01/26/2024
New York, NY

I, [redacted], having been duly sworn by Supervisory Special Agent (SSA) [redacted]., hereby make the following statement to [redacted] and [redacted] on 01/26/2024, [redacted] and [redacted] [redacted] on 08/08/2024, and [redacted] and [redacted] on 10/07/2024, whom I know to be SSAs of the Federal Bureau of Investigation (FBI), assigned to the Inspection Division (INSD) at the time of my statement. My attorney, Richard J. Roberson, Jr., was present during my statement all occasions, via telephone. This statement took place over a three-day period. The statement initiated on 01/26/2024, and again on 08/08/2024, after additional allegations were added:

I entered on duty (EOD) on 02/21/2006, as an Intelligence Analyst (IA). I EOD on 10/08/2008, as a Special Agent (SA) and I am currently assigned to the New York Field Office (NYFO) in that capacity.

I understand that this is an internal investigation regarding an allegation that Special Agent [redacted] improperly stored digital evidence at his residence in violation of 1.6- Investigative Deficiency- Improper Handling of Property in the Care, Custody, or Control of the Government. On 10/30/2023 the following expanded allegations were added: Special Agent [redacted] improperly handled, documented, and stored digital evidence and failed to secure CSAM within policy, resulting in a cyber intrusion in violation of 1.6- Investigative Deficiency- Improper Handling of Property in the

Care, Custody, or Control of the Government and 5.17- Security Violation- Failure to Secure sensitive Equipment/ Materials. On 02/07/2024 the following expanded allegations were added: Special Agent [redacted] exceeded the limits of his authority by contracting an outside company to develop computer software on behalf of the FBI in violation of 2.8 Misuse of Position and 5.23 Violation of Miscellaneous Rules/Regulations.

I have been further advised of my rights and responsibilities in connection with this inquiry as set forth on a "Warning and Assurance to Employee Required to Provide Information" form FD-645 which I have read and signed. I understand from my review of the FD-645 that should I **refuse to answer or fail to reply fully and truthfully during this interview, I can expect to be dismissed from the rolls of the FBI.**

I have been advised by INSD not to provide the details of a whistleblower complaint I have filed with the Department of Justice in which I assert that these allegations are some of many retaliatory actions taken against me by the FBI that stem from a 2023 cyber intrusion of the NYFO's child exploitation forensic lab. While I will not go into details, I believe this is important to mention here given the very genesis of these allegations were derived from a directive to make me a scapegoat for the intrusion. I am happy to elaborate if requested, but in sum I was retaliated against for my having made numerous protected disclosures over the years that went unaddressed,

which likely would have prevented the intrusion from happening. When the intrusion occurred, these disclosures, which I made again, caused FBI Executive Management (EM) to fear repercussions of their own failure to address the issues I presented before an incident like the intrusion could occur. I have proof upon proof that I was then targeted by FBI management as an attempt to make it appear that I and my squad mates were responsible. I know that INSD is in possession of the first of my submitted whistleblower complaints, but there are several other amendments as well as supporting documents that I can provide upon request.

I am currently assigned to CT-25, a Domestic Terrorism squad, but assigned to an Enterprise Investigation that is a hybrid of Domestic Terrorism and Child Exploitation squad. I was assigned to squad CY-3 in May 2010 and officially named on the squad in July 2010. This was when the FBI's child exploitation program was referred to as "Innocent Images" and fell under the Cyber Division, while Squad. C-20 was the Human Trafficking (HT) squad at the time. I believe it was 2015 when Violent Crimes Against Children (VCAC) and HT programs were combined under the FBI's Criminal Division, which led to the merger of the violations in the NYFO under squad C-20. The squad is split and has the HT side and the VCAC side, and I was a VCAC Agent. Agents primarily work their assigned violations, but we come together as a squad for operations.

I have been with the FBI for over 18 years, having spent the last 16 years as an Agent. I have been one of the FBI's leading Agents in Child Exploitation investigations and to this day, I believe that I am one of, if not the only, Court-certified expert witness for the entire FBI for child exploitation. I have personally accounted for over 60 arrests, 150 search warrants, and have been responsible for rescuing several hundreds of children. As is elaborated on in my Curriculum Vitae, which I have provided to INSD and has been introduced to certify me in Court as an expert witness, I also have received numerous awards and accolades, including but not limited to being a two-time recipient of the FBI's Medal of Excellence and the Southern District of New York's (SDNY) prestigious McCabe Award. I have an incredible reputation around the FBI and am seen as one of the hardest working and driven Agents in the FBI. In demonstrating the support I received, after the intrusion when FBI Headquarters (HQ) had begun its efforts to retaliate against me, the NYFO went to great lengths to push-back. Now retired Assistant Director in Charge (ADIC) [redacted] [redacted] defied orders from Assistant Directors (AD) and the Deputy Director (DD) to have me punished. This defiance led the DD to order charges against me, and months later I received the first of the referenced charges. The NYFO however still showered me with their support, with [redacted] singing my

praises to [redacted], stating that he would rather have one "[redacted]" than 10 other Agents. The NYFO also nominating me for the second of the FBI Medal of Excellence awards I would receive in December 2023. Just months ago, in 2024, I was nominated for, but did not receive, the Director's Award, however at the same time I was nominated for an award from the Federal Law Enforcement Foundation and on 10/22/2024, I was informed I am receiving it.

I can expand at length on the accolades and praise I have received from Agents, Analysts, management, HQ, Assistant United States Attorney's (AUSA's), local law enforcement, and more over the years. Even despite my current situation I continue to receive praise and support from all ranks and from AUSAs. Last month, in September 2024, the SDNY Project Safe-Childhood Coordinator (PSC) requested I assist her in providing child exploitation training to SDNY AUSAs. The PSC is aware I am no longer on the child exploitation squad, and finds the actions taken against me to be disgraceful. She also stated that despite it all, she considers me to be the best in the FBI.

Regarding the allegations against me, it is my understanding that they stem, in whole or in part, from interviews conducted by the FBI's INSD in March 2023. Specifically, the statements I made during those interviews

appear to have been the basis for the observations outlined in the subsequent INSD report, which the FBI has reported to be the foundation of these charges. I have since learned that this report was authored by someone two or three levels removed from me, relying on secondhand interpretations of my statements from the notes of the interviewers. I know what I said during the interviews, and the references in the INSD report do not accurately reflect my actual words.

The INSD initially published a draft report around May or June 2023, which included observations closely mirroring the allegations against me. Both I and the NYFO leadership, including my former ADIC, [redacted] [redacted], countered these observations as we believed them to be inaccurate. These inaccuracies were discussed in detail during meetings with [redacted] [redacted] and FBI EM, and we later submitted a formal written rebuttal. However, the final INSD report, published in July 2023, failed to incorporate our responses. The observations based on my statements were neither revised to align with my rebuttal nor updated to reflect supporting evidence.

I have also learned that the interviewers themselves were not provided with either the draft or final versions of the INSD report, nor were the interviewers informed of the responses submitted by me or the NYFO. Instead, the report's author relied

solely on the interviewers' notes, which were not a verbatim transcription of the interview, and the interview itself was not recorded. This left critical context about my statements subject to the author's interpretation. Similarly, the rebuttals submitted to challenge the observations were not addressed. As a result, the final report left the original observations largely unchanged.

In the interest of transparency, I am including the NYFO's final response to the INSD's draft report. This response was a collaborative effort between myself, my SSA, my Assistant Special Agent in Charge (ASAC), and the NYFO's Information System Security Officer (ISSO). It was formally submitted as a rebuttal to the draft observations. Unfortunately, the final INSD report failed to incorporate these responses, leaving the contested observations intact. This is deeply troubling, as the allegations were contested from the outset with the full support of the NYFO chain of command.

After reviewing the draft INSD report, the NYFO was afforded an opportunity to respond in writing to both the INSD "observations" and "findings". The following is the last version of the NYFO's response that had been drafted by [redacted], [redacted], [redacted], and Office of the Chief Information Officer (OCIO) [redacted]. In the "NY's Clarifications to the

Inspection Report's Observations" section you will see listed the "Observation", which was identified by INSD, then the subsequent "Clarification of Facts", which was the NYFO's rebuttal to the observations. Following this section, you will see the "NY's Responses to the Inspection Report's Findings" section. Similarly, you will see listed the "Instruction", which was identified by INSD, then the subsequent "Response", which was the NYFO's rebuttal to the instruction.

NY's Clarifications to the Inspection Report's Observations

Observation 1: NY was operating a device providing Internet access through wireless connectivity in FBI secured space.

Clarification of Facts: NY received authorization from Security Division in 2018 to utilize Wi-Fi devices within FBI space, as long as the device connected to the Wi-Fi was 10 feet from an Enterprise computer. Regardless, because C20 did not request the particular Wi-Fi modem/router which was in the lab at the time of the intrusion, the wireless features were never utilized and presently there are no wireless devices in FBI space.

Observation 2: NY was connecting overtly and covertly purchased IT on the IS.

Clarification of Facts: Axiom, Cellebrite and GrayKey are LE tools purchased by CACHTU and used by DExT examiners in the Field. CACHTU advised the field to utilize UCO funds to make purchases of new equipment to support the tools.

Observation 3: NY was storing DE overnight in an unapproved storage facility.

Clarification of Facts: The previous practice utilized by [redacted] was to image the Original Digital Evidence on the Network Attached Storage, place such in Evidence Control, and then copy the Original Imaged Evidence, creating a Master Working Copy.

During specific times in 2020, [redacted] created a copy of specific files/documents from the Master Working Copy and brought these limited working copy items home via his work laptop to perform work related tasks. The copies he took home to work on were copies of copies and were limited to specific files from the larger forensic images. The files/documents were not

contraband, classified material, CSAM, or sensitive material. Further, in 2020, FBI Management was authorizing and encouraging employees to work from home to limit the spread of COVID 19 in the office. [redacted] did not store any files at his house. Once he completed his analysis he brought the electronic files/documents back to the office and appropriately disposed of same.

Observation 4: NY did not appropriately image DE.

Clarification of Facts: This is an issue C-20 has raised for years with HQ and has routinely asked for hard drives in order to comply with the policy, but has been denied and C-20 was advised they would have to pay for the drives. At the same time, HQ would not supply C-20 with the funds in order to purchase those same hard drives.

Additionally, C-20 takes issue with the outdated process of creating derivative evidence onto an additional hard drive. As the volume of data that is being collected has increased exponentially over time, the amount and cost of using hard drives is impractical and costly. C-20 suggests the use of

servers or cloud storage as a means to store derivative copies of evidence, which can be reused at the conclusion of an investigation and when the evidence (and derivative evidence) is destroyed.

Observation 5: NY did not appropriately verify analyzed images of acquired DE.

Clarification of Facts: NY in fact did appropriately verify analyzed imaged of acquired DE by generating an FD-302 which documented in the substantive case file as well as at 305A-HQ-1654544-DEXT to account for the work performed. Any issues or discrepancies would be documented in the FD-302. A hash verification log was also generated and stored with the DE on the Network Attached Storage, which could be accessed at any time. Going forward, the hash value verification log will be attached to the FD-302 to ensure compliance with policy.

Observation 6: NY was not appropriately documenting and storing ELSUR records in relation to undercover communications.

Clarification of Facts: NY appropriately places OCE/UCE communications in Subfile G of the UCO, which

is where CACHTU policy mandates these communications be placed.

Observation 7: NY did not document meetings between UCE/OCE and SSA every 90 days and the SAC/ASAC every six months.

Clarification of Facts: While the SSA and ASAC met with the OCE/UCE's connected to the UCO on a regular basis, primarily in the squad area and via the file review and CUROC process, NY will draft ECs documenting same in accordance with policy going forward.

Observation 8: NY did not utilize covert methods to procure covertly purchased goods.

Clarification of Facts: The items which were purchased are Law Enforcement only. NY was provided funding from HQ via the UCO to make this purchase with the understanding that it's a restricted purchase. Going forward, NY will ensure if a purchase needs to be made overtly, covert funding will be converted to overt funding by an approved FBI purchaser.

Observation 9: NY was not documenting financial records relating to UCO activity to the appropriate CE subfile.

Clarification of Facts: NY submits a monthly BlueSlip that contains all of the financial documentation for the prior month's financial activity. The same information that is required to be submitted to the CE subfile is contained in the BlueSlip. NY changed the individual who performs the accounting over time on a field office level and, while the information was recorded, it was not put into the CE subfile.

Observation 10: NY did not properly report a security incident within SIRS.

Clarification of Facts: The incident occurred during the night of Sunday, February 12, 2023. In the morning of Monday, 2/13/23, [redacted] noticed his Talino was not operating correctly and began trouble shooting with the company and HQ. Upon determining a potential intrusion may have occurred, [redacted] notified [redacted], [redacted], and CACHTU on 2/13/23. Following notification, [redacted] notified

[redacted] on 2/13/23. During the week of 2/13/23, there were numerous meetings between NY EM, NY Cyber and NY CIO, among others, in coordination with HQ. When there was an understanding of what occurred, [redacted] submitted a security incident report within SIRS on 2/17/23.

Observation 11: NY did not implement encryption on devices or data on the IS.

Clarification of Facts: There are broad contradicting policies as it relates to UCO IS. NY requested assistance in the development and testing the IS over the several years and was met with no response from OTD, CART, OCIO, and other HQ level entities. Going forward, recommendations from OCIO, OTD, etc., are being implemented.

Observation 13: Policy regarding the requirements for patching, ATO, use of an ISSO, security monitoring, remote access, account management, maintenance or IT hardware, use of mobile devices, and approval for custom MAIA solutions to include operational security, cost efficiency, SOPs, technical architecture, accounts and access, system access

records, acquisition planning, user account guidelines, compliance with 0655PG, and training for covert ISs is insufficient.

Clarification of Facts: NY has one ISSO, hired in mid-January 2023. NYO's ISSO is responsible for multiples sites. It is not feasible for one ISSO to effectively monitor and maintain IS's within the NYO. Industry standards recommend multiple individuals in different roles with qualifying credentials to ensure the integrity of IS's.

Observation 15: NY stored CSAM from multiple investigations in an effort to identify victims across multiple cases.

Clarification of Facts: As NCMEC only maintains the "MD5s" or "hash values" of the CSAM, not the actual media itself, NY stored CSAM on the IS for facial recognition and "photo DNA." PG 1157PG requires a CVIP comparison for CSAM which is facilitated through NCMEC and does not prohibit the creation of use of independent ISs to store and compare CSAM across multiple cases and field offices, noted in

draft INSD Report page 7. This should not be prohibited as it is not available through NCMEC/CVIP.

Observation 16: NY did not follow minimal and commonly accepted industry wide security practices for the IS.

Clarification of Facts: As there are numerous conflicting policies and constantly changing guidance regarding the IS, as it falls under a covert network, NY did not willfully violate policies or accepted industry wide security practices and welcomed any and all assistance from other field offices and HQ sections.

Guidance and funding of recommended training, internal and external, should be provided by HQ to provide consistency of enterprise wide IS standards. Properly ensuring IS's are developed, maintained and monitored requires hiring and retaining qualified personnel such as ISSO's and ITS Network Specialist/Architectures. Special Agents and non-ITS Professional Staff are not technically trained and not equipped to act as a System Administrators

NYO has one ISSO with responsibilities spanning NYO's Headquarter City and all Resident Agencies. The ISSO was hired and on-boarded in NYO mid-January 2023. NYO Security does not currently have ITS Network Specialist/Architectures. NYO Security would require a minimum of four ISSO's and five ITS Network Specialist/Architectures to ensure all IS's within NYO have a System Administrator and all IS's are securely developed, maintained and monitored. NIST and other industry standard best practices require designated personnel outside of the operating unit to act in these roles. Separation of duties is required to retain the integrity of the IS's.

NY's Responses to the Inspection Report's Findings

Instruction 1: ADIC NY shall ensure all unauthorized devices allowing Internet access through wireless connectivity are removed from FBI secured space or disabled.

Response All non-approved wireless devices in FBI space are disconnected. Devices approved by division

head and the AD of SecD will remain operational only during mission critical needs at this time.

Communication regarding the prohibited use of wireless devices within FBI space has and will continue to be disseminated on a regular basis. Signage is in place referencing policies prohibiting the use of wireless devices in FBI space. For example, signs are posted in each elevator bank of 26 Federal Plaza.

All owners of overt and covert portable electronic devices (PED's) are required to register devices with NYO's Security unit whereupon the user accepts the terms of use for said devices. The terms of use include but are not limited to the prohibited use of wireless connectivity to include radio frequency connections such as Wi-Fi and cellular based Mi-Fi within FBI space.

NYO's Security unit has engaged with NYO's Technically Trained Agents to begin routine sweeps within NYO's space to identify active RF's. If RF devices are identified without a waiver authorizing

use by NYO's Division Head and the AD of SecD, the device will be disabled and/or removed from FBI space.

Instruction 2: ADIC NY will ensure overtly and covertly purchased IT is not used on the same IS.

Response: While this is a HQ driven process, as CACHTU purchases Axiom, Cellebrite and GrayKey directly from the vendor on behalf of the Field Office and provides these tools to the Field, NY is in contact with CID to ensure IT meets this requirement, or a waiver is granted.

Instruction 3: ADIC NY will ensure evidence is stored in a safe, secure, and approved manner.

Response: [redacted] refutes the assertion he took home and stored DE at his house. NY will ensure that appropriate policies related to storage of evidence are followed.

Instruction 4: ADIC NY will ensure compliance to applicable policy when creating and maintaining derivative DE.

Response: NY has consulted with CART and consistent with CART SOP and PG, the underlining

electronic device, as well as the Master Copy, will be entered into evidence as a 1B. A further additional copy will be made as a working copy on which the actual forensic work will be performed. NY will engage with CACHTU to obtain the appropriate funding required to obtain the required portable electronic storage devices to house the increased numbers of copies. Further, NY is working with NY Evidence and the Laboratory Division's Field Evidence Program to obtain authorization for standalone storage devices to be classified as an appropriate Evidence Control Room to house Derivative Evidence. The standalone storage device would contain the same Derivative Evidence which would otherwise be copied onto hard drives and physically checked into evidence. The storage device would be secured with sufficient user credentials and maintain access logs. The Derivative Evidence would still require an evidence submission to generate 1Bs for the Derivative Evidence. At the conclusion of the case, this Derivative Evidence can be deleted and the space made available for new Derivative Evidence to be stored, rather than continuously purchase new hard drives only to have them destroyed at the conclusion of an investigation.

Recommendation 5: ADIC NY will ensure compliance to applicable policy when creating and maintaining derivative DE.

Response: NY performs post examination reviews and documents them via an FD-302. A hash verification log is also created.

Instruction 6: ADIC NY will ensure compliance with requirements to document ELSUR records in accordance with applicable policy.

Response: NY ELSUR stated any communications that occur via a covert platform (i.e an OCE/UCE cellular phone) is not ELSUR evidence.

Instruction 7: ADIC NY will ensure compliance with requirements to document meetings between undercover personnel and the appropriate SAC/ASAC and SSA.

Response: NY will document meetings held with the SSA/OCE and SAC or ASAC/OCE and place in the appropriate subfile of the UCO via an EC.

Instruction 8: ADIC NY will ensure compliance with requirements to employ covert methods to obtain goods when using confidential funding.

Response: NY will ensure compliance with requirements for making covert purchases. NY Security has implemented approval processes for the purchase of IT equipment. A review of the equipment and purchase method will be conducted and approved appropriately. NY CSO is now a member of the UCO local review board to ensure all policy is adhered to when purchasing, implementing and utilizing overt/covert electronic devices and IS technology.

Instruction 9: ADIC NY will ensure compliance with requirements to maintain and document financial records related to UCO activity.

Response: NY will ensure that all financial documentation will be placed in the CE subfile.

Instruction 10: ADIC NY shall ensure compliance with security incident reporting requirements to report security incidents within SIRS.

Response: NY will work with the NY CSO to ensure all security incidents are reported within the prescribed time frame per policy.

Instruction 11: ADIC NY shall ensure compliance with encryption requirement for the IS.

Response: While this does not apply to the UCO, NY will ensure compliance with encryption policy as applicable. NYO Security has engaged with OCIO to develop secure network protocols based on industry standards such as NIST to include encryption at rest and encryption in transit.

Recommendation 15a: ADIC NY should no longer maintain a set of CSAM for independent analysis outside of the CVIP approved hash based searching tools.

Response: NY fulfills its requirements to submit images of CSAM to NCMEC via the CVIP.

After the final INSD report came out, I was advised that [redacted] received a call from [redacted] and [redacted] who were accusing me of making statements to the effect of having no regard for following policy. This is of course

categorically false and thankfully [redacted] believed as much, especially when neither AD could or would provide any details regarding the allegations such as who heard it, where it was documented, or why it was only then being addressed. However, in response, I submitted the following:

"Bosses,

Regarding the assertion that I made a statement indicating I would violate policy for the sake of an operation is a utter non-sense. Furthermore it is a gross miss-interpretation of the conversation that was had and quite frankly an insult to my character and integrity. Aside from lacking context, the choice of words used is blatantly misleading.

I'm happy to provide as much context as needed, but in short I have never, and would never, jeopardize any investigation (or my career) by intentionally violating policy. What I have done, and would do, is anything to save the life of a child. What I said that has been misconstrued, was that I would do anything to save the life of a child, and that if I were to ever violate policy or the law, it would ONLY be because there was an imminent threat to life in which a clear and articulable exception would apply.

I stand by that statement and take great pride in my knowledge of both the law and policy as it pertains to our investigations and operations. If requested, I can provide several examples of having to act under the emergency exception clause, which have all been justified. If requested, I can also provide examples of times in which I didn't, even though doing so would have been easier for the "operation".

I could write a novel defending myself, my words, and my intentions; and will if requested. For now I'm relying on my 15 years as an Agent with outstanding PARs, numerous awards and accolades, my contributions to policy revisions, and my reputation to satisfy any concern that may exist."

I believe Digital Extraction Technician (DExT) training was opened to VCAC Agents in 2012. [redacted] was my instructor for DExT. As of 2023, I knew Ledford was a Unit Chief (UC) and led the Cyber Action Team (CAT). I believe at least three or four of us initially received DExT training in approximately 2012, but I think all of us working Innocent Images/VCAC on the squad were eventually trained. However, once the child exploitation program moved from the Cyber Division to the Criminal Division, that changed. The funding we received through the Criminal Division was significantly less than what we received through Cyber Division, so the DExT program was no

longer able to put on as many classes and certify as many people as it had before. By the time of the intrusion that forms the basis of this internal inquiry, only about half of the "child exploitation" Agents on my squad were DExT certified. This is while we were still with CY-3.

We got certified because the Computer Analysis Response Team (CART) was long overburdened, and not familiar with the nuances of the child exploitation violation, such as the types of programs used by offenders, the vernaculars, etc. It was also known, and something I witnessed personally, that due to the reliance on CART and how long it would take for them to prepare a case for review, "hands-on" offenders were not being arrested in a timely manner. This resulted in the continuation of child victimization at the hands of the offenders the FBI was actively investigating. This was around the same time Agents working other violations began to also see an increase in the collection and reliance upon digital evidence in their cases. As DExTs, we were encouraged, and in some cases I believe required, to assist CART with their backlog by conducting DExT extractions for other squads. The other reason was to eliminate the lag time in searching evidence and identifying contact offenders (offenders who physically exploited or physically assaulted children) sooner.

VCAC investigations are different than most other FBI investigations since, in VCAC investigations, a search warrant is generally executed in the early stages of an investigation,

and the evidence needed to arrest and charge an offender is usually derived from the materials seized during the execution of a search warrant. Whereas other squads, generally speaking, execute search warrants at the culmination of their investigations.

[redacted] was a UC of the Crimes Against Children Human Trafficking Unit (CACHTU) at FBI HQ and eventually an ASAC at NYFO. He was a huge proponent of DExT. Being DExT trained allowed us to conduct our own data extractions faster, but more importantly, it allowed for a faster and more efficient way of identifying "contact", or "hands-on", offenders and, thus, rescue child victims of sexual abuse before they could be further victimized.

After becoming DExT certified, we received DExT equipment that allowed us to image, process, and better review the digital files. The DExT training allowed us to better use FBI analytical programs to review digital evidence. Being DExT certified allowed us to assist CART by offering an alternative for other squads to use for data extractions. At the time, CART was not located in NYFO Headquarters City (HQC). CART was located in Moonachie, New Jersey. It could take an hour to get to the CART lab from the NYFO. CART evidence reviews needed to take place there and it could take all day. CART eventually moved to NYFO, HQC.

The volume of data extractions we took on lessened the burden on CART. At least in New York, CART only had one or two

examiners who could handle data extractions immediately, and almost certainly none who could respond after hours or on weekends.

Since we dealt with child victims, it was, and is, imperative that the digital evidence be processed immediately. In nearly every child exploitation investigation the digital evidence is quite literally the evidence to prove the crime and without a prompt review, there is no probable cause to effect an arrest, putting the lives of child victims in continued danger. It is that very risk, the risk of continued abuse, that has prompted the FBI to enact new policies requiring expeditious investigation into allegations of child exploitation. This includes the expeditious review of evidence.

Prior to the DExT training, triaging electronic media on the site of a search warrant was not really a practice. We had to take digital evidence back to the office to view it and we relied more on the post-search interview. After a search, we had to go back and arrest an offender once we found the evidence. This made for a significantly more dangerous arrest because the offenders knew we were coming. There was also the potential for offender suicide. We had three offender suicides that I can recall. There was also concern, based on it having actually happened, that during the time it took the FBI to review seized material, the offenders were continuing to engage in the sexual exploitation of minors. The DExT program sought to remedy this problem by expediting the time it took to conduct forensic

reviews, thereby expediting our ability to rescue affected children.

NYFO SAs [redacted], [redacted], [redacted], [redacted], and I were DExT trained. SA [redacted] (aka [redacted]) was also DExT trained. [redacted] was the last to be trained while our squad fell under Cyber Division. At the time, I was the most junior Agent on the squad. Before being DExT trained, all of our digital evidence was submitted to CART for data extractions, imaging, and processing. We did have access to the Case Agent Investigative Review (CAIR) system, a forensic tool for data review, but the program was slow, not capable of handling large evidence reviews, did not work all that well, and did not do what we in the child exploitation program needed it to do. As a result, rather than using CAIR, Agents on the squad opted to travel to Moonachie, New Jersey, where CART was located, to conduct their reviews on site versus over the CAIR network. The ineffectiveness of CAIR was no secret and was widely known, and one of the reasons for the creation of the autonomous DExT labs.

After collecting digital evidence, I would enter the digital evidence into the Evidence Control Unit (ECU) and get a 1B evidence number assigned. I would then enter a CART request with a description of what forensic examinations I needed to be performed and information on the device that needed to be extracted. Then I would submit it to CART. It could take a day or two to get the evidence to CART and the amount of time it

would take CART to process the evidence varied. It could take weeks or months. Once it was extracted, CART would process it in the Forensic Tool Kit (FTK). We could review the data on CAIR or go to Moonachie to review it. Everyone on the squad, for the most part, chose to go to Moonachie. CART Digital Forensic Examiners Stephen Flatley and Carlos Koo eventually set up a spot in NYFO, HQC to do data extractions.

Even after receiving DExT training, we used CART for things like very large media dumps/extractions and encrypted files. We also used them to help us with understanding what some of the digital evidence was. I believe CART may have provided us digital copies of the data extraction and I think it may have been on DVDs. They would have been accessible on Operational Wide Area Network (OPWAN) as well, but we did not have OPWAN and would have to go to CART to access that anyway. I do not recall what we did with the copies on DVD. CART may have checked them into evidence and provided a working copy. The DExT trained Agents would do data dumps on everything we could like hard drives, loose media, and thumb drives. At this time, telephones that were seized still needed to go to CART for processing.

In 2015, generally if it was a device we could image, we would follow this process. We would use write blockers to assure we did not accidentally manipulate the original data. We would create an image of our evidence; sometimes we would use another hard drive. We imaged and processed the data. We had some hard drives, but I am not sure where they came from. I believe HQ

sent us a box of hard drives. I also believe CART may have given us some as well.

We used a forensic duplicator called a TD3, and later a TX-1 as well as FTK Imager, to image a device onto a hard drive and make the derivative evidence. We would then make a working copy image off of the derivative evidence. We would then work off of the working copy.

I am pretty sure the derivative evidence was cataloged and placed in the NYFO ECU if that was the policy, but if that was not the policy we would not have done that. The DExT Program provided us with Redundant Array of Independent Disks (RAIDs). These RAIDs were to be used to house our working copy evidence images. I initially advised the interviewing SSAs, once we ran out of hard drives for derivative evidence, we were instructed to use the RAIDs and that these instructions came from either a squad mate or my supervisor. This is true, as it was the SSA and the case Agent for our squad's Group II whose responsibility it was to request and receive funding and equipment. Any requests that we needed were routed through them, and the Group II case Agent was also one of our DExT Agents who also faced the same issues of not having the hard drives to create derivative evidence. However, I also recall these instructions were provided by HQ, either our Program Manager (PM), the DExT PM, or both. This may have occurred in 2012 when I went through the DExT program and continued over the years. As there has been a revolving door of PMs, I do not recall the names of the people I

spoke with at the time but can provide as many names of PMs who I can recall had been there over the years.

Typically, the person running a Group I or Group II Undercover Operation (UCO) investigation and the squad SSA would be the people who communicated with HQ for resources. As an example, I recall in 2015, I sent an email to SA Tommy Thompson, who was the case agent of our squad's Group II, asking for some large capacity hard drives with our remaining Group II funds. This was one of many requests I made, which were generally verbal, for equipment/resources. At the time we were still merged with Cyber. When we moved to the Criminal Division, our funds were nearly wiped out. Sometime thereafter, [redacted] left NYFO and became a DExT PM at FBI HQ. She would often complain about a lack of funding.

When we first became DExT trained, it was much easier to comply with the policy since the size of the data was significantly smaller than it is today. For example, telephone dumps then often fit on a DVD, or worst case a Blu-ray DVD. Today, DVDs are nearly obsolete as the size of data collections has become enormous, requiring large capacity hard drives which are more expensive and harder to get.

To be 100% compliant with the existing policy each year, it would likely require C-20 alone to purchase over a hundred hard drives, and this is just one squad in one office. To ensure that everyone in the FBI is compliant each year, the FBI would likely have to purchase thousands of hard drives, then do this year

after year. But the FBI does not do this and the policy it created to cover search warrants decades ago has not changed, despite the fact the environment the policy applies to has.

This is one of the several fundamental flaws that I have and continue to voice. If creating derivative evidence is a requirement, then why does the FBI not automatically provide the hard drives? How can the FBI enforce a policy without providing the field with the ability to comply? If, in nearly every search warrant executed FBI-wide electronic media is seized, resulting in the need for derivative evidence hard drives, why is it then incumbent upon each individual squad, in each office, under each program and division, to figure out a way to obtain the funding to purchase them? If the FBI knows hard drives cannot easily be purchased in bulk, and that there are security requirements on where the drives must be manufactured, why does the FBI not just purchase them for us rather than place that nearly impossible burden on us?

In approximately 2017 I took over as case Agent for our squad's Group II. As the case Agent I was able to use Group II funds to make purchases, which were obligated to us through CACHTU.

I was running out of hard drive space for derivative evidence and of storage space in general. The PMs told us buying hard drives in bulk was a problem. The stores had a capacity limit, but I was advised to try anyway but was not successful. I would purchase the drives on Amazon, like I was instructed to do

by HQ, until my covert account was shut down by Amazon since the purchasing of large quantities of hard drives was flagged as suspicious. We were also purchasing hard drives from New Egg, like we were instructed to do by HQ, specifically SSA Heath Graves who was the DExT PM, because they could sell bulk (10 or more) hard drives, but I was later told by someone in the Procurement Unit we could not use New Egg. This left us with very few options for buying hard drives and despite voicing these issues, no one at HQ offered a solution. In speaking with other Agents across the FBI, I learned this was a common problem. I went to CART who gave us what hard drives they could spare. I specifically sought assistance from senior CART Technician Steven Flatley on a regular basis and aside from seeking his expertise, I constantly bothered him for hard drives and other needed items.

In 2017 I began to gain a voice among many FBI Child Exploitation circles. I took over our squad's Group II UCO, and almost immediately converted it into a Group I. This conversion, which allows for the use of sensitive techniques, was done due to my desire to enhance our undercover capabilities and increase our effectiveness by using some of the most robust undercover techniques available at the time. While every undercover operation must be approved every six months in front of the Criminal Undercover Operations Review Committee (CUORC), because ours was now a Group I, it also had to be presented up through CACHTU and approved by the AD. During the CUORC, I brought up

the funding issues. In the funding section we discussed what we spent and what we anticipated to spend. During my time as the case Agent for my squad's Group I, my squad's statistical accomplishments increased exponentially. The number of undercover sessions conducted by my squad increased by 198% in the four years after I took over the NYFO child exploitation program compared to the four years prior. This meant an increase of approximately 2000 undercover sessions in the same four-year span. More significantly, however, was how I tasked undercovers and provided direction to ensure the program worked to identify the most vulnerable of the exploited children; and set out to rescue them. The results cannot be overstated in that the lives of hundreds of children were saved. While I am personally responsible for saving the lives of hundreds, many hundreds, if not thousands more were saved because of how I managed and directed the child exploitation program.

In 2018 I did a five-week temporary duty assignment (TDY) at CACHTU. My former SSA, Sean Watson, was the UC there. My job was to call every VCAC Group I and Group II UCO Case Agent and ask questions about the issues they were having and to provide recommendations on how to better the program, how CACHTU could better assist the field, things that needed improvement, etc. I learned a lot about the issues affecting the entire child

exploitation program and, while there were some differences in the issues facing some offices over others, there were a number of common issues that impacted every office. These issues largely dealt with lack of guidance, direction, training, equipment, DExT support, funding, and personnel. I drafted a summary of the calls I made and created a section for complaints from the field in reference to DExT and provided my assessment to CACHTU leadership. One of the many takeaways was that nearly every office had different understandings of and methods of complying with policy and guidance. The lack of and often conflicting guidance and policy both from CACHTU and from individual field office chains of command had led to each field office having to adapt their ways and creating a complete lack of consistency across the FBI. This summary was also provided to the interviewing Agents, and I can make it available to whomever needs it.

This same assessment, as well as additional details were also provided to Bryan Vorndran, who was the Deputy Assistant Director (DAD) who covered child exploitation, as well as to my immediate supervisor and to the supervisors/PMs at CACHTU. This came as DAD Vorndran separately requested a working group of Subject Matter Experts (SMEs) to address the needs of the VCAC program. I explained to him how we had equipment, training, and guidance needs and provided my assessment both orally and in several documents.

Also in 2018, CACHTU PMs SSAs Michael Deizlak and Matthew Chicantek were presenting to EM on the issues facing child exploitation investigations. SSA Deizlak and SSA Chicantek requested information from me that they wanted to present. I emailed SSA Deizlak and SSA Chicantek, along with UC Sean Watson of CACHTU, the write-up I sent after my TDY as well as a separate, even more detailed summary of the issues. In this three-page summary I talked about the need to appropriate money for equipment, as well as details regarding issues affecting the program, including the DExT, guidance, support, and more.

Others and I made it very clear to HQ that we did not have hard drives. Every now and then they would send us some and every now and then they would send funds, but nothing was consistent. I also informed my SSA of the need for hard drives. I was aware he knew we needed them and there were no funds. Other Agents were dealing with the same issues. It has been, and continues to be, the practice of VCAC Agents to create derivative copies of original evidence if derivative hard drives are available. However, given the long history of not receiving either the hard drives or the funds to purchase them, VCAC Agents have been left with no alternative but to store their derivative evidence on local storage. I would sometimes create a derivative copy of the evidence on the RAID tower, as well as a working copy. If the evidence was a large collection of different computer media, it was not practical to store two copies (a working copy and derivative copy) on the RAID tower

and I would only create one. However, I very often created derivative evidence copies onto either internal or external hard drives that were maintained in our lab, either as having been recycled, repurposed, or acquired. Since, as discussed, we did not have a surplus of hard drives nor did we often have the funds to purchase them, I used ones I was able to get or hard drives that had been repurposed. However, it often was the case where I maintained the derivative evidence of several investigations on a single hard drive. This was due to the scarce nature of the hard drives, and the fact that I did not want to waste the extra storage space that was free if a particular case only took up a portion of the hard drive. As resources were hard to come by, I maximized the resources I did have. These derivative evidence hard drives were separate and apart from the evidence copies maintained on our RAIDs or servers. I was not able to do this for every investigation, due to the limitations discussed, but when feasible it was done. This was my way of going out of my way to create derivative evidence as often as I could, despite not having the resources. I have located some of these hard drives that are still maintained in the C-20 lab, and photographs of them have been provided to the interviewing SSAs.

When I was unable to create true derivative evidence to be checked into ECU or the derivative evidence described above, I considered the working copy of the evidence on my RAID or server as the derivative copy. Regardless, all the evidence copies had

"hash-verification" logs to ensure the copy was a bit-for-bit image of the original. Additionally, the forensic programs we used were designed to prevent changes to the evidence, so there was never a possibility that the evidence copies could be altered.

I have various correspondence with HQ advising there was a lack of funding. This not only affected us getting hard drives, but also various other things. Phung provided us with more RAID towers for storage and instructed us to use the storage to meet our needs. I do not recall her exact words, but I understood her directions to mean I could use the RAID towers for the creation of derivative and working copy evidence.

I also learned funds were available, but not designated for the purchase of the hard drives. Money was either not there or was allocated to something else. I spoke with Heath Graves who was the DExT PM and then Jim Harrison who is the current DExT PM.

In June 2023, I proposed an idea to SSA Seamus Clarke and ASAC Spencer Horn regarding how to address the issue of handling derivative evidence since the long-standing process of using external media to store derivative evidence was no longer practical. [redacted] and [redacted] liked my idea and encouraged me to reach out to the ECU to find a way to pitch the idea.

I reached out to Supervisory Administrative Specialist (SAS) Arlene McKenna, who oversees the NYFO ECU. SAS McKenna also liked my idea and stated any changes in the evidence

guidelines or policy would have to come from the Field Evidence Program (FEP) of the FBI's Laboratory Division (LD). SAS McKenna provided the name of the FEP's Supervisory Management and Program Analyst (MAPA), Adeline Joseph, and suggested I reach out to her.

On 06/07/2023, I spoke with MAPA Joseph via FBINET Skype call. I discussed with MAPA Joseph the issue with the current process, which was feasible years ago when the size of electronic evidence was significantly smaller. In those days, derivative evidence was stored on DVDs and in extreme cases, a blue-ray DVD or thumb drive. However, in recent years the size of electronic evidence seizures has increased dramatically, requiring hard drives to be able to accommodate the data.

I explained that while I personally have never had an issue obtaining DVDs, I could not say the same about hard drives. I explained that while the technical environment the ECU policy/guidance is based on has changed, the FBI's guidance/policy around it has not. This has created the very issue which is part of this inquiry; the frequent inability to abide by the guidance/policy. I stated that it has become increasingly difficult for the field to be in compliance with the existing guidance/policy since the field no longer has the resources to be compliant.

I offered to help figure out another process for maintaining derivative evidence, as I believed it was a waste of money and resources to purchase expensive hard drives for

derivative evidence, which will just be checked into evidence until the conclusion of an investigation, just to then be destroyed. I spoke with MAPA Joseph about creating reusable virtual derivative storage that was stand-alone. I suggested the virtual evidence locker could be a server, which could be controlled by the evidence units and that 1B numbers could still be used and assigned to the folders of the derivative evidence it stored and proposed the use of an electronic chain of custody process to document the access of the electronically stored derivative evidence. I further suggested that since the derivative evidence copies were maintained electronically, there would be no need to waste funds on hard drives that would just end up being destroyed anyway, and that at the conclusion of an investigation when the evidence is to be "destroyed", the media would be deleted, thereby freeing up space for new derivative evidence. MAPA Joseph liked the suggestion and stated she would discuss it with her team, specifically her UC whose name I cannot recall. My SSA and ASAC, [redacted] and [redacted], were both aware of my idea and conversations and encouraged me to follow-up with MAPA Joseph, which I did via email on 06/27/2023. This email, which has since been provided to the interviewing SSAs, stated in part:

"Hey Adeline,

A couple weeks ago we had a discussion about authorizing our lab to store DE on our servers, rather than

the repeated, costly, and wasteful process purchasing tons hard drives to store DE. The server, which would be secure, contain access logs, and still require a 1B for the electronically stored DE, would take the place of the physical hard drives which would save money, time, and eliminate the need to waste tons and tons of hard drives.

I was wondering what you thought and if there is anything we can do to get something like this going?

Thanks so much!

Aaron"

MAPA Joseph responded on 06/30/2023 with the following:

"Good Morning Aaron,

Hope all is well.

Apology for the delayed response. We are conducting in-person training this week for evidence tech's. For your awareness, we are working on wrapping up several projects for this fiscal year. I am adding the DE idea to our whiteboard to discuss this amongst the team to include all key stakeholders that would be involved. If you don't mind, I'll send you a calendar invite so that it's on my calendar to circle back with you to discuss what the team decided.

Kind regards,

Addy"

Since receiving this email, I have not heard back again from MAPA Joseph or anyone in her chain of command regarding this issue.

I have provided a recent example to the interviewing Agents. In this example, which took place in November 2023, after the intrusion and the initiation of this inquiry, C-20 requested funds for derivative evidence hard drives and were denied. After requesting $2,155.62 for derivative evidence hard drives, CACHTU responded to "Please utilize cart for a resource for this. We are under a CR and are very restrictive on what we can approve". C-20 then went to CART, as directed, who in turn stated they did not have any hard drives to spare and recommended C-20 request funds from CACHTU.

This example further illustrates that even despite the intrusion and the negative attention we received regarding derivative evidence hard drives, the squad was again put in the position of being unable to comply with policy because the FBI would not provide the requisite hard drives or funding needed to be compliant.

Sometime later C-20 would eventually receive some hard drives but were then advised by the NYFO ISSO their hard drives were out of policy and that they could not use them since the hard drives were not manufactured in the United States. This, again, put the squad in an impossible situation with no alternatives being offered. It was also quite ridiculous as it is likely that none of our computer equipment is manufactured in the United States.

When interviewed by INSD, I originally stated I was not sure when the standard practice for C-20 members changed to not

adding derivative copies to the ECU. This statement is inaccurate without context. The "change" that occurred was somewhat two-fold and started when the FBI moved VCAC from the Cyber Division to the Criminal Division and the funding we received was dramatically reduced. The other contributing factor was, as discussed earlier, the increase in the size of the electronic media seized during search warrants and the subsequent need for significantly larger and more expensive media to house the derivative evidence. This affected many things, including our ability to purchase hard drives. So, the "change" that led to our inability to regularly comply with the derivative evidence practice was out of our control. Despite that, I personally voiced this concern numerous times over the years, but it was not an issue many were willing to care about. Early on, when VCAC fell under the Cyber Division, we had regular access to these drives, but when the program was moved into the Criminal Division that changed. Despite repeated requests, as well as having alerted everyone within the chain of command, we were told to figure it out.

We had been advised that if derivative hard drives were not available, to store the derivative evidence on our local storage, which is what we did. It may have been in 2016 or 2017 and possibly happened because we did not have hard drives. I believe we were initially getting some hard drives from DExT after completing the certification course. DExT slowly went to no longer providing hard drives to new DExT certified Agents at

all. I do not know what they are teaching about digital evidence storage in DExT or how to get drives, but I know from other Agents who have attended the DExT training more recently that guidance has still been to seek funding from CACHTU, who again has been stating they do not have the funds.

As a more recent example of the FBI's funding issues, on 11/06/2024, I had correspondences with the NYFO finance person Earle Long regarding a $25 bill from T-Mobile to pay for subpoena return. This was a subpoena sent a while ago as part of a child exploitation investigation and normally these are paid for automatically by the FBI. In this case, as you can see in the attached, it was not. According to the finance folks, the funds are not available to pay this $25 for a standard investigative subpoena. I as a case Agent now have to request funds be transferred from HQ on a case-by-case basis for this, the most basic of investigative activities, to happen. This is ridiculous, and underscores the fact that receiving funds for basic things, even those required by policy, does not always happen. I think this example is important to illustrate the issues with funding and paying for things that are required. In this case, it was a subpoena issued pursuant to the identification of a child predator. Until approximately February 2023, the NYFO did not have a designated ISSO. This is a required position, and I think it being left unfilled exacerbated many of the problems that are discussed herein. I have provided INSD with documentation from retired Special Agent

in Charge (SAC) Nicholas Bouchears who created a timeline and report of his years-long request for an ISSO, which was a requirement that the FBI left unfilled in the NYFO until January or February 2023.

The situation was in essence entrapment. We were required by policy to create derivative evidence, but we were not provided with the ability to comply. Despite repeated acknowledgements from FBI HQ about the conundrum, solutions were never provided. We were told to adapt and to figure things out, and we did. The result is that we got punished for it, which is quite insane. We should not be held accountable for a problem we could not fix and were not responsible for fixing, especially when we have brought this problem to the attention of all levels of our leadership time and time again to no avail.

When derivative hard drives were not available, we did as we had been instructed by imaging the original evidence onto the RAID Storage or Network Attached Storage (NAS), and as previously discussed, I even went above and beyond given our limitations by creating derivative evidence copies of multiple cases onto larger internal hard drives so I could ensure I was doing everything within my power to comply with the policy. At times I would create a second copy. If I made a second copy, I would use one as the main copy and the other was the working copy. If I did one copy, that one would be used as the working copy. At times I would make multiple working copies.

According to INSD, I advised I had not been making derivative copies of digital evidence and that I now believe I personally made derivative copies and did whenever I was afforded with the requisite hard drives.

This is incorrect. From the beginning I have never wavered and have always been adamant that I had been making derivative evidence copies whenever possible. As I have also stated, this was an FBI-wide issue that affected many Agents, including many in supervisory positions. The issue is not that derivative evidence copies were not always created, the issue is why the field was not always provided with the ability to create derivative evidence copies.

The issue regarding derivative evidence that I and others faced was well known to our supervisors and specifically to our substantive desk at HQ. The question for us in the field was what do we do? Do we stop investigating our cases because we do not have a sufficient process for creating and storing derivative evidence? Of course not. Just because I, and others, did not always receive the drives did not mean our VCAC investigations ceased. Of course, we had to adapt and overcome and felt that while we may not have been able to create derivative copies for all the evidence, the reasons for that were well documented and out of our control. Had we, or I, decided not to work cases due to the lack of derivative evidence hard drives or funding for them, we would have been punished for that as well. Aside from neglecting work being itself an

offense, there are other policies governing the child exploitation program that explicitly require child exploitation Agents to expeditiously conduct their investigations. It is like being stuck between a rock and a hard place, and I, and others, were told by FBI leadership over the years to make do, as long as the cases were being properly investigated, and that is what we did.

At no point in time have I ever improperly stored digital evidence at my residence. After the intrusion when the FBI's INSD conducted their interviews, I had been asked about "evidence" and reviewing materials from home. I acknowledged that I, like everyone else, had done some work from home. However, the "evidence" being referred to has always been "working copies" and items that are absolutely covered under policy. At no time had I taken original or derivative evidence home.

I believed that I had cleared up any misunderstanding or semantics over the word "evidence", because that word used without a descriptor is just a generic term for *evidence*. The word has *types*, like a classification to distinguish what the evidence is such as "original", "derivative", and "working copy". Then, there are caveats to the *category* of evidence such as "digital", "general", "drug", "valuable", etc. For example, when I review subpoena returns, I am reviewing "evidence", but that does not mean the evidence is "original" or "derivative", and unless those subpoena returns are in paper form, they are

categorized as "digital evidence". Nevertheless, I am authorized to review those from home. The same applies to chat messages derived from a device or having been included in a lead or Guardian.

When discussing this with the Inspectors, I was clear that anything I reviewed outside appropriate facilities was working copies. At no point had I ever discussed with anyone that I have taken original and/or derivative evidence home or in any way in violation of policy. Any assertion to the contrary is categorically false.

I have recently found a folder that I created on my FBINET computer called "to Take home for baby leave". This folder contained items I planned to take home to work on while still under the work-from-home guidance we received during the pandemic, which is also during the time my wife gave birth to our twin boys. The items in this folder are generally indicative of other files I had reviewed from home, none of which are original evidence, derivative evidence, or CSAM.

Other examples that have also been provided to INSD include an email from CACHTU SSA Jordan Hadfield which was sent to all VCAC OCEs. The email was sent during the pandemic when OCEs were working from home and is requesting to know if OCEs were aware of a website contained in the email. SSA Hadfield instructed the OCEs to not use their "HOME COMPUTER" to access the link because it contained CSAM, however SSA Hadfield knew OCEs had their own

FBI-issued misattributed laptops and phones that they could access the link on from home.

Another example is from my supervisor at the time, SSA Sean Watson, who stated in an email dated 03/25/2020:

> *"I will be assigning Guardian lead(s) which can be worked from home or an alternate location. Reminder for 305 leads, do NOT use personal networks to vet out 305 leads. Use covert equipment with an aircard or covert cell phones."*

Throughout most of its existence the C-20 lab was Internet connected. However, and for clarification, the C-20 lab existed long before the DExT program and the misattributed Internet was connected to our squad's misattributed computers. At the time, Online Covert Employee (OCE) work was primarily conducted on computer-based Internet platforms whereas today, the majority of OCE work is on mobile-based platforms.

Back then, we used misattributed FBI-issued desktop computers to conduct OCE sessions from the lab and adjusted our work hours accordingly. As offenders began using mobile-based applications, OCEs were required to do the same. With the use of mobile applications offenders were now online and chatting throughout the day, versus just when they were on their home computers. Thus, the expectation of OCEs changed to emulate that of the offenders. I do not know exactly when we received FBI-issued misattributed cellular telephones, but when we did, we

also received the authority to take them with us wherever we went if we were engaging with CSAM offenders. In fact, OCEs have long been encouraged to communicate with offenders at random hours of the days and on weekends, to send offenders benign photographs while on vacation, at events, etc.; all to better legitimize the OCEs and help to dispel any fear offenders may have that the OCEs are law enforcement.

When we became DExT certified, our computers were not connected to the Internet except when we needed to update software, or some other Internet required task. As the years went on, the need for our DExT computers to be connected to the Internet grew. As discussed, HQ was aware of this and at times even promoted programs that required this. Additionally, two agents from C-20 and our SSA had all gone down to CACHTU to become SSAs and the UC respectively, and they were aware of this practice and need both from having worked on C-20 as well as from their positions at CACHTU. Lastly, as previously discussed, at the time of the intrusion our squad had been participating in a CACHTU pilot program, which included several other VCAC squads from across the FBI and required the computers to be connected to the Internet.

Regardless, our lab has always been "stand-alone", meaning none of our computers were connected to any FBI systems. Additionally, our lab was "misattributed" and able to be used in covert capacities and to access websites that could contain Child Sexual Abuse Material (CSAM).

Initially, in approximately 2012, the C-20 lab was not connected to the Internet, but at the time we had little reason outside of software updates to be connected to the Internet. Several years later that changed as the advancement in our software and capabilities grew, requiring our computers to be Internet-connected. The only guidance or direction we received at the time was that our Internet-connected DExT computers not be connected to a FBI network, but that has changed and we have received mix-messages with some guidance telling us not to connect our machines to the Internet and other guidance telling us we can if we use misattributed Internet. Confusing the matter more has been the implementation of software and programs that require us to be connected to the Internet. When OTD was brought in to bring the C-20 lab back online after the intrusion, they promised FBI EM and the NYFO it had a sensible solution, however nine months later and thousands of dollars spent by OTD in equipment, their solution was abandoned. I have learned that there were differing opinions in OTD about what to do and how to do it, with the OTD executives promising outcomes that the OTD engineers knew to be unattainable. One OTD engineer in particular vented to me personally his frustrations that OTD management is promising things they knew they could not deliver on.

Even FBI HQ implemented investigative steps that required DExT labs to be Internet-connected, such as the method that was used to transmit CSAM to the National Center for Missing and

Exploited Children (NCMEC), whereas previously it had been to do so via a storage media. Later, the FBI created the "SIFTS" program which was an online portal for CSAM transmission. As an example, the FBI's guidance on using SIFTS has been provided to INSD which includes a section that DExT machines must be connected to the Internet to use SIFTS.

In approximately 2022, CACHTU advised the field that the licensing method for one of our most used programs, "Axiom", was moving from dongle-based to cloud-based. CACHTU wanted to pilot the cloud-based method and elicited the assistance of five or six VCAC squads from across the FBI to do so, one of which was our squad. This pilot program, which began prior to our intrusion and continued well after, required the DExT computers to be connected to the Internet. It allowed us to check out a license when we needed to, but to do so, we needed to stay on the Internet to use it. There was some level of security provided by the switch box and some on the NAS itself.

The computers, NAS and RAID tower storage that contained CSAM were then all connected to the Internet. We received guidance from CACHTU, specifically from the DExT PMs, to disable the antivirus to use the Axiom since the antivirus would flag the program. I believe this came from Tommy, Heath, and CART, and others. Squad C-20 did not know how to set up the Internet and the switch box. We reached out to Computer Scientists (CSs) and CART and received some help, and I have numerous emails that I can provide to support this if requested. I do not know

anything about networking and how to set up networks, nor did anyone on my squad. The CSs also did not know. I believe someone from the Operational Technology Division (OTD) told me to Google it and stated that since we were not using OTD's OPWAN, they would not help us. Ironically, we were also told we could not use OPWAN since the building our squad was in did not have an OPWAN connection, plus the size of our dataset would have been too much for OPWAN to handle.

Networking is not a DExT function and is not in my skill set, so I did not even know what questions to ask. As I have stated numerous times, I am not, nor was anyone on my squad, a Systems Administrator. Despite the INSD having labeled us this in their post-intrusion report, we are not. We have never received any training or instruction on systems administration, and labeling us as such implies knowledge we did not possess.

The off-the-shelf security that was in place was what we were using. I and the squad asked everyone we could think of for help - CART, the CSs, OTD, the Office of the OCIO, Management Information Systems (MIS), etc. - however, all were of no help.

CS Jim Walsh helped us set up some of the equipment. Christian Idsola from CART also helped, as did another CART employee whose name I cannot recall. I also asked SSA Francisco Atrusa, the supervisor of the NYFO CART squad, for assistance. SSA Artusa responded back, asking Anthony Broderick, the CART networking and actual systems administrator, for help. Broderick responded that I should read the user manuals and that he did

not have the "bandwidth" to support us. These communications, along with many others, occurred in writing via email and I have provided them to investigators.

In our desperation to find someone with a networking/system administrator background to help us, we put out a Confidential Human Source (CHS) canvass for assistance with our network through our CHS Coordinator. This fact alone should highlight the lengths we went to in order to get our lab networked securely and correctly. The desperate act of issuing a CHS canvas for assistance should also convey the utter lack of assistance we received from within the FBI. We also reached out to OTD, Counterterrorism Division (CTD), and Cyber Division (CyD) for help, but none were able to. An Agent on a CT squad suggested that they had a Counterterrorism (CT) CHS who could come over and look at the network, however the CHS advised networking was not his/her specialty. The CHS was a former contractor for the FBI and had a Top Secret (TS) clearance and was not able to assist.

Our request was simple - to network the few standalone computers in our lab. However, no responsible entity within the FBI would assist, so we had to reach out to friends and colleagues to help on their own. While their help was valuable, none of our volunteered help came from anyone who was a network or systems administrator, and the FBI's network or system administrators would not assist. The various networking and system administrative units in the FBI handle FBI networks, and

the few that handle covert/misattributed networks do not handle CSAM networks. Despite the irrelevance of the latter from a technical perspective, CSAM is off putting and no one wanted to assist and CACHTU did not know what to do. In fact, CACHTU was aware that networking CAC computers was an issue affecting so many other FBI Offices that PMs Stacie Kane, Brenden Roth and James Harrison encouraged us to find the solution so that it could be emulated across the other VCAC DExT labs. In fact, our lab, and the improvements we had been making on behalf of the VCAC program, contributed to several end-of-year "gold" ratings by CACHTU.

As an example, in September 2022, SSA Brendan Roth, who was the PM for the Northeast region for CACHTU, requested that I assist the Albany Field Office VCAC squad who needed to enhance their program. FBI Albany was trying to figure out how to receive funds for their upgrades, and SSA Roth knew that I in the NYFO had been through this process and asked that I assist. After SSA Roth and I spoke over the phone, he sent an email to myself and SA Brian Seymore from the Albany Field Office stating in part the following:

"Aaron
Per our convo about Group I UCO funds for CSAM review stations - CC'ing Brian from Albany.
Maybe you guys can talk and answer questions he had about the process and questions you were asked about it from legal/procurement.

SSA Brendan Roth Criminal Investigative Division | Violent Crime Section Crimes Against Children and Human Trafficking Unit (CACHTU)"

In 2017, our lab flooded after the temperatures in the lab got so hot they triggered the sprinkler system. This devastated our lab and ruined thousands of dollars' worth of DExT equipment. After this flood, some of the equipment was replaced by CACHTU and CART was able to salvage some of the equipment. We moved the C-20 lab to the 10th floor in December 2020. I received approval on 12/22/2020 to purchase switches, NASs, cables and hard drives. This equipment was purchased with $34,000 in CACHTU funding, which also supplied the Long Island Resident Agency (RA) with similar equipment. This was less of an upgrade and more of a replacement for the lost equipment, but it set into motion our upgrades.

CACHTU PM Leslie Adamczyk was a former NYFO Agent and member of C-20 and knew about these issues. SSA Adamczyk similarly had her DExT computer connected to the Internet and similarly did not always create derivative evidence.

During the COVID pandemic there were three of us from my squad who came to the office on a regular basis; myself, SA Matt Deragon, and SA Brian Gander. The guidance, however, was to work from home. The C-20 SSA at the time was Sean Watson. SSA Watson provided guidance to work from home, in addition to the guidance pushed by the FBI Director, our AD, and others in FBI management. This guidance included conducting limited forensics

from home, and CACHTU pushed out to the field temporary AXIOM licenses for the sole purpose of conducting limited forensic reviews from home. This meant that literally the FBI was encouraging Agents to conduct forensic reviews, of evidence, from home. Ironically, however, I did not take advantage of this since the bulk of my forensic reviews meant reviewing CSAM. Due to this reason I came into the office almost daily to do CSAM reviews. This is a fact and can be corroborated by SAs Deragon and Gander, as well as by checking the building access logs which will show I used my access badge to enter the building and the frequency I accessed the building. Other work was done from home. I looked at subpoena returns and reviewed working copy material that did not include CSAM. Anything I took home was covered under policy and was covered under the guidance being disseminated. I have a Bureau-issued laptop computer that I utilized for these purposes. It is categorically false that I violated policy by taking home CSAM, original, or derivative evidence. I have numerous examples of guidance put out by the FBI, including from the Director, CACHTU, the NYFO ADIC, and my SSA about working from home. I have supplied some of these examples to INSD and can provide additional examples if requested.

At the time, I was working on three cases primarily: Robert Hadden, Darnel Feagins, and Jacob Daskal. Only one of these cases, Feagins, was a CSAM investigation. The Feagins investigation was the reason for my having to come to the office

during the pandemic, which eventually changed when, after indicting him, Feagins fled, turning the investigation into a fugitive matter. The Daskal and Hadden investigations were contact offense, or "hands-on" offense, cases that did not involve CSAM.

To conduct the investigation for Hadden I was doing web-based interviews from home and writing FD-302s and subpoena returns which were all non-CSAM-related. For the Daskal case I completed a 68-page DExT review FD-302. I took metadata-related information. Some of it was exported from Daskal's computer, but none of it was CSAM; rather it was data to prove he and the victim of the investigation were together in various locations and certain dates and times. For the Darnel Feagins case I was splitting the work. I did not do CSAM-related work from home. I did not take any storage devices home that were original or derivative evidence. Any copies or data I took home would have been working copies. It would have been impossible for me to take derivative copies home in general.

I was coming into the office every day to do my CSAM reviews. I do not believe I was doing any OCE work at the time since we were instructed not to. We were trying NOT to create a need for Agents to have to run out on warrants or to conduct Knock and Talks (KTs) due to COVID unless it was an emergency - BUT I and other OCEs would do OCE work from everywhere, including home, but all of that was covered under our Group I authority.

According to INSD, during my original interview I advised that Agents believed they were authorized to conduct OCE work outside FBI space and that we now have Electronic Communication (EC) authority to conduct OCE work outside FBI space. This is a slight mischaracterization of my statement as to this day it is our belief that we always had authorization to conduct OCE work outside FBI space. The reference to now having an EC was in response to additional questioning by INSD and did not change the fact we had appropriate authorization prior to the EC. For one, how we functioned as OCEs, to include when and where we conducted OCE sessions, had been directed to us through FBI trainings, FBI HQ, and our supervisors. Second, the authority was written in our bi-annual Group I/Group II renewals, which are reviewed and approved by the entire chain of command and include the NYFO Chief Division Counsel (CDC) and the Office of General Counsel (OGC).

Regarding anything I took home to work on, I have always been certain about what I knew I was authorized to take home and what I was not. As was authorized, I would take home removable storage devices like a hard drive or thumb drive that contained working-copy data and/or other material that would allow me to work from home. Some of my devices, including my FBI-issued OCE telephone and my FBI-issued and encrypted laptop, may have had CSAM on them, but as an OCE who was authorized to conduct OCE sessions from outside FBI space, which included my home and elsewhere, taking these devices home was covered by policy as

these devices were used in authorized and capacities. The OCE and UCE polices allow for these things since communicating as an OCE with VCAC offenders can require around-the-clock communication. There is absolutely zero truth to any notion that I violated any of these policies. I was quite literally doing my job, which as a VCAC OCE, meant taking my OCE laptop and telephone with me outside FBI space to communicate with CSAM offenders. The communications with these offenders and any CSAM I collected as a result, were maintained in accordance with policy and that is just a fact.

As for any evidence review I did from home, all was done in accordance with policy and guidance. Any evidence I did take home was all authorized under policy - it was not original or derivative and was only working copies. As a matter of logistics, I would not have been able to take home original or derivative evidence as I do not have the technical equipment at home to review them on my laptop. Rather, in what I believe was in accordance with policy and guidance, I had copied select datasets from evidence sources onto a thumb drive or external hard drive as working copies, which I would review at home. The original device would have been checked into the NYFO ECU and a copy would have been on the C-20 lab server.

The lab server had to be connected to the Internet to send CSAM to NCMEC. As mentioned previously, the official way to send CSAM to NCMEC is to use the SIFTS online portal. They will

accept hard drives, but it is not what they want, and NCMEC has been moving to eliminate the use of hard drives altogether.

There are conflicting policies, and I brought this up while assisting in revising the policy. I am one of, if not the only, Court-certified expert witness for the entire FBI for child exploitation.During COVID, the concept of remote working was becoming a thing. The idea came up during COVID to be able to do remote work since that is what the FBI was beginning to promote. The idea was continued by hearing from other members of law enforcement, including some within the FBI, that they were using versions of remote computing to access their forensic labs while away, such as on TDY or at a conference. The intention was not to work from home, per se, but rather to increase the efficiency of the forensic review process, as well as to assist the RAs and other FBI offices with their reviews, rather than having to use "Bu-mail" to send working-copy evidence back and forth or to require travel to another office to provide assistance. The steps of imaging and processing evidence before it is ready for review can sometimes take days. During this time there is little for the DExT Agent to do while the computer is doing its processing work. What little there is for the DExT Agent to do is often what separates one stage of this process from the next. So, if a stage is completed on a Saturday, it will not move to the next stage until the DExT Agent does the very few things needed to proceed, which may not happen until the following Monday. This may then kick the process off to the next stage,

but now the Agent may have to wait several hours or longer for the next step. In order to be more efficient and to allow this process to begin on a Friday, for example, and be ready for review on a Monday, I believed the idea of remote computing was a reasonable solution. Remote computing would have allowed for a the DExT Agent to remote in over a weekend to initiate the next stage of a process so that the process took advantage of the weekend to conduct the lengthy steps so that by Monday it was ready for review. The downloading process could take a while, but the steps between the process were three or four clicks. If I knew a hard drive was going to take a day or so to process, and the next process would also take a day or so, and it would not have been practical to go into the office just to click a button. Especially in a densely populated area like New York City during COVID. The idea was to be able to remote in to the server and tell the computer to move on to the next step of the process.

The idea of using remote computing was reinforced a few years ago when I attended training provided by the International Association of Computer Investigative Specialists (IACIS) during which we went through basic computer forensics. I heard about law enforcement use of Microsoft Remote Desktop Protocol (RDP) there. I believe RDP was being used in the Bureau, but I am not sure for what purpose or on what devices. I spoke with several others in the FBI about RDP, including the DExT PM at the time, SSA Heath Graves, who mentioned he had either been using it or

toyed around with the idea. SSA Graves mentioned to me that setting it up and using it was fairly easy, and that all I needed to do was follow Microsoft's directions as they were pretty easy to follow. SSA Graves knew what my intentions were and thought it was a great idea to be able to remote in to cut the lag time of our processing.

The first use of remote accessing software by the FBI that I recall was over ten years ago. Before then, OCEs using desktop computers to conduct their sessions had to be in the office; often having to work night shifts to chat with their offenders. I know that many OCEs used an application called Team Viewer that predates RDP to access their OCE desktop computers remotely from home. I recall Team Viewer was something that was pushed by HQ, however I never used it as an OCE. I also recall that when we were toying with using RDP I asked SSA Graves about Team Viewer and I remember him saying RDP was better and more secure. I do not remember if he said he had used it or not, but I do recall specifically that he suggested RDP over Team Viewer. I think this is important because remote access applications such as Team Viewer and RDP have been used by the FBI for years, have been known by, and even recommended by HQ.

I thought the C-20 system was secure. I attempted to access the C-20 computer lab through RDP. I believed the lab's security prevented me from remoting in. I had no idea that in so doing I had opened the lab's RDP port and that it had worked. I could access the port from in the lab, but once outside the lab, I was

unable to gain access to the network. I thought the security was doing what it was supposed to. I was later advised that the RDP configuration was mostly correct and that I was a step or two away from having set it up successfully and securely. I was not trying to be lazy or silly, I wanted to be more efficient in the download process. Sometimes I would start a process on a Friday only to come in on Monday and see it crashed and needed to be restarted. RDP access would have allowed me to see the crash and restart the process remotely.

I believe enabling remote access to the C-20 computer lab was a good initiative, but it was not executed properly. It was all about improving our abilities to protect children. I had asked for help, but I did not get it, but I did get encouragement. I was going off the guidance I received from the DExT PM and CACHTU supervisor, SSA Heath Graves, who advised me to follow the instructions off the Microsoft website. While I cannot recall verbatim what he said, I am positive it was in the realm of the Microsoft instructions regarding RDP to be "very good" and "easy to follow" or something to that affect. My heart and mind were in the right place, but I lacked the knowledge for networking and was not a system administrator. Yet I was tasked with setting up a network I did not know how to set up, and despite repeated requests for help, I was denied. I should not be held accountable for the FBI's systemic failure, especially when the FBI encouraged me and approved me to enhance our lab. I thought my attempt to remote into the C-20 lab did not work

because the security settings were effective. I asked for help, even help with RDP, from nearly every unit in the FBI that had anything to do with networking, DExT, etc., including CACHTU and the DExT PMs. All I got in response was encouragement in what I was doing, but no form of technical assistance. The FBI cannot say it did not know what I was trying to do, because the FBI did know, and the FBI was suppurative of my efforts.

I attempted to set the RDP up in either the Fall/Winter of 2022 or early 2023. The intrusion happened on Super Bowl Sunday of 2023, and I discovered it the very next day, on Monday.

I provided the interviewing SSAs with an outline I drafted on 02/13/2024 of the intrusion situation which I read out loud. I signed the copy of the outline and provided it to the interviewing SSAs to add to my statement. The following is from my outline. This portion of my statement is written as it appears in the physical outline:

Seamus, below is a timeline of what transpired today, noting that we had no idea this was a potential hack until late this afternoon. Given the potential that someone accessed our lab to do this, and that the issue may have been with the way we setup our network, below is also a little insight to the many attempts we've made to get the FBIto assist in both physical security to the lab and to help with networking:

Today's events (approx times)

-7:30am - I arrived at the office and noticed my Talino computer had restarted.

-7:40am - I logged in to my Talino and a txt file popped up that said in part my network has been compromised and provided an email address to contact. This file was in the "startup" folder so when logging in it opened automatically. I ran my computer's anti-virus software, which was up to date and active, and it identified one potential threat which I attempted to remove. While this is not common, it is also not unusual given the data we recover from 305 subject devices.

-I attempted to remove the potential threat, but my administrative privileges had been removed, and despite many attempts to gain access, I could not

-8:30am - I reached out to Christian Idsola at CART for help, but he was going to be tied up for a couple of hours

-9:00am, I reached out to Talino for help and they walked me through some steps, but nothing worked. They then advised me of a process to take to run antivirus software against my Talinos Operating System hard drive, which took some time but identified the likely source of the threat, which was attributed to a forensic program we use called Axiom. The threat was determined to possibly be a "booby-trap" left by a subject (who is a

hacker) that was tripped when the Axiom forensic program ran across it. After this discussion it was believed that was the reason for the issues and we then began working on a solution, which seemed likely to fix my issue.

-Around this time I also noticed our main server was down, but I didn't think too much of it since we just added a new switch and tried to configure some ports to run at different settings to increase our bandwidth. I assumed at the time the lack of access was a result of incorrectly applying the settings to the "LAG" and "BOND" configurations of the switch. I was able to see that according to the switch, the server seemed to be connected just fine, so I spent some time troubleshooting it.

-Around 11:00am or so I was finally on instant message chat with the makers of the server, Synology, who had us conduct some tests and they ultimately concluded that a possible issue was a defective hard drive in the server. This was a problem sine the server is "raided" and finding the defective hard drive was a time-consuming and difficult task, but several of us began our attempts.

-3:00pm - Is when Christian Idsola and Lewis LNU from CART came over to help. After a bunch of triage and testing we could not figure out why we could not connect to the server, since by all accounts it was working.

-We then noticed that our other servers (NAS1 and NAS2) were also not working properly, although we were able to access their control windows, unlike with the Synology server. After some digging around we noticed the folders that contain our data was missing. Initially we thought this was due to a firmware issue since Christian and I had dealt with that in the past and resembled the same issue.

-Around 3:30pm or so we located the log files and began combing through, which is when we noticed strange IP activity that took place yesterday from two IP addresses. The activity included combing through certain files pertaining to the Epstein investigation. I reached out to one of the case agents to see if they were in the office yesterday, thinking that maybe they inadvertently changed a setting on the NAS or if they noticed anything strange about them.

-Around 4/4:30pm we dove into the IPs and checked all of our computers to see which had the IPs in question. One computer, our discovery computer, matched one of them and is located in a room next to the lab, The other IP is one we don't recognize, but is the same address as the IPson our network, leading us to believe it was a computer that accessed our network somehow. We were not able to identify the computer, but it had to have accessed our network either by being plugged into the network, or possibly by telnetting in virtually.

-5:00pm - we realized we were hacked and discussed what we needed to do to ensure its contained.

-5:15pm, we immediately saved our logs and shut everything down. We disconnected the Internet and ensured anything containing a log file was preserved.

-5:30pm - I began calling my SSA, Bob Whelp in Security, Jessica Cardenas at CART, Amit Patel in Cyber. Physical Security

-Dec, 2021 - Moved into the 10th floor lab

-Dec, 2021 - made numerous requests for an electronic keypad lock on the door only to be told by the locksmith there is no funding for a lock. These requests have been made numerous times from Dec, 2021 until a couple months ago, when the response was to make numerous copies of the key we have to the lab
Networking/Network Security

-Since approx 2017 we have elicited help from CART and Cyber in networking our lab, all to no avail. Some CART and Cyber folks have come over on their good graces, but they were not network savvy and just tried to do what they could. Some months ago (I can look up the exact date) we again requested help from CART, but were told their networking person was too busy to help. This

meant no one with networking experience or ability was willing to help, so we had to figure it out on our own.

- End of the Outline -

Once I realized there had been an intrusion, I called SSA Seamus Clarke, and Bob Welp with Security. I also called CART and Cyber. This all occurred the same day I found out about the intrusion.

The switch box was for the internal network. We had a server rack and a server. We had a switch box, and we just added a second switch box. We also had a misattributed Internet that was connected to the OCE computers. The switch boxes were never connected together. The Internet entered through a router that was connected to the DExT computer and connected to the switch box. I believed all were secure.

I believed, since we had a revolving door of CSs and CART members, and since CACHTU was aware and having other offices emulate the C-20 computer lab, I thought we were good.

When the intrusion happened, we were in the middle of piloting Axiom. I thought of a lot of different things to allow remote access. We were trying to be on the cutting edge and think outside the box. We have a large set of hash files that we sent to NCMEC. A hash is a random string of text used to verify the integrity of a file. Hashes are also like a fingerprint, in that they are unique and can be cataloged. Regarding CSAM, all

files are "hashed" and those hash values are distributed throughout law enforcement and public sector entities. Using these hashes, CSAM can be detected since if a files hash matches that of a CSAM hash, the file can be identified as CSAM without even having to see it. We wanted to share what we had with the RAs. 500 terabytes of data was gone as a result of the intrusion. I was able to recover about 400 terabytes of that data, however, I was told to Google how to recover the data. No one else tried to help us.

The OCIO Section Chief (SC), Matt Smith, was pissed because he found an email I had sent prior to the intrusion requesting assistance that no one had responded to. I spoke with SC Smith who believed this was part of systemic failures. We asked for help, and our requests fell on deaf ears. We were always referred to someone else. I understand I opened the C-20 lab's RDP ports, but the FBI knew I was going to do this, and the FBI had told me to follow the instructions on Microsoft's website on how to open the ports. I was trying to make things better, and moreover CACHTU and other HQ and management entities knew what I was doing and supported me. The policies are not easy to find, are simply not available on the FBI's site, and often contradict one another. In fact, I have examples I can share of attempts to access policy just to find it isn't there.

FBI HQ Criminal Investigative Division (CID) DAD Jose Perez has since acknowledged the policy for the lab was vague or non-existent, which is something he advised EM of in an email that I

provided to the interviewing Agents. This email was sent on 2/28/2023, approximately two weeks after the intrusion. DAD Perez was emailing my, now retired SAC Michael Brodack, [redacted], and Richard Ruggieri, who I believe then was the Section Chief of Cyber. As this email is worth noting, DAD Perez stated, in sum, the following:

> "Following the incident in NY we identified a few other offices who were operating a similar set-up and were told to immediately disconnect from any open internet lines. Before you guys stand things back up I want to know that OGC, OTD, OCIO opine and establish firm guidelines.
>
> Given that this is affecting a few other offices as well we need to provide an alternative solution to the field. Generally speaking we are not opposed to a stand-alone network to review CSAM evidence if it is not connected to the internet while evidence is being stored or connected. I've asked OCIO to provide us with field guidance to specify: 1) a list approved FBI/OTD built tools to facilitate what we need (OpWan, DCAP, etc..) and/or 2) guidelines for an office to build their own tools or network.
> Policy is vague or nonexistent on this issue which we are working to address with formal updates and immediate interim guidance from the AD."

Additionally, a few weeks after the intrusion, DAD Perez, with others from FBI HQ, were visiting the NYFO on un-related matters, however there was a meeting to discuss the status of the intrusion which I was present for. Prior to the meeting, DAD Perez, whom I have known for years, approached me and informed me that he knew I was not responsible for the intrusion. DAD Perez further advised me that our lab was one of many across the FBI that had similar configurations. DAD Perez assured me that he knew the FBI had systemic failures, that we in the NYFO were not alone, that I should not worry, and that FBI HQ would help get our lab back up and running. DAD Perez also acknowledged me for my work and stated he knew I was the kind of hard-working Agent that the FBI needs.

Even as recently as November 2024 there is contradictory information being passed by CACHTU and OTD. As noted in the attached example "2024-CACHTU-dext computers online for cellebrite", an email was sent out from CACHTU to the field regarding the FBI's new method of using the cellphone forensic program "Cellebrite". Specifically, the guidance requires that DExT machines be connected to the Internet. This is along the same lines as the piloting of Axiom discussed earlier. The field is being required to connect their DExT machines to the Internet, much to the opposition of other "best practice" documents.

I was not part of the conversations to conduct a Security Incident Reporting System (SIRS) report.

I am certain, based on the statistics, that if I did not have the initiative, we would not have had our successes, which have resulted in hundreds of children being rescued and their offenders being brought to justice. I continued to receive praise for my work, and CACHTU has continued to ask me to review policy before it is sent out to the field. I took over the Group I UCO and doubled its statistical accomplishments. I have rescued more exploited children than anyone in the NYFO and in most of the Bureau. All I wanted to do was to better the Bureau. I did not know how to do everything right, but I always did the right thing and everything I did was with good intentions. I love this job. I was not reckless. There was no self-interest involved. I was always trying to do the right thing. I also want to point out that I was twice awarded the Medal of Excellence for my work, among other accolades.

Prior to the intrusion the squad was seen as the gold standard for child exploitation programs. Our end-of-year ratings were consistently "gold", and we were often touted as being amongst the highest performing squads in the Bureau. Our squad was responsible for hundreds of child victims being rescued and dozens of offenders being brought to justice. These impacts are directly correlated to our DExT lab and the work we did to enhance it. Even our 2023 end-of-year rating, post intrusion, was initially given as "gold" by CACHTU. CID AD Luis

Quesada later overturned that rating to "yellow", however, and later still the DD, in an unprecedent move, overturned that rating to "red".

After the intrusion we were directed to completely stand our lab down. We were directed to submit all our electronic evidence to CART for imaging and processing. A few months into this process, I and others on my squad compiled statistics comparing our effectiveness before and after the intrusion. At the direction of [redacted], this was provided to OCIO and to others in FBI EM. By comparison, after the intrusion our squad suffered a 95.52% reduction in productivity. During this time frame, my squad had 281 electronic evidence items that needed to be imaged and processed, and all but 12 of these devices had been taken to CART. Prior to the intrusion Agents on the squad could begin imaging evidence they seized the same day and were generally done imaging all their evidence within a few days. However, the average completion time for CART to image devices was approximately 30.5 days. This is a staggering number and is a prime example of why the DExT program is so important and how much of an impact the DExT lab had on my squad's ability to swiftly and effectively conduct child exploitation investigations.

Additionally, this summary highlighted one very unfortunate instance in which, because of the lag time at CART and the amount of time it took CART to image and process devices, an offender who was a citizen of another country managed to flee

the United States before the CART review could be completed. It is almost certain this would not have happened if the DExT review could have taken place in the squad's lab. However, it did happen, and again illustrates the significance of the lab and why the enhancements I made over the years, and the numerous pleas I made for help, were so important.

This summary has been turned over to the interviewing Agents, and I can make it available again if requested.

Completely separate and apart from the intrusion, but occurring simultaneously, ApostleX is both the name of a software company and their product. I had no previous relationship with the company prior to a representative from ApostleX visiting the FBI, NYFO to provide a presentation on their software. They were touring the United States, and approaching law enforcement and intelligence agencies promoting their product. They are a startup company. ApostleX reached out to several entities within the FBI: not just the NYFO. One of the ApostleX employees is a retired agent from NYFO named Chris Braga. I knew Braga from NYFO as a polygrapher. In October 2021 Braga reached out to me and several other individuals in the NYFO about ApostleX. I initially did not care much about the product. They were pitching a preservation tool that was geared towards CHSs. It initially did not sound relevant to what we in C-20 were working. Braga worked it out with others in the NYFO and set up a few information sessions for different NYFO Divisions. Our Gang squad, C-30 had an information session. On

10/20/2021, the C-30 SSA sent out an email to my SSA who sent the invite for the presentation to our squad. Another Agent from my squad and I decided to attend. I attended what I believed was a Bureau-sanctioned information session.

I want to be very clear that I had no previous relationship whatsoever with ApostleX. They approached the FBI, and I initially declined to even attend an information session. It wasn't until my supervisor sent an email to our squad advising of the information session that I decided to attend. All of this is very provable from the many emails and correspondences that I have provided as well as others I can provide.

I showed up late to the NYFO ApostleX information session and left early. The portion I did sit in on talked about how ApostleX helped with CHSs' use of 3rd party apps. The lack of technology available to preserve encrypted apps, or self-destruct communications, was a widely known issue. Self-destruct apps cannot be recovered, which makes them very popular with VCAC offenders. There were no good methods to capture the information. We voiced concerns about this for years, most notably during the CACHTU policy revisions in 2018, but there was no fix. There is a VCAC email distribution list in which CACHTU supervisors are participants, and there have been hundreds of emails over the years of Agents voicing concerns, asking questions, identifying issues etc.; which include concerns about this very issue. We did not have the ability to go after VCAC offenders who used self-destruct apps like Wicker.

There were, and remain, no ways for us to preserve those types of communications. When conducting chat operations, depending on the application being used, the OCEs are unable to preserve the chats with the offenders. Some applications allow for as short as a one second self-destruct period, meaning that after one second of viewing the chat, it is deleted and gone forever. There is no forensic program in existence within the FBI to preserve that chat. Furthermore, these self-destruct apps are designed in such a way that if an OCE attempts to screen record or use a screen shot to preserve a chat they either alert the person on the other end or do not allow the screenshot to be taken. The Bureau's answer to this problem was not really an answer. Some responses to this problem were to use another device to photograph the chats, which is problematic for a variety of reasons, while other responses were for our issue to be passed around. During the post-intrusion interview with INSD, I was advised that a solution would be to use my "Bu-phone" to take photographs of these chats. I asked what to do with the CSAM that I would inevitably be taking photographs of, and the INSD interviewer had no answer.

Once ApostleX came along and I heard what their product did for CHSs, I asked if it would work for encrypted chats and self-destruct chats. They said it would. I left the meeting and met with ApostleX after the presentation was over. When we met, we discussed if their technology would do what I described. They advised they would check and get back with me. They got back to

us in early November 2021 and advised they believed they had the ability to incorporate what I was asking for. I led the effort with ApostleX, but my squad was involved. I spoke with SSA Seamus Clark and ASAC John Penza (retired). We saw the benefit of it for VCAC purposes. My bosses wanted me to explore it. It was early on and we needed to do everything right.

I believe there were a ton of Agents, throughout the Bureau, simultaneously engaged in similar conversations with the ApostleX company, discussing how to purchase the tool. The ApostleX company has been to multiple FBI offices and may have had conversations with Safe Streets, Cyber Division squads, etc. I know this because I spoke to many of these Agents who were also trying to find a way to use ApostleX. I believe the ApostleX company pitched OTD and other ADs. At one point I even had an Executive Assistant Director (EAD) reach out to me personally about ApostleX.

On 11/08/2021, ApostleX requested I sign a nondisclosure agreement. I reached out to NYFO CDC Tara Semos and we may have also spoken with an Associate Division Counsel (ADC). The decision was that we would not sign anything. We did not have the position or authority. I told this to ApostleX, but I also told them that we were not going to steal their intellectual property.

People liked the ApostleX program. The consensus was that it was not a fully developed program, but that it could be developed.

I know there are several programs that are used in the FBI that were either made through Agent input or created entirely by the Agents themselves. I use some of these programs myself, and some of them have even been promoted via the VCAC email distribution list mentioned above.

Axiom is a CART-approved tool that the Bureau uses. I was asked to work with Axiom on how it was useful for us and what changes could be made to make it better for the case Agent. With respect to ApostleX, my understanding was that we were talking to a company that was brought in to us to fix a problem Agents throughout the Bureau were routinely encountering when dealing with a CHS or an OCE, namely the undetected real time preservation of their text chats.

We communicated with CACHTU who liked ApostleX, but said they would not commit funding.

In November 2021 ApostleX was still conceptual. It was in the right direction but needed to be refined. They knew from a big picture standpoint what the problems were. From a technical standpoint the product was a home run.

Just as was the case with the lack of funding for hard drives we discussed previously, nothing I or my squad did with respect to ApostleX was done in a vacuum. We briefed all the way up to the ASAC (Penza) level. He did not want us to go to the SAC or ADIC with a problem. He wanted us to also have a solution before we briefed the ADIC. He wanted the product to be more developed. He did not want an on-paper solution.

At no point did anyone on my squad or I sign a contract with ApostleX, or with anyone else for that matter. We followed the direction of the CDC, OGC, FFD, and others, including now retired AD Mark Gerber, with whom I had several related telephone calls and who was very suppurative of ApostleX and my involvement with it. We spent months going through the Privacy Threshold Analysis (PTA) steps to get the Bureau to sign a contract, as well as other steps and processes we were directed to undertake. We also never orally or verbally agreed to a contract with ApostleX. It was our goal to have the FBI take on pursuing a contract, not us.

At this point ApostleX was a concept and not a product. My chain of command had no issue with me working with ApostleX to develop the concept into a product. We were briefing our chain of command regularly and we even brought in our Intel supervisors. We wanted to make the product useful, not only to us, but to other people throughout the Bureau as well. We brought in CHS Coordinators, people from Intel, and people from the UC program. We did not want to think singularly about our violation.

It is required by FBI policy that we preserve OCE sessions, but even to this day technology does not exist to do that. I saw it, and still see it, almost as an entrapment for OCEs, in that we are required by FBI policy to preserve chats, yet the FBI has not provided us with a means to do so. I realized just how bad the disconnect from FBI HQ and the field was when someone in EM

told me he thought OCE chats were automatically preserved. This blew me away as this could not have been further from reality and shows how bad the disconnect is from what FBI HQ perceives and the reality in the field.

We saw ApostleX as an opportunity to address this and other concerns, follow policy, and follow the law. Current methods include all or nothing solutions, which result in "over-collection" and create potential First Amendment issues, in that they may record the communications of people who are not involved in child exploitation crimes or violating the law. ApostleX addressed this. The support we got from the onset of that vision was incredible.

FBI HQ knew what we were doing because I discussed with them the problems we were having with apps like Wicker. ApostleX was already successful with apps like Telegram and they were working on Signal and a few others. ApostleX engineers figured out how to make their program work with Signal while we were working with them. They were going in the right direction, we just needed to guide them towards a total solution to our actual needs. They were already working on trying to fix the problem OCEs were having in 2021. We just needed to work on how to preserve apps that created secret and self-destructing chats.

The ApostleX company was never given access to FBI information. They did not come into FBI space. We would FaceTime them. We never gave them anything that belonged to the FBI. The ApostleX program was installed on a completely standalone

computer that was connected to a misattributed Internet line. It was never attached to any FBI networks, storage containers, or covert networks, very specifically including the compromised covert C-20 computer lab network that was previously discussed.

The computer with the ApostleX program was in FBI space. It was an old computer that was going to be thrown away. It was a covert computer. I cannot recall if we had a CS wipe the drive of the computer or if it was provided to us with no drives and we installed wiped drives. Either way, we had to install operating systems. The CS was Jim Walsh. The computers were given to us to use at our discretion for misattributed purposes, such as for projects like ApostleX. I do not remember if I told him what the computers were going to be used for. I am not sure if we got the computers before or after we heard the ApostleX sales pitch. One event did not trigger the other, and I believed it did not matter as the computers were for covert use anyway.

ApostleX ran on a main computer. In our case it was the one we set up. The ApostleX database resides on the computer and the computer's sole function was to run the ApostleX server. ApostleX allowed undercover phones to connect to it. ApostleX is a server that sits on a computer and runs in the background. There is a web-based computer interface. It only works from one particular computer which sits behind a Virtual Private Network (VPN). If I am an OCE using the Telegram app I would connect my Telegram account to ApostleX. There is an authentication process. We had the company add an icon that let the OCE know

ApostleX was working in the background preserving the chats. The ApostleX company added a small icon that showed ApostleX was active. ApostleX's integration was chat application specific, so we were only preserving what needed to be preserved. It started with Telegram. Around the time we were told to shut down, it worked with Signal. We were getting close with What's App.

Any Telegram account we wanted to preserve would be added to the ApostleX account. We had the ability to select what was relevant and what was not. With appropriate authorization, we could do an account takeover of a Subject's account. With ApostleX there is an ability to avoid overcollection.

ApostleX was initially grabbing everything, and we would need to check what to preserve. We wanted to make a parameter for how long to keep information that was not checked, which would then be purged. The accounts would be taken over through consent or with a warrant. We were testing the capability of ApostleX to preserve self-destructing chats. Initially, in the testing environment, the disappearing chats were preserved on both the sender and the receiver's telephones, which obviously would not work for us. We worked with the company to address that.

The ApostleX company did not have the ability to access the data we collected from chat applications. The only data ApostleX had access to was the telemetry. I believe OCIO looked at that and was happy with it. SC Matt Smith from OCIO was also involved and sent Requests for Information (RFIs) to our local ISSO, Jim

Eckel, who reviewed ApostleX, the code, and had at least one call with them that I was a part of. I believe he also had additional communications with them that I was not a part of. In the end, I know that OCIO's questions were sufficiently answered.

We never went live with the ApostleX program and only operated it in a testing environment. We did not use active cases. We used dummy phones and OCEs chatting on the Telegram application. We added a bunch of older OCE Telegram accounts to test it out. All the accounts we used were real covert accounts. Some of the accounts were historical. When we synced ApostleX to chat application accounts, the entire history of the chat application account would be pulled. The information was exclusively stored on the local hard drive of the computer running ApostleX. One of the Telegram accounts I used for testing was about 12 years old. The test accounts I used were not involved in any chat groups that were pertinent. I am not sure about the other folks who were testing ApostleX. I do not believe anyone cared about the accounts we used. I believe the historical data attached to the accounts had already been adjudicated but it is possible some of the information may not have been. I cannot say there was no evidentiary data put on the standalone ApostleX computer, which is routine. Many undercover Agents use multiple devices to access their accounts, including both computer and cellular devices. Since the account originates on their FBI-issued undercover phones, any ancillary devices

have no impact. I do not believe having information on the ApostleX computer was any different than having it on any other computer. I did use a historic case to demonstrate how we could export from ApostleX for discovery purposes. The case was not fully adjudicated at that point. I am certain the accounts we were using had no impact on any ongoing investigation. There was likely CSAM from the historical accounts that was extracted and uploaded onto the ApostleX computer when the historic accounts were synced with the ApostleX program. The ApostleX company or anyone else could not see it, however, and this, again, was all known to the chain of command including CDC, OGC, etc.

It took a while to set the standalone ApostleX computer up. We may have hooked the computer up in December 2021 or January 2022. We tested it intermittently for a couple of months. It would be a day's long process to reconfigure things. We would give feedback to the ApostleX engineers who monitored the telemetry data and could see the issues with the ApostleX program from their end as we tested it. Sometimes the fixes took a few hours or a day or two. Once they had a fix, ApostleX engineers would send me a document with instructions on how to fix the issues. Any message that was sent from the company was done through Bureau email. The instructions would be written in the email itself or provided verbally. Though it is possible I may have used my personal telephone to communicate with ApostleX engineers using the video teleconferencing application, Zoom, I do not recall for sure. I do believe I may have used my FBI

laptop and possibly my OCE telephone for the Zoom calls with ApostleX engineers, however.

Sometimes the ApostleX engineer could see me during our Zoom calls and sometimes not. When conducting Zoom calls in FBI space, we sanitized the FBI space if the engineer would be able to see me. We would input the instructions sent by the ApostleX company into the computer with the ApostleX program on it. I don't have a background in computer coding and could not read or understand the coding I input on the ApostleX computer. I also did not have a process in place for an FBI employee who could read the coding to review what was being sent to me. When I was initially interviewed I advised I did not have someone reviewing everything ApostleX sent me. However, there were a couple of times I had "tech people", SA Robert Depresco, SA Martin Nachman, and others, look at the ApostleX computer and to review the code. I also provided the code and entire system to the NYFO ISSO, Jim Eckle, and others from OCIO to review the code and system. Additionally, I advised OTD and FBI HQ that they could review it as well. It is possible I forwarded the codes to other people to look at it.

There was no formalized process set up for updating the standalone ApostleX computer. The updates consisted mostly of updating a configuration file and if I needed to change code it was due to the configuration file. I made the deliberate decision not to let the ApostleX company remote access into the standalone AposlteX computer. During this process, I felt like

the ApostleX company was a verified entity and I was working with someone the Bureau invited in, and more importantly, that I had approval.

We ran the security process through OCIO and the NYFO ISSO, Jim Eckle, and Certified Information Systems Security Officer (CISSO) Robert Cavallo who were all satisfied with the setup. The NYFO did not have either the ISSO or the CISSO positions staffed until February 2023, however. My squad SSA, branch ASAC, CDC, and CACHTU were all aware of ApostleX and of what we were doing with them from the very earliest stages. There were others in the office who knew as well. As we progressed with our testing and development of the program, others were involved to include OGC, the General Counsel himself, the Procurement Office, several SACs, the NYFO ADIC, and various other leaders in FBI management. At a minimum, my squad SSA, branch ASAC and NYFO CDC all knew what we were doing. OTD was involved but not at this initial stage. CACHTU was aware and the Child Exploitation Operational Unit (CEOU) was also aware. I had gone back and forth with them a bit. There was communication on 11/08/2021.

I was passionate about this product as a force multiplier. I can assure you there was nothing done in a vacuum, and I can also assure you that everything I did was "above board". Any notion otherwise is patently false. When I started working with ApostleX on this product, my chain of command knew. My chain gave me the thumbs up to proceed and my guidance was to get to a

point where it was functional before we briefed the ADIC. From the very beginning I had the approval of my SSA, ASAC and CDC. I advised my supervisor on a regular basis on what we were doing, why, and how, but he did not micro-manage me and did not know every little detail that was involved.

I reached out to CACHTU to see who I needed to work with to get it approved. They said if I could develop the tech, it would be great. We also discussed funding, and CACHTU was not sure who would fund ApostleX. They said that perhaps they could fund the VCAC portion of it, but that for an enterprise-wide use funding would have to come from OTD or elsewhere. At the request of INSD I have included some email correspondence to support this. I also have hundreds of pages of documents that cover nearly everything that involved ApostleX, from the first instance I ever heard of them through the PTAs, the correspondences with CACHTU, CDC, OGC, FBI EM, etc. These documents show that everything I did with ApostleX was above board, and any notion to the contrary is unfounded.

As I mentioned previously, in April or May 2022, I went to an IACIS conference and the ApostleX program was working. Leslie Adamczyk, who was a former squad mate and a VCAC PM, was also in attendance. Leslie already knew about ApsotleX since we were good friends, and I was her former training Agent when she was in the NYFO. We spoke regularly and she knew about ApsotleX, but at this conference I showed her some screenshots of it. Leslie was amazed and thought the greater FBI needed to have this, and

she said it needed to be briefed at the Program Coordinators (PCOR) conference, and that when she got back to CACHTU after the conference, she would talk to the other PMs to see about adding me to the list of presenters. That was the perfect venue since it would be attended by VCAC PCORs from every Field Office. I was added to the list of presenters. I had conversations with the PMs and UC who oversaw the conference, and I was added to the agenda. I worked on a presentation and showed it to SSA Adamczyk. She loved it. SSA Adamczyk was a PM for CACHTU at the time and was coordinating with the person who put the conference together. I submitted a summary of what ApostleX was and what I was presenting on. I submitted a draft of my presentation prior to the conference. [redacted] was present during my presentation.

The PCOR conference presentation went well. There were numerous questions, and I had people who called me to talk more about it later. I heard from an Agent in Las Vegas whose SSA, Matt Schaeffer, was on an 18-month TDY to CACHTU as an Assistant Section Chief (ASC). ASC Schaeffer did not like the ApostleX program. The feedback was all positive except what I heard second-hand from ASC Schaeffer. During my presentation I made it clear ApostleX was technology that we were developing but that we did not have yet. If I made comments during the presentation about not following policy in my work with the ApostleX company, it was done as a joke. I was briefing a room full of supervisors as well as CACHTU about a program designed to help all their

Agents. In no way, shape, or form did I ever say, in any serious fashion, that I violated policy and/or that I paid anything for ApostleX. There is a possibility that I may have made jokes about paying the ApostleX company a dollar for the program, but I did not pay them a dollar, nor any amount for that matter. That would have obviously been beyond my authority as a GS-13 case Agent. At some point early on there may have been a conversation with ApostleX about if we should pay the company a dollar. We were concerned that we were using a product for free. I took the question to Legal or maybe even my bosses. The decision was made not to pay them. I remember this conversation occurring, but I do not recall the details since no monetary exchange ever took place. I began hearing rumors in March or April of 2023 about things I said during my ApostleX presentation at the VCAC PCOR conference being taken out of context. There was never a contract between the FBI and ApostleX, either orally or in writing, and if there had been it would have been through approved channels and not with me.

During the PCOR conference, ApostleX was still soliciting the FBI about their product. Around that time, ASAC Penza retired and at some point, Spencer Horn became ASAC. The ApostleX program was not active; there was no contract, and my chain of command was aware of what I was doing. The guidance to get the concept to a place where it was a better solution before it was briefed higher up the chain of command continued after

ASAC Penza retired and [redacted] came in. The SAC was eventually briefed.

A few days after the VCAC PCOR conference I heard from Joanna Pasquarelli who is an Assistant General Counsel (AGC) for OGC. AGC Pasquarelli attended the VCAC PCOR conference and saw my presentation. AGC Pasquarelli informed me we needed to stop testing ApostleX immediately. She did not say we needed to stop working with the ApostleX company, but to shut down the computer with the ApostleX program. We did so immediately. She also informed me we needed a PTA given the direction we were trying to take ApostleX. She also had concerns about the Fair Act and the procurement process in relation to how we worked with the company. We discussed the laws about companies bidding on the chance to work with the FBI on a product as opposed to a single source product. This process eventually included a lot of people from OGC. After sending AGC Pasquarelli my first draft of the PTA, she responded with, among other things, "I read through your draft PTA and you did an excellent job".

I spoke with CDC Semos about my conversation with AGC Pasquarelli. I was sent a "pony" of the PTA which I filled out and returned. AGC Pasquarelli was very pleased with what I turned in. Both she and CDC Semos mentioned orally and over email how pleased they were with the work I had done, and both expressed their eagerness to help. AGC Pasquarelli, CDC Semos, and later numerous others including people in FBI management all reviewed the entire process I had been engaged in and not a

single person expressed concern. To the contrary, all were eager to be involved in the project and to help get the needed approvals to develop and use ApostleX. There were a lot of email communications and Microsoft Teams calls. We had to make some comparisons to see if there were other companies that offered products like ApostleX.

I had spoken with OTD about the issues OCEs were having capturing chats on encrypted applications and capturing disappearing chats in the past. We had tried, unsuccessfully, to get OTD involved prior to this process. After OGC was involved, they required us to check with OTD on what they had to address the issue, or if they could come up with a solution in house. We also asked if OTD would work with the ApostleX company to develop the ApostleX product. We learned there was a product called Eagle Claw available which I believe is so bad that it should be taken off the approved list of tools to use. There was only one guy at the time working on Eagle Claw, and he said what I described of ApostleX was a homerun. Eagle Claw had a lot of limitations. We spoke with a lot of people about existing programs and external products as part of the procurement process. Nothing could do what ApostleX could do. I have and can provide extensive documentation regarding Eagle Claw and other programs, including testimonials, side-by-side comparisons, and more. Some of these products were created by the HQ desk for Safe-Streets, where UC Matthew Cobo was overseeing their attempts to use ApostleX.

I also know that even as of October 2022, CACHTU supervisors, including ASC Schaeffer and then SC Jose Perez, were aware of ApostleX. I know this because I have email communications between them and PMs at CACHTU who were helping to try and arrange a meeting about ApostleX. Never had there been any issues or reservations expressed to me or to the PMs helping to facilitate our meetings.

I continued to work through my chain of command, CACHTU, OGC, Safe Streets, OCIO, NYFO ISSO, Finance and Facilities Division (FFD), OTD and various units within OTD. We were moving along up and through the holidays of 2022. There were a lot of revisions to the PTA. We even worked through an emergency in which the Boston Field Office had a hands-on offender, and they needed to preserve their chat information. Despite initially receiving support, emergency use authority was never granted in that case. I worked with OGC GA Christopher Dearing on PTA revisions. I was delayed getting back to him due to a trial. Once I got back to him, the cyber intrusion of the C-20 computer lab happened.

The standalone computer containing the ApostleX program had been turned off in our testing environment since July 2022, roughly six months before the C-20 computer lab intrusion took place. We were not using it at all. I am not sure if it was even plugged in. I heard there was a rumor that some people believed ApostleX had to do with the C-20 lab computer intrusion. I received an email from CDC Semos that the initiative to use

ApostleX was going to be shut down due to the belief it was involved in the intrusion. This was completely untrue, of course, as two completely separate networks were involved, and the ApostleX network was not even running when the C-20 computer lab intrusion took place. ApostleX had nothing whatsoever to do with the intrusion. I believe CDC Semos cleared this rumor up with OGC. My chain of command wanted ApostleX to continue to move forward because they saw value in it. Before and after the intrusion I had been tasked with providing briefings and information to upper management including SAC Michael Brodack, SAC Robert Kissane, and ADIC [redacted] [redacted]. None were deterred by the intrusion and knew one had nothing to do with the other. These executives, along with the NYFO CDC, Tara Semos, and ADC Dane Christensen, were supportive of the pursuit of ApostleX and had no issue with anything I or anyone else had done. We saw that NYFO Criminal Division and CACHTU were being a roadblock. We had a meeting with [redacted] prior to the C-20 lab intrusion to get the ADIC involved in the ApostleX project to push the needle forward. We wanted to be able to pilot the program. Some of the questions from OGC asked who was supporting the ApostleX project. The intrusion happened before a formal briefing could take place, however.

There was a meeting about ApostleX with NYFO CT Division SAC Robert Kissane in August 2023. CDC Semos, [redacted], the ISSO, SSA of the Tech squad, Eddie Pennetta, SA Depresco, and SA Nachman. The meeting was about trying to use a Domestic

Terrorism (DT) case as a pilot case for ApostleX. There were still conversations about ApostleX taking place until I was notified of this INSD internal investigation.

I was working with CTD's International Terrorism Operations Section (ITOS) and some high-tech unit. They were asking for information to push up to EAD Larissa Knapp, who reached out to me personally. I had my ASAC respond to her on my behalf.

After the C-20 lab intrusion, CACHTU wanted nothing to do with ApostleX. NYFO wanted to see if they could do something with ApostleX on their own. They also got CT involved to see if they could push ApostleX through their networks. There were conference calls with the ApostleX company to field questions. Representatives from the ApostleX company may have also gone to Huntsville, Alabama and spoken with the AD of OTD.

There was confusion on getting the Authority to Operate (ATO). It was a chicken or egg situation. We did not know which one we needed first, the ATO or the PTA. We were working on the ATO process as well.

CACHTU funded the equipment for the C-20 lab. I believe Group I UCOs were exempt from needing an ATO. [redacted] was trying to see if we could get approval to use ApostleX under the Group I because he believed we would not need an ATO. I believe this was discussed with CDC Semos, because I was present when they argued about it. When I was putting together the information for the C-20 lab, I did not know about an ATO requirement. I later found out we did not need an ATO for covert

purchases. I think they may have tried to change that after-the-fact.

There was a financial threshold for the lab purchases. This was approved by Jack Cordes in OGC. It outlined what was needed for the C-20 lab and how we were going to use the equipment. I believe everything that needed an F number received one.

No one ever told me of the requirement for an ATO for the C-20 lab. It came up after [redacted] and CDC Semos had their discussions. This was not my responsibility anyway, as it would have been up to one of the dozen or so entities overseeing our Group I renewals whose job it is to know what is and what is not required from an administrative perspective.

Some of the ApostleX company sits in Ireland and some in the United States (US). They are registered in the US to receive government contracts.

Our squad's end-of-year review for fiscal year 2022 mentioned ApostleX as one of the reasons to give us a "gold" rating. However, ApostleX was also referenced as the reason for a lower program rating for fiscal year 2023. CACHTU initially rated our squad "gold", the highest rating, but DD Paul Abbate later changed our rating to "red", the worst rating, and included the reference to ApostleX and its direct involvement in the intrusion as the reason, which, as discussed previously in greater detail, is categorically false and both physically and digitally impossible. My ASAC attempted to fight this false narrative but was told it could not be changed.

I never understood that just working with ApostleX in general could cause procurement issues, and even to this day as much as I have learned from all of this, I know that my involvement did not and would not cause procurement issues. I have learned that nothing I did was improper and that many programs used by the FBI originate in much the same manner. OGC was trying to figure out how to make it work.

As mentioned previously, I think it is also important to note that NYFO did not have an ISSO or a CISSO when the C-20 lab was set up.

Under no circumstances whatsoever did I exceed my authority by contracting an outside company. There was no contract. My chain of command, including our CDC and later OGC, to include the General Counsel himself, knew I was speaking with ApostleX and creating a solution to a problem. I engaged the PTA process as instructed, working for months with many FBI lawyers, procurement officers, and management, all ensuring our pursuit of this much-needed program was done correctly. Any notion that I violated any policy, rule, or regulation is categorically false.

For perspective, ApostleX first came to the NYFO in October 2021, and despite the vast amount of people, entities, and oversight my work on ApostleX received, not once had I been advised anything I did was inappropriate until I received notice of this inquiry in March 2024. Among the many documents and correspondences I have provided INSD include many with OGC, CDC,

and CACHTU. Specific to CACHTU, I know that ASC Schaeffer did not like ApostleX, and after the intrusion he used it as an excuse to punish me. ASC Schaeffer banned me from being an instructor at the VCAC OCE course, of which I am a founding instructor. ASC Schaeffer accused me of lying when I presented on ApostleX at the PCOR conference. ASC Schaeffer stated that he believed I was supposed to present at the PCOR conference on a case update, but that at the last minute I switched my presentations to present on ApostleX and that no one in CACHTU was aware. ASC Schaeffer says he believed this, but it was months after the PCOR conference before he would eventually make this accusation. Additionally, after the PCOR conference, in approximately October 2022, I was an instructor at a VCAC OCE training and even discussed ApostleX. In advance of this training, I attempted to secure a meeting with then SC Jose Perez to discuss ApostleX since I was going to be at HQ for the training. I have correspondence between CACHTU supervisors/PMs, some of which include ASC Schaeffer, about my proposed meeting with SC Perez, and at no time was this "lie" ever mentioned. After ASC Schaeffer accused me of this lie, I immediately sent him proof that the allegation was false. ASC Schaeffer responded with acknowledgment that I was in fact telling the truth; however, he suspended me from the training anyway. My communications with ASC Schaeffer have been provided to INSD and additional communications are available upon request.

As I repeatedly stated, I attempted to solicit help from every appropriate entity, to include the NYFO "Security Officer", Robert Welp. However, until just weeks before the intrusion this position was only temporarily staffed, and the ISSO and CISSO positions were not staffed at all. I have provided a document to the interviewing Agents that originated from former NYFO SAC Nicholas Bouchears in which he outlines the issue of not having these positions filled and the steps he took to fill them. If these positions had been filled there is little doubt that I would have received the assistance I needed to ensure our network was secure. However, these positions were not filled, and I was nevertheless encouraged to enhance our lab by all levels of management and received the necessary approvals along the way. I should not be punished for failures in hindsight that were out of my control. While I take responsibility for all my actions, I am confident that nothing I did was without approval, and everything was done in the interest of improvement.

There is an abundance of evidence to support that everything I did was with full knowledge and support of FBI EM. I can provide much of this, but the proof consists of copious amounts of emails, numerous iterations of the PTA, and more. As a couple last anecdotes is an email between myself and (now retired) AD Mark Gerber. AD Gerber had reached out to me requesting some information regarding ApostleX back in March of 2023. In the email I mentioned to him that DAD Jose Perez had

been briefed on and supported ApsotleX, specifically this portion of the email states:

"We've briefed this up our chain any my ASAC and SAC are very much on board, as is our ADIC from what I hear.

I've also spoken with DAD Jose Perez, who seems to also support it, as have many others along the CID chain of command. We've coordinated with several units in OTD, all of whom stated the love the program and would provide support however possible, including housing the data, helping with additional features like ELSUR, evidence, etc. I've also spoken with Ma Smith at OCIO who also seems to be a supporter, and is looking to see

who all from HQ needs to approve this before we move forward."

I know this because I personally spoke to DAD Perez about ApostleX when he visited the NYFO, which is discussed above. I also believe that AD Gerber spoke with DD Abbate and possibly Director Wray about ApostleX as well. I later learned that the General Counsel, who at the time was Jason Jones, was also aware of ApostleX and did not have any legal concerns, rather he withheld his approval until OCIO provided theirs.

Additionally, in September 2023, NYFO ADC Dane Christensen advised me that he heard that someone in the FBI EM circles had conflated ApostleX with having been a contributing factor in the intrusion, something that was far from the case and technically impossible, as discussed above. Ironically, the following week

or so, the case Agent assigned to investigate the intrusion reached out to me to request information on ApsotleX. The Agent, Terrence Carthy, had independently learned about AposlteX and was interested in using it for an un-related case. SA Carthy had heard that I had been the point-person for ApostleX and reached out in hopes that he could use it. I informed SA Carthy of the recent assertion that ApostleX was somehow related to the intrusion and he could not believe it. SA Carthy investigated the intrusion and knew exactly what was and what was not related, and until just before reaching out to me, SA Carthey had not even heard of ApostleX. Shortly thereafter, I sent an email for clarification to NY CDC Semos, cc'ing both ADC Christensen and SA Carthy. My email to CDC Semos stated in sum:

> "Last week Terrence Carthy (CCd) from CY-2 hit me up asking about ApostleX. He had only recently heard of it (from someone else, not me) and was interested in where it is in the process. I mentioned to him that the DD needs to approve it and that there is the misconception that ApostleX was related somehow in the intrusion. Ironically, Terrence was the case agent on Cyber for the intrusion, and was a bit surprised since he had never heard of ApostleX until recently. Terrence is happy to clear the air regarding ApostleX and it's (non) involvement in the intrusion, but I wanted to put him in touch with you both."

CDC Semos responded with the following:

"Hey Aaron,

No confusion on our end. Legal is clear on the fact the intrusion and ApostleX are 2 unrelated matters. A/[redacted], OCIO, discussed Apostle X (and maybe the intrusion, I'm not exactly clear) with the ADIC last week. The ADIC advised 2 ADs and the GC were interested in coming to NY to discuss. I think the ADIC tasked Spencer Horn with setting that up at the EM yesterday. Circle back with Spencer b/c the discussion got a little confusing at the meeting. In any event, ADIC will not approve use of Apostle X until GC and the ADs approve of it at the HQ level."

--Tara

Lastly, it should be noted that, since the intrusion, my squad mates and I have been referenced as having been "System Administrators", which we absolutely are not. The INSD report identifies me, and others on my squad, as having been System Administrators despite the fact we were not, have never been trained in system administration, and were never qualified to be system administrators. Despite myself and my chain of command bringing this to the attention of INSD we continued to be referred to in this manner. This is a critical fact since I cannot, nor can my squad mates, be held to the same standard of knowledge as an actual system administrator. The title implies a level of knowledge, and thus a level of responsibility, that I

did not and do not possess. None of us on my squad do or ever have.

In my defense I possess hundreds, if not thousands, of pages of supporting documentation. I have provided a large number of these documents to the interviewing Agents and am happy to provide more if requested. This includes, but is not limited to, the NYFO's opposition to the post-intrusion INSD findings, many of which are provable as categorically false and misleading.

I am including here many of the documents referenced in this statement and will provide INSD with additional documents. These are, however, not all the supporting material I have and can provide more upon request. As I do not know what information has been presented to INSD in support of these allegations, nor do I know exactly who provided the information, I cannot possibly anticipate every document in my defense I possess. I am an open book and will provide anything requested of me in order to reveal the truth.

I am willing to voluntarily take a polygraph examination concerning the truthfulness of the information contained in this signed, sworn statement. I have no other pertinent information regarding the aforementioned allegations. I have been advised that I should submit any additional information of which I may become aware, regarding this inquiry, to the Internal Affairs Section (IAS)/Inspection Division (INSD) or to the Office of Professional Responsibility (OPR).

01/26/2024
New York, NY

I have been given the opportunity to review this statement and make any changes prior to signing it.

I was instructed on 01/26/2024 not to discuss this matter with anyone other than the person(s) conducting this interview, representatives from IAS/INSD, Security Division - Clearance Referral Evaluations Unit, OPR, the FBI Ombudsman, and/or an FBI Employee Assistance Program (EAP) Counselor. I have been told that should I decide to discuss this matter with anyone else, I must first obtain authorization from the interviewer(s).

I have read this statement, consisting of this and 36 other pages and it is true and correct.

Aaron E. Spivack

Sworn to and subscribed before me on the 12th day of December, 2024, in New York, NY.

[redacted].

Witness:

Witness

Ivette M. Hazou