United States Senate Committee On

HOMELAND SECURITY & GOVERNMENTAL AFFAIRS

Chairman Gary Peters

PLANNED IN PLAIN SIGHT

A Review of the Intelligence Failures in Advance of January 6th, 2021

HSGAC Majority Staff Report

June 2023

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 3

II. FINDINGS OF FACT AND RECOMMENDATIONS 7

III. INTRODUCTION 10

IV. FEDERAL AGENCIES' ROLES IN INTELLIGENCE COLLECTION, ANALYSIS, AND DISSEMINATION 13

A. Federal Bureau of Investigation 15
1. FBI Threat Assessment and Information Sharing. 17
2. FBI's role on January 6th. 19

B. Department of Homeland Security 20
1. I&A Threat Assessment and Information Sharing. 21
2. I&A's role on January 6th. 23

C. Multi-Agency Responsibilities 23

V. FEDERAL AGENCIES OBTAINED A LARGE AMOUNT OF INTELLIGENCE INDICATING THE POTENTIAL FOR VIOLENCE ON JANUARY 6TH 26

A. DOJ and FBI 27

B. DHS and I&A 48

VI. FBI AND I&A FAILED TO ISSUE SUFFICIENT WARNINGS ABOUT THE POTENTIAL FOR VIOLENCE ON JANUARY 6TH 53

A. FBI 53
1. FBI issued two limited intelligence documents. 54
2. In lieu of written threat products, FBI-WFO communicated intelligence via informal communications that often downplayed the threat. 59
3. FBI dismissed individual threats as not credible, and failed to fully assess the totality of the threat landscape. 63
4. FBI wrongly focused on the potential for violence between protesters on January 6th rather than the threat to the Capitol. 67
5. After the January 6th attack, FBI and DOJ officials described a clearer picture of the threat, despite their lack of urgent warnings in advance. 70

B. I&A 71
1. I&A issued products about the broader DVE threat nationwide, but did not disseminate reports specific to January 6th. 72
2. Even during the attack on January 6th itself, I&A lacked urgency and failed to effectively share intelligence. 75

3. I&A's experiences in 2020 affected its ability to accurately assess the threat on January 6th. 80

VII. FBI AND I&A FAILED TO FOLLOW THEIR OWN POLICIES AND GUIDELINES TO EFFECTIVELY USE OPEN-SOURCE INTELLIGENCE 82

A. FBI 82
1. FBI leadership mischaracterized the Bureau's authorities to monitor social media. 82
2. FBI personnel conflated agency policies and failed to follow internal procedures for reporting information. 83
3. FBI's change in contracts left it without a key social media monitoring tool just days before the attack. 84

B. I&A 89
1. I&A personnel misinterpreted agency guidance and incorrectly believed they could not report open-source threat information. 89

VIII. LACK OF COORDINATION AMONG FEDERAL AGENCIES CONTRIBUTED TO THE FAILURES ON JANUARY 6TH 91

A. Officials Disagreed as to Which Agency was Designated as the Federal Lead 91

B. DHS Did Not Designate January 6th as a National Special Security Event 96

C. After January 6th, Agency Officials Blamed Each Other for the Failures 99

IX. CONCLUSION 103

I. EXECUTIVE SUMMARY

On January 6, 2021, rioters attacked the U.S. Capitol in an unprecedented effort to disrupt the certification of the 2020 presidential election and our nation's long history of peaceful transitions of power. The attack followed months of repeated and false claims by former President Donald Trump, his lawyers, and certain elected officials, that the presidential election was stolen, culminating in President Trump's call during his speech at the Ellipse in front of the White House on January 6th for his supporters to march to the Capitol. During the violent attack, individuals dragged a police officer into the crowd and beat him, struck another officer with a flagpole attached to an American flag, hit another police officer with a fire extinguisher, and damaged the Capitol Building. Rioters committed hundreds of assaults on law enforcement officers, temporarily delayed the Joint Session of Congress, and contributed to the deaths of at least nine individuals. This attack on our democracy came in the wake of years of increasing domestic terrorism in this country – which top federal law enforcement and national security agencies had previously identified as the most persistent and lethal terrorist threat to the homeland.

In June 2021, this Committee and the Senate Committee on Rules and Administration released a report following a joint investigation on the security, planning, and response failures on January 6th. That report found that agencies tasked with security on January 6th failed to adequately prepare for the Joint Session and quickly respond to the attack. At the direction of U.S. Senator Gary Peters, Chairman of the Homeland Security and Governmental Affairs Committee (HSGAC), Majority Committee staff conducted a subsequent review focused on the intelligence failures leading up to the attack on the U.S. Capitol on January 6th. This investigation found that the breach of the Capitol on January 6th was also the result of a failure by federal agencies to assess and disseminate intelligence about the potential for violence that day.

The intelligence failures in the lead-up to January 6th were not failures to *obtain* intelligence indicating the potential for violence. On the contrary, the two primary domestic intelligence agencies – the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) – obtained multiple tips from numerous sources in the days and weeks leading up to the attack that should have raised alarms. Rather, those agencies failed to fully and accurately assess the severity of the threat identified by that intelligence, and formally disseminate guidance to their law enforcement partners with sufficient urgency and alarm to enable those partners to prepare for the violence that ultimately occurred on January 6th. At a fundamental level, the agencies failed to fulfill their mission and connect the public and nonpublic information they received. Internal emails and documents obtained by the Committee demonstrate the breadth and gravity of the threats these agencies received related to January 6th. For example, FBI and the Department of Justice (DOJ) received tips and information from multiple sources, including:

- In December 2020, FBI received a tip that the Proud Boys planned to be in DC and "[t]heir plan is to literally kill people. Please please take this tip seriously and investigate further."

- On Jan. 3, 2021, FBI also became aware of multiple posts calling for armed violence, such as a Parler user who stated, "[b]ring food and guns. If they don't listen to our words, they can feel our lead. Come armed"; plans to "set up 'armed encampment' on the [National] Mall"; and a tip about "a TikTok video with someone holding a gun saying 'storm the Capitol on January 6th.'"
- On January 4th, DOJ leadership noted multiple concerning posts, including "[c]alls to occupy federal buildings," discussions of "invading the capitol building," and individuals "arm[ing] themselves and to engage in political violence at the event."

In addition to these tips and intelligence, FBI also had the authority (with appropriate restrictions to protect Constitutional rights) to obtain and assess the myriad threats and warnings that were being publicly reported in the press and on social media. Yet while FBI was receiving these and other increasingly concerning reports, internal emails obtained by the Committee demonstrate that the Bureau continued to downplay the overall threat, repeatedly noting that FBI "identified no credible or verified threat."

I&A was also increasingly aware of calls for violence in the days and weeks before January 6th. For example:

- In late December 2020, I&A analysts "identified comments referencing using weapons and targeting law enforcement and the U.S. Capitol building."
- On Dec. 30th, I&A open-source intelligence collectors noted online "[d]iscussions of organizing in Virginia and then driving to DC armed together as the police/military won't be able to stop thousands of armed patriots."
- On Jan. 2, 2021, I&A collectors noted that individuals were sharing a map of the U.S. Capitol Building online, and the I&A collectors messaged each other, "feel like people are actually going to try and hurt politicians. Jan 6th is gonna be crazy," and "[l]ots of discussions of coming armed to DC."

Despite that intelligence, as late as 8:57am on January 6th, a Senior Watch Officer at the DHS National Operations Center wrote "[t]here is no indication of civil disobedience."

FBI and I&A failed to issue sufficient warnings based on the available intelligence indicating January 6th might turn violent. FBI issued only two documents specific to January 6th, both of which were issued by Field Offices the night before the attack, contained only limited raw intelligence, and had limited distribution. This investigation found that in lieu of formal products, FBI communicated intelligence to its partners informally while downplaying the severity of the threat. For example, FBI reported relaying information on calls with its partner agencies, but those agencies reported that on those calls FBI did not issue urgent warnings anticipating violence. This investigation found that part of the reason FBI failed to take more action to warn its federal partners and the public was because it failed to seriously consider the possibility that threatened actions would actually be carried out, and it dismissed each individual threat as not credible in isolation but failed to fully consider the totality of threats and violent rhetoric associated with such a contentious event. FBI also focused on potential clashes between protesters (e.g., the Proud Boys) and counter-protesters (e,g., Antifa) based on its experiences

with previous demonstrations, at the expense of focusing more attention and reporting on the growing threat to elected officials and the Capitol itself.

Similarly, I&A did not issue any intelligence bulletins specific to January 6th, and instead issued only high-level products in 2020 that described general threat trends nationwide. The DHS Office of Inspector General (OIG) and the Government Accountability Office (GAO) found that I&A circulated some intelligence internally but failed to share it with its agency partners, at least in one case because I&A assumed that the U.S. Capitol Police (USCP) was receiving the information from other agencies. Moreover, I&A's mistakes during racial justice demonstrations in 2020 – during which the agency was criticized for over-collecting intelligence on American citizens – resulted in a "pendulum swing" after which analysts were then hesitant to report open-source intelligence they were seeing in the lead-up to January 6th. Internal emails obtained by the Committee also show that even as the attack was unfolding and USCP was urgently requesting intelligence, I&A analysts struggled to assess the credibility of online posts calling for violence at the Capitol. For example, at 2:58pm on January 6th, after a riot had been declared and the Capitol had been locked down, I&A analysts internally noted online chatter that "called for more violent actions but at this time no credible information to pass on has been established."

FBI and I&A have the legal authority to monitor and report on open-source intelligence such as social media, with certain restrictions specific to First Amendment-protected activity – but both agencies failed to follow their own internal guidelines on how to collect and report that information. The Special Agent in Charge of the Intelligence Division at the FBI Washington Field Office on January 6th conflated the Bureau's standards for taking more intrusive investigative action on a tip versus merely reporting it to partner agencies, which was one reason FBI did not share more intelligence it was seeing. GAO also found that FBI employees wrongly concluded that they could not process certain online tips because they determined they were not credible – despite FBI policy requiring every tip to be logged, regardless of credibility. FBI's open-source monitoring capabilities were also degraded mere days before the attack, because the Bureau changed contracts for its third-party social monitoring tool. Internal emails obtained by the Committee show FBI officials were surprised by the timing of the contract change, and lamented the negative effect it would have on their monitoring capabilities in the lead-up to January 6th. Likewise, I&A analysts wrongly believed they could not report the concerning posts they were seeing about potential violence at the Capitol because they did not deem them credible, despite agency guidelines requiring them to report non-credible threat information if it meets other criteria such as providing additional information about a known threat or a risk of violence.

Finally, this investigation found that multiple federal agencies failed to effectively coordinate in the lead-up to January 6th, contributing to the failures that allowed the Capitol to be breached that day. Officials disagreed as to which agency was taking the lead role, with Department of Defense (DOD) officials pointing to DOJ as the lead, but DOJ and FBI officials stated that no agency had been designated the lead. Officials from other agencies also reported confusion about who was in charge. DHS also did not designate January 6th as a National Special Security Event, which it routinely does for significant events and which would have bolstered security and coordination. Furthermore, when asked about what went wrong on

January 6th, officials across agencies passed blame, largely pointing to failures at other agencies for what happened.

To address these failures, FBI and DHS should conduct full internal reviews of their actions in the lead-up to January 6th, improve their processes for assessing and sharing intelligence (including open-source intelligence on social media), designate Joint Sessions of Congress to certify the Presidential election as a National Special Security Event, and improve inter-agency coordination for other significant events, and Congress should review and reform I&A's mission in domestic intelligence. The Committee also faced challenges in obtaining full compliance with its requests, an increasingly regular occurrence across administrations. Congress should reassert its authorities in legitimate oversight of the Executive Branch.

II. FINDINGS OF FACT AND RECOMMENDATIONS

FINDINGS OF FACT

1. **FBI and I&A received numerous early warnings, tips, and other intelligence about plans for violence on January 6th.** Information provided to FBI and I&A included threats of violence and threats to the U.S. Capitol. As early as Dec. 22, 2020, FBI became aware of information about individuals planning for an attack, marching into the Capitol, coming armed, and committing violence. As early as Dec. 21, 2020, I&A noted concerning rhetoric related to January 6th such as online calls to overthrow the government, use weapons against law enforcement, and attack the Capitol.

2. **FBI produced only two limited raw intelligence documents related to January 6th, both issued the night before the attack.** At 6:57pm on January 5th, the FBI New Orleans Field Office issued an Intelligence Information Report that cited intelligence about a specific group planning a Quick Reaction Force in Northern Virginia. At 7:37pm, the FBI Norfolk Field Office issued a Situational Information Report that cited limited, specific online posts with threatening language. FBI did not distribute these documents to all federal partners, and FBI did not issue any products related to January 6th from its Washington Field Office or HQ.

3. **I&A did not issue any intelligence products specific to January 6th, and instead provided only general information on nationwide threats.** In the months leading up to the attack on January 6th, I&A's intelligence products were not specific to January 6th or the U.S. Capitol. I&A published 15 reports in the preceding year, but they were about the general "heightened threat environment" around the country such as broad trends in election-related violence.

4. **Despite claims by some agency officials and analysts, FBI and I&A have authority to monitor open-source intelligence, including social media – and agency guidelines require them to report certain online threats.** DOJ guidance states that certain FBI activities "may involve proactively surfing the Internet" for public information, and FBI guidance further clarifies that agents may "conduct proactive Internet searches." Likewise, DHS guidance allows I&A to collect and report open-source information, including on social media, with protections to safeguard constitutionally-protected activity. I&A collectors may report open-source information if it contains true threats, enhances understanding of a known threat, or demonstrates a risk of violence.

5. **FBI had a contract with a third-party software provider to search and flag potential threats online that expired December 31, 2020, undermining their efforts days before January 6, 2021.** FBI officials raised concerns internally that its contract to identify potential threats on social media expired six days before January 6th, leaving FBI without certain capabilities. Internal communications reveal that FBI officials did not adequately plan for the transition to a new contract, which did not occur until January 1st, days before the attack.

6. **FBI and I&A failed to follow agency guidelines on the use of open-source intelligence.** The Special Agent in Charge of the Intelligence Division at the FBI Washington Field Office on January 6th conflated the Bureau's standards for what type of information is actionable for further investigation (a higher standard) versus what is merely reportable to partner agencies (a lower standard), and as a result, FBI did not share certain tips and intelligence about January 6th. FBI also did not develop certain tips about January 6th because they were deemed not credible, contrary to FBI policy that requires every tip received to be logged as long as it meets an "authorized purpose" for investigation, regardless of credibility. I&A also failed to report concerning online posts in the lead-up to the attack – including individuals who discussed storming the Capitol – because I&A intelligence collectors considered them to be hyperbole, despite I&A guidance requiring open-source information to be reported if it meets other criteria (such as information that demonstrates a risk of violence), regardless of credibility.

7. **DHS did not designate January 6th as a National Special Security Event (NSSE).** The DHS Secretary can designate an NSSE when a significant event has national interest and requires elevated and coordinated security, intelligence, and preparation across multiple agencies, such as an event that may be a target of domestic terrorism. DHS did not designate January 6th an NSSE, which likely would have increased security and response coordination and capabilities before and during the attack.

RECOMMENDATIONS

1. **Conduct internal after-action reviews on the intelligence collection, analysis, and dissemination processes in the lead-up to January 6th.** FBI and DHS have not yet completed comprehensive reviews of what went wrong in the lead-up to January 6th. FBI and DHS should complete full internal after-action reviews (directed by the Attorney General and DHS Secretary) to identify, at a minimum, what intelligence they obtained regarding the potential for violence on January 6th, what additional information they should have obtained, how they processed the information they obtained, what actions they took in response, and what additional actions the agencies should have taken. The reviews should then assess the agencies' internal procedures and practices to identify necessary changes, and the agencies should share the results of their reviews with relevant Congressional committees.

2. **Review and reform I&A's mission in domestic intelligence collection and dissemination.** Congress created I&A in the wake of the September 11, 2001, terrorist attacks to address intelligence sharing failures related to that attack, and coordinate homeland security efforts and related domestic intelligence. In the 20 years since its creation, and despite the shifting threat landscape, there has been no comprehensive review of I&A's mission. Congress should review and reform I&A's mission in domestic intelligence, including how it analyzes intelligence and coordinates intelligence sharing with federal agencies, other DHS components, and external partners such as fusion centers.

3. **Improve FBI and I&A policies, guidelines, and procedures for collecting, analyzing, and disseminating intelligence to partner agencies.** FBI and I&A should reassess how they determine the credibility of threats, consider the totality of threats (including non-credible threats), determine what is reportable, and characterize the threat in intelligence products. As part of those efforts, the agencies should assess potential biases toward discounting intelligence that indicates an unforeseen or unprecedented attack or event. DOJ and DHS should also evaluate the criteria for issuing Joint Intelligence Bulletins (JIBs).

4. **Clarify agencies' policies and procedures for using open-source information, including social media.** FBI and I&A should ensure their policies and guidelines clearly delineate how and when open-source intelligence should be collected and reported, and include all appropriate Constitutional protections. The agencies should then provide sufficient and recurring training on those policies and guidelines to ensure employees know their responsibilities and limitations for collecting and reporting this information. FBI should also provide guidance and training on the effective and consistent use of its third-party software tool for analyzing social media information, review why this contract migration led to degraded capabilities in the weeks before January 6th and the Inauguration, and mitigate the risk that similar challenges occur again.

5. **Designate Joint Sessions of Congress to certify the Presidential election as an NSSE.** The DHS Secretary should designate Joint Sessions of Congress to certify the Presidential election on January 6th as an NSSE.

6. **Improve inter-agency coordination for significant events and consider designating a lead federal agency.** Because an NSSE designation (with the U.S. Secret Service serving as the lead agency) might not be the appropriate posture for every significant event, federal law enforcement and intelligence agencies like FBI and I&A should also consider additional ways – such as through the Special Event Assessment Rating process – to increase coordination and intelligence sharing during preparations for significant events that are not NSSEs. Agencies should also assess whether to designate a lead federal agency for such events, and increase coordination during real-time responses to unfolding events. Because past experience might not be a reliable indicator of the potential for violence at a given event, agencies should also broaden their consideration of what events require increased coordination and take into account current intelligence.

7. **Responsibly reassert Congressional oversight authorities over the Executive Branch.** For decades, the Executive Branch has increasingly shielded itself from congressional scrutiny. To fulfill its Constitutional oversight obligations, Congress should consider additional ways to ensure compliance with its investigations and oversight requests, including reassessing the accommodations it grants the Executive Branch.