I, Aaron E. Spivack, having been duly sworn by Supervisory Special Agent (SSA) Dannie W. Price, Jr., hereby make the following statement to SSA Price and SSA Matthew A. Zavala on 01/26/2024 and SSA Price and SSA Claudia Dubravetz on 08/08/2024, 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 on both occasions, via telephone. This statement took place over a two-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 Aaron E Spivack 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 Aaron E. Spivack 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 Aaron E. Spivack 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 am currently assigned to CT-25, which is a hybrid Domestic Terrorism and Child Exploitation squad. I was assigned to CY-3 in May 2010 and officially named on the squad in July 2010. This was when Innocent Images was combined with Cyber. C-20 was the Human Trafficking (HT) squad at the time. I believe it was 2015 when Violent Crimes Against Children (VCAC) and HT were combined under 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 believe Digital Extraction Technician (DExT) training was opened to VCAC Agents in 2012. Scott Ledford was my instructor for DExT. As of 2023, I knew Ledford was a Unit Chief and led the Cyber Action Team (CAT). I believe at least three or four of us initially received DExT training, but I think all of us eventually were 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, as 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

victimization at the hands of the offenders the FBI was actively investigating. This was around the same time Agents working other violations began to see an increase in the collection and reliance of digital evidence. 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 time the gang and drug squads were seeing more digital evidence with their investigations.~~ 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 other FBI investigations since VCAC usually does a search warrant at the beginning of our investigations, where other squads do them last to complete their investigations.

Mike Osborn was a Unit Chief (UC) of the Crimes Against Children Human Trafficking Unit (CACHTU) at FBI Headquarters (HQ) and eventually an Assistant Special Agent in Charge (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 the NYFO Headquarters City (HQC). CART was located in Moonachie, New Jersey. It could take an hour to get to the CART lab. CART evidence reviews needed to take place there. 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 ~~a few~~ examiners who could handle data extractions immediately, and almost certainly none who could respond after hours or on weekends. ~~Some of them would delay them.~~

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. ~~an awful feeling that a person who violated a child could not be arrested because we did not have the proper technical capabilities.~~ 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, on-sight forensics 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 there could be a delay in reviewing evidence that, if seen sooner, would allow us to remove a child from harm's way.

NYFO SAs Linh Phung, Tommy Thompson, Mitch Thompson, and I were DExT trained. SA Cindy Wolff (aka Cindy Dye) was also DExT trained. Cindy 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 CAIR, a forensic tool for data review ~~extraction~~, 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, NJ, where CART was located, to conduct their reviews on site vs 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. ~~Additionally having to rely on CART for evidence processing, and it was faster to use the programs at CART to conduct the actual evidence review.~~

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 ~~downloads~~ 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 a digital copy of the data extraction and I think it may have been on DVD. It would have been accessible on Operational Wide ~~Local~~ Area Network (~~OpLAN~~ - OPWAN) as well. 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. All telephones we seized initially 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 ~~Black Box~~ a TD3, and later a TX-1 as well as FTK Imager, to image a ~~the~~ 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 work off the working copy.

I am pretty sure the derivative evidence was cataloged and placed in the Evidence Control Room (ECR) 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. Once we ran out of hard drives for derivative evidence, we were instructed to use the RAIDs. I believe these instructions were provided by HQ, either our Program Manager (PM), the DExT PM, or both. ~~I was told by a squadmate or a supervisor to image the data to a Redundant Array of Independent Disks (RAID) tower.~~

Typically, the person running a Group I or Group II Undercover Operation (UCO) and the squad SSA would be the people who communicated with HQ for resources. I recall in 2015, I sent an email to ~~my~~ SA Thomas Thompson, who was the case agent of our squad's Group II, asking for some large capacity ~~two to three terabyte~~ hard drives with our remaining Group II funds. At the time we were still merged with Cyber. When we moved to the Criminal Division, our funds were wiped out.

Linh Phung left NYFO and became a DExT PM. She would complain about a lack of funding. 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. 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 purchasing from New Egg, like I was instructed to do by HQ, specifically SSA Heath Graves who was the DExT PM, who 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 ~~for purchases~~. I went to CART who gave us what hard drives they could spare. 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, which included 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 ~~was~~ 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. After the Inspection that was related to the C-20 computer lab cyber intrusion, the squad received some hard drives, and then was denied funds for hard drives from CACHTU who told us to go to CART. CART then referred us back to CACHTU.

I worked with someone from the Laboratory Division to help figure out another process. I believed it was a waste of money

and resources to purchase expensive hard drives just to get destroyed. I spoke with a UC about creating reusable virtual derivative storage that was stand alone. The UC liked the suggestion.

In 2018 I did a five-week TDY at CACHTU. My former SSA, Sean Watson, was the UC there. My job was to call every VCAC ~~agent working~~ 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. ~~that big offices were doing a lot of DExT stuff, but that smaller offices were not, and generally that there was a lack of training, guidance, direction, and personnel within the program.~~ I drafted a summary on the calls I made and created a section for complaints from the field in reference to DExT, and provided my assessment to CACHTU leadership. 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 and training needs, and provided my assessment both orally and in several documents.

In 2018 I sent an email to SSA Michael Deizlak and SSA Matthew Chicantek, who were PMs at CACHTU, as well as to UC Sean Watson of CACHTU. In addition to the write-up I sent after my TDY, I sent 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. ~~If we had hard drives to create derivative copies, we would place a copy in evidence. If we didn't, we wouldn't.~~

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 ~~we would have to go~~ in front of the Criminal Undercover Operations Review Committee (CUROC), because ours was now ~~it is~~ a Group I, it ~~would~~ also had to be presented up through CACHTU and approved by ~~to~~ the Assistant Director (AD). During the CUROC, 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.

The practice of creating derivative evidence copies onto separate hard drives to be checked into evidence was dependent upon whether or not we were provided funds to purchase the drives or the drives themselves. 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. ~~I'm not sure when the standard practice for C-20 members changed to not adding derivative copies to evidence, but it happened.~~ 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.

Until approximately February 2023, the NYFO did not have a designated Information System Security Officer (ISSO). This is a required position, and I think it being left unfilled exacerbated many of the problems that are discussed herein.

As recently as December 2023, my squad has attempted to get funds for derivative hard drives. On a couple of occasions the funds were obligated, however in other requests the funds were not. In those requests CACHTU stated, via email, that there were no longer funds for the drives and that the squad should inquire with CART to obtain them. Subsequently, CART denied the request as they too needed their hard drives. Even after the intrusion and the negative attention we received regarding derivative evidence hard drives, the squad was again put in a position where they were unable to comply with policy because the FBI would not provide the requisite hard drives or funding needed to be compliant. When the squad had been able in some instances to

use case funds to make a hard drive purchase, the newly-appointed ISSO found the drives to be in violation of policy since the hard drives themselves 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.

The situation was in essence entrapment. We were being required by policy to create derivative evidence, but we were not being provided 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. ~~When we had funds to get hard drives, it was denied by security because they were not made in the USA~~

After the process changed, we would image the original evidence onto the RAID Storage or Network Attached Storage (NAS). 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.

I ~~was~~ personally made derivative copies whenever I was afforded with the requisite hard drives. However, just because I did not always receive the drives did not mean my VCAC investigations ceased. Of course, I as well as others, still had to adapt and overcome and felt that while I may not have been able to create derivative copies for all of the evidence, the reasons for that were well documented and out of my control. Had we, or I, decided not to work cases due to the lack of derivative evidence hard drives or funding for them, I 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 quite literally 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 I did.

At no point in time have I ever 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 the word is not exclusive to "original" or "derivative". For example, when I review subpoena returns, it is quite possibly "evidence" that I am reviewing. Or 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. ~~not making derivative copies and did not have the resources to do so and I did not know what else to do.~~

Throughout most of its existence the C-20 lab was Internet connected. One or two of the DExT machines were connected to the Internet, but we were "stand-alone" and not connected to any FBI systems. Additionally, our lab was "missattributed" and able to be used in covert capacities and to access websites that could contain Child Sexual Abuse Material (CSAM). ~~I recalled being instructed that the DExT work station was stand alone.~~ 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, and as far as I have always been aware that is the only policy on the matter as well. 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, 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. ~~In 2012 it was. We then began receiving programs that needed internet access~~.

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. ~~The C-20 lab was piloting a cloud based Axiom licensing~~. It allowed us to check out a license when we needed to. In order 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, 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 and CART and received some help. I do not know anything about networking and how to set up networks. The Computer Scientists also did not know. I believe someone from the Operational Technology Division (OTD) told me to Google it. Networking is not a DExT function and is not in my skill set, so I did not even know what questions to ask. 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 Computer Scientists, OTD, the Office of the Chief Information Officer (OCIO), Management Information Systems (MIS), etc. - however, all were of no help.

Computer Scientist 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. Anthony Broderick who is the NYFO CART networking guy was asked for help. He told me to read the manuals and said he did not have

Commented [DW1]: Should I put something in about how the Inspection report - of which the charges are likely derived from - refer to me as a system administrator. I want to point that out as I am NOT. I cannot be viewed from the same lens as someone who is a sysadmin
D W
2024-09-16 21:33:00

Commented [JR2R1]: Yes! I'm glad you remembered that. Please add.
Jim Roberson
2024-09-17 10:41:00

the bandwidth to support us. These communications, along with many others, occurred in writing via email and I can provide them to investigators.

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 this was an issue affecting so many other FBI Offices that it encouraged us to find the solution so that it could be emulated across the other VCAC DExT labs.

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. I also reached out to OTD, and Counterterrorism Division (CTD) Cyber looked at our network and could not figure it out. We had a Counterterrorism (CT) CHS come

over and look at the network and he/she advised networking was not his/her specialty. The CHS was a former contractor for the FBI and had a TS clearance. This occurred when the lab was on the 9th floor prior to it getting flooded.

After the 9th floor lab flooded, 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.

CACHTU PM Leslie Adamczyk was a former NYFO Agent and knew about these issues.

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. ~~AXIOM gave everyone limited access to work from home.~~ However, since the bulk of my forensic reviews meant

reviewing CSAM, I came into the office almost ~~I was in the office in the lab~~ 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 ~~gmail~~ 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.

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 include 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 review. 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 ~~all~~ working copies. ~~If I did take data home, it would have been a working copy.~~ It would have been impossible for me to take derivative copies home in general.

I was coming in every day to do my CSAM reviews. ~~I would log into telegram with my misattributed laptop. I was taking my Online Covert Employee (OCE) devices home to conduct work and my SSA and ASAC knew about it. Agents believed they were authorized to do it. We now have EC authority. Those Devices may have contained CSAM work.~~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.

As I was authorized to do, 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 phone and my FBI-issued and encrypted laptop, may have had CSAM on them. As an OCE, I was authorized to do this since communicating as an OCE with VCAC offenders requires around-the-clock communication. This is all also covered under our Group I authority.

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 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 ECU and a copy would have been on the C-20 lab server.

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

~~NCMEC will not accept it any other way~~. 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 ~~while~~ 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. 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 precede, 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, 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, and the next process would also take a day or so, I did not want 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 into the server and tell the computer to move to the next step of the process.

Our use of remote computing was reinforced ~~I came by this idea~~ a few years ago when I attended training provided by the International Association of Computer Investigative Specialists (IACIS) ~~Science~~ during which we went through basic computer forensics. I heard about law enforcement use of Remote Desktop Protocol (RDP). I believe RDP was being used in the Bureau but I am not sure what for purposes 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.

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 ~~I did not know~~ 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. ~~later found out I was a step or two from making it super secure but did not know what I was doing.~~ 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. The RDP would have allowed me to see the crash and

restart the process remotely. ~~I had the idea of teleworking in during COVID.~~

I believe enabling remote access to the C-20 computer lab was a good initiative, but it was not executed properly. ~~lacked the proper execution skills~~. ~~However,~~ 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. ~~bad judgment~~. 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 ~~good~~. 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.

I attempted to set the RDP up in either the Fall/Winter of 2022 or early 2023 ~~December 2022 or January 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 FBI to 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 it was 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 Computer Scientists 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 tried to figure out Python and Github and I talked to people on how to write script~~. 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. ~~They can be used to ensure that a download file is legitimate~~. 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 ~~it was my fault for turning on the RDP sights.~~ 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. 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 Executive Management of in an email that I provided to the interviewing Agents.

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

I believe that if I did not have the initiative, we would not have had our successes. 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 better the Bureau. I did not know how to do everything right, but I always did the right thing and ~~but~~ 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

Commented [JR3]: Excellent!
Jim Roberson
2024-09-17 10:50:00

Commented [CT4R3]: I modified this a little. Want to chat with you about it later.
C20 TechTeam
2024-09-18 11:13:00

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 ~~given a~~ "gold" ~~rating~~ ,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.

After the intrusion we were directed to completely stand our lab down. We were directed to submit all of 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. By comparison, after the intrusion our squad suffered a 95.52% reduction is 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 an instance in which, because of the lag time at CART and the amount of time it took to image and process devices, an offender who was a citizen of another country managed to flea the United States before the 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.

I briefly mentioned ApostleX earlier in my statement. It is both the name of a company and their product. I had no previous relationship with the company. ApostleX came to the FBI. 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 showed up late and left early. The portion I did sit in on talked about how ApostleX helped with their CHS's 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 not good methods to capture the information. We voiced concerns about this for years, but there was no fix. 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 that. 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 ~~once the UC saw the app or image, it was gone. If~~ if an OCE attempts to ~~you~~ 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.

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 ~~lead~~ 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. I believe the ApostleX company pitched OTD and other ADs. At one point I even had Executive Assistant Directors (EAD) reach out to me personally about ApostleX.

On 11/08/2021, ApostleX requested I sign a nondisclosure agreement. I reached out to NYFO Chief Division Counsel (CDC) Tara Semos and we may have also spoken with an Assistant 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 it could be developed. I ~~believe~~ know there are currently ~~were~~ a number of programs that are used today in the FBI that were made through Agent input, and some that were created entirely by Agents themselves. 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

~~we~~ 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 routinely encounter 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.

Nothing I or my squad did 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 Assistant Director in Charge (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 were going through the Privacy Threshold Analysis (PTA) steps to get the Bureau to sign a contract. We also never orally or verbally agreed to a contract. 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 the technology does not exist to do it. I saw 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. We saw ApostleX as an opportunity to address ~~our past~~ this and other concerns, follow policy, and follow the law. ~~I believed certain methods to preserve were~~ 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 were 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 were working on Signal and a few others. ~~The~~ ApostleX ~~program~~ 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 ~~nudge them~~. 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 ~~did not give~~ 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 not attached to any FBI networks, covert networks, or storage containers. 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 Computer Scientist (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. 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 it did not matter as the computers were for covert use anyway.

ApostleX ran ~~runs~~ 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 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 not over collect.

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, but they could see the telemetry coding. I believe OCIO looked at that and were 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. ~~dealing with that.~~

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 of the accounts we used were real covert accounts. Some of the accounts were historical ~~information attached to them that were exposed to ApostleX~~. 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. I do not believe having information on the ApostleX computer was any different than having it on any other 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 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 ~~don't believe~~ the accounts we were using had no impact on ~~would have~~

~~compromised~~ 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.

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 days 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 ~~text~~ document with instructions on how to fix the issues. Any message that was sent from the company was done through Bureau email. The instructions ~~It~~ would be ~~a text document,~~ 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. ~~I used a mixture of personal and Bureau devices to receive the instructions and communicate with the ApostleX company. At times~~

~~I used my personal telephone to conduct telephone calls or video chats with the ApostleX engineers while I was in FBI space. I predominately used Bureau equipment.~~ Sometimes the ApostleX engineer could see me during our Zoom calls and sometimes not. 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 do not 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 a FBI employee who could read the coding to review what was being sent to me. (This is sounding way off-base, as if ApostleX was up to no good. We need to clarify some of this - I think this should be removed)~~ There were a couple of times I had "tech people", SA Robert Depresco, ~~and~~ 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 for other people to look it. ~~I did not have someone reviewing everything they sent me.~~ 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

Commented [JR5]: I'm not sure how to incorporate this information into the sentence, Aaron.
Jim Roberson
2024-09-16 10:12:00

Commented [CT6R5]: I'm not sure either. I was in FBI space when speaking with them, but so what?
C20 TechTeam
2024-09-17 06:37:00

Commented [JR7R5]: OK. Just delete it, then?
Jim Roberson
2024-09-17 10:54:00

Commented [JR8]: OK. Fix it and remove whatever is misleading or incorrect.
Jim Roberson
2024-09-16 10:15:00

Commented [CT9R8]: Can we just delete it?
C20 TechTeam
2024-09-17 08:59:00

Commented [JR10R8]: Yep. Delete it. If INSD makes an issue of it we can talk it out with them.
Jim Roberson
2024-09-17 10:55:00

made the deliberate decision not to let the ApostleX company remote access into the standalone ApostleX computer. During this process, I felt like the ApostleX company was a verified entity and I was working with someone the Bureau invited in.

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. ~~Only~~ My squad SSA, branch ASAC, ~~and NYFO~~ 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 the Office of General Counsel (OGC), the General Counsel himself, the Procurement Office, several Special Agents in Charge (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 also involved but not at this 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. ~~My~~

~~supervisor did not know everything that was involved~~ 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 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 ~~fucking~~ 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. ~~They said it was not going to be funded and I did not believe CACHTU would fund it until there was a working product.~~

As I mentioned previously, in April or May 2022, I went to an IACIS conference and the ApostleX program was working. Leslie Adamczck, who was a former squad mate and a VCAC PM, was also in attendance. I told her about the product. She said it needed to be briefed at the Program Coordinators (PCOR) conference. 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 were in charge of the conference, and I was added to the agenda. I worked on a presentation and showed it to SSA Adamczck. She loved it. SSA

Commented [JR11]: OK. Remove it.
Jim Roberson
2024-09-16 11:14:00

Adamczck 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. SSA Clarke was present during my presentation.

The PCOR conference presentation went well. There were numerous ~~a hand full of~~ 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). ~~The~~ 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 that 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 of 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. At some point early on there may have been ~~was~~ 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 ASAC Horn came in. The SAC was eventually briefed.

A few days after the VCAC PCOR conference I heard from Joanna Pasquarelli who is a General Attorney (GA) for OGC. GA Pasquarelli attended the VCAC PCOR conference and saw my presentation. GA 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. 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. I spoke with CDC Semos about my conversation with GA Pasquarelli. I was sent a "pony" of the PTA which I filled ~~it~~ out and returned. GA Pasquarelli was very pleased with what I turned in. There were a lot of email communications and Microsoft Teams calls. We had to do some comparisons to see if there were other companies who offered products similar to ApostleX.

I had spoken with OTD about the issues ~~with~~ 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 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 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 worked through an emergency in which 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. 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. 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 ApostleX was going to be shut down due to the belief it was involved in the intrusion. This was completely untrue, of course. ApostleX had nothing 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 Michael Driscoll. 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 SAC Brodack 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 Counterterrorism (CT) Division SAC Robert Cassane in August 2023. CDC Semos, ASAC Horn, 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 noticed of this INSD internal investigation.

I was working with the International Terrorism Operations Section (ITOS) and some high-tech unit. They were asking for information to push up to EAD Larissa Napp, 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 the egg situation. We did not know

Commented [JR12]: Can you identify this unit by name?
Jim Roberson
2024-09-16 12:41:00

Commented [CT13R12]: Ill try to find their name - there were a couple units that worked on the development of tech - some in CT some in Crim, maybe one in OTD
C20 TechTeam
2024-09-17 09:15:00

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. ASAC Horn 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. ~~who had a did not agree with ASAC Horn's assessment~~. 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. Noone ever told me of the requirement for an ATO for the C-20 lab. It came up after ASAC Horn and CDC Semos had their discussions.

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 ~~listed~~ referenced as the reason for a lower program rating for fiscal year 2023. CACHTU initially rated our squad "gold", the highest rating, but Deputy Director 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 is categorically false. My ASAC attempted to fight this false narrative but was told it could not be changed.

I never understood ~~understand~~ 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. As I have mentioned, 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

Commented [JR14]: Are you talking about the NYFO Chief Security Officer, or CSO, here? If so use his/her title.
Jim Roberson
2024-09-17 11:03:00

Commented [CT15R14]: I don't know that he even had a proper title. He was filling a vacancy
C20 TechTeam
2024-09-18 15:04:00

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 of my actions, I am confident that nothing I did was without approval and everything was done in the interest of improvement.

Under no circumstances whatsoever did exceed my authority by contracting an outside company. There was no contact. 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.

Lastly, it should be noted that, since the intrusion, my squadmates 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.

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.

I am willing and eager 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).

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.

Commented [CT16]: I provided far more than 36 pages - if he is referring to my attachments then this number is far off
C20 TechTeam
2024-09-17 11:00:00

Commented [JR17R16]: I think this is only referring to the number of pages of the actual statement itself. Not the attachments. You can fix it. The statement is a lot longer now than it was originally due to all of our edits.
Jim Roberson
2024-09-17 11:11:00

_____

Aaron E. Spivack

Sworn to and subscribed before me on the Xnd day of September, 2024, in New York, NY.

_____

Dannie W. Price, Jr.

Witness:

_____

Witness