| Feedback for Future | # |
|---|---|
| follow the crisis response plan in it's intended structure. | 2 |
| I don't remeber hearning any information about public transportation. Was it safe to take public transporation during the recent events? | 4 |
| Draft procedures for future 'like' events occurring focusing on what worked exceedingly well, and of course, identify what should not be done again where things did not go so well. | 5 |
| Help to protect people theirs a job | 6 |
| When hearing a threat, take it seriously and plan it out beforehand. | 7 |
| It would have been helpful for those working the IOC if the SIAs overseeing the shift started off by introducing themselves, giving an update, and highlighting the priorities for the shift and any changes in processes. I would also recommend scheduling out the IOC further than you anticipate it will be needed because it is easier to cancel shifts than it is to scramble on a Friday afternoon to staff the weekend shifts, which is exactly what happened. I would recommend adding UNET computers to the IOC because we experienced issues with UVDI every day, which slowed us down when we were handling leads and conducting social media exploitation. Finally, I would also recommend a more extensive after-action survey than 3 questions. | 8 |
| I have heard colleagues speculate about "what really happened" on January 6th and in the lead up to it and about the roles of various groups and actors. In order for our office to not become a casualty of divisiveness and misinformation, I suggest, if possible, we continue to inform employees internally of "what really happened" in such a way that we are all on the same page. I know the investigations are ongoing but I think it is paramount that we all understand the same facts. Unfortunately, we are not immune to misinformation.<br><br>In addition, I would suggest, if possible, that there is a communication about why our response seems to have varied so much between last summers events and that of January 6th. The disparity has not gone without notice and without explanation, it has the potential to undermine from within.<br><br>Finally, I'd like to suggest an annual CP exercise. I was told that before the summer of 2020 the last major unplanned CP had been in 2013. I think we'd be a more agile response force if we could practice some of the skills that seem to be routinely relied upon when standing these up quickly. Perhaps it would be good for the whole office to do together but even if the Intel Division did it yearly, I think we'd see better preparedness, more linkages across the office and an increase in the number of personnel who are prepared to take on leadership roles in a CP. | 9 |
| N/A | 10 |
| Investigate credible threats of election fraud so Americans don't get so upset in the first place.<br><br>(Look, I know you're not going to take any this feedback seriously. WFO is a hopelessly broken office that's more concerned about wearing masks and recruiting preferred racial/sexual groups than catching actual bad guys. The front office is comprised of yes-men who've never opposed a single thought from the Good Idea Fairy. We had a ADIC retire on a Friday at 4:30pm with nothing more than email, and a Deputy Director suddenly retire in the midst of largest manhunt in the history of mankind. Yet we're all supposed to pretend that everything is just fine. Emails from the Director with focus group language aren't going to cut it anymore. It's time for someone to admit that WFO has serious problems so that trust can begin to be repaired.) | 11 |
| Unfortunately, the horrific events of 1/6 has given us a blue print for the future. I would suggest better communication over all along with clear guidance and direction. | 12 |
| Emforce and investigate equally, outside of political biases. | 13 |
| Send out an alert via phone. | 14 |
| Have CAST use the normal process for submitting CALEA requests through the Field Office. The Field Office will be responsible for administering the collection and must take control of the process. CAST is there to assist the process, not circumvent it. | 15 |
| I would recommend more space in the IOC in case one has to stay extra to finish work, so as not to take up computer space away from incoming shifts. | 16 |
| Management needs to think of their staff in times of crisis. Providing information and reaching out is the bare minimum. This was lacking at the time and continues to this day. | 17 |
| Follow ALL protocol. | 18 |
| The FBI should make clear to its personnel and the public that, despite its obvious political bias, it ultimately still takes its mission and priorities seriously. It should equally and aggressively investigate criminal activity regardless of the offenders' perceived race, political affiliations, or motivations; and it should equally and aggressively protect all Americans regardless of perceived race, political affiliations, or motivations.<br><br>FBI leadership is not just accountable to its leadership—it is also accountable to its personnel and the American people. It should consider that, realizing it is only effective with a willing and loyal workforce. Given the FBI's ongoing, politically-biased stance, WFO leadership should begin working with FBIHQ, the FBIAA, and Congress to identify viable exit options for FBI personnel who no longer feel it is legally or morally acceptable to support a federal law enforcement and intelligence agency motivated by political bias. | 19 |
| There should be training exercises periodically to work through potential scenarios and to determine likely requirements. This would allow for proactive troubleshooting of challenges and needs that may arise. (i.e.- what supplies or equipment will be needed; what administrative support will be needed or helpful). The team that starts off in the CP will likely set the tone for the duration of the operation. An example of this is what type of reporting will be needed, requested, or helpful for Executive Management and others. The reports or talking points need to be consistant (and understandably will evolve) throughout the operation. Having some basic reports and procedures to draw from prior to an event would enable better flow of operations. Perhaps providing training and a general SOP to personnel identified in advance of the need would allow for smoother more efficient operations. | 20 |
| Consider immediately standing up the OPA web tips portal and processing leads. It seems like people were more postured for security at the Capitol and not assigned to working the investigation at the outset. | 21 |
| I wish you all would pay more attention to our safety than what type of masks we wear. If you are going to deploy us to a riot situation, then give us the proper damned safety equipment--helmet, face shield, protective clothing--and training! This is the second time the whole office has been deployed to handle such a situation and nothing NOTHING was learned from the previous crisis over the summer. The only differences are new inept leaders who just want to put us out there for a photo OP for the media. It is a miracle no one was seriously hurt or worse. Are you really going to wait until something like Miami happens to one of us at WFO? That's on your conscience if it does. | 22 |
| The FBI needs to be politically impartial, it needs to treat all crimes with an equal hand whether from left or right, and it needs to have its final goal come, ultimately, from the integrity of our Republic. The very source of that is a transparent electoral system. It is not so now. | 23 |
| Leadership needs to be present and do what executive leaders are promoted to do - manage resources which is their people. They need to let the ground troops do what they do best and not micro manage. They need to be consistent with their policy and how they treat all employees regardless of squad. | 24 |
| Focus on the investigation. That is what we do well. Stop trying to throw agents at problems. Support and listen to your followers. Thank you. | 25 |

| | |
|---|---|
| 1. Place one individual in management in the position to make decisions about resource allocation from the instant an incident like this occurs.<br><br>2. The Burearu as a whole must be flexible and understanding that if a situation like this ever occurs, and the supervisor of the squad that is directly responsible for these investigations is tied up in another administrative responsibility, they HAVE to be willing to release that individual immediately so they can use their expertise and manage their squad to effectively handle cases of this magnitude.<br><br>3. NEVER remove the supervisor of a specialized squad in the middle of a crisis incident, especially when the crisis is being handled by their squad. By doing this, and removing a supervisor who has the intimate knowledge of the specific Domestic Terrorism violation in the middle of this investigation without clear cause, not only creates resentment from those who worked for them, but also places an individual in charge of the squad who has no knowledge of these violations or how to properly execute these investigations. Now, not only is that squad scrambling to catch up on the investigations, but they have to spend more of their time helping teach the new supervisor how these violations are handled, when that would be completely avoided. This action alone has set back these investigations by a massive amount.<br><br>4. Communicate more effectively. SOMEONE needs to take responsibility and control from day 1 and steer the direction and plan of how these incidents will play out. How the case load is going to be distributed and how the resources will be allocated in a efficient manner. A drafted plan that states that "specific squad of main identified violation handles initial assessment and then all squads are filtered into the following duties," ..... is rather easy to draft. Any squad can be rotated into a position on that plan and filter in to assume the job and necessary taskings in any investigation. | 26 |
| Work on better communication to office and deployed teams.<br><br>Create an app for accountability for an alternate way to track personnel.<br><br>Train radio operators in CP. | 27 |
| Pool the office to learn what experience people have working crisis events so it's understood where and how best to incorporate skills appropriately.<br>Consider streamlining how communication is filtered down to the staff. For example, after the inauguration was over guidance as to our revised posture or even a posture outlook post-inauguration would've been helpful. | 28 |
| The command post should have been at NVRA since it has a large training room where everyone could sit together while still maintaining some distance (for COVID reasons). Asking all staff to report to DC when the city was shut down was not a great idea. | 29 |
| COMMUNICATE WITH ONE ANOTHER!!!!!! | 30 |
| (1) Work with the FBI to create a single enterprise solution for collection, storing, processing, and reviewing raw information we collection during all of our investigations - and a system that is directly linked to Sentinel.<br><br>(2) Develop an SOP that will actually be used in a crisis, and one that is fully integrated with Sentinel - our case management system. We should not be uploading/tracking anything in SharePoint (the IOC uses in every command post!)- Sentinel has the complete functionality for our needs. | 31 |
| - create an intel division crisis response plan that mirrors other WFO division plans. This has been a problem since after the 2013 Navy Yard shooting and must be addressed ASAP.<br>- require as many workflow processes to go through Sentinel Crisis as possible.<br>- incorporate RDOs/strict shift times into the crisis response plan at approximately day 8. We are lucky to have a huge office, and after ~10 days there was no good reason to still have everybody working every single day with no end in sight. Some professional staff were working 16+ hour days, every day. That pace is unhealthy, unsustainable, and does not produce good work after more than roughly 10 days. Everyone hit a wall and morale cratered as a result. You need to encourage & require "self-care" (the basics - sleep, a day off, real meals) from an executive level down.<br>- feed us! Especially with so many businesses closed due to COVID and then the inauguration, there was a frustrating lack of food available and we all had to fend for ourselves. This is a small thing but it really helps when you know there will be real food (not just chips and cookies) available during your shift. | 32 |

Treat all incidents the same way. As a minority employee of the FBI, I'm embarrassed by the way we responded to "protect the first amendment right" of the BLM-related protests over the summer. Regardless of what FBI/DOJ leadership said, we were part of a show of force meant to intimidate mostly peaceful protesters. A few months later, we knew protesters who have been violent in the past (e.g. Charlottesville) were planning a large demonstration and we did absolutely nothing to prepare. I cannot help but think that preparations for the events on January 6 would have been handled very differently if the racial makeup of the protesters had been different. Whether USCP requested our assistance or not is irrelevant, we should have been better prepared to respond. Over the summer, DC leadership did not want our assistance but we were there anyway, the same should have happened this time around.

33

Create a WFO Rapid Deployment Team to address these critical incidents. This should be a dedicated group (50 to 100) experienced Agents from different branches (Criminal, CT, Cyber, CI) that could jump start the investigative efforts after a critical incident. This group should be carefully selected and should not be performing security functions, but jump starting the investigative efforts, such as collecting video, getting tower dumps, obtaining GeoFence data, interfacing with witnesses and other Agencies, etc.

34

There needs to be one ASAC and or SAC on scene for each shift when something like this occurs so they can rotate off just like a shift of agents do. The SAC should be in the command post while the ASAC is on the ground coordinating with SSAs and agents responding to anything if the offices is put in a situation to do so.

Why is there an intel response team when members of the team are able to reject showing up to staff these events. The purpose of that team is to have people immediately available for at least the first 24-48 hours of a shift. The method in which intel is gathered is done like shooting from the hip. It is always the same squad responding to the social media groups or whatever other specialized shifts are available. Why would you have those teams and not have it comprised of individuals from CI, Crim and CT? CT doesn't know what gangs in the area look like, CI doesn't know what a CT red flag may be, and so on... If we really need to cover our bases and that's a concern then we need to actually do so.

Let embedded intel personnel assist with their squad case loads. We have domain, collections and ROs that only handle strategic products...why on earth would those squads not be responsible to serve in the IOC after the 24/7 posture of a command post is over.

Instead of sending out emails every 10-15 minutes advising people of new procedures etc... will lead to confusion and emails going unread. The office needs to have an overall SOP for these situations and then tailor the basics to fit those needs not addressed instead of reinventing the wheel every time. It is clear that Intel executives specifically, do not know how to handle these crisis situations and should be thankful for some SIAs being able to handle the pressure for them.

A main sharepoint site needs to be created for this specific situation and made available to all personnel who may be working in an emergency situation. That site should contain all of the SOP for obtaining access to critical incident systems that may be used and be available to the entire office.

There needs to be a threshold for leadership allowing them to think about their personnel and the other cases going on in our office. The people of the office need to be considered and thought about instead of politics involved in these situations.

Currently, the US Attorneys office is dictating what it is that gets investigated. This is a dangerous precedent because we can barely get them to prosecute investigations that clearly meet thresholds needed for Federal prosecutions. However, their willingness to conduct a search warrant on someone's life for a misdemeanor seems ridiculous. It is unreasonable for the FBI to conduct investigations involving misdemeanor violations at a federal level...it is not our role. 35

With regard to Crisis capability within Sentinel:
- add a Search function for all lead evaluation roles (Crisis Case Agent, Lead Evaluator, Lead Manager) to be able to find a particular lead via keyword search
- add a way to "check out" a lead for all lead evaluation roles so two people aren't looking at the same lead at the same time
- have designated accountable leaders for the various components (who's overseeing the lead teams, including evaluators and crisis case agents, and ensuring everyone's handling leads the same way? Who's looking for pCHSs? Who's got the overarching picture of how all the pieces fit together and what's missing?)
- ensure everyone understands the pieces of their team. For the leads teams: what does the Evaluator do? what does the Crisis Case Agent do? What are the specific pools of people designated to handle different kinds of leads? Is there a team specifically for video review? for social media analysis? for baseline checks, or is that done by the Lead Evaluator? etc 36

| WFO Did Poorly | # |
|---|---|
| communications on expectations or what the chain of command was - who was running what. | 2 |
| I don't have a Bu phone. What is the plan to communiate information to people that do not have a Bu phone? First line management to tell employees? | 4 |
| Nothing noted | 5 |
| SWAT, DEA, POLICES, NCIS, ATF AND ETC NEED WORK TEAM TOGETHER | 6 |
| Nothing i have knowledge of. | 7 |
| I worked multiple IOC shifts and there was a lack of consistency in the guidance we received. Oftentimes, the SharePoint or workflow tracker changed from shift to shift, but the SIAs did not articulate the changes. We were left to find out from the shift we were relieving how things were being done that day. Also, it seemed as though ops did not know how to contact the IOC for analytic support for the first several days. But once they did find out, the IOC received many leads for basic checks the SAs should have handled themselves. I handled multiple requests for baseline checks, only to find the requesting SA had not even checked Sentinel to see if it was duplicate. The SIAs rarely pushed back on these requests and because the SAs did not require SSA approval to send them, we were overloaded with menial tasks, which took us away from other taskings. | 8 |
| I don't know the particulars of WFO's posture or mindset leading up to January 6 but it certainly appears as though we were not appropriately prepared for what happened. I heard colleagues suggest that Proud Boys are pro-law enforcement and therefore are / were not a threat. I wonder if our biases affected our preparedness. | 9 |
| Lack of adherence to mask requirements | 10 |
| WFO did a poor job of following the Constitution, obeying the rule of law and protecting Americans from force and fraud. | 11 |
| I wouldn't say if was poorly but from my perspective, there were changes and request that were provided after thousands of media clips had been reviewed and then specific information was requested and it was not feasible to go back and review media clips for that specific information. There could have been more feedback as to the progress made on arrest. Most of the information we received came from social media or the mainstream media outlets. Better communication always work best. | 12 |
| Send confusing emails to those it didn't apply to. Expended all resources on one thing. Made many work long hours for mostly trespassing charges, which I am still trying to find that portion of the constitution giving the FBI authority to do so. Im not seeing any interstate commerce in that one. | 13 |
| N/A | 14 |
| Allowed CAST to insert themselves in the service provider requests (CALEA) before taking control/ownership of the process. This misstep almost caused a breach in lawful intercept/collection. A supervisory CAST member directly spoke to one of the service providers, stating a preservation order was in the works. For this request, a preservation order was not necessary, as the information was less than 6 months old. Regardless, the dates/times stated by CAST was different than what was authorized by Court Order. This led to confusion and rework by the service provider and delay in receiving the actual data to continue the investigation. | 15 |
| N/A | 16 |
| My individual squad's leadership did not provide a single notice of the events or any messages in the hours or days after the riot. Had I not been paying attention to the news, I would have been completely unaware of what was going on. | 17 |
| Follow protocol for vast amount of things ranging from putting in IT trouble tickets to not leaving computers unattended while signed in, etc... | 18 |
| Generally speaking, I have little interest in the political preferences of FBI leadership or whether the agency as a whole is more supportive of one political party than another. However, the FBI irreparably damaged its credibility among the American public and a great percentage of its personnel by abandoning its mission and priorities.<br><br>In approximately 2008, the FBI stopped an ongoing public corruption investigation (Operation Board Games--Blagojevich) just shy of potentially implicating a sitting president (Democrat) due to the damage it might cause to the United States. Approximately eight years later, the FBI began actively and publicly investigating and attempting to unseat a U.S. president (Republican) through deceit and abuse of its authorities (Crossfire Hurricane).<br><br>In 2020, WFO assumed a mission for which its personnel were untrained and underequipped to protect and defend a plaza dedicated to a group of "domestic terrorists" (left-leaning, and with a history of violence and criminal activity during its first amendment activities), then took a knee on command. In January 2021, WFO immediately and aggressively began targeting anyone accused by the public of having been in the geographic vicinity of similar crimes perpetuated by another group of "domestic terrorists" (right-leaning, and with little to no history of violence or criminal activity during its activities).<br><br>This ongoing, obvious, unapologetic and, for all intents and purposes, legally-sanctioned bias has thoroughly demoralized the FBI's personnel and the American public, further endangered its agents as they interact with the public in the conduct of their official duties, and jeopardized the ongoing safety and security of the United States and its citizens. | 19 |
| We were reactive vs. proactive. | 20 |
| From complainant reporting - there was no confirmation on the OPA tips website that a complaint had successfully been submitted. Additionally, when the OPA tip generated a lead and was assigned, the original media was not attached. It was a circuitous path to go and find the original media and seemed to be unnecessary. | 21 |
| For starters how about equal reaction to equal riots--no matter what side of the political spectrum they are on. Actually they weren't so equal; the summer riots were far worse than on 1/6. During the summer, where was the whole office response of dropping all its cases and spending weeks identifying and arresting Antifa and Black Lives Matter terrorists that were looting and burning D.C. and cities across the US? Exactly. There wasn't such a response. Believe me when I tell you this has NOT gone unnoticed by the Agent personnel at WFO. Most do not want to rock the boat for fear of retribution, they want their promotion, or whatever their reason. I, however, am not afraid to respectfully dissent and tell you we do NOT want to work for the enforcement arm of the DNC/Democrat party/Deep State--or any political organization. It has become apparent to me in the past few years this is the case and now in the 2021 FBI, justice is in fact NOT blind. I hope you can step a step back and look at the optics of this from a line Agent's perspective, because I know you were all in our shoes before. I can not and will not work for an organization whose ethics and integrity are this maligned. My resignation letter is written, and I'm happy to personally turn in my creds, badge and gun to the ADIC, because this was the last straw for me. | 22 |
| We poorly assessed our own culpability in the distrust the American people have for the lack of transparency in this election. The appearance of any lack of transparency at any polling/counting venue should be vigorously investigated by the FBI. We have not done this. Our not taking responsibility for the political bias of the Mid Year investigation, and the politically biased crimes committed by FBI employees in the Crossfire Hurricane investigation make us morally unfit to render justice in the eyes of too large a percentage of the public. During this last summer we virtually ignored riots that were direct attacks on life, property and local and federal government. We have, jn fact, due to our actions and inactions, lost our most prized asset in our pursuit of justice; the confidence, admiration and gratitude of the American public. As an agent I am not alone in this perception. Without a change in course, our current trajectory will drive the likelihood of civil unrest by conscientious citizens (and possibly domestic terrorism from fringe groups) who fear the loss of their Republic from a number of different mechanisms that have been made raw by our inattention to our core values. | 23 |

| | |
|---|---|
| *Executive Leadership was poor. Ownership of who was doing what. Who was in command and making decisions. Duplicative work was being done by the field, HQ Units and CT components. creating confusion in the field.<br>*once immediate threat to life was over the rapid pace could have been scaled back after a week. Approximately 3 weeks was over kill just to say were are doing something (and majority of violations are misdemeanor trespassing).<br>*very disappointed in my executive management for crim branch. During response I never saw SAC or various ASACs. For the first 1st week never did any ASAC ask if we needed anything or how we were doing and what can make our job easier (especially being involved in all digital media intake for the office) NOT ONCE. After the first week the ASAC showed up only to demand BOLOs and when I requested assistance told me to figure it out and still did not ask what I needed to make the job easier. Luckily SAC Christine O'Neil and Jennifer Moore asked us (DIVRT) what was needed to help our job be more efficient. We asked for faster internet for uploads, more direct connections, dry erase boards, etc and they were immediately met. They also came in almost daily to check on us as personnel. Something Crim division management lacked in doing.<br>*extreme frustration over inconsistent policy by ADIC. Covid policy's don't get erased just because of crisis response. You are not less likely to get exposed during a crisis yet all restrictions are lifted to accomplish the mission. Now squads are going back to 1 week in and a week out of office. Posture is demoralizing for squads who have been non stop and figured out how to make it work for months working daily, weekends, etc. Yet many squads barely work in office prior to crisis and now going back to the same posture. Its either a policy or not for entire office. Not just for CI or CT but entire office minus reactive squads. You need to be consistent and make everyone work. | 24 |
| WFO did not deal with the aftershocks of the event. It seems like WFO continually tries to put agents in places they don't fit, thus putting them into administrative and physical harm. It also puts management in places they don't fit.<br>Also, management does not support its people. There is no top-cover whatsoever. Agents know how to do their job, they are not the crux of these problems. Shuffling leaders around isn't helping. Bringing outside management is a terrible message. | 25 |
| Communication and allocation of resources. WFO assigned everything that was happening to one squad in the first few days while that squad's supervisor was tasked with an inventory task for another field office. This supervisor asked to be removed from the inventory task and was prevented from doing so for 3 days. This put the work on a squad that was already limited in man power and not advised of the tools at their disposal. The squad did their job and focused on the problems at hand, however becuase of lack of communication and foresight, management didn't allow their supervisor to assist. This created a massive discconect with plans on how to operate this incident from day 1.<br><br>By not having a swift response to assist in the multiple incidents that occured, it was impossible to properly address every situation from the start. by placing both the capitol case(including thousands of individuals) and the pipe bomb case on the shoulders of one squad from day 1, that squad had to break down it's already limited team into even smaller teams, creating a massive man power issue. This coupled with the lack of communication from management to this squad as to available man power, (even though the request for assistance was voiced multiple times) it took over 72 hours for those resources to be brought to fruition. This put the investigations at a major disadvantage and have massively cripled the ability to obtain pertinent information for the investigations (especially relating to the pipe bomb case.) | 26 |

WFO's response, as compared to June, slightly improved. There was still little adherence to the CRP, i.e. recalling 100% of the criminal division. This type of decision ineffectively deploys resources to an incident. Were all agents needed? Tasked appropriately? Prior to resources being deployed to an incident, this should be appropriately coordinated through Incident Command (typically CT-10 as first on-scene) and through the OSC in the Command Post.

WFO's Crisis Management Program needs to be addressed. The negative performance and lack of attention to detail by the program coordinator was very apparent. i.e. the role of the lead CMC is to facilitate and ensure effective use of Sentinel Crisis Tool. The lead CMC seemed to be removed from the crisis case as a whole, to include assisting with setting up, assigning roles, etc and leaned heavily on other division reps to handle the job (i.e. MSD, CMU, etc). WFO should consider realigning this program with another WFO Division and/or new program coordinator who is able to fully carryout the roles of the CMC.

Misleading information received from Agents: i.e. don't self-deploy vs receiving an email to deploy Crim agents. 27

Sent everyone downtown initially to work when WFO main doesn't have the capacity to incorporate all the personnel who regularly sit at the NVRA. Additionally, many of the squads at the NVRA have misattrib capabilities organic to their workspaces which does not exist on other squads at WFO main. Many agents were inexperienced in the revisions made to Guardians and there was little guidance in how to complete them.
There was poor management of where to plug squads in and what shifts to put them on. Some squads had their mission and shifts changed 3-4 times in the course of 3-4 days. While maximum flexibility is needed during a time like this families take a huge hit when their loved one can't maintain some consistency, even in a crisis event. I realize this is a hard one to plan for but I felt it must be mentioned. 28

-The location of the Command Post at WFO.
-Recruiting all staff to work this event when it was no longer a "crisis". The crisis ended when there was no more threat to life/limb, ie when the Capitol Building was cleared and secured. The CT (IT/DT) squads should have worked on these cases as "historical cases" and recruited TDY help where it was necessary. To make all Agents and Professional Staff stop their daily work to focus on running down duplicate social media (TikTok, facebook, false leads that had nothing to do with the capitol insurrection, etc.) leads was ineffective and caused a great deal of harm to the FBI's on-going missions as well as the FBI employees' morale. 29

COMMUNICATE. This situation lacked communication from the start. Multiple people were doing the same task, agents were investigating the same subject and did not know about this until they went to swear out a complaint on the subject. WAY TOO MANY hands were involved with this (Which rightfully so, its a huge investigation) but in the beginning a course/plan of action should have been established and then from there, people should have been incorporated as needed. The case agents for the 176 did not have what they needed resource wise and no one would answer questions pertaining to questions that arose because the posture/guidance kept changing from HQ. An ALL OFFICE email should have been sent with guidance for the investigations and it was not, even though it was requested several times. This would have saved SO MUCH TIME.

There are also way to many spreadsheets for this investigation. Due to this, information is being placed on one and not the other and important things/updates are missed. There should be ONE spreadsheet for everyone to use in events of such large measure. Also listen to the agents actually involved in the case. Questions were asked and agents answered those questions, but supervision did not listen and would ask the same question every single meeting (which was addressed by agents EVERY SINGLE TIME).
Again...COMMUNICATION. NEEDS IMPROVEMENT.

Reallocation of resources in a crisis is not helpful. Subject matter experts for that crisis should remain with that team since they possess the knowledge to answer any questions and know current resources to properly direct anything new that is required. 30

While the FBI does an excellent job at throwing agents, analysts, and professional staff in sheer numbers to tackle a problem, it (1) woefully underutilizes technology and (2) creates inefficient processes. We need a better singular enterprise-level solution for collecting, storing, processing, and reviewing all of the information we take in across all investigations. Sentinel is a great case management system, but we need something for the intake side of the equation that directly links to Sentinel. Additionally, we are not great at creating processes on the fly. We have a crisis management SOP, but seemingly we throw it out the window when responding to such events as the January 6th riots. 31

WFO intel response was unnecessarily confusing and divorced from the rest of the office. If there is a central crisis response plan for WFO ID it is not posted to the CTOC sharepoint site and is not known by the average IA or SOS in the office. SIAs wasted dozens and dozens of hours putting together schedules for the different intel missions (IOC, war room, digital media, tactical, etc) and needing to adjust them as individual's became unavailable. If intel division had a crisis plan that was integrated with the rest of the office's plan, each squad could have been assigned to a specific shift for a specific mission for the duration of the crisis.

The intel workflow for the IOC was based on Sharepoint, not Sentinel Crisis, which resulted in significant duplications of work and general confusion. While Sentinel Crisis is not perfect, in the future if the IOC is requested to create baseball cards for individuals, the workflow should be run through Sentinel - assign leads, upload the completed cards for approval in Sentinel Crisis, send completed cards as info leads to the assigned SAs, etc. There is no reason for it to be Sharepoint based and circumvent the Sentinel process.

32

Too much duplication of tasks. People assigning leads need to be better coordinated so tasks targeting same subject are not sent to multiple agents, who are unaware that others are working on the same thing they are working on. This was understandable at first, but it lasted for days after the initial rush was over.

33

ommunication and Guidance

Communication from the Command Post (CP) could have been clearer and more concise:

For example: Information from the Command Post shifted multiple times (tracking sheets, etc) and sometimes would include too much detail.

Updated Guidance on how to respond to these critical incidents is crucial:

During 2020-2021, WFO Agents have responded to two (2) similar critical incidents, yet there has been no training or guidance on how to properly respond to these incidents; and the implications with our deadly force policy and available tools in relation to these situations has not been discussed.

Tools and Resources

Agents not assigned to WFO (main office) had to scavenge for desk spaces and computing resources. This proved to be inefficient and limited our response and capability.

There was very “little” to “NO” support from IAs and SOSs for agents assigned with investigating cases. No real Team effort.

Logistics

Having most, if not all, of the WFO Agent population at WFO (main office) during the incident response would have been detrimental if a more substantial/coordinated attack had taken place. Leveraging offsite locations are essential to be able to respond to these incidents while safekeeping the overall capability for WFO. For example: in case of a biological based attack, all of the Agents would have been taken offline.

Shifts: Although Agent shifts provided coverage in depth, this proved to be inefficient for Agents assigned to investigate cases. The nature of investigating cases cannot be constrained by shifts, as AUSAs, witnesses and investigative functions might not align with a specific shift. Shifts can be efficient if they are aligned with specific roles – for example, shifts can be established for squads solely responsible to provide security and/or a tactical response capability.

34

The push to have intel personnel stage downtown is unacceptable. There is no reason for intel personnel to travel into the district during the height of riots and any other type of violence. Intake shift would be staffed more quickly if the necessary flexibility is provided. There is an extremely large secondary office located in Manassas, VA that is more than capable of housing a command post. There is definitely a necessity to have people downtown physically to respond and be available to executives but insisting individuals w/o BU-vehicles drive downtown, without light packages or personal defense in the middle of violent incidents is reckless, dangerous and unacceptable.

The riots were one of several major events that occurred in the last year and it seemed that we learned nothing from the previous riots and never put a plan in place. There should never be an entire office recall to an emergency situation unless it is an end of the world scenario. The office was set-up for failure right out of the gate when it did that. The initiation of an emergency response should immediately push agents and intel personnel onto a 8, 10 or 12 hour shift so the personnel are able to be backfilled with fresh bodies instead of having the entire office work around the clock.

Deploying agents into a riot situation is a terrible idea especially when agents have never managed something as small as a traffic stop before. Deploying agents in such a scenario should be a last resort and only be done per that agencies request. There are no less than lethal qualifications that agents have that would help in those types of situations. The role should be to stand back and provide support if need be to other first responding groups or focused on the aftermath as in what investigations will be coming out of this and starting that process. Emergency teams like SWAT who are equipped to handle situations like riots should be the only ones deployed up front to assist with those situations.

35

- transparency of schedules - would've been nice to put schedules on SharePoint a few days ahead of time to let everyone know when they needed to work
- role on 1/6 was murky - to arrive at WFO, be given a riot helmet, and told to "go clear the Capitol" was a task I didn't feel prepared to do, since we're not trained in riot countermeasures

36

| TOC RADIO LOG 01/06/2021 | | | |
|---|---|---|---|
| **TIME** | **FROM** | **TO** | **MESSAGE** |
| 01/06/2021 2:16:00 PM | SWAT | CP | Comms check |
| 2:25 PM | SWAT | TOC | departed WFO for Capitol by way of Union Station. 15x en route, 6x on standby at WFO, BA SWAT on standby at Cheverly |
| 2:28 PM | BA TOC | WF TOC | Comms check |
| 2:35 PM | BA TOC | WF TOC | BA team kitting up, preparing to depart en route to WFO |
| 2:49 PM | [redacted] | WF TOC | 5x operator moving to assist downed officer. Entering Capitol |
| 2:52 PM | [redacted] | WF TOC | All operators (15x) entering Capitol to assist down officer and make linkup with CIRG |
| 2:52 PM | BA STL | WF TOC | Leaving Cheverly now, 25min ETA |
| 2:59 PM | [redacted] | WF TOC | WF swat holding on 1st floor south side entrance |
| 2:59 PM | BA TOC | WF TOC | BA TOC en route WFO |
| 3:07 PM | BA SWAT | WF TOC | 8 min out |
| 3:12 PM | BA TOC | WF TOC | Outside WFO |
| 3:15 PM | BA TOC | WF TOC | 19 BA Operators arrive at Hart Bldg |
| 3:36 PM | [redacted] | WF TOC | 15x WF operators in Capitol Rotunda; linked up with USSS; no specific tasking |
| 3:52 PM | [redacted] | WF TOC | 11 Operators in 3 vehicles departing WFO for Longworth; ETA 7 minutes |
| 3:58 PM | WF TOC | ALL | MPD TO DEPLOY GAS ON WEST FRONT OF CAPITAL BUILDING |
| 4:10 PM | [redacted] | WF TOC | [redacted] and [redacted] located at Longworth |
| 4:26 PM | [redacted] | TOC | 16 Pax 3 vics staged at New Jersey/Independence standing by for link up or follow on tasking |
| 4:32 PM | [redacted] | WF TOC | Comms check |
| 4:52 PM | [redacted] | WF TOC | Comms check |
| 5:01 PM | Bravo element | WF TOC | Located vic. Lot 16 with unified command |
| 5:03 PM | [redacted] | WF TOC | WFO Alpha element holding in H131. Bravo holding at New Jersey/Independence intersection. CERT requesting |
| 5:05 PM | HRT Gold | WF TOC | Comms check |
| 5:07 PM | [redacted] | WF TOC | Alpha is holding in the US Capital in room H131,WF Bravo is holding outside the Longworth building at the intersection of New Jersey/Independence, BA SWAT Hart Building awaiting ocupants to depart, Secret Service is holding in their hard point at the Captial, CERT is requesting WF SWAT to back fill them as they depart the Capital, Captial Police and Secret Service are requesting that now further tactical units be sent to the Capital at this time. |
| 5:55 PM | BA STL | BA TOC | BA SWAT holding in Hart Senate Office Building; lawmakers may return to Capitol. |
| 6:44 PM | [redacted] | WF TOC | No change to posture |
| 6:58 PM | [redacted] | WF TOC | HRT Gold sending 2 vehicles with 13 operators to the corner of NJ and Louisiana Ave - to link up with Secret Service - HRT has 14 Operators at corner of Constitution and Delaware |
| 7:05 PM | [redacted] | WF TOC | At 1915 senators will be poving in packs of 10 back to capital - Baltimore has linked up with Capital Police to facilitate moving |
| 7:45 PM | WF TOC | | Baltimore SWAT has been requested to return to WFO and will be cut loose |
| 8:00 PM | [redacted] | WF TOC | WFO SWAT element of 14 operators staged at WFOHQ have been released |
| 8:31 PM | [redacted] | WF TOC | Alpha unit at the US Capital is consolidating preparing to return to WFO. |
| 8:40 PM | [redacted] | WF TOC | Alpha and Bravo and consolidating equipment at the US Captial, upon consolidation Alpha will RTB to WFO |
| 8:56 PM | [redacted] | WF TOC | Alpha RTB to WFO |
| 9:03 PM | [redacted] | WF TOC | Radio Check on bearcat |
| 11:28 PM | TOC | [redacted] | Radio Check |
| 11:57 PM | WF TOC | | HRT Gold at US Capital - HRT Silver and HRT Blue have returned to base and are on strategic reserve |

# 2021 Capitol Riots

# After Action Report

# Division Submissions



## Mission Services Division

### MSD [redacted] Highlights

- Confusion and lack of communication regarding how the case would be handled.
  - Duplicative lead assignments.
  - No guidance on lead compliance.
- Lack of basic Covid-19 protocol
  - Elimination of the elevator limit.
  - Lack of mask wearing.
  - No social distancing.
- Security concerns
  - Leaving doors propped open.

### MSD [redacted] Highlights

- Best Practice – would be to have a loaner set of unclassified laptops marked for crisis to deploy in times like this. We luckily had some CARES Act devices that had not been assigned yet that we were able to use in this way. However, this may not always be the case so it would be wise to have a small inventory for this purpose.
- OPSEC for unfiltered lines must remain in place. For planned CPs, this is not an issue. For crisis CPs, we need to continue to ensure all non-FBI mobile devices entering FBI space are approved and users certify Wi-Fi and Bluetooth functionality are disabled. [redacted] and [redacted] are very

engaged on this important matter, but with more and more unfiltered lines being utilized, this must remain extremely tight.

- Any outside agency that needs to connect their IT equipment to our unfiltered network must coordinate with ET/IT/TTA staff before establishing connectivity. Our ET/IT employees were ahead of this and assisted as needed, but some of these agencies bring their own embedded IT folks with them. We need to maintain span of control over anyone utilizing our infrastructure.
- ET/IT personnel are often tasked with large requests, in passing, while they are in the CP providing support on an issue. These requests come from a variety of FBI employees and vary in size from pulling network lines to installing several UNET computers. The respectful ask is employees making these requests understand some of these projects need to make their way to the MSD ASAC or even SAC for approval. It's very difficult to complete these projects in the middle of packed CP.
- The recent events highlighted the need for the main CP/Invest room to have greater network/IT functionality. We recommend every CP workstation have the necessary infrastructure to support a red/green tower, at minimum and that this upgrade happen ASAP.
- It is recommended that a permanent junction box be installed on the exterior of WF to support external CPs, such as Big Blue. This will allow the TTAs/ETs to provide the necessary network lines to Big Blue without running these cables through doors, etc. When not in use, our teams can ensure the connection on the interior of the building is disabled.
- Telephone services would like to ensure they have adequate funding to keep a good stock of regularly requested items during CPs/crisis events. They regularly give out external battery packs, cases, charging cables, etc. from their "normal" stock to support major events.

## MSD [redacted] Highlights

### Best Practices:

- The response time for agents and professional staff alike exceeded expectations as everyone reacted in a timely manner.
- The WFO-All email to Agents and staff to not engage or respond to the Capitol events on their own came out quickly and provided guidance for all until proper procedures could be placed.
- Proactive working groups were effective in their ability to accumulate resources and provide guidance to individuals responding to the Capitol Riots and the Command Posts.
- IT and Mission Services were heavily relied upon for supplying Agents and Professional Staffers with tech and equipment was near instantaneous on many requests.
- Professional staffers were quick to volunteer for the work and fill positions that were needed, which greatly helped alleviate staffers from being over-worked or taking on too many responsibilities.
- Temp Checks – Armbands and logs

### Room to Grow:

- Communication:
    - "Side-stepping" Chain of Commands to request items caused confusion and item requests not getting fulfilled.
    - Ensuring that there is a clear Supervisor POC for support staffers so they can continue to be utilized effectively and have clarity on who to report to as well as what their duties and responsibilities are.

- Have communication between management and facilities when Ops or Command Posts may be expected so teams can ensure that there are sufficient supplies to disseminate to groups and individuals.
- For prolonged events or Command Posts, facilities should be aware of the individuals or teams that they are responsible for communicating with and supporting.
  - Example: CIRG, SWAT, 24 Hour Posts that require support
- Find options that would allow for Command Posts to reach out for supplies needed.

- Staffing:
  - Preparing a list of Professional Staffers that are "fit" to work special events to alleviate individuals getting over-worked or burnt out. This would allow for the core individuals to receive proper breaks as well as ensure consistency in the Command Post for the Agents and Executive Management.
    - Inviting individuals to take the CMAT course.
    - CIOS-CMC trained personnel
  - Having staff aware of extension cords and other electronics that are being utilized to not overload the building's electrical. This would also be beneficial in allowing facilities to know when they need to ask for additional resources or funding from HQ to prevent potential issues.

## Challenges/After Actions:

- Keeping lines of communications open so to not miss issues or requests from Command Posts or individual requests.
- Settling concerns of Professional Staffers and offering directions on how to get into the city and ensuring their overall safety.
- Switch / Junction Box on the outside of WFOHQ – Prioritize this with FFD for a FY21/22 Small Projects
- Identify key roles for PS employees in a crisis type situation – ensure they get regular training – annual training. Coordinate with Crisis Management folks.
- Folks who are indexing need to be plugged in from the very beginning.

## Additional group feedback items:

### Lack of coordination by [redacted]

- Resource requests were poorly managed.
  - [redacted] sent mass emails out to the field requesting assistance as opposed to detailed information and instructions to contact [redacted]
  - [redacted] directed volunteers to WFO POCs as opposed to managing all aspects of resource requests.

### ASAC shift rotation

- Lack of consistency in ASACs from shift to shift made it difficult for certain ideas to be implemented.
  - Great ideas but not much follow through/ownership of process

### MSAs

- Being tasked directly by various ASACs and other individuals in addition to carrying out their main responsibilities
    - Providing some direct supervisory support to the MSAs would be helpful moving forward.
        - Suggestion to have the ADICs Special Assistant to provide direct supervisory support to MSAs.

## Criminal

[redacted]

**Comment #1:**

**Communication and Guidance**

- Communication from the Command Post (CP) could have been clearer and more concise:
    - For example: Information from the Command Post shifted multiple times (tracking sheets, etc) and sometimes would include too much detail.
- Updated Guidance on how to respond to these critical incidents is crucial:
    - During 2020-2021, WFO Agents have responded to two (2) similar critical incidents, yet there has been no training or guidance on how to properly respond to these incidents; and the implications with our deadly force policy and available tools in relation to these situations has not been discussed.

**Tools and Resources**

- Agents not assigned to WFO (main office) had to scavenge for desk spaces and computing resources. This proved to be inefficient and limited our response and capability.
- There was very "little" to "NO" support from IAs and SOSs for agents assigned with investigating cases. No real Team effort.

**Logistics**

- Having most, if not all, of the WFO Agent population at WFO (main office) during the incident response would have been detrimental if a more substantial/coordinated attack had taken place. Leveraging offsite locations are essential to be able to respond to these incidents while safekeeping the overall capability for WFO. For example: in case of a biological based attack, all of the Agents would have been taken offline.
- **Shifts:** Although Agent shifts provided coverage in depth, this proved to be inefficient for Agents assigned to investigate cases. The nature of investigating cases cannot be constrained by shifts, as AUSAs, witnesses and investigative functions might not align with a specific shift. Shifts can be efficient if they are aligned with specific roles – for example, shifts can be established for squads solely responsible to provide security and/or a tactical response capability.

**Recommendations:**

- Create a WFO Rapid Deployment Team to address these critical incidents. This should be a dedicated group (50 to 100) experienced Agents from different branches (Criminal, CT, Cyber, CI) that could jumpstart the investigative efforts after a critical incident. This group should be carefully selected and should not be performing security functions, but jumpstarting the investigative efforts, such as collecting video, getting tower dumps, obtaining geofence data, interfacing with witnesses and other Agencies, etc.

**Comment #2:**

Initial response was better than summer as personnel were staggered.

- Once immediate threat to life was over the rapid pace could have been scaled back after a week. Approximately 3 weeks was over kill just to say were are doing something (and majority of violations are misdemeanor trespassing).
- Very disappointed in my executive management for crim branch. Extreme frustration over inconsistent policy by ADIC. COVID policies don't get erased just because of crisis and you're more likely to get exposed but all restrictions are lifted to accomplish the mission. Now squads are going back to 1 week in and week out of office. Posture is demoralizing for squads who have been nonstop and figured out how to make it work for months working daily, weekends, etc. Yet many squads barely work in office prior to crisis and now going back to the same posture. It's either a policy or not for entire office or not. Not just for CI or CT but not reactive squads.

**Comment #3:**

The actions on January 6, 2021 were absolutely despicable and unacceptable in a civilized society. What is even more unacceptable was the hypocrisy displayed by the FBI and its leadership in their attempt to go after those involved in the Capitol Riots, while we as agents, watched cities burn across America during the summer of 2020. The conspiracy to commit crimes at the Capitol on January 6th, were also committed by bad actors during the summer riots of 2020 leading up to the election on November 3, 2020. Agents stood by on the ground in Washington, D.C. and observed stores being looted, burned, and ripped of anything of value. Even worse, officers were assaulted in the streets in broad daylight with

cameras rolling, and yet our response then was nothing like the Capitol Riots response on and after January 6, 2021. I do not recall a single instance where the FBI, specifically FBI WFO, made any attempt to put the resources behind the summer riots of 2020, as they did during the Capitol Riots. I cannot recall a single tip line, BOLO poster, or Twitter post being blasted out by the FBI in an attempt to identify any bad actor during the summer riots in Washington, D.C. I was assigned many leads for people standing on the Capitol lawn, but I have yet to see one looking for a suspect bashing a Secret Service police officer in the head in front of the White House. Here are some of the headlines from national press related to the riots of 2020 in Washington, D.C.:

"Night of destruction across D.C. after protestors clash with police outside White House" (The Washington Post, June 1, 2020)

"Fires light up Washington DC on third night of George Floyd protests" (The Guardian, June 1, 2020)

"Protests Near White House Spiral Out of Control Again" (The New York Times, May 31, 2020)

WUSA (D.C. local news) June 11, 2020. WUSA 9 verified that 155 police officers from Metropolitan Police, U.S. Secret Service, U.S. Park Police, and other agencies in D.C. were injured during the riots that occurred in D.C. between May 29 to June 7.

**Comment #4**

I have been asked by members of my community why there were two very different responses from my agency, when both riots appear to be the same to them at face value. It's a shame that I can't answer that question. I have heard U.S. Secret Service Police ask why their alleged assaulters during the summer of 2020 riots weren't sought out like those who assaulted officers at the Capitol. Again, I can't answer that question. We were once an apolitical organization, but I no longer see us as such looking from the ground up. We have been used as pawns in a political war, and FBI leadership fell into the trap and has allowed it to happen. We are supposed to call balls and strikes, regardless of political pressure, now we can't even be trusted to be on the field.

I want to be clear so it's not misconstrued, both the summer riots of 2020 and the Capitol Riot were repulsive. The FBI's response to one and not the other is unacceptable in an organization that is supposed to be independent and apolitical. On May 3, 2018, *TIME* magazine published an article "The FBI Is In Crisis. It's Worse Than You Think". In the article, the writer Eric Lichtblau, describes the *many* failures that have accumulated most recently in the FBI. The most sobering stat referenced stated that an April 2018, PBS News Hour Survey showed a 10-point drop-from 71% to 61% among Americans who thought the FBI was "just trying to do its job". I would not like to see the result of that same survey today, because I have not seen any faith restored in this organization. FBI leadership needs to be reevaluated in the strongest sense possible. We have been infiltrated by political pawns who are sinking the ship many of us work hard to make sail every day. Someone in a leadership position at WFO needs to step up and make things right again. That may mean pushing back when someone wants an outcome that appears political in nature, because our response to the Capitol Riot reeks of political bias.

**"You can't make the same mistake twice. The second time you make it, it's no longer a mistake. It's a choice." –Anonymous**

**Comment #5**

1. It is not clear whether the CMC or Crisis Management squad was contacted to assist with organizing this response or to help manage the continued posture during the first day(s) of the crisis (1/6 - 1/8). Although they were preparing for the inauguration, the CMC team would have been able to help organize the teams/squads and ensured key roles were staffed up immediately.
    - Key recommendations –
        a. Ensure all WFO EM (15s and above) take the Crisis Management training for EM as soon as practicable; they did not seem to know many of the key roles that are needed to run a CP/crisis event.
        b. Ensure the crisis response plan (CRP) is updated to pre-plan for certain types of responses (e.g., if a CT lead response, then designated CI squads immediately report to the CP for staffing of lead evaluation and other sets of squads are already pre-designated to start running as lead coverage squads, etc).

2. The WFO org chart was not updated in January so we wasted a lot of time trying to build correct contact and staffing sheets for SSAs across the office.
    - Key recommendation - Ensure the office org chart and CRP is updated with correct names and contact information, respectively, on a bi-weekly basis.

3. There was no clear unity of command or chain of command for the response. Having no clear chain of command made it difficult for consistent decision-making or leadership. ASACs rotated every shift and there were two non-operational SACs seemingly in charge of the response, but this was never clarified to the SSA and SAs working the event. Additionally, having two operational ASACs running parts of the case created confusion for who was actually in charge and had key decision rights. [The] coordinating roles were the only consistent position every day to ensure issues were tracked efficiently and decisions were implemented effectively.
    - Key recommendation - Ensure a clear chain of command and regular shift staffing is implemented for better command and control of, and decision-making during, the crisis.

4. Having three "CPs" between the war room, first floor, and 3rd floor CPs hampered information sharing and created a lot of duplicative effort.
    - Key recommendation - Centrally locate all CPs into one location. This is a basic tenant of crisis management response planning.

5. Effectively addressing the lead evaluation "bucket" was a problem, b/c we did not have trained lead managers or trained lead evaluators in the office who could in turn train other field offices and WFO staff until much later in the process. We were seemingly re-creating the wheel of what should already exist in the crisis response plan and training.
    - Key recommendation - WFO needs to have certain squads and SSAs trained on lead evaluation and lead management to more efficiently respond to a crisis.

6. Information flow to squads, subject tracking, and case coordination within WFO was a mess for a couple of weeks. Key processes like the facial recognition tracking, assigning cases, video training/photo distribution to investigators, needed to be addressed more efficiently and effectively. (additional details below). Some of this is inherent in responding to any crisis, but

having a clear chain of command and unity of command across the lead case SSAs and ASACs would have helped with that.

- Key recommendation - designate a Crisis Management Coordinator (or SSA to fill that role) as well as clear chain of command/authority for the crisis response as soon as an event occurs to lead the crisis response posture of the office.

Some background details, but I believe my points above covered them:

- The initial lead process was a bit rough in part because they set out the guidelines and then once we were working on it, sent out a lot of changes, additional info, etc. I know it is tough trying to develop the system and sometimes you have to learn as you go, but it is also a challenge to try to learn it, work it and then have relearn it all because of the changes. I'm not sure how much of it could have been helped, but maybe a little extra time on the front in planning the workflow would have smoothed it out. Another place that would have helped was with the face recognition process. They might have figured out earlier on that the information was being stripped out.
- I guess related to that, or maybe more of a systems issue…the MPD email tips seemed to come in ok, but the text message tips were really messy and usually the images came through separately from the text. It made it difficult, if not impossible to marry up the images with the text, so the information often had to be submitted out of context. Hopefully that makes sense. Not sure if there is a way to address the software or system that handles that, but if there were a way to make sure the images and text stay connected, it would be more helpful and reduce the extra work.
- There was also a lot of redundancy in the video review process. You end up reviewing the same images a LOT. I think the derivatives tags helped with some of that, and I would not have the slightest idea of how that might be addressed in the system, or if it can be without risking a loss of information. I would guess though, that maybe a quarter to a third of what we reviewed included repeated images/videos. I'm sure someone smarter than me who understand the tech, could find a way to streamline it.
- Last thing I can think of we already talked about a while ago. With the RO4 (pipe bomb suspect) only one image was included in the initial instructions for what to look for. I found some better images that were on our FBI.gov site and sent them over for distribution, because they showed the individual's outfit in better detail. When I sent that over, they went ahead and sent out multiple other photos that I had not seen and that were not on our website. So that communication maybe could have been a bit better/faster. Those extra images ended up being really helpful, but I feel like we lost some time/opportunity in not having them as soon as they were available. All that said, to be fair, maybe they did send that out as soon as they could. It didn't happen until I reached out with the other pics though, so I am not sure. Bottom line, just sending out additional information as soon as possible, if it will help when looking for a needle in a haystack

[redacted]

**Comment #1**

1) Both June and January did not implement the Crisis Response Plan despite there being a clear format and schedule for crisis response. Accordingly, you had entire criminal [redacted] agents, for example, respond on-scene despite the fact that they then had to return the next day for

their newly appointed shift. We're being told to be familiar with the plan and our response requirements, but it does not seem management values or is familiar with the CRP.

2) As in June, agents were again deployed onto the streets (specifically around the Capitol) and simply told to stand behind MPD. No other direction. When asked specifically what they were supposed to do or who to check in with, they were told simply that management said to go there and there was no answer. FBI agents do not have training for, nor equipment for, riot control. MPD looks at the agents as a liability standing behind them with no equipment and no comms. At one point, MPD told them to put their gas masks on, which of course they did not have. Management cannot keep sending agents into harm's way simply as a show of force.
3) Related to 2, if agents are going to be sent out for riot control, then WFO needs to stock up on helmets and gas masks.
4) There was very unclear leadership over the command post. There were multiple ASACs, and occasionally some SACs, covering shifts, but who was responsible for overall decision making? What answer you got seemed to vary depending upon which shift you were working. If there was a command structure, it was not apparent, which means a communication issue.
5) It took far too long for the office to get out of emergency response mode, which caused significant problems in advancing the ultimate investigate mode. There seemed to be no one looking at the big picture while everyone else was running around. Perhaps this would have been solved by relying on the roles and responsibilities laid out in the CRP, but having people step out of processing information and look at what gaps there on the process and what will be needed long-term to then start implementing process and procedures sooner. It was a mess for over 2 weeks with pieces of intel and process being emailed out office wide before people started putting ponies and SOPs into the sharepoint system. There was no way to keep track of all the emails and "word of mouth."
6) HQ has resources, and they should have been tapped into sooner on this. This event was not just "in D.C." It affected the U.S. capital. It was a nationwide event. Processing of tips and lead eval could have been done by a significant number of HQ bodies, and allowed WFO to focus on the investigative and legal process steps.

**Comment #2**

1. CI-4 SSA [redacted] did an outstanding job as my shift's lead manager. [redacted] immediately stood out as a leader and problem solver. During shift change meetings, [redacted] was instrumental in addressing any issues the investigative team was facing and quickly offered well thought out solutions. [redacted] helped devise and implement a plan to streamline the lead screening/assignment process that immediately increased the quality of our leads. [redacted] was always positive, calm under pressure, and a pleasure to work with. If possible, I humbly recommend singling him out for praise with his ASAC, Derek Pieper.
2. ADIC Visibility: During the June riots, we never saw or heard from the ADIC. I know there was a lot going on behind the scenes, but that lack of visibility and communication played a part in the confusion and uncertainly felt throughout the division at that time. It was important that the ADIC was seen and heard from often this time, and that he regularly attended shift change meetings, even at times he didn't have any pertinent information to pass. Just being present was important and I appreciated it (but the tropical background during Teams meetings has got to go!)
3. Subfiles: Letting Case Agents actually be Case Agents was key to giving everyone ownership of this case and help it run smoothly. After the confusion of doing a non-FBI mission in June, there was immediate buy-in from our folks when we were allowed to go out, be investigators, and

build cases on our own. It's easy getting our folks to support this mission when they are allowed to do what they do best.

And one simple suggestion:

4. Mission-Type Orders: The night of 1/6 was understandably chaotic. We were instructed to park at UCSCP HQ, but had no direction about where to go or what we were supposed to do. I took my squad down to the West lawn of the Capitol where we linked up with [two other squads], stood behind MPD as they cleared out protestors, and then quickly realized we'd be useless if the crowd decided make a concerted push to get back to the Capitol. For these types of situations, I think a simple mission-type order coupled with a Commander's Intent statement is essential (i.e., arrive at Capitol Building, make contact w/ X, strong point Capitol to ensure it is not over-run). If I'm given a mission type order and a Commander's Intent, I can better figure out what to do on scene, and also advise when there might be better ways for us to accomplish the overall intent.

**Comment #3**

1. Streamline the lead process –
    - One team, or a certain number of squads, should be assigned as lead managers and that is their assignment for the duration.
    - Improve the lead tracking process to decrease the number of duplicative leads.
    - Eliminate the ability to circumvent the lead process.
2. If in the future there is a plan to include logistics SAs in the CP, canvass WFO for SAs volunteers to be part of the crisis response / CP team. There are IAs and SSAs who have this assignment. For those volunteers, there should be a baseline briefing/training on the roles needed in the CP, so that folks know what to expect once a CP is initiated.
3. Accountability for number of leads squads take on to ensure it is done in a more equitable manner. It appears that leads/cases were mostly assigned to those who raised their hands.
4. Assign a small team of SAs to cover grand jury, similar to the duty AUSAs. This will expedite the GJ process.
5. If a crisis event and the office response will last for weeks (as it did in this case), incorporate a duty schedule to increase efficiency. For example, (if feasible) squads could be divided into Alpha and Bravo Teams, with alternating days in the office. This could alleviate the following:
    - Overcrowded office space. Having all personnel in WFO at the same time was not efficient. Lack of parking, computers, etc created unnecessary problems.
    - Have a "back-up" team in the event of a secondary crisis.
    - Avoid burn-out by employees
    - Employees can assist and work leads/cases remotely on days they are not in the office.

**Comment #4**

- The Crisis Management Plan should be updated to include WFO's expected response to riot situations, and the plan should be articulated often (i.e. during quarterly legal training). Though the plan is on WFO's site, management has to own the articulation of it to the workforce. People do not generally know what to do in a crisis situation.
- Both oral and written communication should be better in timeliness, accuracy, and succinctness.
- The visibility and presence of senior leaders is very important in crisis situations.

- There should have been some guidance regarding clear articulation of violation of the pertinent laws. For example, we were seeing many leads initiated by lead evaluators regarding claims that individuals had been present at the Capitol. Background should have been provided to those involved in the case such as:
    1. Was the protest lawful;
    2. What were the boundaries of the Capitol that were restricted (barriers/ walls/ doors/ scaffolding etc.) so it would be clear to agents based on locations of potential subjects whether their location was or was not a violation of a law;
    3. Similar education could have also been pushed out to the public in so far as when the public is providing tips, they would be aware of what was and what was not a violation of federal law, and they could provide pertinent details in their complaints that would better direct the investigation (a lot of the complaints received were that so and so was present at the riots or insurrection – this does not address whether they were participating in the protest or violating a federal law). This lack of education could result in potential issues for the bureau regarding actions that may have been taken against protected speech.
- After the inauguration and any potential ongoing threats, it was unclear why WFO continued to operate in a crisis/shift mode. The explanation the field was given was that "it's important," however, to trained investigators, this does not answer the question of why we needed to operate in a shift mode. For example, if the answer was because the field needed to be ready to deploy, then that explanation should have been provided and then any intelligence regarding the pending threat should have also been communicated so the field could be prepared to address the type of situation we may be asked to mitigate. If there was no pending threat, then it seems like WFO could have asked agents to give a certain number of hours per week devoted to the case or different metrics to meet. There did not seem to be a clear objective for what was needed to be accomplished to move us out of a crisis posture.

**Comment #5**

1. The initial response of having us again respond to a riot by "standing the line" did not seem appropriate because we do not have the gear, equipment, or training for riot control. Our deadly force policy is also not equipped nor do we have continuum like the police in a riot situation. If someone were to throw a brick at an Agent, the Agent would be justified in using deadly force under our deadly force policy. Police have other options like rubber bullet etc. Also, many times we are a 3rd party investigator to civil rights violations; therefore, we must appear neutral in these situations. This was the same feedback I gave through the SAAC during the summer riots to ADIC Slater. It further concerned me when they issued us bike style helmets as if the situation could easily happen again. I think they need to give us the training or gear for riot control or we continue to stick to what we are good at which is investigations.
2. In our squad's case, I did not understand the need for 24/7 shifts in order to work the cases. We could have worked our cases during the day, and been on standby during the evening in case a response was needed. By working at night we were not as productive due to exhaustion.
3. I was upset to see they were not sealing the complaints or a very least redacting Agent's names on the initial complaints. This puts the Agents in danger unnecessarily.

**Comment #6**

As requested, I am passing along some the responses received re: the events of 1/6/21, and our Division's response thereto. I have copied and pasted, in the raw, responses from members of my squad, though I have reserved their names at the moment. If needed, I can provide those, but I believe the information contained in their responses is more valuable than necessarily who made the comment.

The two overarching themes that I found in the responses were:

1. We found ourselves repeating some of the same responsive actions that we employed during the summer, and did not really seem to learn from what worked well and what didn't from prior events. This mainly concerns the lack of guidance on a specific objective during the call out response. Specifically, we were not issued a clear SMEAC on our deployment to assist MPD and CPD elements, nor was the specific legal authority outlined, and in my experience that night, there was a good bit of justifiable concern over deploying agents to the scene of a potential violent riot armed only with our sidearm and issued tactical gear (a vest). As with the summer, our response opened the office up to the potential for additional Hobbs Act issues/photos as we saw, or worse yet the potential for significant injury to personnel who are ill-prepared and ill-equipped to engage in crown control activities/assignments.
2. The lack of adherence to the approved, documented and disseminated crisis response plan, resulted in conflicting or incomplete orders pushed down to the ground elements. The fact that the crisis response plan was not followed had lasting impact in regard to the ongoing responses, shift work, etc.

Below you will find unedited responses from the members of my squad that responded to me.

- My first concern involves officer safety. We are lacking in training and equipment to fulfill a crowd-control mission. Placing rank and file agents in that situation is unsafe for us, unsafe for our law enforcement partners, and unsafe for the people with whom we interact. I fulfilled a similar role while on a SWAT years ago, when we responded to civil unrest. We, as a cohesive tactical team with extensive training, abundant equipment, excellent communications, and a clearly defined chain of command, were still unsure of precisely how to best accomplish our mission – it was well outside our normal operations. It is unrealistic to expect that a group of agents thrown together at the last minute should be able to take this kind of thing on in a safe and effective manner.
- Similar to the BLM situation over the summer, we were asked to fulfill a nebulous mission without being provided a clear objective or methodology through which to accomplish it. In the BLM situation we had virtually no objective at all. In the Capitol matter we were told to back up MPD as they moved protesters down Constitution Avenue. Within minutes that objective was out the window as we had no legitimate contact with MPD and were instead placed in a skirmish line keeping protestors away from the Capitol. Our lack of training and capability for that mission quickly became apparent, as protestors were allowed to meander in and out of our ranks without consequence. This was a function of us not having a clear sense of our mission or our specific authority to act.
- Regarding our authority, our legal guidance essentially boiled down to being told the deadly force policy and then asked to use our best judgment. While I am confident in my judgment, I do not think this is an appropriate way to go about our business.
- I remain confused regarding our initial call-out. Throughout the early hours of the crisis, we received separate and conflicting guidance. On one hand, the crisis response plan was initiated and we received specific guidance as to which squads should deploy and which squads should

not. As you are aware, our squad was on the list of squads to remain on call and plan to arrive at 0600 the following day. On the other hand, you passed on information from the ASAC indicating we should ignore the crisis response plan notifications and instead deploy immediately. I am interested to know what decisions led to this disconnect, as we devote significant resources to planning our crisis response.

- I'm concerned that, organizationally, we did not learn or implement any changes from our response this summer (the BLM/Threat to monuments). We were again put out on 1/6 with no clear mission, into a crowd control situation without appropriate gear or training. Agents repeatedly asked what we were doing and how were we to respond. There was no significant guidance beyond "use your judgement." We were told we were not to be on the front line, but to be behind the police in a "support" role. However, we were then deployed on the flank of the police line with direct contact with the protesters. While we were not confronting the thick of the crowd, we did attract small groups of disgruntled protesters and were lucky they chose not to escalate matters or that others did not join them. It could easily have gone badly. This was aggravated by several pods of 2-3 agents that would either be behind our position or took it upon themselves to wander 30-50 yards ahead into positions where they could have been cut off and isolated. It was poor judgement, but we cannot ignore that it highlights a lack of training of how to work crowds.
- When the decision was made to deploy us initially, it appeared to be all of [WF's criminal division] going. While in our cars responding, we then received email and phone alerts saying the crisis action plan was being initiated. A specific list of squads were told to report, conflicting with the initial directive. We then received word to ignore the alerts. The question is why? Is the crisis plan deficient? Is this sort of circumstance truly not considered? It would appear that for the second time in 6 months, the plan to which the FBI has committed significant resources has been found to be unacceptable.

**BLUF**: Good emphasis from lower and middle management to sustain workforce. Computer systems as well as cumbersome resource/personnel management degraded efficiency and productivity.

**Sustain**:

- Lower and middle management efforts to sustain workforce- There was a continuous effort by lower and middle management to allocate RDOs and move "shifts" to a more intuitively logical time period (e.g. not between the hours of 2100 and 0700). These efforts allowed for a sustainable operations tempo.
- Turnaround time for facial recognition and providing TTK accounts- Two of the most used tools for this incident were TTK and facial recognition. Support for these systems was timely and effective.
- Information flow- Though there was an unnecessary amount of FRAGO and changes, there was a consistent effort to convey information to the lowest level. This helped sustain morale, and promote a sustainable operations tempo.

**Improve**:

- Utilization of organic workspace- WFO Squads have workspaces, individuals and squads have their work area, desks, and computers set up to be efficient. Moving squads from the NVRA to WFO for non-field work was counterproductive and unnecessarily degraded efficiency while providing negligible benefit. Degraded efficiency included but was not limited to; finding workspace each day given constantly changing "shifts," parking, congested work area (especially

during COVID), system access issues and bandwidth, decreased maneuver capability outside city limits, tools and supplies spread between normal work area and squatting work area, etc. Negligible benefits include; physical proximity to executive management, and access to technical support.

- 24-7 Shifts- There is limited utility in working full staffing between the hours of 2100 and 0700. There are virtually no active investigative actions that can be accomplished during that time. No one will be knocking on doors, calling witnesses, reaching out to businesses, etc. Individuals working during that time are essentially relegated to database searches, and video review.
- IT systems- There is significant room for improvement. For example since physical UNET machines have been phased out, in order to access TTK agents must log into their virtual FBINET desktop, from there log into their Virtual UNET, from their log into a third VM hosting TTK. When individual video files are up to 16GB and you are accessing the file through 3 virtual machines relying on the stability of just as many overloaded and out dated network connections, efficiency is diminished. Agents should be provided with more powerful laptops, that can handle large video files, and be encouraged to find WIFI that can handle accessing TTK through non UNET/FBINET systems. Food for thought, a single moderately powerful laptop would cost less than the overtime and holiday hours paid to a single agent during the month of January, and that laptop would have saved the agent more time then they ended up billing for overtime and holiday pay.
- Triaging leads- This is probably the single most important area to increase efficiency. Duplicate leads or leads that have no substance should never make it to a squad.

1) The response on the day of was chaotic and appeared to not be in accordance with the crisis response plan. The DENs message conflicted with instructions we were getting via email. There also did not seem to be any type of organized strategy when we arrived on site. It was unclear what our responsibilities were supposed to be which meant we were in a situation where we were interacting with some of the protesters without really knowing what our authority was for where or how to direct them off the grounds.
2) Specifically related to my role in the command post, there was no apparent or consistent chain of command for those of us that came on in an ad hoc fashion vs. as an entire squad; this was most challenging when it came to scheduling as the command post was winding down.

There seemed to be animosity from other field offices that they had to dedicate resources to “our case”. Although I am not certain what was driving that, perhaps enhanced communication/messaging at higher levels from WFO to other field offices could help alleviate some of that. Understand that people’s personal feelings are what they are, but it was disheartening to feel like we weren’t all one team.

**Comment #7**

INCIDENT MANAGEMENT:
I believe the most critical missing component in the response to the Capitol Incursion was a single individual in charge of the event. I believe this individual should be an ASAC because at that level they remain close enough to Ops, have a solid understanding of Administrative requirements, and have the authority to make decisions with little oversight. I think it goes without saying this should be an ASAC with strong experience with criminal process and ideally with crises. From my vantage point, it felt as if we had six ASACs in charge, two for every shift. This does not allow for effective continuity from shift to shift. All ASACs were well-meaning, but when communication between shifts broke down, it caused

significant inefficiencies in decision-making and I believe was one of the causes of the chaotic environment, particularly early on. Continuity means the ASAC in charge is there for the majority of the day, say 7a-7p. This allows for a single decision maker who will make decisions on the spot or help triage those decisions with subordinates, peers, and/or superiors. This individual, because of his/her enduring presence, will have at least a basic understanding of the multiple components of a given crisis, and how those components interrelate, allowing for effective decision-making. That ASAC-In-Charge would need a strong deputy who is in lock-step, to cover down on overnight shifts, in addition to a strong individual like Runyan for example, who took charge of scheduling, etc. As screwed up as the June crisis was, at least we knew we had a constant presence in ASAC Vorndran. We knew he was the one go-to leader who would handle immediate decisions and engage EM when necessary. For as long as I can remember, we have always had an "On-Scene-Commander" so to speak, during a crisis. For some reason we have moved away from this. Sorry to belabor this point, but I cannot say enough how critical I believe it is.

WFO CRISIS RESPONSE SCHEDULES:
As you know, WFO has a well-established, long standing crisis response schedule. One that for as long as I can remember, is immediately tossed out the window the minute a crisis begins. The reasons for this are WFO EM has failed to review the schedule, has reviewed but did not find it applicable, or tried to implement it and failed. Regardless of the reasons, the schedule is clearly ineffective as written. I will use the example of [my squad]. My squad, per the crisis response schedule, does not start its first shift until 72 hours into a crisis. A full three days after the initial "boom." It is clear to me the schedule as written is not nimble enough to be adapted to every, or at least most crises. In my view, the crisis response schedule should be simple enough to be committed to memory and easily articulated in 30 seconds or less. Instead of scheduling out every squad three days out, consider scheduling Branches or Divisions. For example, if it's a CT crisis, CT Division [redacted] will respond to office immediately, [redacted] will be on standby, and so forth. Same if it's a criminal crisis. Our specialty teams/response teams will follow their crisis protocol. Admin can do the same to support ops. We have, as an office, proven repeatedly this year we can respond quickly to a crisis. We can add structure to the schedule as the crisis evolves over the first three days.

MISSION:
While I know much has been said about being asked to conduct a mission for which we are not trained or equipped. We must be mindful of the fact there are incredibly effective ways for us contribute in any crisis without having to resort to a "show of force" in the streets where we are largely useless. The obvious one, intel teams, where we are in plain clothes, gathering useful intel for MPD/USPP, etc. This is a proven model that has worked incredibly well for as long as I can remember. This worked incredibly well in early 2000s when agents would ID trouble makers and MPD would respond to remove them. Simple yet effective. While I think most of us would accept any mission given to us, WFO EM should be prepared to offer solutions to our partners that utilize our strengths.

FEEDBACK:
During the June crisis, feedback was sought from everyone on how we could improve. We provided feedback, and heard nothing afterward. Nothing crushes morale more than telling our people to provide feedback so we can make things better, and then never coming full circle to tell our people how we made things better, what we plan to change, or keep the same, etc.

[redacted]

**Digital Evidence Collection Best Practice**

1) **Obtain a Google Geofence warrant**
    a. A Google geofence creates a perimeter around a location which Google and use to provide records show were within that location during the specific time period provide. If the device has a Google Account (Gmail, google maps, chrome etc), Google will return records associated with that device as well as the devices approximate location during a specified time.
2) **Obtain AdTech Warrants**
    a. Ad Tech describes an ecosystem of companies and tools which leverage data derived from user devices to target them with ads. This data includes users' IP addresses, ad ids, pages visited, Apps used, past purchases, location data, other social demographics, etc. Ad Tech companies collect all this information and link it to an anonymous ID number, such as an Ad ID. Please note, some Adtech companies are ECPA providers while others are not.
3) **Obtain Cell Tower Dumps**
    a. A cellular tower dump requests obtains a list devices that hit a specific tower in a given location during a time period. Each carrier will provide devices that are utilizing their specific networks. This technique requires that the cellular device actually was in contact with a tower at some point within a defined time period.

*CAST and IS-2 can assist investigators with search warrant returns, location mapping, as well as assist with identifying follow-up legal process which can develop evidence and intelligence.

**Audio/Video Collection Plan**

1) **Create the Digital Evidence Response Team (DERT**), with individuals who are trained in DIVRT techniques, Digital Extraction Technician (DEXT), Field Audio Video Program (FAVP), and Triage Tool Kit (TTK). This team would be similar to ERT, but would be dedicated to the collection of digital evidence. This would be separate from the CART program, but would serve as a team to complement CART capabilities.
    a. WFO has approximately 15 individuals who are DIVRT (Digital Imaging and Video Recovery Team) trained including three CART examiners. However, these individuals are spread across the entire division with no protocol or requirement to participate as a DIVRT member.
    b. All DERT personnel would be subject to call out similar to ERT.
    c. DERT personnel would be required to attend regular training and provided with equipment needed for DIVRT and DEXT extractions.
    d. Include DERT in the Crisis response plan (see Boston's CONOP for Digital Evidence Team).
2) **Install DCAP @ WFO** for a faster review of digital evidence @WFO.

## Counterintelligence

*The WF CI CSSA collected information via individual interviews with each SSA. Responses are summarized below.*

- Lack of a cohesive command and control structure which led to operational inefficiencies and an environment of uncertainty and indecisiveness. There was no clear ownership/direction.
- EM failed to communicate the role for the FBI during the unfolding event which led to poor coordination across the field office.
- EM failed to designate a responsible SAC from the onset to help prepare for the investigative process and deconflict questions.
- Requests, orders, taskings, and concerns were coming from several different SACs at one time. There was no continuity for EM and there were redundant requests happening daily from different EM.
- Failure to identify specific roles from squads and specific squads for the investigations led to ineffectiveness and confusion in handling the first actions surrounding two major investigations
- Communication to the division was poor. There were no EM briefings to the teams working various assignments to understand role into overall investigation. This should have occurred on a daily basis from the SAC in charge of the investigation.
- EM was disconnected from the workforce and did not properly address and update the field office

- There was no clear understanding of the overall process and you were asked to perform tasks outside your process lane. EM should be in charge of process flow and documenting each role and provide guidance to teams.
- Changing the lead to CID with no one prepared to pick it up, once it was determined that wasn't happening there has been no update from EM on the structure or organization of the case. It appears WFO EM no longer cares about the investigation however teams are still working daily on it.
- Shift work for 24/7 should have been scaled back earlier. The prolonged posture with no real need led to morale issues and tiring out the workforce.
- DOJ/HQ messaging across the field to identify this issue as an FBI priority. The field was echoing that this was a WFO investigation and not an FBI investigation. Guidance from the D/DD level should have been provided early and often indicating this was a full FBI endeavor.
- There is a Criminal SSA who is doing a phenomenal job keeping all of this together however it is not in her job role or even chain of command to be doing this and it adds to the perception that no one wants to be in charge of this investigation.

***

- Lack of investigative command and control caused delays in the investigative process and caused the lack of a standardized investigative process. Having a standard process in place prior to an event may alleviate this.
- EM should have placed 15s with previous crisis response experience in key roles and should have limited turnover of the 15s to avoid confusion and reinventing the wheel at every shift change
- Initial briefing cycles were too redundant and not spaced appropriately. This led to the revolving door of 15s trying to manage data for the calls instead of the investigation.
- Remaining in the crisis case posture once the situation stabilized created unnecessary redundancies and an unnecessary admin burden.
- The investigative case team should have had an SSA/SA embed with video coordination team to deconflict leads and investigative matters. This task was all program management. MXU assistance needs to be available and someone should be here to assist in a timely manner. Once this team is established it will allow an easier transition of resources once the crisis has completed and the investigation needs to continue.
- WFO needs to better understand our digital evidence and how we collect and process it. Also WFO needs to understand how all of this digital evidence will be utilized during discovery and provide guidance.
- There is an overwhelming number of TTK leads that will one day need to be transitioned to real leads. This will amount to over 2000 new leads that no one is aware of or looking into. No one from EM seems to understand that there is an overwhelming amount of unreviewed information that needs to be addressed ASAP in TTK. There are 9000 intakes that have been tagged as relating to an investigation which require someone to review and put into Sentinel.
- Currently the video review coordination team is led by an SSA and three rotating SSAs and two rotating SAs. This team of five needs to be reduced to one competent person to work with the lead SSA and MXU.
- Continuity of leadership was not established. SACs were changing, ASACs were changing constantly. Every time investigative momentum was gained we had to restart. To alleviate this issue WFO needs to identify key roles and responsibilities. Follow through on the endeavor and prevent Groundhog Day.

- There were no clear owners of the two main investigations from the beginning. Although there was lack of ownership at the beginning the division still feels that we still do not have a clear focus on where the case is going and who is in charge.
- HQ is not stepping up to help coordinate all the moving parts and field offices becoming resentful of WFO as WFO is trying to PM cases.
- Need to prepare better for partner liaison work. Several partners were thrown into the CP with no direction or guidance from EM. Investigators wasted several days trying to figure out what was required. Identifying SMEs from those relationships prior would help eliminate wasted time.
- WFO should create alternative CRPs for different types of events. Also exercise the plan periodically. Management needs to experience the CRP and build muscle memory because of the executive turnover. Have crisis management experts on shift.
- Organizationally look at our responses from the summer vs what we did this winter. Make sure we do not be observed as political.
- Field is willing to help but FBI was not paying field offices for OT or weekend pay. HQ needed to incentivize the field.
- Better explanation of COVID posture during command post and transition to major case.
- 15 ASACs is too flat of a structure to coordinate a whole of office effort. There needs to be an SAC of who owns it. Maybe two shifts and an org chart of what was happening.
- Did not move enough resources to the 266 quickly.
- Make sure intel and ops are communicating with each other. Work was getting done on intel that was not making it down to the ops agents.

# Counterterrorism

## Capitol Incursion CTD/CIM AAR Executive Summary

A review of detailed comments provided from across the CT/CIM division has identified the following key areas with respect to best practices and areas for improvement related to the events on 1/6/21 and the follow-on investigations. A review of comments indicated varying perspectives on similar topics in several instances, which can be an indication of a lack of consistency of application and execution in those respective areas.

**Best Practices:**

- Use of SharePoint was very helpful as a central repository for information and updates.
- Identification and assignment of SSA logistical roles in the CP assisted in organization, workflow and finishing tasks.
- Long term planning of schedules for lead review, etc. assisted in allowing personnel to coordinate personal schedules across extended periods.

- Positive speed of seeking information regarding AAR comments.

**Areas for Improvement:**

- Lack of clear implementation and adherence to the Crisis Response Plan (CRP), along with a lack of broad training across the office to ensure personnel understand their roles and responsibilities.
- FBI technical infrastructure insufficient in several areas including UNET bandwidth, uplift and downdraft applications for operational and analytical needs, particularly TTK.
- BOLO releases would benefit from greater coordination POA, substantive investigative squads, lead pool squads, and TTK review teams.
- NVRA personnel would have benefited from pre-deployment briefings prior to being sent to WFO, the ability to remain working at NVRA as much as possible, assigned temporary workspace for NVRA personnel at WFO, and more parking availability at WFO.
- EM communications could have benefited from limited SITREPs to SSAs and line personnel, getting HQ approval prior to socializing office structure changes, and better synchronization of messaging with DOJ.
- SAs should maintain basic skills and access to tools that allow social media exploitation.
- The office would benefit from a better defined and accessible process for gaining Intelligence assistance.
- The office should find a better method of avoiding duplication of effort while working on tips from the public.
- TTK reports are too long and confusing to efficiently decipher and use. All SAs working a crisis event should have TTK training prior to the event, and TTK reports need simplified.
- If WFO is going to be working crowd or riot control, they should be equipped and trained for that mission.

## Capitol Incursion CTD/CIM AAR Detailed Comments

### Best Practices:

- **Use of SharePoint** - Establishment of SharePoint on UNET to house all ponies and POCs was extremely helpful as a central location for information. Organization and frequency of updates could have been better, but the idea of a centrally located repository was helpful.
    - Recommend quickly mirroring on FBINET
- **Assign competent SSAs to handle logistical roles in the CP** - The establishment of the logistics and special projects SSA and staffing those positions with the same SSAs every shift was helpful and removed the need to have to rely on rotating ASACs across multiple shifts to perform those functions.
    - Recommend building these roles in to the CRP and pre-define individuals who will fill these roles in a crisis response so they are appropriately trained and can develop effective ponies.
- **Building shift schedules out days in advance** - While shift scheduling was a source of frustration, there were two blocks of time where schedules were built out days in advance. This was incredibly helpful and allowed people to plan personal lives while being able to effectively respond to tasking. Waiting until less than 24 hours before releasing a shift schedule was difficult to plan for.
    - Recommend following schedules already built in to the CRP for consistency and decreasing the need to make changes.
- **Conducting an AAR** - Arguably, some of the issues experienced during Capitol response could have been addressed or at least discussed if an AAR had been conducted.
    - Recommend a WFO wide AAR after every event or crisis response.

### Room for Improvement:

**Crisis Response Plan**

- **Lack of clear implementation of the CRP** - The CRP was not implemented in any meaningful way beyond an email saying it was activated. Squad assignments per the CRP were replaced with ad hoc, unclear squad tasking. In the span of 12 hours, some squads received 3 different assignments with varying report dates and times, the last being an email sent from an SAC of another Division at 1230 am to report 2 hours earlier.
    - Recommend reviewing CRP and establishing a simple yet flexible framework which can be applied and adapted to various kinds of responses. Continuing to reinvent the wheel mid response makes WFO less effective in managing a crisis and the follow-on investigation.
- **Little training provided to Agents in anticipation of crisis situations** - Large scale civil disturbances with tens or hundreds of thousands of protesters/rioters/looters require potentially thousands of law enforcement officers to contain. A response into the city may not necessarily be limited to an "investigative" capacity but may evolve in unpredictable ways. Agents may respond to a scene as investigators but may need to immediately transition into an

active first responder role (active shootings are occurring, or a detonation etc.) As everyone is aware, there is a difference between FBI and TFOs responding to a crisis as "First Responders" vice Investigators. In the case of the civil disturbance and the Capitol Incursion there was some ambiguity as far as initial roles and understandable apprehension.

  - Recommend periodic training for this before an event is critical coupled with round tables both on a squad level and broader field office are imperative. Interagency cooperation and joint training is key for response and on the ground integration. The National Capitol Region is an area with a high likelihood of protests, riot activity, and general violence. A bi-annual joint training and coordination exercise (JCET) with all the relevant partners will go a long way in clarifying lanes of responsibility, incident command, communications/signals, immediate actions, safe havens, triage locations, riot-control Tactics/Techniques/Procedures, urban isolated persons procedures (agent becomes separates from his squad.) Agents are constantly rotating to squads so it's imperative that this training happen regularly so all agents are equipped properly in terms of equipment, comms, and mission objective. Also, a solid presentation from Capitol, Park, and METRO PD on civil disturbance procedures would help agents understand how local PD moves crowds throughout the city is paramount for advance situational awareness.

- **Lack of use of Crisis Response Plan** – Crisis Response Plan was activated on day 1, but was not adhered to. EM went to locations they were not designated, squads were pulled to places by an executive who did not coordinate with the command post, roles identified in the plan were not filled and the preset schedule was not adhered to.
  - Recommend continuous training of the plan and actually following the script. If the plan is not going to be followed then create a framework which will so the office is in a better place to respond. Mandate training on the plan for everyone from line level employees to front office personnel.

**Challenges of UNET Infrastructure**

- **Current FBI UNET infrastructure is insufficient for large file captures/downloads** - SAs spent days trying to get legal returns simply downloaded because of insufficient FBI IT infrastructure. UVDI was incredibly slow and would either crash or time out before returns could be saved. Even standalone UNET machines were too slow to download returns resulting in the Provider LE portals timing out. SAs were forced to utilize standalone laptops purchased via case funds and home internet connections to download returns. Because uplift is capped at 100MB, there was no way to move returns from UNET to FBINET and even then, Sentinel's 100MB 1A file size limit meant returns had to be saved to USB thumb drives and saved as physical 1A envelopes.
  - Recommend raising the max file size limit on Uplift and Sentinel to 10GB. This will enable most returns to be captured in Sentinel. If you can't fix UNET bandwidth or UVDI (which is borderline unusable), either create a standalone HQ unit or task Field Office Computer Services to support downloading large files in response to SWs. Make it a requirement that all social media/email SW returns are uploaded to DWS. E-mail and social media SW returns are the one type of data DWS is well positioned to handle and it makes the data available to the enterprise especially via DIVS searches. Otherwise, there are TBs of SW data sitting in physical 1A envelopes that are unsearchable to the

enterprise. This is significant risk for the organization and needs to be addressed immediately to ensure we have all available data to make investigative connections and prevent subsequent criminal activity.

**BOLO Challenges**

- **Insufficient BOLO tracking** - BOLOs were released by WFO PAO. Initially, BOLOs were haphazard with little context or prioritization. Once AFO BOLOs were released, there was little to no communication with other investigators that the BOLOs were being released and no prioritization. No subfiles were opened before the BOLOs were released so even if information came in about a BOLO, there was nowhere to house this information beyond the 176 and 89B main case files. As a result, BOLO tips got lost in the sea of information. Additionally, no case agent or squad was initially assigned to the BOLOs for days. As a result, even if investigative squads, through their own investigation, identified BOLOs, squads had to hunt down CR squads to open BOLO subfiles. Even once subfiles were open with IDs on BOLOs, many of the subfiles sat (and some still sit) unworked because CR wanted CR squads to work the subfiles. Lastly, BOLO status updates were inconsistent and untimely. BOLOs were not updated to the public on a consistent basis so crowd sourcing online actors would expend time investigating BOLOs that had long been identified. Even after a month, the subject tracker does not consistently capture the accurate status of all the BOLOs.
    - Recommend BOLO releases be coordinated across POA, substantive investigative squads, lead pool squads, and TTK review teams. When a BOLO is released, a BOLO subfile, case agent, and tracking mechanism should already be in place. Like the 176, let non-CR squads run point on 89B cases to relieve the crushing burden of all those cases falling solely to CR. If this worked for the 176, why wouldn't it work for the 89B (for that matter, do we even need the 89B)? Once a BOLO has been identified, all parties at WFO should be notified and this should be denoted in an easy to find repository. Once a BOLO has been arrested, the BOLO on the FBI website should be updated immediately. Lastly, proactive use of social media and an army of online actors would (and still could) be a force multiplier in crowd sourcing BOLO identification. Use of hashtags and strategic CHS recruitment would allow for FBI to better direct crowd sourcing efforts. Groups like Seditionhunters and Capitolhunters on Twitter compiled photo collages and established hashtags that were much more effective than grainy BOLO photos released on the FBI website. The FBI should work in tandem with these groups to streamline online efforts.

**Challenges for NVRA Personnel**

- **Mandatory assignment of all participating SAs to WFO** - At the outset of the Capitol response, all SAs were told to report solely to WFO. This is understandable for the initial response and day following. However, once the incident response ended and the office moved to an investigative posture, requiring all SAs to only report to WFO was inefficient and made WFO less capable of effectively investigating. Because RA personnel did not have assigned desks at WFO, RA SAs were forced to squat at random desks with little to no infrastructure to support them. Many WFO SAs would not allow RA personnel to sit in their desks. Parking was insufficient for all WFO personnel to report at the same time. Once security ramped up for inauguration, it took SAs

hours to get through check points. At the line level, the decision to require all SAs to have to report to WFO seemed more focused on the optics of how WFO's posture would look to HQ. It took weeks for this posture to eventually be relaxed.

  - Recommend once the need for available personnel to physically respond to an incident has subsided, thoughtfully allow squads to work where they are most efficient and can best address investigative requirements. If there is a specific role a squad needs to fill by being at WFO, this is understandable. But requiring the entire office to consistently report to WFO limits the effectiveness of the workforce and ultimately limits the full availability of said workforce.

- **Lack of pre-deployment briefing for NVRA personnel** – There was not a briefing for personnel at the NVRA for personnel that were deploying to WFO. The briefing should have included the traditional S.M.E.A.C. as with all Op Plans written in the FBI. The inability to provide this briefing with the key components indicates a lack of understanding of why personnel are being deployed.
  - Recommend having ASAC and/or SSA conduct a floor or squad level pre-mission brief at NVRA prior to the agents driving into the Capitol or the briefing can occur at a staging area in Northern Virginia (parking lot at a grocery store prior to crossing the bridge in DC.) This will allow for agents to consolidate cars so we save on parking at WFO and also for safety reasons (2-4 agents in a vehicle is safer while driving thru the city which has active civil disturbance and rioting.) It also controls the response and allows for a hasty equipment and comms check and gets everyone on the same page before they drive into a volatile operating environment.
- **Lack of temporary workspace to accommodate influx of personnel** - NVRA agents deployed to WFO were often not able to locate a desk to work. Some WFO desks had signs specifically stating NOT to use those desks.
  - Recommend NVRA agents remain on standby or at NVRA unless absolutely necessary to travel to WFO for multiple reasons, including separating WFO's agent population should something happen at WFO or DC; minimize COVID exposure; and agents can continue to support the mission from their desks at NVRA where they have all necessary systems, including COVERT stations. If NVRA agents need to deploy to WFO, desks at WFO should be available and/or signs like those found should be unacceptable.
- **Unnecessary assignment of NVRA personnel to WFO** - I recognize the uncertainty of events between 06-20 Jan. However, in the future, NVRA Agents should be provided an area in which to sit if called downtown. Especially in the Covid era, we were uninvited guests on the 7th floor, and had to squat at various peoples' desks each day.
  - Recommend allowing personnel to work at regularly assigned workspaces if we are simply being assigned leads which can be handled by running database checks or making phone calls to people outside the DC area. This will help resolve the squatting issue as well as general personnel in the respective offices.
- **Logistical constraints with building access and parking availability** - Parking at WFO was a challenge due to limited parking availability. Additional challenges were created when the inauguration security was added on top.

**EM Communication Challenges**

- **EM communication** - The communication from WFO EM was inconsistent and infrequent. SAs and SSAs went weeks without seeing SACs. Much of the communication at turnover meetings, mostly via rotating ASACs, was focused on managing anxiety and not providing tangible information or direction.
    - Recommend transparency and guidance, even if its bad news. Does the FBI intend to hold everyone who entered the Capitol criminally responsible and plan to work tirelessly as an organization and office until that's done? If so, say this. Do SAs need to prepare to work 7 days a week with sporadic RDOs until this mission is accomplished? If so, say this. WFO has shown an ability and willingness to work hard. SSAs can communicate organizational expectations and plan scheduling in a way that allows for sufficient family support and flexibility. When the workforce does not know the organization's vision and mission for an incident and does not know how long or to what degree that mission needs support (even if it's going to be long term but undefined), anxiety and the amount of unknowns grows. This is corrosive to morale and to the confidence the workforce has in its leaders. WFO EM should be physically seen and communicate meaningfully and clearly. Boilerplate emails about how EM is proud of the workforce falls on deaf ears. Tell us your expectations and we will strive to meet those expectations. Sometimes people need leaders to lean into the mantra "needs of the Bureau."
- **Lack of SITREPs to SSAs and line personnel** - While SITREPs were being circulated amongst EM, SITREPS or pared down SITREPs were never disseminated to SSAs or investigative personnel. Leaks are always a valid concern in situations such as this. However, the workforce had no idea what was going on beyond shift turnover meetings and what was in the media. As a result, SAs who were investigating individuals who entered the Capitol were left to review Sentinel and talk amongst peers to try to figure out broader intelligence gaps.
    - Recommend sending basic updates or SDRs on FBINET to SAs so at a minimum, they know what they should be looking for including modes of communication, group markings, TTPs, etc... Otherwise, SAs are doing their best but with limited direction or insight about the broader picture.
- **Socializing significant changes to Divisions without HQ approval and predetermined staffing plans** - Following the Capitol response, all personnel at WFO understands significant changes would be coming to include the overall structure of the Capitol investigation, changes to substantive squads to manage emerging threats, etc. Having these changes introduced piecemeal without a thorough plan for implementation and predetermined staffing created confusion amongst all Divisions and uncertainty amongst the workforce. Everyone was concerned they would be moved and because of the lack of clarity of future direction of WFO, they had no idea what they could potentially be moving to. This has been increasingly disruptive to the workflow and placed frontline leaders in positions where they do not have answers which diminishes morale.
    - Recommend spending time incorporating all relevant stakeholders to thoughtfully devise an implementation framework and strategy to introduce relevant structural changes to WFO. This should be as detailed as possible and include leadership, specific staffing, seating, and HQ concurrence BEFORE rolling out to the workforce. Inform front line leaders of these changes and when possible, explain rationale for changes so

SSAs/SIAs can proactively work to support EM's vision and allay anxieties/concerns of the workforce. Introducing change in a thoughtful, timely manner expedites buy-in, minimizes uncertainty, and cultivates confidence in leadership.

- **Lack of EM Guidance** – SAs feel they have received little guidance from EM. DOJ and WFO do not appear to be in sync with the pace of these investigations and SAs feel that EM has not made decisions quick enough to get the two agencies on the same page.
    - Recommend EM within WFO coordinate across the divisions and provide clear guidance which is agreed upon by everyone to avoid differences in messaging resulting in confusion.
- **Lack of communication between EM and SSAs/SAs** - There was limited communication from executive management to directly and personally address Agents deployed to WFO to cover shifts and/or the Capitol. SSAs tried their best to answer questions but they had limited or no information to share. There were a lot of emails sent out, but not one clear message from leadership. We did not hear from the ADIC personally until Sunday January 24th when he joined via video and talked to all WFO personnel. Without such direct communication from leadership, agents were left to wonder what was being done, how and why, and most importantly, why their flexibility and availability – to include positive mentality – was going to be essential to address the problem at hand.
    - Recommend SAC or above to do a video lync call early in the crisis at time when most Agents can attend (example 3PM to be able to include those agents who did the overnight shift). The video call should address what occurred at the Capitol or the incident, what EM was currently doing (i.e. addressing how to best use agents to address the needs; explain what those needs are (i.e. leads, video collection, video review, interviews, etc.) and how agents will be asked to do various tasks/roles. Hearing from our leadership early on is very important for the agents to understand what WFO is doing to address the situation based on the available information at the time.

**SA Social Media Exploitation**

- **Inability of line investigators to exploit social media** - The vast majority of WFO SAs were unable to exploit social media leads and more broadly, conduct basic unclassified and commercial database checks. Minimal SAs had Slipstream access. Many SAs did not have basic commercial database access such as Clear and Accurint. Further, many did not know Accurint was available via GMAN. Minimal SAs had access to LinX, NCIC Mobility, or CCD.
    - Recommend for social media, if SAs are not capable or willing to maintain their own social media exploitation capability, WFO should invest in commercial solutions to bridge this gap. For the other databases mentioned, there is no excuse for every SA to not have access to these databases. You can make this part of the file review process but it comes down to ownership and being a prepared investigator. Relying on Intel to conduct social media and baseline checks is inefficient and unreliable. SAs should have the same accesses and be able to run the same checks as Intel. Even one month in, there still isn't a sustainable solution for social media exploitation for the Capitol investigation. Considering most, if not all, of these cases have a social media aspect, we are less effective as an office by not being more capable to conduct these basic investigative checks.

- **Lack of consistent database access and training across personnel** - When answering leads, agents needed access to CLEAR to conduct name checks. The Accurint database available via Gman is not as comprehensive as CLEAR on UNET, and not all agents are provided or maintain accounts. Agents also had issues viewing various video formats within FBI systems.
    - Recommend Have a CLEAR POC available to quickly create accounts for agents or have the tactical intelligence component of the command cost have an account to run checks for agents on the spot. Also, purchase covert laptops that can be available during a crisis situation. Agents will be able to download videos as well as download software to view videos which normally cannot be viewed or downloaded on UNET due to security settings.

**Better Process for Gaining Intelligence assistance**

- **Minimal Intel support** - During crisis events, embedded Intel personnel generally fall back to their ID squads which is expected. However, from the line SA level, it was unclear what, if any, Intel support existed and if so, how Intel support could be requested. Initially, SAs were directed to leverage email distros and ID-16 via leads, but this was ad hoc and there was little follow up. Hundreds of leads sent to ID16 went unaddressed and were eventually dumped back in CT-4 lead bucket with no discussion or attempt to address. Tasks would go into an Intel black hole and never come out. Other than the production of targeting packages, Intel was a mystery to everyone. Intel did not work the same schedules as SA shifts. Intel generally had no latch up with anyone but Intel's own chain of command.
    - Recommend defining Intel's role, even if it is narrow, make them accessible, and build a simple workflow that everyone understands. Define POCs and make them be available and visible. Otherwise, Intel becomes irrelevant and/or people expect support that never materializes. Intel support provided by other offices which much easier to understand and ultimately resulted in a deliverable much more so than WFO Intel. Not a criticism of WFO Intel; a criticism of process and lines of communication.

**Challenges with tips**

- **Duplication of efforts on tips** - In the first two weeks following the attack on the Capitol, multiple tips came in related to the same individuals. This is to be expected. Because of a lack of consistent process for lead evaluation, minimal database checks or indexing was done by lead evaluators and leads were assigned for action; duplicates were not caught. Some SAs in receipt of those leads ran checks, found duplicative leads/tips, and worked with lead evaluators to get these assigned to the same person to avoid duplication. This fixed the issue in these cases. Many SAs in receipt of leads did not conduct baseline checks and while they conducted interviews and did relevant investigative activity, failed to document anything in Sentinel. As a result, on many occasions, SAs who did conduct appropriate checks would submit prosecution packets or case openings only to learn that other SAs had been working tips tied to the same individual. These SAs who did not conduct any checks staked claim to these subjects, even though none of their work was ever documented, and directed others SAs to stand down and provide all relevant work conducted. This wasted days of time and contributed to unnecessary friction between Divisions.

- Recommend the process for case openings in general, including in a large scale crisis event, be streamlined and clearly communicated. As part of their SOPs, lead evaluators should conduct baseline checks to determine if duplicative tips or existing cases already exist on individuals. While understanding a USAO is willing to charge is preferable in a vacuum, getting a case opened to enable further investigative action should take precedence; we can always close a subfile if insufficient evidence exists to charge. Streamlining case openings along with thorough indexing puts a marker on these subjects and provides a central clearinghouse for related information be housed in Sentinel i.e. a 176 subfile. As a result, dueling lines and duplication of efforts are mitigated significantly.

**TTK Improvements**

- **TTK is insufficient for actioning leads based on video review -** This feedback is related to recipients of TTK leads, not use of TTK as a video review/triage tool. TTK reports are too long and incredibly confusing to decipher. While some images were available in the TTK reports, much of the structure of the TTK reports look like file paths on a computer; not something a human can understand. Even for tips that were submitted by complainants, the actual complaint was difficult to find and lacked context. How to find the underlying media referenced in the TTK report was difficult. In many cases, recipients of TTK reports could not even figure out what they were being asked to do, much less use the information to benefit investigations. Instructions on how to access TTK to review media from TTK reports was not sent out for weeks. Even when SAs submitted TTK access requests, the administrators providing access only worked during normal business hours and not on weekends. Given the scope of this event, this posture delayed actioning of leads for days.
    - Recommend all SAs working a crisis event be given access to TTK at the outset. This is a broader FBI issue, but TTK reports need to be revamped to make sense for the reader. Otherwise, SAs are likely missing valuable evidence or intelligence because what has been ingested into FBI holdings is undecipherable.

**Crowd Control and Riot Situations**

- **Lack of appropriate training and equipment for crowd control situations** - Agents are normally not trained on crowd control and riot response these duties.
    - Recommend if agents may be deployed to do crowd control, there should be some type of training or guidance to do crowd control or other duties such as site protection, or protection of government officials. As such, guidance or a refresher should be initiated should an incident like this occur again. Also, the topic of deadly force policy when responding to crow control situations should be addressed. Lastly, if agents are deployed to do crowd control or site protection, they should be provided with necessary equipment to do so.
- **Lack of structure and coordination for the 176 case -** A common theme is the lack of structure that exists for the 176 investigations. Squads/SAs have been designated to work 266 and 89 cases, but the same has not been done for 176 cases, specifically the conspiracy investigations. Cases are spread throughout WFO, across divisions and branches. SAs from across WFO should have immediately been TDY'd to exclusively work 176 matters. SAs are

frustrated they are working multiple investigative programs without a clear chain of command. It has been five weeks since 1/5/2021 and coordination with other Field Offices is still left to individual SAs. DTOS in not engaged with SAs and in at least one instance DTOS was unaware that 176 subjects were being arrested. A lack of a centralized GJS tracking system has resulted in multiple SAs serving subpoenas on the same hotels and ISPs for the same information. Investigative activity is too often occurring at WFO and not the FO where the subject is located.

- Recommend developing and implementing and overarching 176 case team and disseminating clear investigative guidance addressing investigative and management matters.

## Intelligence

CRISIS MANAGEMENT FEEDBACK

1. Recommend re-aligning crisis management under agnostic SAC. Designate ASACs to support. Define and provide a description of positions, functions, roles, responsibilities and people reporting to them identified from the SAC/ASAC agnostic to the threat itself. Recommend personnel infrastructure not distracted by outlying events.
2. Create an appendix to the crisis response plan with shift assignments and role descriptions. Ensure clear communication regarding rest periods during 100% staffing. Two different thoughts on crew rest: Trust supervisors to look out for each other. Clearly communicate this to give them autonomy. Make sure people know they need to take care of each other.
3. COOP setup – how do we leverage our other properties to respond to activities outside the NCR. Should that be set up earlier?
4. Communications – build in shift-turnover model – quality of comms depended on the supervisor – ensure comms to everyone – perhaps create a template for consistency. All-hands communication sooner.
5. June/Jan commonality – consider identifying a specialty team of LEOs with riot training. These members potentially better understand the environment and how to handle tactically - designate as TLs or own response team?
6. Helmets – no one wants – what's the point? If we don't normally wear, why are we issuing? Not trained with, not fitted, not comfortable. If we issue gear, we should plan ahead and have them fitted, then provide training with them. Plates – status on issuance?
7. TTX – check-in for 14s and above briefed on crisis response program/plan and their potential roles/responsibilities. Recommend conducting a TTX every 6 months and walk through an exercise while not under stress. Beneficial due to high turnover.
8. Physical layout - how do we factor in TDYers/outliers? CTOC well-designed? Crisis team vs inauguration team? Do we have a better idea? Do we use the COOP? Outfitting the ADIC's conf room, is that what we would have done if we had planned ahead?
9. Sentiment about the manner feedback was being provided – would prefer anonymity – do not want names discoverable. Do not want constructive criticism to be politicized. Recommend setting up an anonymous feedback box set ahead of time or near real-time.
10. Some of this was feedback from June – looking for feedback on prior feedback to ensure EM is truly interested in making things better. Folks want to feel listened to and see changes.
11. WFO should have their own Critical Information Operation Specialists (Sentinel crisis case support personnel).
12. Ensure clear leadership over the CP
13. Recommend providing formal training for On-Scene-Commanders
14. Sit down with Crisis Management Coordinators and figure out how these things ought to be run
15. Utilize HUMINT reporting better and sooner to add value
16. Allow SIAs outside the CP branch to participate in training or during regular command post operations to gain experience (e.g., July 4th or State of the Union)
17. Have a back-up for the SSIAs and clearly define delineated responsibilities
18. Provide training for IAs outside the threat IAs to receive training on certain databases that are utilized for the CP

19. TTK - TTK was necessary because it allowed files to be submitted, but we need to find an enterprise solution that allows tip information with attachments to feed into our existing processes for receiving information. Background: TTK is a stand-alone system that does not feed information into any of our existing processes. For example, information about future threats could have potentially sat in TTK for days or weeks before being reviewed. Then it took an IA/SOS manually moving the file from unclass TTK to FBINet, serializing it to one of our Type 3 assessments, and setting an action lead to that field office. Ideally this information would be a Guardian since there are required timelines and checks for those leads. We found ways to make it work but we were making up new processes when the FBI has existing processes that we just couldn't plug into.
20. Create an SOP for reviewing and processing Digital Media Tips. The SOP was made up on the fly and guidance changed daily.

**(U) DMT Hotwash**

(U//FOUO) As the digital review process through Triage Toolkit was a new process for most of the intelligence division and the domain squad (ID-5), Team Lead IA [redacted] wanted to take the time to discuss with colleagues on his squad to get their feedback on the DMT review process, while fresh in their minds. IA Falls mentioned the initial thoughts on convening this hotwash during their weekly ID-5 squad meeting. He followed up with colleagues to learn of their potential availability, and then set the date and time for the meeting via Microsoft Teams. IA Falls, developed some main topic areas to stimulate participants' ideas as they recalled their experience and the process. IA Falls lead his colleagues through an hour-long discussion about the DMT process, addressing issues related to initial training, SOPs, scheduling, team leads, and other strengths and weaknesses that were identified during the process, all with the purpose of learning to improve for subsequent projects. Several individuals who could not make the discussion emailed their thoughts, which were incorporated with thoughts that resulted from the discussion. IA Falls outbriefed the hotwash to his SIA and squad during their weekly squad meeting, with hopes to learn from the previous process and apply to similar processes in the future.

**(U) Popular themes from discussion**

- (U//FOUO) DMT trainings improved. Initial trainings were not quite as thorough as trainings held even a couple days later.
- (U//FOUO) Reviewers were unsure of where/how what they were doing fit into the larger picture of the process. Reviewers were curious as to what happens to the files after they tagged them a certain way.
- (U//FOUO) Use of Team Leads was successful – they were always available to provide accurate information and act as intermediaries to the SIAs/SSIAs.
- (U//FOUO) Communication was successful. The use of emails, chat functions, and discussions to distribute information to the reviewers was successful in keeping reviewers aware of most current information.
- (U//FOUO) Development of a clear and thorough SOP relatively quickly was beneficial and served as a road map for reviewers to follow.

- (U//FOUO) Reviewers were reluctant even after some training and given materials to make the 1st amendment protected decisions related to Future Threat tagging. It was good to have TLs and SSIA to confer with.

**(U) Topics discussed**

**(U) TRAINING**

*(U) Successes*

- (U//FOUO) Timely- Trainings happened immediately and regularly - got us access to databases almost immediately- not like some access requests for other databases that take much longer in our normal jobs.
- (U//FOUO) Training improved over time- Initial trainings were a bit rushed and just covered the basics. Training during the first couple of days was definitely not as thorough as training that happened just a few days later. Some people who attended one of the first trainings and attended a subsequent training thought training a few days later was much more thorough.
- (U//FOUO)Subsequent trainings that included legal experts were good as they helped inform reviewers about Future Threats and 1st Amendment protected information.
- (U//FOUO) Regularly offered- With the trainings being offered almost daily people could jump on and get a refresher, or if they were confused could join to ask questions.

*(U) Challenges*

- (U//FOUO) Initial trainings were brief and basically told reviewers how to log into DCAP and TTK but were not really as detailed on the review process.
- (U//FOUO) Initial trainings did not all include walking you through an entire case and assessing it (review process evolved and increased so it would not have covered everything we were doing later in reviews as it would have initially).
- (U//FOUO) Future threat training still left people feeling reluctant to determine future threats/1st Amendment protected speech (it was good to have access to TLs and SSIAs to clarify questionable cases).

**(U) PROCESS/SOP**

*(U) Successes*

- (U//FOUO) Reviewers were able to gain access and training very quickly to start reviewing files.
- (U//FOUO) Being able to do the reviews from home, especially during the time of COVID, enabled a lot of people to help review the cases, possibly getting a lot more volunteers than if everyone was required to be in the office together.
- (U//FOUO) By establishing an SOP so quickly, that was clear and thorough, reviewers did not need much more explanation to follow to review a file. The SOP served as a good roadmap to review cases.
- (U//FOUO) The SOP was updated regularly, and the TLs highlighted the changes made, making it easy for reviewers to be aware of those changes.

- (U//FOUO) Some reviewers thought possibly creating a slicksheet, checklist, or flow chart could have been helpful for reviewers to follow the lengthy SOP- showing the process or flow of a case.

*(U) Challenges*

- (U//FOUO) Not all SOPs/directions for cleanups were located in one central location for the reviewers to access. They were emailed out to reviewers regularly but there were a couple of different places to access information, so in the future keeping all things in one Sharepoint would have been beneficial.
- (U//FOUO) The SOP was long- especially once doing reviews for RO2, RO4, RO5, RO6, and RO7. Some reviewers thought possibly having the "known faces" pages as a separate document would have been useful as flipping to the end of the SOP where the known faces section was currently located was difficult to turn to and then have to find where you were in review process again.
- (U//FOUO) Updates to known faces- It did not seem like the known faces pages were updated much, or at all, after the first couple of days.
- (U//FOUO) Dates were not always updated on SOP, so reviewers accessing the SOP on the Sharepoint were not always clear if it was the most up-to-date version. Reviewers appreciated that the TLs did a good job sending the SOP out regularly to reviewers to ensure reviewers were always using most up-to-date version.
- (U//FOUO) BOLO information and FBI wanted posters were not always clear where reviewers could access this information.
- (U//FOUO) Some reviewers thought that a list of current US Congressmen and Congresswomen would have been useful as some reviewers do/did not know who congress personnel were to do that tagging correctly.

**(U) Communication**

*(U) Successes-*

- (U//FOUO) Daily emails to reviewers from TLs with plans/tasks for the day were very helpful and highlighted any changes.
- (U//FOUO) The use of Microsoft Teams on UNET and the Skype function on FBINET between TLs and reviewers was very useful. Both chat functions provided a quick and easy way for communication between the reviewers and the TLs, as well as the various reviewers to communicate with one another. The chat function enabled reviewers to see similar questions and answers that they may also have and if using Microsoft Teams, the discussions are saved so reviewers were able to refer back to the conversations if they had a question that they knew was already discussed.
- (U//FOUO) "Over communication" was looked at as a good thing for this project. Some people do not like too many emails, meetings, phone calls, but in this case, providing more information to the reviewers was generally seen as a good thing.

*(U) Challenges-*

- (U//FOUO) Not having the initial email address "digital review" inbox set up made it so people who were in the office doing their own reviews were slowed down having to respond to requests from home. Also, it was not always clear who was in the office to run searches for the reviewers at home. This turned into a success though once the

Digital_review inbox was set up and people were designated for that role to respond reviewers from home.

- (U//FOUO) When at-home and reviewers requested in-office system checks, the responses back were not always consistent in terms of the information shared back, even when the process was taken over by the review inbox. A specific standard could be set up for all responses.

**(U) STAFF**

*(U) Successes-*

- (U//FOUO) TLs added much needed guidance and direction to the review process. Many reviewers commented about the appreciation of having the TLs available to answer questions and provide information.
- (U//FOUO) Reviewers liked the TL structure because reviewers could reach out for advice and information to a peer and did not have to be asking a supervisor. If reviewers had to reach out to a supervisor, reviewers might have been more likely to try to figure out things on their own, which may have not always been correct or accurate.
- (U//FOUO) The scheduling of the staff was efficient and up-to-date. It was easy to sign up for shifts and the schedule was saved in a shared location for all to access. The schedulers provided new updates and responded to requests in a timely manner.

*(U) Challenges-*

- (U//FOUO) People doing reviews in office at first were only ever really able to respond to requests from reviewers at home, thus people in office were not actually getting reviews done (this changed through the implementation of the digital review inbox so it was fixed along the way).

**(U) TECHNOLOGY**

*(U) Successes-*

- (U//FOUO) At home reviewing was both a success and a challenge. Being able to use the technology and do things remotely helped greatly but there were some functional issues of using the program at home (many reviewers could not see the annotations and comments within a file even with changing sizes and other suggested fixes. A work around was possible by generating the report though). Additionally, at-home reviewers were unable to run their own case checks when needed.
- (U//FOUO) Everyone seemed to be able to gain access quickly to DCAP and TTK and get set up with accounts, unlike some other program we request access to during our everyday jobs.
- (U//FOUO) Program functionality was relatively intuitive. It was not without flaws/quirks but overall TTK was pretty easy to use.

*(U) Challenges*

- (U//FOUO) Tips that came in with multiple images or videos were not able to be kept together, people did not know how to find the other files initially, but we were able to figure some tricks to do so later on in the process. (for example- doing text searches in TTK related to one of the related images to find another image with a similar identifier).

- (U//FOUO) There is not an easy way to go back to a tip you had previously reviewed. Could a way be created in the program to track the tips you reviewed?
- (U//FOUO) It would be useful to be able to create saved queries. If TLs would be able to create some saved queries for the reviewers to use, this would help reviewers and TLs working on a couple different tasks (RO2 reviews, future threats, cleanups). Reviewers would not need to go back and enter all pieces of the queries for each of the various tasks. Reviewers could click on the RO2 saved query or the Future Threats saved query, reducing the risk of inadvertently entering wrong parts of a query and reducing the time to create a new query each time.
- (U//FOUO) If a reviewer had a file open and did not immediately tag RO2 review, someone else could still open file and possibly make tags as well, or remove tags just placed on a file. Is there a way for the program to lock down being able to open a file if it is already open?
- (U//FOUO) Remove the Green + box at the top of the Tagging tab as it looks like a search function, or make it that only TLs or approved individuals can add new tags in the system.

(U//FOUO) Overall, reviewers thought the DMT review process on the mass scale that it was completed was a great achievement. There were certainly areas where reviewers learned and grew, but everyone was willing to step in to help and adapt quickly. The contributions of the many made a much lighter load for everyone. Hopefully, FBI Washington Field Office can apply elements learned from this hotwash to other projects that are worked in the future.

# CAST

**CAST Capitol AAR Notes**

**1. Executive Summary**

- Beginning on Sunday, January 10, 2021, FBI CAST deployed assets to support the WFO investigation of the Capitol Riots, the DNC/RNC Pipe Bombs, and assaults on federal officers that occurred on or about Jan. 5 – 6, 2021.
- From Jan. 11 – 26, CAST personnel supported the investigations on-site at WFO. While on-site, CAST:
    - Provided consultation to investigating squads
    - Leveraged contacts with cellular networks regarding legal process wording and returns
    - Conducted cellular and WiFi survey of the Capitol and its environs
    - Analyzed tower dump and geo-fence files, identifying numbers/device tags of interest
    - Analyzed tolls, CDRs and other CSLI on specific numbers to support the location of identified devices related to the Capitol Riots and the DNC/RNC Pipe Bomb investigation
- On Jan. 27, CAST assets transitioned to providing assistance remotely.
- Future CAST support the ongoing investigations and prosecutions will be conducted:
    - For the Capitol Riots:
        - Case agents seeking to check numbers against the tower dump records should visit the FBInet DTOS SharePoint and enter the phone number into Splunk via their OPWAN account for a check against tower dump and Google geo-fence records
        - Analysis of specific numbers, including reports for prosecution and trial, will be treated as typical CAST requests and assigned to any CAST asset available to support
    - For the DNC/RNC Pipe Bombs: six CAST assets will continue to provide investigative support to address new requests or leads as they are developed

**2. Deployment Roster**

CAST CP Liaisons: SSA [redacted] (CID/DE) Jan. 10 – 22
SSA [redacted] (CID) Jan. 19 – 26

<u>Group 1 (Jan. 10 – 13)</u>
SSA [redacted] (PG)
SA [redacted] (CID/CO)
SA [redacted] (CID/PD)
SA [redacted] (KC)

<u>Group 2 (Jan. 13 – 16)</u>
SA [redacted] (CID/CG)
SA [redacted] (CID/SE)
SA [redacted] (SF)
SA [redacted] (SD)

<u>Group 3 (Jan. 17 – 22)</u>
SA [redacted] (CID/LA)
SA [redacted] (CG)
TFO [redacted] (KC)
SA [redacted] (BH)
SA [redacted] (CID / NK)

<u>Group 4 (Jan. 22 – 27)</u>
SA [redacted] (DL)
SA [redacted] (BA)

3. **Challenges**
   - Difficulties in getting WFO to accept help. Deployment delayed
     - CAST reached out the day of the incident to offer help
     - WFO CAST personnel (SSA [redacted]) advised management to seek CAST assistance
     - CASTU supported however, limited engagement from OSS EM
   - Lost opportunity to obtain data under exigent circumstances
     - Further restricted by the court resulting in limited data for exploitation
   - Early reluctance by the case squad to use the resources of CAST
     - Fundamental misunderstanding of capabilities
       - Easier to exclude and dismiss the assets trying to help
   - Despite efforts to work with intel personnel, not much interaction reciprocated
     - SOMEX focus without simultaneous cellphone exploitation
       - Subject tracking sheet did not have a column for a possible phone number
       - Focus appeared to be on content of posts without simultaneous concern for location of subject
         - Explained to intel SIAs CAST may assist in resolving a social media account to a number we could potentially track for a subject of concern.
   - WFO CAST assets assigned other tasks unrelated to specialty
     - Further delayed ability to obtain records quickly
   - Disconnect between the case squads
     - Appeared to operate in silos other than daily briefings
       - Did not appear there was consideration that the pipe bomb subject may also be one of the rioters
         - Until CAST started asking these questions, hence the creation of the DTOS SharePoint spreadsheet
       - Not sure if questions related to pipe bomb were posed to anyone arrested for Capitol activities
     - Prosecutorial priorities, early on, focused on rioters more than bomber and assault suspects
4. **Positives**
   - WFO management was accommodating once CAST arrived on scene
     - Station created in CP for CAST liaison
     - Work area identified for CAST assets deployed on site
     - Additional internet lines run upon request
     - FBINET computer installed upon request
     - Whiteboard and supplies provided upon request
   - CAST and WFO IS2 and others collaborated to develop a solution for compiling data to be exploited within the restrictive parameters of the court.
     - DTOS Sharepoint created a spreadsheet repository
     - Splunk/OPWAN system conceptualized, developed, and deployed
     - Data scientists were instrumental in parsing out “over-collected” data
   - Collaboration with USAO, Capitol Police, Squads, TFOs, providers, data scientists improved throughout deployment.
     - Continues to this day

**5. Recommendations**

- Field office CAST assets should be assigned immediately to CAST related activities
    - Initiate emergency disclosures
    - Collect and organize available data
    - Serve as POC to coordinate additional assets
    - Facilitate liaison within the office for deployed assets
- Allow for CAST asset deployment to augment division assets
    - Particularly when CAST proactively offers to assist
    - Team dedicated to obtaining and analyzing records
        - Extensive knowledge of records available versus piecemeal knowledge of squads
        - Experienced operating in a crisis/CP
- CASTU work with HQ channels to ensure appropriate crisis response by CAST

| DEPLOYMENT DATE | POSITION TYPE | EVENT | FIELD OFFICE/ HQ DIVISION | TOTAL PERSONNEL COUNT* | NOTES |
|---|---|---|---|---|---|
| 1/6/2021 | AGENT | 1/6 INCIDENT | WFO | 274 | This number includes agents that responded to the Capitol grounds as well as inside the Capitol, the pipe bombs, and the red truck that was believed to contain explosive devices as well as CDC/ADCs. |
| 1/6/2021 | ATTORNEY | 1/6 INCIDENT | WFO | 0 | |
| 1/6/2021 | IA | 1/6 INCIDENT | WFO | 14 | |
| 1/6/2021 | OTHER | 1/6 INCIDENT | WFO | 75 | This number includes professional staff that are part of specialty teams, OSTs, SOSs, PSSs, computer services, ETs, and others. |
| **1/6/2021** | **TOTAL** | **1/6 INCIDENT** | | **363** | |
| 1/7/2021 | AGENT | 1/6 INCIDENT | WFO | 432 | |
| 1/7/2021 | ATTORNEY | 1/6 INCIDENT | WFO | 0 | |
| 1/7/2021 | IA | 1/6 INCIDENT | WFO | 20 | |
| 1/7/2021 | OTHER | 1/6 INCIDENT | WFO | 70 | This number includes professional staff that are part of specialty teams, OSTs, SOSs, PSSs, computer services, ETs, paralegals, MSAs, and others. |
| **1/7/2021** | **TOTAL** | **1/6 INCIDENT** | | **522** | |
| 1/8/2021 | AGENT | 1/6 INCIDENT | WFO | 469 | |
| 1/8/2021 | ATTORNEY | 1/6 INCIDENT | WFO | 0 | |
| 1/8/2021 | IA | 1/6 INCIDENT | WFO | 17 | |
| 1/8/2021 | OTHER | 1/6 INCIDENT | WFO | 65 | This number includes professional staff that are part of specialty teams, OSTs, SOSs, PSSs, computer services, ETs, paralegals, MSAs, and others. |
| **1/8/2021** | **TOTAL** | **1/6 INCIDENT** | | **551** | |
| 1/9/2021 | AGENT | 1/6 INCIDENT | WFO | 503 | |
| 1/9/2021 | ATTORNEY | 1/6 INCIDENT | WFO | 0 | |
| 1/9/2021 | IA | 1/6 INCIDENT | WFO | 16 | |
| 1/9/2021 | OTHER | 1/6 INCIDENT | WFO | 60 | This number includes professional staff that are part of specialty teams, OSTs, SOSs, PSSs, computer services, ETs, paralegals, MSAs, and others. |
| **1/9/2021** | **TOTAL** | **1/6 INCIDENT** | | **579** | |
| 1/10/2021 | AGENT | 1/6 INCIDENT | WFO | 446 | |
| 1/10/2021 | ATTORNEY | 1/6 INCIDENT | WFO | 0 | |
| 1/10/2021 | IA | 1/6 INCIDENT | WFO | 16 | |

| | | | | | |
|---|---|---|---|---|---|
| 1/10/2021 | OTHER | 1/6 INCIDENT | WFO | 59 | This number includes professional staff that are part of specialty teams, OSTs, SOSs, PSSs, computer services, ETs, paralegals, MSAs, and others. |
| **1/10/2021** | **TOTAL** | **1/6 INCIDENT** | | **521** | |

| DEPLOYMENT DATE | POSITION TYPE | EVENT | FIELD OFFICE/ HQ DIVISION | TOTAL PERSONNEL COUNT* | NOTES |
|---|---|---|---|---|---|
| 1/15/2021 | AGENT | INAUGURATION | WFO | 58 | |
| 1/15/2021 | ATTORNEY | INAUGURATION | WFO | 1 | |
| 1/15/2021 | IA | INAUGURATION | WFO | 7 | |
| 1/15/2021 | OTHER | INAUGURATION | WFO | 59 | |
| **1/15/2021** | **TOTAL** | **INAUGURATION** | | **125** | |
| 1/16/2021 | AGENT | INAUGURATION | WFO | 85 | |
| 1/16/2021 | ATTORNEY | INAUGURATION | WFO | 1 | |
| 1/16/2021 | IA | INAUGURATION | WFO | 8 | |
| 1/16/2021 | OTHER | INAUGURATION | WFO | 65 | |
| **1/16/2021** | **TOTAL** | **INAUGURATION** | | **159** | |
| 1/17/2021 | AGENT | INAUGURATION | WFO | 120 | |
| 1/17/2021 | ATTORNEY | INAUGURATION | WFO | 1 | |
| 1/17/2021 | IA | INAUGURATION | WFO | 7 | |
| 1/17/2021 | OTHER | INAUGURATION | WFO | 76 | |
| **1/17/2021** | **TOTAL** | **INAUGURATION** | | **204** | |
| 1/18/2021 | AGENT | INAUGURATION | WFO | 134 | |
| 1/18/2021 | ATTORNEY | INAUGURATION | WFO | 1 | |
| 1/18/2021 | IA | INAUGURATION | WFO | 6 | |
| 1/18/2021 | OTHER | INAUGURATION | WFO | 81 | |
| **1/18/2021** | **TOTAL** | **INAUGURATION** | | **222** | |
| 1/19/2021 | AGENT | INAUGURATION | WFO | 261 | |
| 1/19/2021 | ATTORNEY | INAUGURATION | WFO | 0 | |
| 1/19/2021 | IA | INAUGURATION | WFO | 10 | |
| 1/19/2021 | OTHER | INAUGURATION | WFO | 94 | |
| **1/19/2021** | **TOTAL** | **INAUGURATION** | | **365** | |
| 1/20/2021 | AGENT | INAUGURATION | WFO | 312 | |
| 1/20/2021 | ATTORNEY | INAUGURATION | WFO | 0 | |
| 1/20/2021 | IA | INAUGURATION | WFO | 9 | |
| 1/20/2021 | OTHER | INAUGURATION | WFO | 113 | |
| **1/20/2021** | **TOTAL** | **INAUGURATION** | | **434** | |

| 1/21/2021 | AGENT | INAUGURATION | WFO | 88 |
|---|---|---|---|---|
| 1/21/2021 | ATTORNEY | INAUGURATION | WFO | 0 |
| 1/21/2021 | IA | INAUGURATION | WFO | 8 |
| 1/21/2021 | OTHER | INAUGURATION | WFO | 57 |
| 1/21/2021 | TOTAL | INAUGURATION | | 153 |

*ALL NUMBERS ARE APPROXIMATE

| EVENT | COST CATEGORY | [redacted] | DEPLOYMENT DATE | NOTES |
|---|---|---|---|---|
| 1/6 INCIDENT | PPE | [redacted] | | Plexiglass for Command Post |
| 1/6 INCIDENT | OTHER | [redacted] | | Funds utilized to purchase light refershments for the command post. |
| 1/6 INCIDENT | OTHER | [redacted] | | Source and case advances/expenses for Capitol Riots investigation |
| INAUGURATION | OTHER | [redacted] | | Funds utlized for operational supplies, clothing, juice packs, ammunition, raid jackets. |