The following is from an audio recording and in some cases, it may be incomplete, or inaccurate due to inaudible passages, or other transcription errors. Nothing from this show or any others would be construed as legal advice. Please consult an attorney for any legal issue. Nothing from this show is endorsed by the Federal Government, Air Force, or any of its components. All content and opinions are those of our guests and host. The inclusion of hyperlinks and references does not imply any endorsement by the author(s), by the Federal Government, Air Force, or any of its components. They are meant to provide an additional perspective or as a supplementary resource. The Department of the Air Force or any other department or agency of the United States Government does not exercise any responsibility or oversight of the content at the link destination.

AFJAGS Podcast: Episode 52

2021 Military Justice Update with Major Ryan Brunson and Major Jessica Delaney







Major Ryan Brunson, USAF

Major Jessica Delaney, USAF

HOST: MAJOR ERIN DAVIS

GUESTS: MAJOR RYAN BRUNSON AND MAJOR JESSICA DELANEY

In this special edition of the podcast, Major Ryan Brunson and Major Jessica Delaney educate explain some of the recent, pertinent changes to military justice and how those changes impact legal offices and practitioners.

MAJOR ERIN DAVIS:

Hello and welcome to a special edition of The Air Force Judge Advocate General's School's Podcast. I'm Major Erin Davis. Today, we're excited to be teaming up with our friends in the Military Justice Domain to bring you this update on some of the most important recent changes impacting the military justice realm. Recently, Major Jessica Delaney and Major Ryan Brunson sat down to discuss these developments and educate the corps.

So, this episode will feature their conversation with each other, where they break down these developments and share with us not just some of the actual changes in law or rules, but how those impact JAGs in the courtroom and how JAGs can use this information to better serve their clients. If you are an Air Force JAG listening to this for your annual certification, please stay tuned to the end of the episode for instructions on how to certify.

[upbeat intro music]

Here are a few clips from today's episode.

SHOW EXCERPTS

MAJOR RYAN BRUNSON:

What's important to know is that CIP capability is not statutorily required like the SVIP capability. The CIP is just sort of an expanded, collaborative approach that the Air Force has decided to take. So, you won't necessarily find an equivalent in the other services [fades out].

MAJOR JESSICA DELANEY:

And one of the ways some bases do that, which is very helpful to our Director of Trial Operations, is sending SIRs up along with the request. So that way the Directors of Operations are able to see, is this a special needs case as opposed to just receiving a notification that some sort of a 120 is going on the base [fades out].

MAJOR BRUNSON:

... via a memorandum from the trial counsel to the Central Docketing office that requests that a military judge be detailed for the purposes of a 30a [fades out].

MAJOR DELANEY:

We need a way just to tie our military subject to that signal. So, the basic subscriber information via an investigative subpoena will help us make that initial link between the pseudonym on the Kik or Facebook Messenger, whatever he's using and the individual subject.

PODCAST

MAJOR DELANEY:

Good morning. Welcome to the 2021 Military Justice Annual Refresher. I'm Major Jessica Delaney from AF/JAJG and I'm joined by Major Brunson from the AF/JAJM. Today we're going to be talking with you about CIP, which is the criminal investigation and prosecution capability; SVIP, the special victims' investigation prosecution capability; and investigative processes. But before we dive into it, Major Brunson, do you mind introducing yourself to everyone?

MAJOR BRUNSON:

Sure. Good morning. Major Ryan Brunson from the Department of the Air Force JAJM, Military Justice Law and Policy Division, and I'm the Chief of Military Justice Policy there. Prior to this assignment, I did an LL.M. in military law with an emphasis in criminal justice from the Army JAG School and Legal Center in Charlottesville, Virginia. Prior to that, I was a circuit trial counsel in the central court a couple of years, and an area defense counsel before that.

MAJOR DELANEY:

I also started in base legal like Major Brunson. Did a tour as area defense counsel before working as the executive officer for the Air Force Judiciary and Appellate Government Counsel for three years. In my current capacity, I'm one of the CTC-SVUs, one of the Special Victims' Unit's CTCs, as well as the Assistant Director of Operations in charge of the CIP program.

So, as we get started, let's start with sort of where this collaborative approach to investigations first began, which was with SVIP. Major Brunson, where did that come from?

MAJOR BRUNSON:

Sure. So originally the SVIP capability was a Congressionally mandated requirement from the 2013 NDAA. And it first appeared in the Air Force Instruction AFI 51-201 as early as 2015. And since then, the program has only gotten more enhanced and robust. And now you can find the current guidance for the SVIP capability in Chapter 22 of DAFI 51-201.

MAJOR DELANEY:

And sort of the goal of SVIP is to ensure collaboration between all of the partners in our Special Victims investigations. So, our military criminal investigating officers or MCIOs, which is going to be OSI for most SVIP cases, as well as the base legal office, senior prosecutors, VWAP personnel. And then ensuring that there's coordination with the SAPR program, SVCs, domestic abuse victim advocates or victim advocates. But those

are sort of all the partners who are the actual required members on an SVIP team.

MAJOR BRUNSON:

Right. So, if you look at again that chapter 22 of DAFI 51-201, you're going to, you're going to find that the four required members of a SVIP team are, and these are folks that have to have special qualifications and enhanced training, but that's going to be your investigator from the Air Force Office of Special Investigations, a judge advocate who's qualified and certified, and then a circuit trial counsel who is SVU qualified and also a seven level paralegal.

MAJOR DELANEY:

So that's our SVIP team. And SVIP now in the Air Force actually falls within a more broad capability, so a more broad collaborative team. And that's what I referred to earlier as the criminal investigations and prosecution capability, CIP. So Major Brunson, where can people find out about the CIP capability?

MAJOR BRUNSON:

Sure. So, if you want to look at the actual requirements for the CIP capability, that's also going to be found in chapter 22, or section 22 of AFI 51-201. And that details the sort of expanded CIP capability. What's important to know is that the CIP capability is not statutorily required like the SVIP capability. The CIP is just sort of an expanded collaborative approach that the Air Force has decided to take. So, you won't necessarily find an equivalent in the other services. And the thing about CIP is that it's just across the board. So, it's going to apply to all of your criminal investigations and prosecutions.

MAJOR DELANEY:

So Major Brunson, who are the personnel involved on the CIP team?

MAJOR BRUNSON:

Right. So, your CIP team is sort of easy to remember because it's just going to be sort of a scaled down version, with fewer requirements for your SVIP team. So same folks. Just not necessarily the same level of training or enhanced capabilities there.

So, your CIP is going to be composed of a base level trial counsel, whether or not that person's qualified and certified; a base level paralegal, who does not have to be at any certain level, five or seven level, it's just any paralegal at the base level; a circuit trial counsel, who does not have to be yet SVU qualified; and then of course, your OSI, or SFOI investigator who's actually assigned to that case.

MAJOR DELANEY:

Now, some CIP cases can also involve victims or a large number of witnesses. So every CIP team is not going to use VWAP personnel. Right? So if it's a naked urinalysis or a drug case, you may not need VWAP personnel involved. But if the CIP investigation does include any victims or witness, you'll also have your VWAP personnel.

MAJOR BRUNSON:

Sure.

MAJOR DELANEY:

Now, we've talked about the different personnel required for SVIP and CIP. What sort of offenses require the SVIP capability?

MAJOR BRUNSON:

Right. So, the SVIP capability according to the regulations, and again, refer to section 22 of the DAFI 51-201. But that's going to involve intuitively what you would think it would involve. So, your sex assault cases, your domestic violence cases, your aggravated assault cases, and then even cases that are serious that are not necessarily listed in regulation and murder comes to mind. Murder is not actually part of what's required to have a SVIP team assigned, but you're normally going to do it for that kind of case.

MAJOR DELANEY:

Right. So as Major Brunson pointed out, special victims, the SVIP capability can be used in any case that uses a

victim. It is, however, required in three specific scenarios. So, adult sexual assault; child abuse that involves child sex assault, or aggravated assault; and domestic violence, aggravated assault or sexual assault cases.

So, there could be some aggravated assault cases that do not require the SVIP capability, but in which you're certainly able to utilize that capability. So, when do these teams first become capable? What triggers the capability?

MAJOR BRUNSON:

Sure. So, there are essentially three events that can trigger the requirements to compose that CIP or SVIP team. And that's going to be when your military law enforcement agency gets a report of an offense. So, a reported offense comes to SFOI or OSI that's going to trigger that requirement.

The second can be if a non-military law enforcement agency gets a report of a crime and then transfers the investigation from the civilian authority to the military authority. And then third would be a situation where the Air Force request and obtains jurisdiction over a case that's already in progress.

MAJOR DELANEY:

So, we sort of talked about how this capability came to be, and how the teams are composed. But let's actually talk about what it is that team does during the investigation and potentially during the prosecution of an offense.

So Major Brunson, we talked about it being a collaborative intent, but really what is the intent of the CIP team or SVIP team?

MAJOR BRUNSON:

Sure. So, it's sort of what the name suggests, right. So, a combined investigation and prosecution capability is ... the ultimate goal is to sort of create a synergy of our military law enforcement capabilities and our military legal capabilities. And the goal is to produce better

investigations on the front end and better prosecutions on the back end.

And sort of the idea there is that if we can, if we can integrate legal into investigations on the front end, and that's an initiative that the Air Force has been, has been encouraging for several years now. And if we can do that, then we're going to sort of eliminate some of the evidentiary problems that we see down the road in trials. We're going to produce better witness and victim interviews.

And then the, soft of the second part of that, is that the investigators will stay engaged in the cases after that ROI is produced and after the case goes to legal and to the commanders for disposition, right. And so, the idea is just to create the sort of synergy between legal and between investigators to have a better overall product.

MAJOR DELANEY:

Right. So, it's sort of like during the investigative process, the JAGs are supporting our investigators. And then once the report investigation is published, the investigators support us in the final disposition of the offense, whether it's a prosecution or whether the investigation reveals that there should be no disposition taken.

MAJOR BRUNSON:

All right, Major Delaney, let me ask you this. So, what is our, what are the things that, practically speaking, your trial counsel or your circuit trial counsel are going to be able to do as part of a CIP or SVIP capability to assist law enforcement on the front end of those investigations?

MAJOR DELANEY:

So, there's a lot of legal processes that actually are involved in investigations, quasi-judicial processes and legal advice. So by keeping this cohesive team from the beginning, we're able to provide quick advice on search authorizations, assist with subject interview plans, and hopefully be present for those subject interviews to provide advice, assist in formulation of an investigative plan and interviewing witnesses, and then the additional

legal processes of granting immunity for witnesses in cases that those witnesses need an immunity or obtaining investigative subpoenas or court orders to help OSI obtain the evidence that they need as part of their investigation.

MAJOR BRUNSON:

All right. And I remember just when I was in a base legal office and assisting OSI maybe by going and watching interviews of either the subject or the victim, is that something that's still part of, you know, I guess do to be part of helping out with the investigation? Or is it, you know, should we be going beyond that?

MAJOR DELANEY:

No, I mean, that's absolutely something we should be doing. You mentioned going beyond. I think that's what's important is we used to have this structure where the investigators would have their investigative plan and we would have our proof analyses. And these were two separate things. And really, what's CIP and SVIP are aimed at, is allowing the integration of that. So for us to advise on the investigative plan to ensure that we're not only discovering evidence of elements, but also assessing whether there's legal defenses, which might not be part of a traditional investigative plan.

So, it's really looking at this wholesale investigation with a gear toward the potential of going to a court-martial and taking that investigation into the courtroom.

MAJOR BRUNSON:

And I've talked about chapter 22 of DAFI 51-201 and the requirements that it creates for JAGs specifically. But what about OSI and SFOI? I mean, what if someone out there is watching this and saying, well, all this sounds really nice, but, you know, maybe we don't have an awesome relationship with our OSI or SFOI And maybe we're not sure about how willing that they're going to be to, you know, to sort of engage enthusiastically in this initiative.

MAJOR DELANEY:

Major Brunson makes a great point, which is that communication collaboration are a team effort. And we recognize that sometimes that's a struggle. What's fantastic about CIP is this is not something that is just in the 51 series AFIs.

So, this past spring, there was actually an agreement between JAJ, Commander of OSI, and Commander of SFS to support this CIP capability, and that included a commitment from us to work better with our investigative agencies during the investigation itself. And we'll discuss what's called cumulative case review in a moment, but it also commits them to support following the investigation.

So, in every case, your MCIO is going to be critical after the investigation concludes. They maintain the case files. They maintain all real and physical evidence. They assist with discovery and providing discovery to defense counsel. And then, of course, they produce evidence and testify at courts-martial. This agreement also commits them to helping us with any pretrial investigation.

Now the goal is to limit the amount of pretrial investigation. Now both of these capabilities are meant to be flexible, they're meant to be something that's workable for every base legal office. So, a lot of base legal offices have standing CIP teams.

So, for instance, the Chief of Military Justice and the NCOIC of military justice may be permanently appointed to a CIP team. And no matter what offense comes in, those are going to be the two people involved.

And then, of course, the investigator, the case agent will change case-by-case. And the CTC may or may not change case-by-case, with the exception, obviously, that if the chief of justice or whoever else is on that permanent CIP team are not SVIP qualified, there will have to be some accommodations for SVIP cases.

MAJOR BRUNSON:

Major Delaney, in addition to the folks who are required to be part of the SVIP team, are there other personnel who SVIP teams should consult with when necessary and who might those folks be?

MAJOR DELANEY:

So, in addition to the actual team for SVIP cases, they're going to be consulting with the Special Victims' Counsel, if one has been appointed, defense counsel, the SARC, if it's a case involving sexual assault, a domestic abuse victim advocate, if it's a case involving domestic abuse, and other victim advocates, if there's a victim advocate involved in the case.

MAJOR BRUNSON:

Okay. And could you give us an example of a time that an SVIP team might need to consult with a defense counsel? Maybe that's not necessarily intuitive to some of our practitioners why SVIP would want to consult with defense counsel.

MAJOR DELANEY:

So, off the top of my head, I can sort of think of two primary reasons. So, one would be if there's a case involving immunization of other witnesses, presumably those other witnesses have committed some sort of crime or could be implicated in a crime. They might have defense counsel. So, it's not just defense counsel in your case. It could be other defense counsel.

I think what it's really talking about in the regulation that was talking about the defense counsel who represents the subject of the offense that trigger SVIP. And that's where it's sort of counterintuitive. But when you think about it, the subject these offenses is often a fountain of information as well. He or she also knows a lot about the offense.

And there's definitely cases where the subject of the investigation wants to present evidence to investigators. And the way the SVIP team is going to do that, once they're represented, is through consultation with

defense counsel. So, whether that's getting a subject in for an interview after invocation of rights, whether it's consenting to searches or actually providing evidence himself.

MAJOR BRUNSON:

And might there be a time when you're talking about the actual disposition of an offense when the SVIP team would consult with the defense counsel?

MAJOR DELANEY:

Oh, yeah, absolutely. I was sort of talking about during the investigative phase, but once we've reached disposition, obviously, if the legal office or the NAF or the GCMCA is looking at alternative dispositions, plea agreements, anything like that, they're going to be consulting with the defense counsel on those matters.

MAJOR BRUNSON:

Major Delaney, we've talked a little bit about the origins of the CIP and SVIP capabilities and the requirements for those capabilities, but as a career prosecutor, let me just ask you from sort of practical perspective, why do we want a specialized SVIP capability in the sorts of cases that we've talked about?

MAJOR DELANEY:

So, there's a few different reasons. There's practical considerations, and then there's legal considerations. So first on the practical element, there's a lot of unique psychological things to consider when dealing with intimate partner violence and also with child violence. We want to ensure that our prosecutors and our investigators and our paralegals all have the additional training to interact with that population.

Then on the legal side, of course, we have different rules of evidence that apply in these sexual cases that don't apply in other cases. So, we have Military Rule of Evidence 412, 413, 414, and the constant weighing of a victim's Article 6b rights and privacy rights against an accused's due process rights. So, there's a lot of additional considerations that come into play in SVIP

cases that aren't necessarily implicated by our other criminal offenses.

Major Brunson, what is the actual timeline for the activation of the CIP team and the steps they have to take?

MAJOR BRUNSON:

Sure. And so, the timeline is again going to be detailed in section 22 of DAFI 51-201, but in addition to that, this is part, this will be one of the slides in the presentation that corresponds to this refresher [there are no slides with this presentation]. But essentially, we've talked about the triggering event. So, within 24 hours of a triggering event, the SJA is going to appoint the base JA members.

So, that's the folks that we've talked about. Whether it's the CIP team, and that's just any trial counsel, and any paralegal; or an SVIP team that's going to have to have a qualified and certified trial counsel, and a seven-level paralegal. So those folks are appointed within 24 hours of the SJA learning of the triggering event.

And then within 24 hours from that, the SJA is going to request that CTC support. That CTC support should be provided within 72 hours. And so, once the SJA learns who the composition of the entire team is going to be, they have one duty day to actually memorialize, in writing, that entire team.

MAJOR DELANEY:

And that's actually an inspectable item, isn't it?

MAJOR BRUNSON:

It's actually, yes, it's a major inspection item.

And so, once that team is designated, then you're going to have either 48 hours or five duty days to conduct that initial case consultation. And of course, 48 hours if you're talking to SVIP, five days if you're talking a CIP case. Those consultations are going to continue weekly until AFOSI or SFOI within ten days of the publication of the report

of investigation. They'll give a ten-day notice, and that's when that cumulative case review is going to occur.

MAJOR DELANEY:

And then that cumulative case review is really a pivotal part of the collaboration. This is the point at which trial counsel should be bringing to the table their proof analysis. And then at this point, OSI and SFOI have committed to providing trial counsel with the entire case file. So, this is the point for the JAGs and the case agents to really look over and make sure every investigative lead have been followed.

And this is sort of the last point in the investigation phase for trial counsel to request additional avenues of investigation. So, this is the time to ask for additional witnesses to be interviewed, for additional evidence to be collected or tested, or any other steps.

MAJOR BRUNSON:

If those requests are not made at that cumulative case review, does that mean that SFOI or OSI doesn't have any more role in the prosecution of the case down the line?

MAJOR DELANEY:

Absolutely not. As we said, they've all agreed to provide some investigative support, even after publication of the ROI, but it is something that the JAGs should be respecting. The entire reason that we have this collaboration is for us to be working on that proof analysis along the way. So that when that ROI is published, we're able to immediately provide advice to our commanders on appropriate disposition and then to move forward efficiently and efficaciously.

MAJOR BRUNSON:

Sure. And when talking about the cumulative case review, so I've talked a lot about the requirements that are actually listed in section 22 of 201, is the cumulative case review something that our trial counsel in the field are going to find in 201?

MAJOR DELANEY:

It's not. And it's not yet in any SFOI or OSI actual policy memorandums. However, that's part of that agreement which has been signed by all of the commanders that was made in May of this year.

So, you mentioned the weekly case consultation

MAJOR BRUNSON:

Right.

MAJOR DELANEY:

Is there a specific requirement for how those consultations are conducted?

MAJOR BRUNSON:

No, actually the AFI specifically says that there's flexibility about how you can accomplish those weekly case consultations. So, for instance, we've all been operating in a very sort of modified way, even for this presentation today. And so, you can accomplish those weekly case consultations however it best works for all the parties involved. Whether that's in-person, obviously that's not going to happen a lot, because your CTC is normally not stationed there at the same base, but you can do that via phone, VTC, Zoom, just however it best works.

MAJOR DELANEY:

So, one thing I do want to add with that, because you mentioned the CTC is not often at the base. Is one of the things that we should all be thinking about when we're using our CIP and SVIP capability, is maximizing the use of the CTC when they are on base.

So, when a CTC is present for motions hearing, even if it's a different case, it's a great time to do your weekly case consultation. The same thing when they're present for Article 32s or witness interviews or anything, because I think we've all learned over the last year and a half that some things are just easier to do in-person than virtually.

So, you mentioned doing these phone call or video teleconference case consultations. Can you also do them via e-mail or text message or anything like that?

MAJOR BRUNSON:

Sure. And I should have mentioned that e-mail's another way to accomplish the weekly consultations. However, when you start to talk about communications that are written via e-mail or text message or whatever else you might have, you want to be cognizant of discovery obligations that might come along with that.

And that's where we did want to mention that just because we have these regulatory requirements where we designate these teams as CIP teams or SVIP teams. That does not change the privilege rules that are in play or the confidentiality or the discoverability of these communications. So even though investigators might be part of a "team" now, you know, our communications with them are still not necessarily protected or privileged any more than they used to be.

MAJOR DELANEY:

Yeah, that's a really great point because there is no privilege that applies to investigative agent, and we sometimes waive attorney work product. So, when I've been talking about the proof analysis, it's a great example of how that proof analysis is generally attorney work product and that privilege attaches. And we want to be bringing those to our consultations with the OSI, but we don't necessarily want to provide that proof analysis to them.

Because once it becomes part of that case file, it's likely going to be discoverable because of a waiver of privilege. And I don't want anyone out there to think this means that Major Brunson or I are saying that you shouldn't ever be putting any of these things in writing. It's just something to consider that if an OSI agent, during a consultation for instance, sends an e-mail to everyone on the team summarizing a witness' testimony, there's not a privilege that attaches to that communication.

So, if you're doing consultations via written or recorded means, just be cognizant to the fact that when that discovery request comes, you need to review those communications as well.

MAJOR BRUNSON:

Major Delaney, I would sort of suggest that what the field should be obviously most concerned with at this point is what are the current requirements for CIP and SVIP capabilities, and how to meet their obligations. But some folks might be wondering, well, how do we get from these sort of generalized requirements or the generalized mandate from Congress in the 2013 NDAA, and how did that progress over time to where we've really sort of spelled it out in the AFI.

MAJOR DELANEY:

Well, so the NDAA did not itself actually create the SVIP capability. What it did was it directed the secretaries of each military department to create an SVIP capability. So, the congressional statute outlines what needs to be included, but it left it to the services to set up. And then where we went from that, was the Secretary of Defense issued the DoDI which mirrors almost identically the language from the public law and formally directs each service secretary to create their own capability.

So, AFI 51-201 is the Air Force's implementation of that congressional mandate. So, each service is going to use different language, different terminology for the different members of the team. For instance, many of you know that while we have Special Victims' Counsel, the other branches just call them victims' counsel. So, the Army regulation implementing SVIP is going to be different than the Air Force implementation.

MAJOR BRUNSON:

Major Delaney, one thing I wanted to ask you about, because we've talked about CIP and the SVIP CTC consultations. So, if you have a CTC assigned as part of your CIP team and that case ultimately goes to court, is that CTC going to be your detailed circuit trial counsel for your court-martial?

MAJOR DELANEY:

No, not necessarily. So ideally, we want to keep the same CIP and SVIP team throughout the entire process. But as you'll notice in the AFI, every single investigation requires the CIP capability. However, we don't detail CTCs to every single court-martial. We just don't have that manpower. So, it's possible a different CTC could be detailed to the court.

MAJOR BRUNSON:

And is the same true for the SVIP cases, or in those cases is it even more of a priority to keep those CTCs on the case that goes to court-martial?

MAJOR DELANEY:

It's absolutely a bigger priority in our SVIP cases, especially the ones in which the CTC-SVU has interviewed the victim in the case and has formed a relationship, because that's really a pivotal part of the prosecution.

MAJOR BRUNSON:

And speaking of CTCs and special, or CTCs that are assigned to SVIP teams which can only be SVU CTCs, correct?

MAJOR DELANEY:

According to regulations.

MAJOR BRUNSON:

According to the regulations, right. So how does a CTC go from being a circuit trial counsel to being a special victims' unit qualified circuit trial counsel? What is that process with that, because that is also not part of 51-201, correct?

MAJOR DELANEY:

That's correct. It's not. And it's a number of factors that go into it. So SVU designation is given by the Chief of JAJG. She's the one who determines when an individual possesses the qualifications and necessary characteristics to be a CTC-SVU. And what the Chief is always looking at is additional specialized training. So,

we send all of our CTCs to different trainings, prosecuting special victims' offenses, and those sorts of things. And they're also looking at expertise demonstrated in court, and a proficiency in working with victims in offenses, and complex investigations and prosecutions generally.

MAJOR BRUNSON:

And currently, do you know how many SVU-CTCs there are?

MAJOR DELANEY:

So, out in the field we currently have ten CTC-SVUs. But that number is always being reevaluated as some of our CTCs request certification as SVUs.

MAJOR BRUNSON:

And so ideally amongst those ten current SVU-CTCs, they are consulting on all of the SVIP cases for the Air Force.

MAJOR DELANEY:

So that is, that is definitely the goal that we have and that's where it's really important for the bases to be notifying us of which cases are CIP cases and which ones are mandatory SVIP cases. And one of the ways some bases do that, which is very helpful to our Director of Trial Operations, is sending SIRs up along with the request. So that way, the Directors of Operations are able to see is this a special needs case as opposed to just receiving a notification that some sort of a 120 is going on at the base.

So, we've talked a lot about the collaborative process that's involved in the CIP and SVIP capability. And we've also spent a lot of time talking about how trial counsel can assist in obtaining evidence. I want to drill down now and talk both practically about how we do that, and then also the legal basis. So, we've mentioned investigative subpoenas. What's the legal basis for a trial counselor or JAG to obtain an investigative subpoena?

MAJOR BRUNSON:

Sure. So, from a statutory starting point, the statutory authority for the government to obtain evidence for use in a criminal prosecution is Article 46 of the UCMJ. And you've probably heard about Article 46. Essentially, every time you do a discovery request or you respond to the discovery request, you're going to see references to Article 46 and for the ability of the defense counsel to equally be able to obtain witnesses and evidence for courts-martial.

So yeah, Article 46 is ultimately that statutory authority to obtain evidence. And then within the R.C.M.s, where we get into the authorities for investigative subpoenas it's in R.C.M. 703.

MAJOR DELANEY:

So, I think we all know, and talked ad nauseam about the Military Justice Act, but how did that change and alter Article 46 and the subpoena authority of prosecutors?

MAJOR BRUNSON:

Right. So previously, pre MJA 16, one of the reasons that we're talking about this today is because even though this was all implemented on 1 Jan 2019 as we all now know, it's still relatively fresh; and so those enhanced authorities, and enhanced capabilities for prosecutors to go out and obtain evidence, even for use at sort of the investigative phase, that might be something that we're all still sort of getting used to. And it's important to kind of refresh and talk about that in a little bit more detail.

So, the way to answer your question, Major Delaney, the way that those authorities changed pre MJA 16 to post MJA 16 really has to do with being able to issue subpoenas in the investigative phase of a case rather than just post referral.

Because, if you're someone who's practiced previously and maybe you're doing a different job now or what have you might think, well, trial counsel has always been able to issue subpoenas and that, to some extent, that's true. But you're thinking probably of post referral trial counsel subpoenas where you were able to get certain limited information, like from an electronic communications provider, you might be able to get basic subscriber info through those post referral investigative subpoenas.

Well now, post MJA 16, what you're able to do is get that same sort of information, just earlier on in the case. And that's what the changes to Article 46 of the UCMJ and R.C.M. 703 allow for.

MAJOR DELANEY:

And this is where we need to be proactive with our investigators too, because they're also used to the old forms of obtaining evidence. So, there are still investigators who are reaching out to DoD IG to obtain subpoena authority.

And that's going to be a way more arduous process, than for trial counsel to obtain a subpoena from someone who's been working the case. Now, trial counsel can't just get out the form sign it though. There are some additional steps that need to happen before trial counsel can issue a subpoena. So, what does trial counsel have to do before they can issue a subpoena?

MAJOR BRUNSON:

Right. Well, first of all, you need to think about what kind of evidence you're trying to get, because that's going to determine whether that trial counsel investigative subpoena is going to be sufficient or whether you might have to go beyond that, and we'll talk more about some more protected electronic evidence here momentarily.

But as an initial matter, trial counsel needs to realize that you don't have that authority inherently. So that authority has to be essentially given to a trial counsel from the General Court-Martial Convening Authority. Or the General Court-Martial Convening Authority can delegate that to the Special Court-Martial Convening Authority. But in any event, that's an authorization that has to be granted to the trial counsel. It's not a, it's not an authority that the trial counsel has inherently under the rules.

MAJOR DELANEY:

Right. And the rules actually state that the General Court-Martial Convening Authority cannot delegate the authority to trial counsel. So Major Brunson mentioned that you can delegate that to Special Court-Martial Convening Authority. And that's certainly a way to alleviate some of the routing in these cases.

So, if the GCMCA delegates its authority to authorize subpoenas to a installation commander, for instance, it just gets rid of a level of routing and makes us able to obtain that evidence a little bit faster and easier. So, it's something for all of our SJAs to consider in whether they're, the commanders that they're advising, want to delegate that authority, or want to receive that authority, if they are advising a lower-level commander.

MAJOR BRUNSON:

Sure. And frankly speaking, that as you said, Major Delaney, that just makes all the difference in whether or not that package is going up to a wing commander or a NAF commander for all practical purposes.

MAJOR DELANEY:

Now, investigative subpoenas can only cover certain things, right? So, subpoena power does not give the authority to require a witness to do an interview. All you can do is subpoena a witness for appearance at a deposition or at an actual court proceeding.

So, this doesn't make it any easier for people to conduct interviews with civilian witnesses. Investigative subpoenas are also great for obtaining pieces of real evidence. So physical property.

But a lot of things that we want to subpoen have additional privacy protections attached to them. So, you mentioned electronic communications. Are there any sort of broad categories of information that can't be reached by subpoena?

MAJOR BRUNSON:

Sure. So, when you're talking about electronic communications, and that's where we're going to spend the bulk of this part of the presentation.

So, electronic communications have additional privacy protections depending on whether or not we're talking about content, non-content, or basic subscriber info. And so, what you need to remember is that for trial counsel investigative subpoena, the only category of information that you're going to be able to get from an electronic communications service is that basic subscriber info.

And so, what do we mean by that? Well. Suppose you have an eBay account. Basic subscriber info is just going to be all of the information that you put into the different data fields when you were signing up for that account.

So, for me, for instance, it would say name Ryan Brunson, username, and then it would have a date of birth or e-mail address or physical address that's linked to my account.

But we're not talking about messages that I might have sent or received, or the even the transaction logs of every time I got onto the eBay account or what I may have bought and sold from other users. That's going to be beyond the scope of basic subscriber info.

And so, you're going to have to consider other means and tools of getting that information. That's going to involve additional process beyond just a trial counsel getting that authority from the GCMCA to issue a subpoena.

MAJOR DELANEY:

So, let's talk a little bit about electronic communications, because there are sort of two ways that we can get electronic communications. One is to get a search authorization or search warrant, obtain a subject's phone and then search that phone. But of course, there's cases where that's not within our ability either, because the actual device has been destroyed, or we can't unlock it with a passcode, or there's been some other destruction of the physical evidence.

So, how can a military prosecutor or investigator obtain underlying communications other than a search warrant or authorization?

MAJOR BRUNSON:

Sure. So, when we're talking about electronic communications, or anything more than just basic subscriber information, that really puts us into the realm of the Stored Communications Act.

And this is a good jumping off point because just sort of stepping back, we think of the Stored Communications Act as part of our new authorities post MJA 16. And so, we might think about Stored Communications Act as some sort of investigative process or investigative tool. But that's not what it is.

Of course, the Stored Communications Act which is the statute that was passed first in 1984 is actually meant to do the opposite. It's a statute that protects communications and electronic data from government, from the government being able to obtain that, but it of course, does allow for judicial process.

And so, the important thing between pre MJA and post MJA 16 is that the Military Justice Act of 16 actually designated courts-martial and military judges as courts of competent authority to be able to exercise essentially those judicial processes under the Stored Communications Act.

And so that's why we can now go to our military judges in Article 30a proceedings to try to avail ourselves of that actual content or other information more than just basic subscriber info.

MAJOR DELANEY:

So, let's talk about that because there are sort of three categories of information that can be obtained, right.

MAJOR BRUNSON:

Sure.

MAJOR DELANEY:

You talked about basic subscriber, and there's non-content, and there's content. So, what is a non-content?

MAJOR BRUNSON:

Right. So non-content information is not the actual substance of the communications, but it's going to be things more than just the information that the user puts in when they first create the account.

So, for instance, to go back to the, to an eBay example, non-content info ... content information is going to be how many times and on what dates did this user log into the account and who did they interact with on that platform? And potentially what was, what was bought and sold?

You know, all of that is information that you might want to develop further investigative leads, or that might have evidentiary value in a court-martial, but you're not actually getting into the substance of communications between two parties.

MAJOR DELANEY:

So, for instance, different activity on the platform would be non-content. And then content is the actual communication itself. The Facebook message between people or the photo and the text in the Snapchat message.

MAJOR BRUNSON:

Right. And it doesn't even necessarily have to be communications where it goes from one individual to another person. It could just be a communication broadly. So, for instance, if you think about your Facebook wall and something you post on a Facebook wall that is going to be content under the Stored Communications Act.

MAJOR DELANEY:

Or going back to your eBay example, the actual photo of the item and the cost of the item for sale, that's the content. That's what's being communicated to other people.

Okay. So, when we're talking about the Stored Communications Act, what sort of entities actually fall within that?

MAJOR BRUNSON:

Right. So statutorily you're going to have two different types of entities. So, first thing being what's called ECS, or electronic communication services, and then RCS, or remote computing services.

So, an electronic communications service is essentially just any platform over which you can send and receive messages. So, that's phone-based text messaging, or a app like Facebook Messenger, or Snapchat, or Kik, or anything where you can send messages to another person.

Remote computing services, essentially you just need to think of that in terms of the cloud. So, Microsoft OneDrive or your Google storage. Just anything where you can save communications or any other sort of information or data on a cloud server.

MAJOR DELANEY:

Now, one important thing to recognize about these entities is they're not required to maintain communications for any set amount of time. Right?

MAJOR BRUNSON:

Sure.

MAJOR DELANEY:

So, whenever we are looking at third parties, right. These cloud-based platforms, these messaging platforms, one of the things you want to look at is preserving the evidence while we obtain judicial process in order to actually serve a court warrant or order.

MAJOR BRUNSON:

Right. So, once you determine that you're interested in information that's covered under the Stored Communications Act, your first thought should be sending a preservation request, because as Major Delaney said, there's going to be this time period between when you realize that information could be there and is of evidentiary value, and when you're ultimately able to potentially obtain an order or warrant through a 30a proceeding to get that information.

And so, you don't need to wait. You should go ahead and either through your law enforcement agencies, so through SFOI or OSI, or yourself, as the trial counsel, go ahead and issue a preservation request to that SCA entity to preserve that information. And that's something they're required to do. However, as Major Delaney also mentioned, is this doesn't change their procedures.

So, for instance, if you have let's say Verizon, and Verizon only keeps the content of text messages for 14 days, that's not going to require them to alter their policies to now keep that information for longer. It just means that whatever they have at that point, that they received that preservation request, that has to be preserved.

And of course, the next question is well for how long? And the answer is 90 days, at which point you can issue a follow up request or an additional request to ask them to preserve that for another 90 days.

And so ultimately, you're talking about if you issue preservation request, you need to make sure that the judicial, the judicial process has been accomplished within 180 days, or that entity is going to be under no obligation to continue to keep that data.

MAJOR DELANEY:

And realistically, you usually want it to be even sooner. Because as Major Brunson mentioned, they have to preserve what's already in their storage at the time they receive the preservation request. But if they regularly delete things in 14 days, every message between the date they receive that preservation request and the 14 days after, is going to start being deleted.

So, unless you're going to be sending subsequent preservation requests, you need to be getting the actual court warrant, court order served on the entity in a timely manner, so that they haven't deleted any additional messages not covered by the preservation request.

Now, under the SCA, there is some ability for the covered entity to voluntarily disclose information. How often does that actually happen?

MAJOR BRUNSON:

Well, you shouldn't count on it, because that's a, that happens very rarely. And the reason is because there's a, again the SCA, the point of the SCA is to make it to where that these covered entities cannot share this information with the government, except through judicial process or in these very limited permissive exceptions. So, the permissive exceptions really only apply, say for instance, when the entity is itself a recipient of the message.

So, if you have Gmail, for instance, I don't know why someone would do this, but if you actually just sent an e-mail to Gmail, then under the SCA they could permissively release that to the government with or provide that to the government or to a prosecutor without judicial process.

Another example, one that we probably run into the most is with NCMEC. So, anyone who's ever prosecuted a child exploitation or ICAC or child pornography case, you may know that for a lot of these electronic communication providers like say, Dropbox, or even the recent example where iPhone may start to scan its users' accounts for contraband.

But some of these Stored Communications Act entities are able to permissively turn over to the government any information about NCMEC hits that are found on their servers.

MAJOR DELANEY:

Now, that doesn't mean that everything else within that folder or that communication is also going to be disclosed. So, a NCMEC hit alone is probably not going to be enough in your case.

Now, we've been talking about these investigative subpoenas and we been talking about court orders in the investigative phase. Isn't there a concern that the subject of an investigation could find out about these court orders?

MAJOR BRUNSON:

Sure. And the rules for courts-martial account for that. And so, what you'll see in R.C.M. 703a, which is the rule that implements essentially the process for us to be able to obtain these orders and warrants through an Article 30a process, is that it also talks about non-disclosure orders. And so, when you actually apply for an order or warrant from a military judge to obtain information under the SCA, part of what's going to be on that form is essentially a block to annotate about whether or not you're also requesting a nondisclosure order.

And a nondisclosure order prevents the covered entity, prevents the electronic communication service or the remote computing service from notifying the subscriber that their information is being sought. Which is something that most entities are going to do reflexively if they get this kind of order or warrant, unless there's also the nondisclosure order.

And those nondisclosure orders, there's a list in 703a of reasons why you can ask for a nondisclosure order. And trial counsel is going to need to be able to articulate in the warrant or order application what reason justifies the entity not notifying the subscriber.

And going along with that, just as, after a search warrant is executed or search authorization is executed, the owner of the premises or the owner of the property is going to receive a copy of that search warrant. And the same sort of true with SCA orders and warrants, where at the end of any sort of nondisclosure period they are going to be notified of when what's in the application and what information was sought, what information was turned over by that covered entity.

MAJOR DELANEY:

I think it's also important to mention that we're filing these applications via e-mail, generally speaking. These aren't 39a sessions that are held in court. The article 30a session is a submission of an application via e-mail. So those also need to be maintained not only for discovery purposes, but they're also mandatory to be included in the record of trial.

MAJOR BRUNSON:

Major Delaney, for investigative subpoenas, court orders, warrants, we talked about all of those so far within the context, essentially the prosecution of the case. But for our defense community out there, is there a way for defense counsel to avail themselves of these same resources, with these same tools?

MAJOR DELANEY:

So, not under the statute of the R.C.M. itselves. These are tools that are limited to trial counsel submitting the affidavits for law enforcement.

Now, the one caveat to that is, of course, we talked earlier about how prosecutors have to consult as necessary with defense counsel throughout the CIP and SVIP capability. And one thing that defense counsel can do, is they can request that trial counsel issue the subpoena, or request a court warrant or order.

Of course, in order to do that, they're going to have to disclose a little bit of strategy, and they're going to have to meet the standards under the R.C.M. to obtain that investigative process.

MAJOR BRUNSON:

And then does the trial counsel have the discretion at that point to decide whether or not they do want to initiate that 30a proceeding to get an order or a warrant?

MAJOR DELANEY:

Yeah, I mean, it really is discretionary on that prosecutorial function because there is no ability for the defense counsel to go direct to either the GCMCA for authorization or to the military judge.

So, we talked a little bit about the Article 30a process. How is that actually initiated?

MAJOR BRUNSON:

Sure. So, the initiation of an Article 30a process is going to be via a memorandum from the trial counsel to the Central Docketing Office that requests that a military judge be detailed for the purposes of a 30a, and that docketing request essentially is also going to include information about whether or not the government's going to request a nondisclosure order.

It's going to include a request about, or it's going to include a note about whether or not the government is, how many applications essentially that the government is going to be submitting to the military judge during the 30a. And how many warrants or court orders that the government is looking to issue.

MAJOR DELANEY:

Is there also an ability to ask that this be an *ex parte* hearing, that defense counsel not be involved?

MAJOR BRUNSON:

Right. And that's going to be a standard part of that central docketing office request. And I think we may have mentioned previously that these 30a proceedings

typically are and can be *ex parte*, and *in camera* for obvious reasons, because you may not have all the parties appointed yet.

And in the case of a court order for an investigation for some information under the SCA, it's not even necessary that you have a known subject, necessarily at that point. And so, typically these proceedings are *in camera* and *ex parte*, but you still do need that request to the CDO.

MAJOR DELANEY:

So once there's actually a military judge detailed the Article 30a proceeding, what does the trial counsel have to submit in support of their application?

MAJOR BRUNSON:

Well, you should think of this as essentially either motions practice or uses, essentially the same process as getting a search authorization. So, it's not just a proffer is not good enough. A proffer would never, from trial counsel would never be good enough in a motions hearing or a proffer from an OSI agent would never be good enough to get a search authorization.

So, what you actually are going to need is, you know, specific and articulable facts and sworn evidence or testimony from law enforcement agents. Just the same as you would in a search authorization.

And when you actually make the application, which the application is going to be on an Air Force Form 3057. When you actually make that application as part of the 30a proceedings, you're going to attach to that all of the necessary evidence in sworn affidavits.

MAJOR DELANEY:

Yeah. I think one of the important things is the same way in a search authorization process, the judge may have questions. They may need more facts articulated. They may want more particularity in the affidavit or the sworn statement. Just because a judge has these additional questions, it doesn't mean the process is over. Trial counsel can amend the application. They can

reach out to the agent, and if the agent has additional information, can include that and incorporate it into the affidavit and continue that proceeding on.

MAJOR BRUNSON:

And just like with a, we've talked about warrant, we've talked about an order, what we need to talk about is the different standards that apply to each of these tools. And there's a helpful chart that kind of compares the different standards in the corresponding slideshow to this refresher [slides not shown]. But essentially, you're going to have three different standards that escalate as you go from investigative subpoena to a warrant.

And of course, for the investigative subpoena, whether that's issued by a court or by a trial counsel, that is going to issue under the same standard as anything else under 703. So relevant and necessary. Is that evidence that you're seeking to obtain relevant and necessary for an ongoing investigation?

For a court order, where you need more than just that basic subscriber information, but not necessarily content, that standard is a little bit higher, and that's going to be you're going to have to show specific articulable facts that the evidence being sought is both relevant and material for an ongoing investigation.

And then the standard that we're most familiar with for a warrant is going to be the same as a search warrant or a search authorization. Where you're going to need to have probable cause that there's evidence of a crime located within that information to be sought.

MAJOR DELANEY:

And those are the standards that the military judge are looking to, in determining will they grant your request or not.

MAJOR BRUNSON:

Major Delaney, I want to talk for a moment about a hypothetical, sort of illustrating some of these different

tools and the different standards at play, and what you would use the different investigative tools for.

So, supposing we have a Internet Crimes Against Children case where, you know, you may have communications between an offender and someone posing as a child. But suppose you had another victim in that case, that you've been able to identify, that you're not able to get those messages between the offender and the victim.

How would we use, let's say an investigative subpoena in a case like that, just to initially draw some links or further investigative leads?

MAJOR DELANEY:

Well, sure. So, one thing these chances are the subject is using a pseudonym on whatever platform he's using to engage with the ICAC agent. So, we need a way to tie our military subject to that pseudonym. So, the basic subscriber information via an investigative subpoena will help us make that initial link between the pseudonym on the Kik or Facebook Messenger, or whatever he's using, and the individual subject.

MAJOR BRUNSON:

And just to review, is that something that a trial counsel can do, or is it something we need to go to the court for with a 30a proceeding?

MAJOR DELANEY:

So, either the GCMCA or his delegee can authorize trial counsel to issue an investigative subpoena for that, or an investigative subpoena can be obtained through a military judge.

MAJOR BRUNSON:

Okay. And what might be in this hypothetical, what might be the sort of information that we would need to know that's beyond basic subscriber information, but not necessarily yet the content of those communications?

MAJOR DELANEY:

Sure. So even if we now know that's his account, we still need to establish that he's the individual at the computer sending the messages. And one way we can do that is by getting non-content information that would be his accessing chat logs or logging into the application. And then that gives us a timeframe at which we can track whether he had access to the computer at that time or not.

MAJOR BRUNSON:

And that's something we can do via a court order?

MAJOR DELANEY:

That's correct, right.

MAJOR BRUNSON:

Through an Article 30a proceeding.

MAJOR DELANEY:

30a proceeding, but trial counsel could not get that in an investigative subpoena alone.

MAJOR BRUNSON:

And if we got that information through a court order, what would be essentially the showing that we would have to make in order for a judge to issue that order.

MAJOR DELANEY:

So, you still need particular facts, articulable reasons, to show that that information is going to be relevant and material to your investigation.

MAJOR BRUNSON:

Ok. And then finally, to get the actual content of those communications so that you know the evidence of the crime itself, what is the tool used to do that?

MAJOR DELANEY:

So that's where we're going to go all the way up to a court order, if we're trying to get that cloud-based or messenger third-party based information.

MAJOR BRUNSON:

A warrant.

MAJOR DELANEY:

A warrant. Right. Exactly. I mean, there's the Fourth Amendment warrant, which we could seize his computer and search his computer. But under the Stored Communications Act, we can also get a warrant to serve upon the third-party provider.

MAJOR BRUNSON:

And when we apply for or when the, you know, our law enforcement agent applies for that warrant, what other things should we be thinking about in terms of disclosure and preservation of that evidence?

MAJOR DELANEY:

Absolutely, that's one of the considerations between whether we want the warrant under the SCA or a search warrant and seizing his computer. Is if you're doing the cloud-based a data service, you want to use a preservation request immediately. We want to do a nondisclosure order along with our request. We want to see if we can get those communications without the subject being aware.

MAJOR BRUNSON:

Major Delaney, before we close today, any sort of final thoughts about these topics that you'd like to share from a JAJG prosecutor's perspective?

MAJOR DELANEY:

Absolutely. So, we talked a lot about these investigative processes, and nobody is alone working on these. You should be consulting with your CTC at all times. They have access to all of the JAJG resources. And additionally, if you just, on your own, want to look up more, we have lots of information on the Stored Communications Act, on the processes for obtaining investigative subpoenas and warrants. All of that is on our KM site, along with samples, templates, just a lot of really valuable information to assist bases in these investigative phases.

And I guess, Major Brunson I will throw it back to you. Any final thoughts you would like people to know from a JAJM perspective?

MAJOR BRUNSON:

Sure. I would just say, and the attached PowerPoint that's going to correspond to this refresher [PowerPoint not included], I will give you a lot of this information, but we always try to make folks aware, and make better use of the Virtual Military Justice Deskbook. A lot of the templates, the forms for these different processes can be found there as well as the things like the template for the memo to the Central Docketing Office to request a 30a proceeding.

And I've harped several times today on section 6 and 22 of AFI 51-201. But that's where you can find all the really detailed guidance in the actual no kidding base level requirements to not only understand these CIP and SVIP processes, and the 30a proceedings, but also to make sure that you're complying with all of the Air Force regulations.

[upbeat music]

ANNOUNCER:

Thank you for listening to another episode of The Air Force Judge Advocate General's School Podcast. One of the best ways you can support this publication is by following or subscribing the show and leaving us a rating. You can find this episode, transcription and show notes at https://www.jagreporter.af.mil/Podcasts. We welcome your feedback.

DISCLAIMER:

Nothing from this show should be construed as legal advice. Please consult an attorney for any legal issues. Nothing in this show is endorsed by the federal government, the Air Force, or any of its components. All content and opinions are those of its guests and hosts.

CERTIFICATION PURPOSES

For those JAGs who listen to this refresher for certification purposes, be sure to navigate to the certifications page under the management system dropdown on Flite. On that page, mark the appropriate radio button corresponding to your status and requirements. Thank you.

GLOSSARY

- AFI: Air Force Instruction
- AFOSI: Air Force Office of Special Investigations
- **CDO:** Central Docketing Office
- CIP: criminal investigations and prosecution
- CTC: Circuit Trial Counsel
- CTC-SVU: Circuit Trial Counsel, Special Victims Unit
- DAFI: Department of Air Force Instruction
- ECS: electronic communication services
- GCMCA: general court-martial convening authority
- ICAC: Internet Crimes Against Children
- JA: judge advocate
- JAG: judge advocate general
- JAJ: Military Justice & Discipline Directorate
- **JAJG:** Government Trial & Appellate Operations Division
- JAJM: Military Justice Law and Policy Division
- LL.M.: Master of Laws
- MCIO: military criminal investigating officer
- MJA 16: Military Justice Act of 2016
- NAF: Numbered Air Force
- NCMEC: National Center for Missing and Exploited Children
- NCOIC: noncommissioned officer in charge
- NDAA: National Defense Authorization Act
- **OSI:** Office of Special Investigations
- R.C.M.: Rules for Courts-Martial
- RCS: remote computing services
- ROI: report of investigation
- SAPR: Sexual Assault Prevention and Response
- SARC: Sexual Assault Response Coordinator
- SCA: Senior Civilian Advisor
- **SFOI:** Security Forces Operations Investigators
- SFS: Security Forces Squadron
- SIR: supplemental information request
- SJA: Staff Judge Advocate
- SVC: Special Victims' Counsel
- **SVIP:** Special Victim Investigation and Prosecution
- SVU: Special Victims' Unit
- SVU-CTC: Special Victims Unit, Circuit Trial Counsel
- UCMJ: Uniform Code of Military Justice
- VTC: video teleconferencing
- VWAP: Victim and Witness Assistance Program