption methods, exploit covert communication techniques, and operate on illicit Dark Web networks. New platforms and applications showcase ever-increasing security technologies, which are then adopted by subjects. The FBI – and law enforcement in general – lacks large-scale technological solutions to proactively address children being sexually exploited via end-to-end encrypted platforms and livestream applications. The evolution of the technology and criminal methodologies requires a sustained effort to train the FBI workforce, as well as a significant investment in investigative tools. The FBI sees an increasing need for technical expertise, equipment, and global collaboration to combat child sex offenders using sophisticated techniques and technical tools, and will continue to focus its resources on accomplishing these goals.

18. When I asked you about an FBI report indicating that 87 percent of law enforcement agencies participating in the FBI's hate crime data collection program have reported zero hate crimes in their jurisdictions, you responded that "We do want the percentage of departments who are cooperating and voluntarily responding to go up."

    a. What steps will you take to ensure that more law enforcement agencies are accurately reporting the hate crimes that occur in their jurisdictions? Are additional resources required for the FBI to ensure better cooperation from law enforcement agencies with its hate crime data collection program?

Response: The FBI Criminal Justice Information Services (CJIS) Division's Audit Unit conducts periodic reviews of Uniform Crime Reporting (UCR) crime data, including hate crimes reported to the FBI UCR Program. Each state's UCR Program is subject to review at least once every three years to evaluate the state's compliance with the FBI UCR Program's hate crime reporting guidelines. Hate crime audits focus on classification procedures and correcting previously identified errors. After the audit, the auditor provides a report of their findings to the local agency and to FBI UCR Program hate crime personnel.

The FBI UCR Program transitioned all federal, state, local, college/university, and tribal law enforcement agencies nationwide to the National Incident-Based Reporting System (NIBRS) on January 1, 2021. This transition will ease the ability for agencies to submit hate crime data as NIBRS includes a designated field for law enforcement agencies to report hate crimes. Therefore, reporting via NIBRS will improve the quality, reliability, and accuracy of hate crime data.

To support federal and tribal reporting, the FBI deployed the NIBRS Collection Application (NCA). The FBI developed the NCA, which is available on the Law Enforcement

Enterprise Portal, to provide a no-cost solution for federal and tribal agency users to submit NIBRS data to the FBI UCR Program and to comply with the Uniform Federal Crime Reporting Act of 1988. As the NCA's functionality became more robust, the NCA became a viable option for non-transitioned state and local agencies to submit NIBRS data. The NCA is an extension of the UCR system and enables users to directly enter and submit NIBRS crime data to UCR for processing, retention, and publication.

The *Hate Crime Guidelines and Training Manual* was developed to assist law enforcement agencies in establishing a hate crime training program to allow personnel to collect and submit hate crime data to the FBI UCR Program. The manual provides suggested model reporting procedures and training aids for capturing the bias-motivated incident data reported to the FBI. The FBI UCR Program is currently revising this document to remove all Summary Reporting System (SRS) verbiage and adding all federal and tribal law enforcement offenses. The SRS collected hate crime data on 13 offenses versus the 70 offenses collected in the NIBRS. The manual is located on the FBI.gov website at: https://www.fbi.gov/file-repository/ucr/ucr-hate-crime-data-collection-guidelines-training-manual-02272015.pdf/view.

In 2021, the FBI UCR Program also published a hate crime article titled, *Hate Crime Data Helps Law Enforcement Address Threat.* This article was published in the *CJIS Link* on the FBI.gov website at: https://www.fbi.gov/services/cjis/cjis-link/hate-crime-data-helps-law-enforcement-address-threat. The *CJIS Link* article informs readers of the serious nature of hate crimes across the United States.

In addition, the FBI UCR Program developed a hate crime flyer containing the bias motivation categories for law enforcement officers to reference while investigating bias-related incidents. The flyer is made available to stakeholders during FBI CJIS Division conferences, Department of Justice Civil Rights trainings, and FBI UCR Program hate crime trainings.

The FBI UCR Program finalized a 2021 Hate Crime Outreach and Communications Plan with a focus on most-in-population law enforcement agencies (over 100,000 inhabitants) and college/university law enforcement agencies. Through the NIBRS transition, the FBI UCR Program anticipates that participation in hate crimes reporting will improve over the next few years as agencies continue to transition to incident-based reporting.

The FBI UCR Program offers a training program for our law enforcement community via webinars. During these training sessions, the FBI provides an overview of the hate crime statistics collection and hate crime scenarios, the two-tiered decision-making process, and bias motivation indicators. It also discusses the importance and benefits of reporting hate crime incident data (increases understanding, long-range planning, promotes transparency, information sharing, and address threats). These instructional opportunities allow FBI staff to meet with the law enforcement community from reporting agencies. The training emphasizes the need and benefits of the Hate Crime Statistics Collection, and in turn encourages participants to discuss this important topic with law enforcement colleagues within their local agencies and communities. The overall goal is to increase participation in this data collection.

QUESTIONS FROM SENATOR COONS

19. You testified that social media has become a "catalyst" of domestic violent extremism. You also testified that the FBI has "tried to work with social media to get them to more aggressively use the tools that they have to police their own platforms under terms of service, etc."

    a. Please elaborate on these statements.

Response: The FBI maintains strong private sector partnerships and ongoing communications regarding threats, violence, and malign foreign interference. The FBI routinely engages with the technology sector to educate them on the threats, and many companies are proactively identifying threats and notifying the FBI. To succeed in finding plots where violent rhetoric or hate speech online has turned to planning, social media companies need to be spotting and warning of dangers. The FBI does not, however, police speech and does not get involved until speech crosses the line and becomes a violation of federal criminal law. Up to and until that point, it is up to the private sector companies to craft and enforce their own terms of use on their platforms.

    b. Please describe the extent to which, and in what ways, the January 6 insurrection was organized and coordinated through social media platforms.

Response: Radicalization of DVEs most often occurs through self-radicalization to violence online. Social media has increased the speed and accessibility of violent extremist content, while also facilitating greater decentralized connectivity among extremist supporters. According to publicly available court documents, the Department of Justice has charged a number of defendants involved in the attack on the U.S. Capitol with conspiracy, either to obstruct a congressional proceeding, to obstruct law enforcement during a civil disorder, and/or to injure an officer. In order to protect the integrity of all investigations, as a general policy and practice, the FBI does not comment on the status or existence of any potential investigative matter. Given that this question relates to hundreds of ongoing investigations and pending prosecutions, it would be inappropriate to provide further information at this time.

    c. Please describe the extent to which the FBI has observed disinformation on social media platforms contributing to domestic violent extremism through radicalization.

Response: The FBI is concerned about any source that stimulates or motivates violent extremism. However, radicalization of DVEs most often occurs through self-radicalization to violence online. Social media has increased the speed and accessibility of violent extremist content, while also facilitating greater decentralized connectivity among extremist supporters. Some DVEs will continue to be inspired by an individualized mix of various beliefs, picking and choosing themes of different ideologies in an attempt to justify their violent acts. Trends continue to evolve, but long-standing DVE drivers, including racism, anti-Semitism, perceived government or law enforcement over-reach, socio-political conditions, legislation, and other world events, combined with personal grievances, remain constant. Additionally, the FBI

assesses some DVEs will continue to personalize their own ideology in an attempt to justify their violent acts.

d. Please describe the extent to which the FBI has observed efforts by domestic violent extremists to recruit members on social media.

Response: Over the years, DVEs have increased their use of the Internet and online platforms, which often play an important role in an attacker's radicalization to violence and have been used for the creation of violent rhetoric, spreading violent extremist ideology, and recruiting like-minded individuals to DVE causes. Additionally, increased use of encrypted applications affords users anonymity and operational security, while ensuring their material remains widely accessible to online audiences. However, the FBI does not investigate or collect based solely on ideology or assembly. The FBI predicates investigations on individuals, not groups that exist to express First Amendment-protected activity, and does not investigate group membership.

e. What are the kinds of content that remain on platforms that, in your view, represent the greatest law enforcement threats? Please explain.

f. Is there more that the FBI believes social media platforms could be doing to address the incitement of violence on their platforms? Please explain.

Response: The FBI does not police speech and does not get involved until speech crosses the line and becomes a violation of federal criminal law. Up to and until that point, it is up to the private sector companies to craft and enforce their own terms of use on their platforms.

The volume of data online proliferated by the growth in communications platforms requires increased resources and the ability to address end-to-end encryption. The FBI also needs technology companies to retain the ability to provide electronic evidence when we come to them with a lawful court order that we obtained to gather evidence pertinent to the planning or commission of a federal crime.

20. Please clarify the FBI's policies on social media monitoring in light of Assistant Director Jill Sanborn's testimony and subsequent press reports.[1]

a. What social media monitoring was the FBI conducting in connection with the events that culminated in the Jan. 6 insurrection?

Response: Although the FBI does not have the authority to persistently and passively examine Internet traffic and social media conversations, the FBI does proactively review, observe, and collect information from open sources when there is a valid law enforcement or national security purpose and the FBI's activities are done in a manner that does not unduly infringe upon the speaker's or author's ability to deliver his or her message. After the 2020 election, and in advance of January 6, 2021, the FBI performed standard preliminary open source analysis to

[1] *See* Ken Dilanian, "Why did the FBI miss the threats about Jan. 6 on social media?" *NBC News* (Mar. 8, 2021), *available at* https://www.nbcnews.com/politics/justice-department/fbi-official-told-congress-bureau-can-t-monitor-americans-social-n1259769.

identify any threats of violence or criminal activity related to potential protest activities in the National Capital Region (NCR).

In the weeks leading up to January 6th, the FBI Counterterrorism Division engaged with all 56 Field Offices to collect information on threats to the NCR connected to January 6th. 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. A review of the reporting indicated only unsubstantiated threats and did not identify any specific or corroborated threats to the activities planned for January 6th.

b. Why wasn't the FBI able to develop more verified and actionable intelligence in advance of the Jan. 6 insurrection?

Response: Throughout 2020, the FBI issued multiple external intelligence products to its federal, state, and local partners on the threats posed by DVEs. The FBI had been assessing and warning of credible threats of violence from DVEs over the past year related to the election and the transition process, the elevated threats posed by AGAAVEs, and the potential for DVEs to exploit First Amendment-protected activities. The FBI shared these intelligence products with its federal, state, and local partners through, for instance, its JTTFs and joint interagency Command Posts.

21. Does the FBI plan to conduct an after-action review of its intelligence-gathering and law enforcement response to the events culminating in the Jan. 6 insurrection?

    a. If yes, please provide details of the scope and nature of this review, and whether it will assess potential policy changes. Please also explain whether this Committee will be briefed on the findings.

    b. If not, please explain.

Response: Any time there is an attack, the FBI will look at what could have been done differently, and how to improve collecting, analyzing, and disseminating information. As the FBI continues to examine the events of January 6th, and what led up to that day, the FBI welcomes the opportunity to learn from collective experiences and work to prevent such an attack from ever happening again.

Currently, the Department of Justice Office of the Inspector General, along with other agency Inspectors General, is conducting an investigation into how the agencies prepared for and responded to the events of January 6th; the Government Accountability Office (GAO) has initiated an assessment in response to January 6th; and several Committees have made oversight requests. The FBI is fully cooperating with each investigation and review, consistent with its law enforcement and national security obligations to protect ongoing investigations and cases.

22. Commentators have posed the question of "the role of implicit bias in blinding the FBI to the gathering storm in the run-up to Jan. 6," asking whether the intelligence and law enforcement response would have been the same had the identities of the participants been different.[2]

    a. What is your response to this concern?

    b. Will the potential role of implicit bias be a part of any after-action review of this incident? Please explain.

Response: Consistent with the FBI's mission to protect the American people and uphold the Constitution of the United States, the FBI does not investigate anyone based solely on First Amendment-protected activity, to include speech, political affiliation, association, or assembly. The FBI is focused on threats or acts of violence or other federal criminal activity, regardless of underlying motivation or socio-political goal.

23. The Russian-perpetrated SolarWinds attack penetrated at least nine federal agencies and 100 companies, and appeared to be part of an effort to move beyond espionage to create capabilities and access that could be used for information campaigns, political manipulation, and a potential foundation for more active disruption of things like critical infrastructure.

    a. How did this attack persist without detection, and why was it uncovered by the private sector and not government agencies charged with cybersecurity? How can federal agencies better partner with the private sector on cyber security?

Response: For years, the FBI has warned of China's and Russia's efforts to inject malware into programs, undermining trust in software and automated updates. This has been evident in recent years with Russia's NotPetya malware, which inserted malicious code into seemingly routine updates, and China's Tax Bureau mandated software that contained malware that installed a hidden backdoor to the networks using the software. The SolarWinds intrusion takes it to a more dangerous level. By purposely infecting a product widely used by enterprises to manage their networks, the adversary gained incredible access and visibility, and executed their plan with a degree of sophistication, tradecraft, and thoroughness that made it extremely difficult to detect. This incident shows the investments in time, money, and talent that U.S. adversaries will make to harm us, and the importance of imposing risk and consequences on adversaries to deter this type of activity. It drives home that only a whole-of-society approach will be effective against these threats. The FBI appreciated the proactive cooperation of the private sector in the Solar Winds incident, which made a difference in the Unified Coordination Group's (UCG's) ability to investigate, mitigate, and learn from the incident.

The SolarWinds incident highlighted how vital private sector cooperation is to the FBI's broader work protecting America from cyber threats. The virtuous cycle of working together has been on display in the SolarWinds response: information from the private sector fuels the FBI's

[2] *See* Tia Sewell and Benjamin Wittes, "The Questions FBI Director Christopher Wray Wasn't Asked," *Lawfare* Mar. 5, 2021), *available at* https://www.lawfareblog.com/questions-fbi-director-christopher-wray-wasnt-asked.

investigations, allows identification of additional victims, evidence, and adversary infrastructure, and enables information sharing with intelligence and law enforcement partners that enables their operations. These partners then put that information to work and provide the FBI more information than originally known, which can be used to then arm the private sector to harden itself against the threat. By leaning into partnerships, all who are combatting malicious cyber activity become stronger while weakening the perpetrators together.

In this context, "private sector" refers to two main groups:

- Providers—those in the IT and cybersecurity industry whose products and services give them unique visibility into how adversaries are traversing U.S. networks; and

- Victims—those whose hard drives, logs, and servers give the technical dots to piece together who compromised them, how, and who they might target next.

With respect to enhancing public-private information sharing, this generally refers to the FBI's relationship with providers. But enhanced engagement from the victims who have unique visibility is also very important.

The most sophisticated adversaries make pervasive use of strong encryption. They may connect from their home operating base, through multiple servers in third countries, to one in the U.S. then to a victim. They are usually working through an encrypted tunnel along that whole chain.

However, on the victim network, they show their hand. There is not a substitute for visibility into what the adversary is doing to victims, or to the information victims have about where the adversary went next. Very often, actors use different infrastructure to exfiltrate (steal) data than they used to gain initial access. The FBI needs to be able to find that next destination, to figure out what else the adversary is doing from those servers, and to position to disrupt that activity. This is just part of why FBI devotes so much effort across the country to working with victims, and with companies it assess adversaries are likely to target.

b. Are the Russians exploiting a statutory gap between domestic and overseas intelligence activities? If so, how can Congress help the administration close these gaps?

Response: It is not surprising that malicious foreign actors try to avoid detection by the FBI domestically and by other IC agencies overseas. So, the FBI, NSA, and others are always working on ways to limit those actors' ability to hide their activities. Working together is most powerful—which is an advantage that the more competitive intelligence services in Russia and China, for example, do not enjoy.

One area that is so important is increased visibility into what adversaries are doing, especially when they are on privately-owned infrastructure. That includes the NSA, CIA, and FBI as intelligence agencies; and, CISA as the defenders of Federal Civilian Executive Branch

networks and major Internet and IT service providers whose networks and software are ubiquitous. The FBI needs to keep getting faster and better at sharing what it sees, in a way that protects privacy but leads to faster detection and action. Over the past few years, U.S. government agencies have all learned to lean hard into sharing, but need to get better at pulling in the information and working with the experts in the private sector. Ultimately, the goal is always to disrupt threats before they occur, and to do so it is critically important that the FBI have the information needed to respond quickly and limit the damage.

c. What technical, organizational, and legal improvements can Congress make to prevent these attacks to the extent possible, detect them faster, and minimize their damage?

Response: The FBI is working with its federal agency partners and the Administration on ways to improve U.S. Government's cyber incident prevention, detection, and mitigation efforts. The FBI will also continue to work with the Administration on any proposals for Congress to assist the Executive Branch with these interrelated lines of effort.

One critical aspect to incident detection and mitigation is entities notifying the Federal Government when they have suffered an intrusion or are observing malicious cyber activity. These notifications, especially when made promptly, are oftentimes critical to containing the damage caused by cyber threat actors exploiting specific vulnerabilities. Receiving notifications of malicious cyber activity from industry, and cooperation with the FBI when it responds, assists federal efforts to warn the public about ongoing cyber threat activity, assists the public and private sectors with detection and mitigation measures, and also supports cyber investigations that uncover the scope of computer intrusions, develop cyber threat intelligence, and ultimately hold cybercriminals accountable.

24. China's government-sponsored cyber-attacks are frequent, sophisticated, and widespread, with a recent attack discovered earlier this month compromising an estimated 30,000 - 60,000 public and private entities in the United States alone, and as many as 250,000 servers infected globally. These hacks are a major threat to not only our national security but also risks the theft and ransom of proprietary data for a massive number of U.S. businesses – a threat to consumers, the protection of intellectual property, and economic activity in the U.S.

    a. Reports indicate that this attack went undetected by U.S. cybersecurity firms for weeks, and may have been picked up a few weeks earlier by researchers in Taiwan. How can we better cooperate with allies and partners, including with private sector tech and cybersecurity firms, to detect and counter these cyber threats?

Response: In December 2020 and again in early January 2021, a Taiwan-based cybersecurity firm alerted Microsoft of the Microsoft Exchange Server vulnerabilities. Microsoft developed a patch and released it along with a public announcement on March 2, 2021, attributing the activity to a group it calls Hafnium, which Microsoft assesses to be a Chinese state-sponsored intrusion set.

Stitching together a complete picture of a cyber threat or incident requires information from many sources. The Microsoft Exchange Server vulnerability as well as the SolarWinds hack underscore the essential value of using law enforcement authorities, voluntary sharing by third parties, and victim cooperation in order to triage data and exploit evidence, to provide assistance to victims, and to work with industry victims and partners to gather information.

The private sector owns approximately 90 percent of the critical infrastructure in the United States, but that figure does not fully capture the private sector's importance in cyber defense. Information from the private sector fuels FBI investigations, allows FBI personnel to identify evidence and adversary infrastructure, and enables the FBI to hand off leads to intelligence and law enforcement partners here and abroad.

Key to the FBI's cyber strategy is using the information and insight developed through FBI investigations to support a full range of public and private sector partners who defend networks, build international partnerships, sanction destabilizing behavior, collect foreign intelligence, and conduct cyber effects operations. These collective actions to combat cyber threats are most effective when they are joint, enabled, and sequenced for maximum impact.

Each Intelligence Community (IC) agency needs to do more to improve the quality and quantity of data points contributed to cyber incident response, which is accomplished by leaning into partnerships and increasing information sharing. Enhancing public-private information sharing generally means relationships with providers—those in the IT and cybersecurity industry whose products and services give them unique visibility into how adversaries are traversing U.S networks—but enhancing cooperation from victims is also critical. Their networks hold insights into how the adversary is operating, and who they may target next, which no one else has.

This is just part of why the FBI devotes so much effort across the country to working with victims and with companies *before* they suffer an intrusion. The FBI's pre-existing partnerships with the private and public sectors throughout the country are critical to identifying threats, understanding their scope, and pursuing attribution to impose risk and consequence on adversaries. Sharing and collaboration with the private sector (and across agencies) is steadily improving. As the IC gets better at this, and builds trust with key industry stakeholders, visibility gaps will steadily close.

b. I understand the administration is considering the creating of a cyber "Unified Coordination Group." Can you say more about what this group is expected to do to respond to this situation and hold the government of China accountable? Will it remain active to detect and prevent future cyber-attacks from China's hacker army?

Response: The UCG construct was established for cyber incident response in Presidential Policy Directive (PPD)-41, but has its roots in incident response in the physical realm, specifically, the National Response Framework. This allows for interoperability of UCGs in the event of a hybrid cyber/physical event. PPD-41's principles balance concurrent lines of effort: national security and investigative requirements (FBI's role in a UCG) with restoration and recovery (CISA's

role). The FBI's role in a UCG is Threat Response, which includes investigating and gathering intelligence in order to attribute, disrupt, and hold accountable the responsible threat actors. In practice, this means:

- The FBI leads the investigation of the activity against affected entities and engages victims to collect forensic evidence and identify adversary tactics and techniques. The FBI shares that information with a variety of partners inside and outside government for multiple purposes, including intelligence, investigation, and network defense to prevent additional victims. The FBI also shares that information with partner operational agencies to enable further action.

- The FBI engages industry partners who, through what they see on their infrastructure, can help point to additional victims.

- The FBI analyzes what it learns and combines that with other information at the FBI's disposal as part of the IC to attribute the activity—i.e., to identify who is responsible and warn of a broader threat.

- The FBI can use that attribution to pursue the threat actors and, through the National Cyber Investigative Joint Task Force, to convene partners to coordinate a response through joint, sequenced operations.

25. Russian activist Vladimir Kara-Murza was poisoned in Russia in 2015 and again in 2017, with evidence indicating the involvement of FSB personnel. Following both poisonings, samples of his blood were accepted for testing by the FBI, and tests were performed, but the results of those tests have not been fully released. On July 5, 2018, Mr. Kara-Murza submitted a request pursuant to the Freedom of Information Act and Privacy Act (FOIPA) to the FBI (FOIPA Request No. 1410820-000) for documents relating to his poisonings. The heavily redacted documents released to him acknowledged he had been poisoned with a biotoxin, but did not include the toxicology test results, nor did it include more than 270 pages of documents under review by other agencies.

    a. Will you direct that the 562 pages of documents that were redacted by the FBI be re-reviewed with an eye to releasing as much information as possible to Mr. Kara-Murza about the circumstances surrounding his poisonings and the nature of the agent with which he was poisoned?
    b. To which other agencies of the federal government did the FBI refer documents responsive to Mr. Kara-Murza's FOIPA request?
    c. With respect to each such referral, what was the date of the referral, and how many pages were referred to each agency?
    d. In January 2018, did you or other FBI officials discuss Mr. Kara-Murza or his poisonings in meetings with the then-visiting heads of Russia's FSB, GRU and SVR (Sergey Naryshkin, Alexander Bortnikov or Igor Korobov)?

Response: The FBI Lab has essentially exhausted its capabilities and has been unable to identify the specific poison or compound that was utilized on Mr. Kara-Murza. Additional testing

conducted at the FBI Lab for potential agents and known variants utilized in other high-profile incidents also yielded negative results. The Lab has preserved the remaining sample to allow for further testing at a facility with capabilities/certifications exceeding those currently available at the FBI Lab. That said, the FBI's Washington Field Office has already relayed this information to Mr. Kara-Murza personally and has made it known that they will do what they can to get him a copy of the full FBI Lab report as soon as its completed.

The FOIA litigation is ongoing, so all exemptions and actions are still subject to change. The documents released, to this point, were not particularly heavily redacted. The most substantial redactions are of: (1) classified information/intelligence source and method information protected by the National Security Act of 1947; and (2) information that would identify confidential source(s) and/or any information provided by such a source. There were other exemptions cited, including for privacy and law enforcement sensitive information.

QUESTIONS FROM SENATOR BLUMENTHAL

Questions for Director Wray

26. As you are aware, several insurrectionists who attacked the United States Capitol on January 6, 2021, have been identified as active duty servicemembers, reservists, retirees, and veterans.[3] I am concerned that federal, state, and local law enforcement agencies may, too, have White Supremacist Extremists (WSEs) and other violent fringe extremists in their ranks, evidenced by reporting that law enforcement officers were among those who participated in the January 6 insurrection.[4]

    a. Is the FBI taking steps to investigate WSEs and other extremists among federal law enforcement officers and other personnel in the Bureau?

        i. If so, please describe these steps and how the FBI intends to prevent, address, and neutralize extremist ideology within the Bureau.

        ii. If not, please explain why not.

    b. Is the FBI taking steps to assist other federal agencies and departments, including, but not limited to, the Bureau of Alcohol, Tobacco, and Firearms, the United States Marshals Service, the United States Secret Service, the Drug Enforcement Administration, Immigration and Customs Enforcement, Customs and Border Protection, the Bureau of Prisons, the Department of State, and the Department of Defense to investigate WSE and other violent fringe extremism in their ranks?

        i. If so, please describe these steps.

        ii. If not, why not?

    c. Is the FBI taking steps to assist state and local law enforcement agencies to investigate WSEs and other extremists in their ranks?

        i. If so, please describe these steps.

        ii. If not, why not?

Response: The FBI works closely with federal, state, local, tribal, and territorial law enforcement partners through the FBI-led JTTFs to detect, identify, and disrupt any and all DT threats, especially those that may stem from trusted communities and positions of authority within government entities at any level. One way is by providing regular training on DT matters

[3] Gina Harkins, Hope Hodge Seck, *Marines, Infantry Most Highly Represented Among Veterans Arrested After Capitol Riot*, Military.com (Feb. 26, 2021), https://www.military.com/daily-news/2021/02/26/marines-infantry-most-highly-represented-among-veterans-arrested-after-capitol-riot.html.
[4] NPR, *The Capitol Siege: The Arrested and Their Stories*, (March 5, 2021) https://www.npr.org/2021/02/09/965472049/the-capitol-siege-the-arrested-and-their-stories.

to partners through FBI Field Office partnerships, as well as through established entities, such as the JTTF and the National Academy. Topics of training include mobilization indicators, iconography, and symbology for the violent extremism threats investigated by the FBI.

It is important to note, there are more than 13,000 law enforcement agencies in the United States with more than 800,000 sworn law enforcement officers.[5] Those agencies do not have a centralized mechanism for communicating with the FBI about the issue of DVEs in their ranks, and there is no mandatory requirement to notify the FBI if they see indications of violent extremism in an employee. However, agencies have contacted the FBI when they have concerns about current or former employees. For example, on January 7, 2021, the day after the attack on the U.S. Capitol, officers of a local police department in Georgia provided the FBI information about a former fellow officer who allegedly participated in the attack. The FBI opened an investigation into that former officer and arrested him on January 15, 2021.

d. Recent reports indicate that at least one then-member of the Trump administration was among those present at the Capitol during the insurrection.[6] Please state whether the FBI identified any other federal government employees, including both political appointees and career civil service personnel, who participated in the January 6 insurrection.

Response: In order to protect the integrity of all investigations, as a general policy and practice, the FBI does not comment on the status or existence of any potential investigative matter. Given that this question relates to hundreds of ongoing investigations and pending prosecutions, it would be inappropriate to provide further information at this time.

27. The FBI's data shows that there were 7,314 reported hate crimes in 2019—a 10-year high and 7% increase from 2015.[7] These numbers, shocking as they may be, fail to reflect just how pervasive and pernicious the problem is, given the vast underreporting of hate crimes and hate crimes that are not identified as such by law enforcement.

    a. Please explain the benefits to law enforcement of complete and accurate reporting of hate crimes.

Response: When federal, state, local, college/university, and tribal law enforcement agencies provide complete and accurate hate crime data to their state and local governments and the FBI Uniform Crime Reporting (UCR) Program, a more open and transparent environment is created for the communities they serve. Reliable statistics also enable law enforcement agencies to understand the hate crimes occurring in their jurisdictions, assist law enforcement agencies in developing preventative measures to combat these crimes, and assist the FBI to provide a national representative picture of hate crimes nationally to inform, educate, and strengthen communities.

[5] 2019 Unified Crime Reporting Program Report, "Crime in the United States."
[6] Josh Gerstein, *Trump appointee arrested in connection with Capitol riot*, POLITICO (Mar. 5, 2021 3:54 PM), https://www.politico.com/news/2021/03/04/trump-appointee-arrested-for-capitol-riot-473825.
[7] *Hate Crime Statistics, 2019*, FEDERAL BUREAU OF INVESTIGATION (2019), https://ucr.fbi.gov/hate-crime/2019.

i. Please summarize the steps the FBI is taking to improve hate crime reporting and hate crime identification at the federal-level, including coordination with FBI field offices and U.S. Attorney offices as well as partnerships with community-based organizations.

Response: To support federal and tribal reporting, the Federal Bureau of Investigation (FBI) deployed the National Incident-Based Reporting System (NIBRS) Collection Application (NCA). The FBI developed the NCA, which is available on the Law Enforcement Enterprise Portal, to provide a no-cost solution for federal and tribal agency users to submit NIBRS data to the FBI Uniform Crime Reporting (UCR) Program and to comply with the Uniform Federal Crime Reporting Act of 1988. The NCA is an extension of the UCR system and enables users to directly enter and submit NIBRS crime data to UCR for processing, retention, and publication.

ii. Please summarize the steps the FBI is taking to improve hate crime reporting and hate crime identification with and by state and local law enforcement agencies, including, but not limited, providing state and local law enforcement with best practices, training, and technical assistance on hate crimes reporting and identification.

Response: The FBI Uniform Crime Reporting (UCR) Program transitioned all federal, state, local, college/university, and tribal law enforcement agencies nationwide to the National Incident-Based Reporting System (NIBRS) on January 1, 2021. This transition will ease the ability for agencies to submit hate crime data as NIBRS includes a designated field for law enforcement agencies to report hate crimes. Therefore, reporting via NIBRS will improve the quality, reliability, and accuracy of hate crime data.

To support federal and tribal reporting, the FBI deployed the NIBRS Collection Application (NCA). The FBI developed the NCA, available on the Law Enforcement Enterprise Portal, to provide a no-cost solution for federal and tribal agency users to submit NIBRS data to the FBI UCR Program and comply with the Uniform Federal Crime Reporting Act of 1988. As the NCA's functionality became more robust, the NCA became a viable option for non-transitioned state and local agencies to submit NIBRS data. The NCA is an extension of the UCR system and enables users to directly enter and submit NIBRS crime data to UCR for processing, retention, and publication.

The *Hate Crime Guidelines and Training Manual* was developed to assist law enforcement agencies in establishing a hate crime training program to allow personnel to collect and submit hate crime data to the FBI UCR Program. The manual provides suggested model reporting procedures and training aids for capturing the bias-motivated incident data reported to the FBI. The FBI UCR Program is currently revising this document to remove all Summary Reporting System (SRS) verbiage and adding all federal and tribal law enforcement offenses. The SRS collected hate crime data on 13 offenses versus the 70 offenses collected in the NIBRS. The manual is located on the FBI.gov website at: https://www.fbi.gov/file-repository/ucr/ucr-hate-crime-data-collection-guidelines-training-manual-02272015.pdf/view.

The FBI UCR Program finalized a 2021 Hate Crime Outreach and Communications Plan with a focus on most-in-population law enforcement agencies (over 100,000 inhabitants) and college/university law enforcement agencies. Through the NIBRS transition, the FBI UCR Program anticipates hate crime participation to improve over the next few years as agencies continue to transition to incident-based reporting.

In 2021, the FBI UCR Program also published a hate crime article titled, *Hate Crime Data Helps Law Enforcement Address Threat.* This article was published in the *CJIS Link* on the FBI.gov website at: https://www.fbi.gov/services/cjis/cjis-link/hate-crime-data-helps-law-enforcement-address-threat. The *CJIS Link* article informs readers of the serious nature of hate crimes across the United States.

In addition, the FBI UCR Program developed a hate crime flyer containing the bias motivation categories for law enforcement officers to reference while investigating bias-related incidents. The flyer is made available to stakeholders during FBI Criminal Justice Information Services Division conferences, Department of Justice Civil Rights trainings, and FBI UCR Program hate crime trainings.

The FBI UCR Program offers a training program for the law enforcement community via webinars. During these training sessions, the FBI provides an overview of the hate crime statistics collection and hate crime scenarios, the two-tiered decision-making process, bias motivation indicators, and discusses the importance and benefits of reporting hate crime incident data (increases understanding, long-range planning, promotes transparency, information sharing, and address threats). These instructional opportunities allow FBI staff to meet with the law enforcement community from reporting agencies. The training emphasizes the need and benefits of the Hate Crime Statistics Collection, and in turn encourages participants to discuss this important topic with law enforcement colleagues within their local agencies and communities. The overall goal is to increase participation in this data collection.

28. In April 2019, the FBI created the Domestic Terrorism-Hate Crimes Fusion Cell at FBI Headquarters in Washington, D.C., "to address the intersection of the complementary FBI missions to combat domestic terrorism and provide justice to those who are victims of hate crimes." The Fusion Cell is "[c]omprised of subject matter experts from both the Criminal Investigative and Counterterrorism Divisions" and "offers programs coordination from FBI Headquarters." It "helps ensure seamless information sharing across divisions and augments investigative resources to combat the domestic terrorism threat, ensuring [the FBI is] not solely focused on the current threat or most recent attack, but also looking to the future to prevent the next one."[8]

[8] Michael McGarrity & Calvin Shivers, *Confronting White Supremacy*, Statement Before the House Oversight and Reform Committee, Subcommittee on Civil Rights and Civil Liberties (June 4, 2019), https://www.fbi.gov/news/testimony/confronting-white-supremacy.

During this hearing, you testified that the Fusion Cell seeks to bring together people focusing on "crimes [that] could fit either into a domestic terrorism bucket or a hate crimes bucket," "with the goal of trying to be proactive against some of the threats that are coming."[9]

a. Please provide a detailed explanation of the work the Fusion Cell has done since it was established in April 2019, including a summary of the categories of domestic terrorism and bias-motivation cases with which the Fusion Cell has been involved and the disposition of these cases.

b. Please describe the operational and analytical capacity of the Fusion Cell, including—

    i. How many agents, analysts, and other staff are assigned to the Fusion Cell;

    ii. When the Fusion Cell is activated, deployed, or otherwise involved in a domestic terrorism or hate crime investigation;

    iii. Whether the Fusion Cell engages in interagency coordination, including, but not limited to, the National Security and Civil Rights Divisions at the Department of Justice, U.S. Attorney offices, and the Department of Homeland Security; and,

    iv. Whether the Fusion Cell partners with state and local law enforcement agencies and community organizations, and, if so, in which jurisdictions.

c. When the FBI investigates bias-motivated violence as a hate crime, does the FBI also investigate the potential scope of the threat posed by the alleged offender, including, but not limited to, whether the alleged offender is also a domestic violent extremist, including a racially- or ethnically-motivated violent extremist, and whether the alleged offender has ties to racially- or ethnically-motivated violent extremist groups or organizations?

    i. If so, please describe the statutory and investigatory tools the FBI uses to assess the potential scope of the threat posed by an alleged hate crime offender. In addition, please describe the subsequent steps the FBI takes upon making a determination that the alleged offender presents a domestic terrorism threat.

    ii. If not, please explain why not.

[9] *Oversight of the Federal Bureau of Investigation: The January 6 Insurrection, Domestic Terrorism, and Other Threats*, *Hearing Before the S. Committee on the Judiciary*, 117th Cong. 37:18-38:3 (2021) (statement of Hon. Christopher Wray, Dir., Fed. Bureau of Investigation) ("Wray testimony").

d. When state and local law enforcement investigate bias-motivated violence as a hate crime, is the FBI consulted, brought in, or otherwise involved to assist state and local law enforcement investigate the potential scope of the threat posed by the alleged offender, including, but not limited to, whether the alleged offender is also a domestic violent extremist, including a racially- or ethnically-motivated violent extremist, and whether the alleged offender has ties to racially- or ethnically-motivated violent extremist groups or organizations?

    i. If so, please describe how the FBI assists state and local law enforcement in assessing the potential scope of the threat posed by an alleged hate crime offender. In addition, please describe the subsequent steps the FBI takes, with or without state and local law enforcement, upon making a determination that the alleged offender presents a domestic terrorism threat.

    ii. If not, please explain why not.

Response: Hate crimes and DT incidents are often not mutually exclusive. A hate crime is targeted violence motivated by the offender's bias against a person's actual or perceived characteristics, while a DT incident is a criminal act, including threats or acts of violence made to specific victims, made in furtherance of a domestic socio-political goal. To address the intersection of the FBI counterterrorism and criminal investigative missions to combat DT and provide justice to those who are victims of hate crimes, the FBI formally created the Domestic Terrorism-Hate Crimes Fusion Cell in April 2019.

The Fusion Cell creates more opportunities for investigative creativity, provides multi-program coordination, helps ensure seamless information sharing, and enhances investigative resources to combat the DT threat. The Fusion Cell is a standing entity that covers all DT threat categories and does not need to be "activated" for it to function. The Fusion Cell has had significant successes. For example, in November 2019, the work of the Fusion Cell resulted in the arrest of Richard Holzer, a Colorado man who ultimately pleaded guilty and was sentenced to over 19 years in prison for federal hate crime and explosives charges for plotting to blow up a synagogue in Pueblo, Colorado. This was the first time in recent history that the FBI made a proactive arrest on a federal hate crimes charge.

QUESTIONS FROM SENATOR GRAHAM

Vladimir Kara-Murza, a prominent opposition activist in Russia, was poisoned in Russia in 2015 and again in 2017, and nearly died on both occasions. Following both poisonings, samples of his blood were accepted for testing by the FBI, and tests were performed, but the results of those tests and the FBI's assessment of the cause of Mr. Kara-Murza's poisonings have not been released to either interested Members of Congress or Mr. Kara-Murza. On July 5, 2018, Mr. Kara-Murza submitted a request pursuant to the Freedom of Information Act and Privacy Act (FOIPA) to the FBI (FBI FOIPA Request No. 1410820-000) for documents relating to his poisonings, including the results of tests performed by U.S. government agencies. Mr. Kara-Murza has been informed that 277 pages of documents responsive to that request have been referred by the FBI for review to other, undisclosed agencies of the federal government. Of those 277 pages, 251 have yet to be released to Mr. Kara-Murza pending consultation with other government agencies. Additionally, 15 pages of responsive documents have been withheld from disclosure by the FBI on varying grounds, including that they contain classified information. A further 562 pages that were released by the FBI have been redacted.

29. In January 2018, or at any other time, did you, or any other official of the Department of Justice, discuss Mr. Kara-Murza or his poisonings with Sergey Naryshkin, Alexander Bortnikov or Igor Korobov?

Response: The FBI Lab has essentially exhausted its capabilities and has been unable to identify the specific poison or compound that was utilized on Mr. Kara-Murza. Additional testing conducted at the FBI Lab for potential agents and known variants utilized in other high-profile incidents also yielded negative results. The Lab has preserved the remaining sample to allow for further testing at a facility with capabilities/certifications exceeding those currently available at the FBI Lab. That said, the FBI's Washington Field Office has already relayed this information to Mr. Kara-Murza personally and has made it known that they will do what they can to get him a copy of the full FBI Lab report as soon as its completed.

The FOIA litigation is ongoing, so all exemptions and actions are still subject to change. The documents released, to this point, were not particularly heavily redacted. The most substantial redactions are of: (1) classified information/intelligence source and method information protected by the National Security Act of 1947; and (2) information that would identify confidential source(s) and/or any information provided by such a source. There were other exemptions cited, including for privacy and law enforcement sensitive information.

QUESTIONS FROM SENATOR LEE

30. Director Wray, can you please tell us how the FBI is obtaining the geolocation and cell phone data of Americans who were in DC on January 6th?

Response: The FBI has only sought January 6th-related geolocation and cell phone data through legal process, including, as appropriate, search warrants, grand jury subpoenas, and statutorily authorized emergency disclosures.

31. What specific authorities is the FBI relying on to access this data?

Response: Please see the response to question 30.

32. Has the FBI obtained probable cause warrants to secure this data?

Response: Please see the response to question 30.

33. Is the FBI using facial recognition technology to identify Americans who were in DC on January 6th? If so, what authority is the FBI relying on to employ this technology against American citizens?

Response: The FBI's Facial Recognition (FR) technology is limited to producing investigative leads; no identifications are made. FR results are prohibited by FBI guidelines for use as the sole basis of an arrest or other law enforcement activity.

34. If you cannot answer these questions because of the nature of the ongoing investigation, will you commit to attending a classified briefing on these issues?

Response: The FBI has deployed its full investigative resources in response to the attack on the U.S. Capitol on January 6th, and as part of the investigations, the FBI has used location data and FR technology. The FBI has only sought or accessed January 6th-related geolocation and cell phone data through legal process, including, as appropriate, search warrants, and statutorily authorized emergency disclosures. As has been disclosed in public charging documents, geolocation data has been cited as a way that the FBI has been able to corroborate other information – such as a tip from the public based on the FBI's "Seeking Information" posters – about a person's participation in the attack. In the process of obtaining cell tower data, the FBI uses what is sometimes referred to as an "exclusion list" to sift out mobile devices authorized to be in a location in order to focus on those devices that were unauthorized, and therefore more likely to be related to the breach.

The FBI practices highly responsible use of FR technology and remains committed to privacy and civil liberties protections in its use. FBI internal policy prohibits the results of FR searches to be used as the sole basis of an arrest, positive identification, or other law enforcement action. The FBI only relies upon FR results for "lead" information that requires further investigation to determine if the person identified is, in fact, the subject associated with the investigation. FR technology has assisted the FBI and authorized law enforcement users in

identifying, arresting, and convicting dangerous criminals and terrorists, locating missing and endangered children, and protecting our nation's borders.

QUESTIONS FROM SENATOR BOOKER

35. Our nation is confronting a rising national security threat in domestic terrorism perpetrated by white supremacists and other far-right extremists. We know the majority of terror attacks in this country since 9/11 have been perpetrated by right-wing extremists, and the majority of those have been white supremacists.

    When you last testified before this Committee in 2019, you said that "a majority of the domestic terrorism cases that we've investigated are motivated by some version of what you might call white supremacist violence." And at last week's hearing, you testified, "I elevated racially motivated violent extremism, the vast majority of which is what you would call white supremacist violence, to our highest threat priority, where it has stayed."

    a. Given your testimony that the "vast majority" of "racially motivated violent extremism" incidents are perpetrated by white supremacists, can you provide a more specific breakdown of exactly what a "vast majority" means?

Response: In Fiscal Year 2020, the FBI, along with law enforcement partners, arrested 180 DT subjects, and 84 of those arrests were of RMVE subjects. Of those 84, 75 arrests – representing the vast majority – were of RMVEs advocating for the superiority of the white race.

    b. Can you provide this Committee with data regarding the number of domestic terrorism incidents perpetrated by white supremacists, including relative to all categories of domestic terrorism incidents and relative to the FBI's category of "Racially or Ethnically Motivated Violent Extremist" incidents?

    c. According to the FBI's data, how many violent attacks, and how many fatalities, since 2000 are attributable to "Racially or Ethnically Motivated Violent Extremists"?

    d. According to the FBI's data, how many violent attacks, and how many fatalities, since 2000 are specifically attributable to white supremacists?

    e. What steps have you taken to elevate the FBI's efforts to address the threats posed by "Racially or Ethnically Motivated Violent Extremism"?

Response: Between 2015 and 2020, there have been at least 26 fatal attacks perpetrated by DVEs, resulting in a total of 83 deaths, as follows:

- RMVEs were responsible for 19 attacks, resulting in 72 deaths. Of those: 11 attacks and 52 deaths were the result of attacks perpetrated by RMVEs who advocate for the superiority of the white race; and 8 attacks and 20 deaths were the result of attacks perpetrated by RMVEs motivated by racism and injustice in American society, the desire for a separate Black homeland, or religion-themed reasons.

- AGAAVEs were responsible for 5 attacks, resulting in 5 deaths. Of those: 3 attacks and 3 deaths were the result of attacks perpetrated by MVEs; one attack and one death were the result of an attack perpetrated by SCVEs; and one attack and one death was the result of an attack perpetrated by an AVE.

- An Abortion-Related Violent Extremist was responsible for one attack and 3 deaths.

- A DVE with a personalized violent extremist ideology ("All Other DT Threats") was responsible for one attack and 3 deaths.

f. Beyond those actions, what steps have you taken to elevate the FBI's efforts to address the threats posed by white supremacist violence specifically?

Response: In June 2019, the FBI elevated the RMVE threat to the highest threat priority, on the same level as the Islamic State of Iraq and al-Sham (ISIS) and Homegrown Violent Extremists (HVEs). This designation means that all 56 FBI Field Offices are required to collect and distribute intelligence on RMVE threats and to produce intelligence products on trends they are seeing in this realm. Elevating the threat has had a positive impact on disruptions. Since 2019, arrests in the RMVE threat category have nearly doubled, and nearly every FBI Field Office has an ongoing investigation in this category.

36. During the Trump Administration, the FBI changed the way it classified and tracked domestic terrorism incidents. Violent incidents involving white supremacists were folded into a catch-all category of "Racially or Ethnically Motivated Violent Extremists." This change would seem to make it harder to track incidents of violence perpetrated by white supremacists and potentially obscure the seriousness of that threat. Chair Durbin and I, as well as other members of this Committee, have written a number of letters to you raising this issue over the last two years, including most recently in a letter signed by 10 members of this Committee on February 24, 2021.

    a. Why did the FBI change its longstanding approach to tracking domestic terrorism incidents involving white supremacist violence and fold them into the broader category of "Racially or Ethnically Motivated Violent Extremist" incidents?

    b. When this change was made during the Trump Administration, did anyone at the White House direct, request, or suggest that the FBI eliminate the white supremacist category?

    c. When this change was made during the Trump Administration, did anyone at the Department of Justice direct, request, or suggest that the FBI eliminate the white supremacist category?

    d. Which official(s) directed the FBI to reorganize its domestic terrorism threat categorizations?

e. Can you make a commitment to review this classification system for domestic terrorism incidents, rescind it, and reinstate the longstanding practice of tracking white supremacist violence as a distinct category of domestic terrorism incidents?

Response: Since 2018, the FBI has used the term "Racially or Ethnically Motivated Violent Extremism," (RMVE) because it focuses on the violence and motivation, not First Amendment-protected activity. This change was made as part of the FBI's annual Threat Review and Prioritization (TRP) process. The large majority of the FBI's RMVE investigations involve RMVEs who advocate for the superiority of the white race; but there are some RMVE threat actors who use political reasons – including racism or injustice in American society, the desire for a separate Black homeland or starting a "race war," or draw on aspects of religion, including elements of Christianity, Islam, and Judaism – as justification for their use or threat of force or violence. Integrating all types of racially or ethnically motivated violence into one threat category allows FBI Field Offices the latitude to collect intelligence and allocate resources to combat all RMVE threats, regardless of ideological motivation. More importantly, the FBI's internal threat-naming conventions do not dictate what Domestic Terrorism agents investigate; instead, the intelligence and violent criminal conduct dictates what is investigated. The FBI will continue to challenge, review, and evaluate intelligence to ensure it is appropriately identifying and categorizing threats.

37. In February 2020, you testified before the House Judiciary Committee that hate crimes are "a close cousin of domestic terrorism." From an investigative perspective, what is the relationship between hate crimes and domestic terrorism? What steps has the FBI taken to specifically target the linkages between the two and combat these terrible acts?

Response: Hate crimes and DT incidents are often not mutually exclusive. A hate crime is targeted violence motivated by the offender's bias against a person's actual or perceived characteristics, while a DT incident is a criminal act, including threats or acts of violence made to specific victims, made in furtherance of a domestic socio-political goal. To address the intersection of the FBI counterterrorism and criminal investigative missions to combat DT and provide justice to those who are victims of hate crimes, the FBI formally created the Domestic Terrorism-Hate Crimes Fusion Cell in April 2019.

The Fusion Cell creates more opportunities for investigative creativity, provides multi-program coordination, helps ensure seamless information sharing, and enhances investigative resources to combat the DT threat. The Fusion Cell has had significant successes. For example, in November 2019, the work of the Fusion Cell resulted in the arrest of Richard Holzer, a Colorado man who ultimately pleaded guilty and was sentenced to over 19 years in prison for federal hate crime and explosives charges for plotting to blow up a synagogue in Pueblo, Colorado. This was the first time in recent history that the FBI made a proactive arrest on a federal hate crimes charge.

38. According to a recent FBI report, hate crimes increased by almost 20 percent during the Trump Administration. The same report also noted that hate-motivated murders—mostly perpetrated by white supremacists—climbed to their highest level in 28 years. In your

assessment, what factors account for this dramatic increase in hate crimes during the years of the Trump Administration?

Response: In 2019, the FBI and DHS assessed RMVEs, primarily those advocating for the superiority of the white race, likely would continue to be the most lethal DVE threat to the Homeland. Both agencies had high confidence in this assessment based on the demonstrated capability of RMVEs in 2019 to select weapons and targets to conduct attacks, and the effectiveness of online RMVE messaging calling for increased violence. Additionally, other DVEs likely would continue to engage in non-lethal violence and other criminal activity, and DVE reactions to socio-political events and conditions could increase attacks. The year 2019 represented the most lethal year for DVE attacks since 1995, with five separate DVE attacks resulting in 32 deaths, 24 of which occurred during attacks conducted by RMVEs advocating for the superiority of the white race. Themes like "gamification" and "accelerationism" partly inspired some of the attacks in 2019 and likely will continue to inspire future plots. Gamification is a term where fatality counts in attacks are referred to as "scores," as the actor desires to accomplish "achievements" or high kill counts. Messaging from RMVEs espousing the superiority of the white race has furthered this narrative by framing previous attacks as resulting in a "score." Additionally, widely disseminated propaganda on online forums and encrypted chat applications that espouse similar themes regarding kill counts could inspire future attackers to mobilize faster or attempt increasingly lethal and more sophisticated attacks. These online forums and chat applications also reference accelerationism, a belief amongst some neo-Nazi and/or fascist RMVEs that the current system is irreparable, without apparent political solutions, and hence violent action is needed to precipitate societal collapse to start a race war.

39. At the hearing, we discussed the diversity of the FBI's workforce, and you indicated that you would be willing to provide specific information to the Committee after the hearing. Please provide aggregate data about diversity at the FBI at the following levels:

    a. Applications to work at the FBI;

    b. The overall FBI workforce;

    c. By branch, division, and/or office, as available; and

    d. The FBI's leadership.

    Please provide data, if available, about how these numbers have changed from 2000 to present.

Response: The FBI appreciated the opportunity to provide a briefing to your office on diversity, which is a Director Priority Initiative. Four years ago, extensive data analysis showed the diversity of the FBI's Special Agent cadre lagged significantly behind the nation's demographics. Since this time, the FBI has spent considerable time and effort to identify and remove any inadvertent barriers that could result in disparate treatment of female and minority candidates. For example, the FBI significantly revised the Special Agent recruitment process, mitigated risks of disparate impact of testing on candidates, and helped candidates be better

prepared for the process. As a result, in 2020, 44% of the FBI's Special Agent applicants were minorities. In 2020, 26.6% of the FBI's workforce were minorities; 31.9% of professional staff employees were minorities; 22.8% of intelligence analyst employees were minorities; and 18.6% of Special Agent employees were minorities. As of 2020, 13.8% of the FBI's leaders in Senior Executive Service were minorities. The FBI will continue to use technology- and date-driven strategies to strengthen its recruiting and hiring program to ensure a full-staffed and diverse workforce.

QUESTIONS FROM SENATOR GRASSLEY

40. News reports have suggested that after the attack on January 6, the FBI acquired electronic records from people at the scene. Reportedly, that included members of Congress given their proximity to the event. Are those news reports accurate and, if so, has the FBI acquired the content of those communications or is the data limited to location data?

Response: The FBI has deployed its full investigative resources in response to the attack, and as part of the investigations, the FBI has used location data. The FBI has only sought or accessed January 6th-related location data through legal process, including, as appropriate, search warrants, grand jury subpoenas, and statutorily authorized emergency disclosures. Given that this question relates to hundreds of ongoing investigations and pending prosecutions, it would be inappropriate to provide further information at this time.

41. At a Rules and Homeland Security Committee hearing, witnesses testified that they believed the January 6 attack was "coordinated." Do you agree that it was coordinated beyond small groups? In the context of an attack like this, what does "coordinated" mean? For example, how many attackers communicated with each other before and during the attack?

Response: These investigations are on-going, but the FBI has seen indications of some small cells of individuals alleged to have been conspiring and communicating with each other prior to their involvement in the attack. According to publicly available court documents, the Department of Justice has charged a number of defendants involved in the attack on the U.S. Capitol with conspiracy, either to obstruct a congressional proceeding, to obstruct law enforcement during a civil disorder, and/or to injure an officer. In order to protect the integrity of all investigations, as a general policy and practice, the FBI does not comment on the status or existence of any potential investigative matter. Given that this question relates to hundreds of ongoing investigations and pending prosecutions, it would be inappropriate to provide further information at this time.

42. As you know, the FBI operates approximately 200 Joint Terrorism Task Forces (JTTF) within the U.S. These Task Forces are our nation's front line of defense against terrorism, both international and domestic, and exist to coordinate and share information with local, state and federal law enforcement. How many of these Task Forces issued joint intelligence bulletins warning of the possibility for unrest at the Capitol on January 6, 2021.

Response: Throughout 2020, the FBI issued multiple external intelligence products, including multiple Joint Intelligence Bulletins (JIBs), to federal, state, and local partners. These products contained the FBI's assessment and warning of credible threats of violence from DVEs related to the election and the transition process, the elevated threats posed by AGAAVEs, and the potential for DVEs to exploit First Amendment-protected activities. However, there was no JIB published specific to the possibility for unrest at the U.S. Capitol on January 6 2021.

43. What type of mutual aid agreements does the FBI have with other law enforcement agencies in the National Capitol Region? Are these mutual aid agreements sufficient as they are currently written?

Response: The FBI maintains strong liaison relationships with local partners and provides specialized response to incidents when partner agencies request authorized assistance.

44. What is the total number of FBI international terrorism investigations, homegrown violent extremism investigations, and domestic terrorism investigations? In addition, please answer the following:

    a. Of terrorism investigations of all types, how many are white supremacists?

    b. Of terrorism investigations of all types, how many are jihadists?

    c. How many investigations are classified as antigovernment extremists?

    d. How many as anarchist extremists?

Response: The FBI is conducting approximately 4,000 international terrorism (IT) investigations and approximately 2,700 DT investigations; approximately 1,000 of the IT investigations involve HVE subjects. Of the DT investigations, approximately:

- 18 percent involve RMVEs, with more than 80 percent involving RMVEs who advocate for the superiority of the white race;
- 34 percent involve AGAAVEs, with approximately: 16 percent involving SCVEs, 32 percent involving AVEs, and 51 percent involving MVEs;
- Less than one percent involve Animal Rights/Environmental Violent Extremists;
- Less than one percent involve Abortion-Related Violent Extremists;
- 11 percent involve "All Other DT Threats"; and
- 34 percent involve civil unrest or antiriot laws.

45. During yours and AD Jill Sanborn's testimony the following day, you each repeatedly said that "some" white supremacists were involved in the Capitol riot. When the FBI opens an investigation, it captions a case with certain numbers and letter combinations that track the type of investigation. A caption of "266" refers to a domestic terrorism investigation. A caption of 266H refers to antigovernment extremism. A caption of 266N refers to white supremacism. How many 266H and how many 266N subjects do you have from the Capitol riot?

Response: As of April 2022, of the approximately 775 subjects arrested for their participation in the violent unlawful entry of the Capitol on January 6th, more than 55 percent require additional investigation to determine the primary motivation or ideology. Approximately 26 percent are categorized as AGAAVEs, under 17 percent are categorized as "All Other DT Threats," and approximately two percent are categorized as RMVEs who advocate for the superiority of the white race.

46. How many Capitol rioters were armed?

Response: The FBI has arrested multiple subjects who unlawfully entered the U.S. Capitol with weapons such as bear spray, Tasers, and other weapons of opportunity, including a crutch and a fire extinguisher. Since January 6th, but stemming from the events of that day, at least four subjects have been arrested for federal firearms charges, including: unlawful possession of a firearm on Capitol Grounds/Building; possession of an unregistered firearm; possession of unregistered ammunition; and possession of large capacity ammunition feeding devices. Investigations are on-going and additional subjects may be charged with firearms violations. In order to protect the integrity of all investigations, as a general policy and practice, the FBI does not comment on the status or existence of any potential investigative matter. Given that this question relates to hundreds of ongoing investigations and pending prosecutions, it would be inappropriate to provide further information at this time.

47. You said in your hearing testimony that the Capitol riot was domestic terrorism. I agree. Were the months of attacks on the Portland courthouse domestic terrorism? Were the federal offenses charged in Portland limited to vandalism?

Response: Regardless of ideology, the FBI will aggressively pursue those who seek to hijack legitimate First Amendment-protected activity by engaging in violent criminal activity such as the destruction of property and violent assaults on law enforcement officers that occurred on January 6th and during protests throughout the U.S. during the summer of 2020. The majority of the investigations the FBI has opened related to the unrest during the summer of 2020 are being handled as DT investigations through the JTTFs and worked with the same dedication and comprehensive approach that the FBI brings to all of investigations. Related to the unrest in Portland, Oregon, the FBI continues to investigate violations of federal law within the FBI's purview, specifically focusing on violent actors using the civil unrest to mask their activities. The FBI arrested multiple individuals involved in violence and federal criminal activity in Portland during the summer of 2020 for charges including assaulting a federal officer and destruction of federal property.

48. In response to my questioning, you indicated that you are taking steps to improve your anarchist extremism program, including developing sources and a better understanding of tradecraft. Specifically, what steps have you taken to improve this program?

Response: The FBI continues to improve its understanding of DT subjects, including those categorized as AVEs, a subset of the AGAAVE threat category. The AGAAVE threat category is a top priority for the FBI, and thus all Field Offices are required to proactively work to better understand the threat in the office's area of responsibility, identify intelligence gaps, and

investigate associated violence and criminal activity. Based on an assessment of increasing violent criminal activity from AVEs, the FBI has increased its national targeting efforts and is further leveraging human and technical sources to address this threat. For example, to obtain information about the threat and address intelligence gaps, FBI Field Offices have issued multiple Collection Priorities Messages recommending their squads proactively canvass their confidential human sources to collect threat reporting related to violence and criminal activity.

49. The Trump administration is the first to designate a foreign white supremacist group as terrorists: the Russian Imperial Movement. Further, the Trump Administration added the threat from domestic terrorism including racially motivated violent extremists in the 2018 updated National Strategy for Counterterrorism. Under the Trump administration in 2019, the FBI first moved white supremacist extremism to top threat status, with homegrown violent extremism and the Islamic state. Until that time, only the threat from jihadists had been rated a top threat. Is it accurate to say that no resources were decreased from fighting white supremacism during the Trump Administration?

Response: In June 2019, the FBI elevated the RMVE threat to the highest threat priority, on the same level as the Islamic State of Iraq and al-Sham (ISIS) and Homegrown Violent Extremists (HVEs). This designation means that all 56 FBI Field Offices are required to collect and distribute intelligence on RMVE threats and to produce intelligence products on trends they are seeing in this realm. Elevating the threat has had a positive impact on disruptions. Since 2019, arrests in the RMVE threat category have nearly doubled, and nearly every FBI Field Office has an ongoing investigation in this category.

The FBI currently has multiple units singularly focused on tackling the DT threat at all levels from the operational, strategic, and analytical perspectives. The FBI continues to evaluate and reallocate resources in the Counterterrorism Division at FBI Headquarters to meet any evolving operational needs and focus on the most significant terrorism threats, including DT. The FBI conducts regular strategic threat assessments to prioritize and allocate resources in a dynamic fashion.

The number of DT investigations has increased steadily over the past several years, and after the events of January 6th, the number of investigations has grown exponentially. In the last year alone, the number of domestic terrorism investigations has doubled. The FBI does not anticipate this phenomenon waning in the near term. The FBI has done what it can to address the increased volume internally by surging personnel from other critical counterterrorism, national security, and criminal areas. In 2021, the surge accounted for a 260% increase in DT personnel.

50. In questioning the day after your testimony, AD Sanborn indicated the FBI does not review public source information in domestic terrorism investigations. It seems this would seriously hamper the FBI's ability to detect riots before they occur and that this likely contributed to the FBI's inability to foresee the 2020 riots and the Capitol riot. I understand that the Privacy Act prohibits the collection of information that is not for a criminal investigation. However, I do not understand the text to restrict the FBI's ability to look for evidence of public criminal activity. It seems in order to comply with the law,

the FBI should not collect open source information that is irrelevant to a crime, but would still be free to look on the internet for evidence of potential criminality. Please describe the steps you are taking to ensure agents can review public source information for evidence of crimes such as organizing and incitement to riot.

Response: The *Attorney General's Guidelines for Domestic FBI Operations* (AGG-DOM) establishes a set of basic principles that serve as the foundation for all FBI mission-related activities, including online investigations. The AGG-DOM prohibits the FBI from "investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States."

In accordance with those guidelines, the FBI may review, observe, and collect information from open sources as long as the FBI activities are done for a valid law enforcement or national security purpose and in a manner that does not unduly infringe upon the speaker's or author's ability to deliver his or her message. The FBI does not have the authority to persistently and passively examine the World Wide Web, Internet traffic, and social media conversations. The core requirement is that the authorized purpose must specifically be tied to federal criminal or national security purposes, usually to further an FBI assessment or predicated investigation, with due regard to the First Amendment.

51. I noticed that your written testimony for this hearing was similar to written testimony used in the Worldwide Threats hearings at the end of last year. However, you removed a written reference to China as a serious threat (though you alluded to this threat verbally). Is China a serious national security threat?

Response: There is no country that poses a more severe counterintelligence threat to the United States than China. The FBI has active investigations across all 56 field offices and a new investigation is opened approximately every 12 hours. The counterintelligence threat from China is a whole-of-government approach, wherein professional intelligence services as well as non-traditional collectors, Chinese companies, and Chinese R&D entities collect sensitive information, acquire technology, and conduct malign foreign influence activities to pursue China's economic, technology, military, and diplomatic goals. Recent Chinese economic espionage cases indicated that China seeks to acquire U.S. science and technology by stealing the material. Some examples include self-driving car schematics stolen from Apple, integrated circuits stolen from Analog Devices, and turbine data files stolen from General Electric.

QUESTIONS FROM SENATOR HAWLEY

52. In its investigation of the January 6 riot, has the FBI solicited in any way any customer information from Bank of America or any other financial institution including, but not limited to, customer names or transaction histories?

Response: The FBI has deployed its full investigative resources in response to the attack, and one aspect within the investigations is if, and how, the attacks were funded. The FBI is using lawful methods in its investigations, and there has been no sweeping collection of financial records or any voluntary disclosure of financial records outside established lawful processes.

Financial institutions are regulated by the Bank Secrecy Act, which legally obligates those institutions to know their customers and report suspicious activity via the Suspicious Activity Report (SAR) process. The USA PATRIOT Act expanded the SAR requirements to help combat domestic and global terrorism. Because of these obligations, and the potential for terrorists and criminals to use and misuse the financial system, the FBI routinely engages with the financial sector to educate them on the threats they face to help them better monitor their data and customer activity for what they determine to be suspicious activity.

In order to protect the integrity of all investigations, as a general policy and practice, the FBI does not comment on the status or existence of any potential investigative matter. Given that this question relates to hundreds of ongoing investigations and pending prosecutions, it would be inappropriate to provide further information at this time.

53. In its investigation of the January 6 riot, has the FBI requested customer information from Bank of America or any other financial institution as part of a formal inquiry such as a subpoena or search warrant as outlined in 12 U.S. Code § 3402?

Response: Please see the response to question 52.

54. If the FBI has obtained financial records from Bank of America or any other financial institution pursuant to a warrant, subpoena, or other legal process, please provide a copy of the legal process or, in the alternative, please reproduce verbatim the request(s) in the legal process to which the financial records were responsive.

Response: Please see the response to question 52.

55. Please describe with specificity the categories of any financial records, as defined in 12 U.S. Code § 3401(2), that the FBI has obtained from Bank of America or any other financial institution in conjunction with its investigation of the January 6 riot, and the number of Bank of America customers, or the customers of any other financial institution, whose financial records were provided to the FBI.

Response: Please see the response to question 52.

56. Has the FBI notified any Bank of America customers or customers of other financial institutions that they may have been subjects of investigation in conjunction with the January 6 riot? If so, how many?

Response: Please see the response to question 52.

57. What other consumer-facing retail institutions, technology platforms, or telecommunications companies has the FBI corresponded with regarding its investigations of the riot at the U.S. Capitol on January 6th or security activities in preparation for the Inauguration?

Response: The FBI maintains strong private sector partnerships and ongoing communications regarding threats, violence, and malign foreign interference. The FBI routinely engages with the technology sector to educate them on threats, and the events of January 6th and the lead-up to the Inauguration are no different. In order to protect the integrity of all investigations, as a general policy and practice, the FBI does not comment on the status or existence of any potential investigative matter. Given that this question relates to hundreds of ongoing investigations and pending prosecutions, it would be inappropriate to provide further information at this time.

58. Has the FBI notified any telecommunications company customers that they may have been the subject of investigation in conjunction with the January 6 riot? If so, how many?

Response: In order to protect the integrity of all investigations, as a general policy and practice, the FBI does not comment on the status or existence of any potential investigative matter. Given that this question relates to hundreds of ongoing investigations and pending prosecutions, it would be inappropriate to provide further information at this time.

59. What call logs or metadata, if any, has the FBI sought through legal process or otherwise collected from telecommunications company customers in conjunction with the January 6 riot?

Response: The FBI has deployed its full investigative resources in response to the attack, and as part of the investigations, the FBI has used telecommunications data. The FBI has only sought or accessed January 6th-related telecommunications data through legal process, including, as appropriate, search warrants, grand jury subpoenas, and statutorily authorized emergency disclosures. Given that this question relates to hundreds of ongoing investigations and pending prosecutions, it would be inappropriate to provide further information at this time.

QUESTIONS FROM SENATOR WHITEHOUSE

60. Who would be the most knowledgeable about the supplemental background investigation for then-Judge Brett Kavanaugh, particularly any communication with the White House?

Response: The FBI serves as an investigative service provider (ISP) for federal background investigations (BI). This means that the FBI responds to requests from the Office of White House Counsel and other government entities to conduct BIs of candidates for certain positions. The FBI, as an ISP, provides the collected information to the requesting entity to assist the entity in its decision-making process concerning the candidate's suitability for federal employment and access to classified or sensitive information. The FBI division responsible for conducting BIs is the Security Division.

With regard to positions requiring Senate confirmation, the FBI follows the standard process established pursuant to a March 2010 memorandum of understanding (MOU) between the Department of Justice and the White House. That process requires the FBI to promptly notify the requesting entity if it becomes aware of new information (received prior to a candidate assuming a nominated position) that raises questions of the candidate's suitability or trustworthiness.

Serving in its ISP role, the FBI conducted then-Judge Kavanaugh's background investigation at the request of the Office of White House Counsel in connection with his nomination to serve as an Associate Justice of the Supreme Court of the United States. The BI was completed and results disseminated to the Office of White House Counsel on July 18, 2018. On September 12, 2018, the FBI received information from a Senate office, which the FBI forwarded to the Office of White House Counsel on September 13, 2018, pursuant to the MOU. On September 13, 2018, the FBI was asked by the Office of White House Counsel to conduct supplemental background investigations, specifically, limited inquiries. The FBI completed the limited inquiries on October 4, 2018, and provided the results to the requesting entity.

61. Who would be the most knowledgeable about the information channel provided to Senate Republicans for information about the Crossfire Hurricane investigation?

Response: The Department of Justice under the prior Administration determined it was in the public interest to release to Congress documents and information regarding the Crossfire Hurricane investigation to the extent consistent with national security interests and with the January 7, 2020, order of the Foreign Intelligence Surveillance Court.

62. As of February 26, 2021, more than 280 people have been arrested for their involvement in the insurrection on January 6.[10]

    a. Congress defined domestic terrorism as criminal acts occurring "primarily within" the U.S. that are "dangerous to human life," violate federal or state criminal laws, and "appear … intended" to "influence the policy of a government by

[10] Tal Axelrod, *More than 300 charged in connection to Capitol riot*, The Hill, Feb, 26, 2021, https://thehill.com/policy/national-security/540801-more-than-300-charged-in-connection-to-capitol-riot.

intimidation or coercion." 18 U.S.C. § 2331. How many of the people arrested for their acts on January 6 does the FBI consider "domestic terrorism subjects"? If the answer isn't "all of them," why isn't it?

b. At least 16 people arrested following January 6 appear to have links to the Proud Boys, a racist far-right gang[11] which the FBI has designated as a violent extremist group.[12] At least 10 of the defendants have alleged ties to the Oath Keepers, which the Anti-Defamation League calls an "anti-government right-wing fringe organization."[13] Has the FBI categorized all of those arrests as arrests of "domestic terrorism subjects"? If not, why not?

Response: As of April 2022, of the more than 775 subjects arrested for their participation in the violent unlawful entry of the Capitol on January 6th, more than 55 percent require additional investigation to determine the primary motivation or ideology. Approximately 26 percent are categorized as AGAAVEs, under 17 percent are categorized as "All Other DT Threats," and approximately two percent are categorized as RMVEs who advocate for the superiority of the white race.

These investigations are ongoing, but to date, individuals who self-identify as associated with the Proud Boys and Oath Keepers have been arrested. For example:

- In February 2021, six individuals associated with the Proud Boys were indicted with conspiring to obstruct or impede an official proceeding and to impede or interfere with law enforcement during the commission of a civil disorder, among other charges.

- In February 2021, six individuals associated with the Oath Keepers, some of whose members were among those who forcibly entered the U.S. Capitol on January 6 were arrested for conspiring to obstruct Congress' certification of the result of the 2020 Presidential Election, among other charges.

- In April 2021, two individuals associated with the Oath Keepers were indicted in federal court in the District of Columbia for conspiring to obstruct Congress, among other charges.

Additional information related to the defendants charged in federal court in the District of Columbia related to crimes committed at the U.S. Capitol on January 6, 2021, as well as links to the court documents referenced above and, *inter alia*, related superseding indictments, are available at: www.justice.gov/usao-dc/capitol-breach-cases.

---

[11] *The Capitol Siege: The Arrested And Their Stories*, NPR, Feb. 24, 2021, https://www.npr.org/2021/02/09/965472049/the-capitol-siege-the-arrested-and-their-stories.
[12] *FBI Categorizes Proud Boys As Extremist Group With Ties To White Nationalism*, NPR, Nov. 20, 2018, https://www.npr.org/2018/11/20/669761157/fbi-categorizes-proud-boys-as-extremist-group-with-ties-to-white-nationalism.
[13] *The Capitol Siege: The Arrested And Their Stories*, *supra* note 2.

63. The ATF investigates almost every federal gun or arson case, including many cases that involve violent extremist groups, such as white supremacy violent extremists. For example, in October 2020, an ATF investigation led to the arrest of twenty-four people, including alleged members of the Aryan Circle, a white supremacist prison gang, on charges related to shootings, stabbings and killings in eleven states.[14]

    a. Would the FBI count the ATF's October 2020 arrests of white supremacists as arrests of "domestic terrorism subjects"? If not, why not?

    b. How would the FBI become involved in an ATF investigation of a domestic extremist group?

    c. Should every case involving a violent extremist group be treated as a domestic terrorism case and handled by the FBI Counterterrorism Division? If not, why not?

    d. What steps does the FBI take to ensure that it captures activity by domestic violent extremists that is investigated by other federal law enforcement agencies in order to accurately assess the threat these groups pose?

    e. What steps does the FBI take to ensure that it shares intelligence about domestic violent extremists with other federal law enforcement agencies? What steps does the FBI take to ensure that other federal law enforcement agencies share intelligence about domestic violent extremists with the Bureau?

Response: The FBI works closely with its federal, state, local, tribal, and territorial law enforcement partners to investigate and disrupt domestic terrorism. The front line of the counterterrorism mission in the United States is the FBI-led Joint Terrorism Task Forces (JTTFs). The FBI maintains about 200 JTTFs nationwide across all 56 FBI Field Offices and in many satellite Resident Agencies, with the participation of over 50 federal and over 500 state, local, tribal, and territorial agencies, including the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). The ATF is also a member of the FBI's NJTTF, which serves to enhance communication, coordination, and cooperation between federal, state, and local government agencies by providing a point of fusion for terrorism intelligence and by supporting the JTTFs nationwide. These relationships are critical to effective information sharing and the leveraging of local expertise and experience in FBI investigations.

The eGuardian system is the FBI's case management system for handling initial threat information of counterterrorism, counterintelligence, cyber incidents, criminal complaints, events, and suspicious activities received from federal, state, local, tribal, and territorial law enforcement agencies, and the Department of Defense. Threat information is then migrated to the FBI's internal Guardian system where it is evaluated to determine whether the information meets the criteria for an assessment, already exists in FBI holdings, or is for situational awareness only. Starting in 2019, the FBI implemented a process to specifically identify reports of possible DT incidents to enhance program management and operational oversight. The FBI

[14] Juan A. Lozano, *24 indicted in probe of white supremacist prison gang*, ABC News, Oct. 15, 2020, https://abcnews.go.com/US/wireStory/24-indicted-probe-white-supremacist-prison-gang-73636966.

received approximately 675 referrals of possible DT incidents in 2019. Although reports are not available within the eGuardian system to identify the disposition of each referral, as of 2019, approximately 20 percent of the FBI's DT investigations were opened based on information and referrals from FBI partners.

The FBI does not refer DT incidents where there is an indication of federal criminal activity to other partners, as the FBI would be the lead investigative agency for those matters.