Carol Johnson: Thank you very much Parker. Appreciate the introduction. I just want to go back to the purpose of this presentation, which is to research guidance. The goal here is to provide best practices on the remediation of unapproved technical reference model. Many of us know it as TRM software on VA networks. So this is role-based training that we’re provided to research stakeholders and I’m excited to provide this training because I know that it has been an ongoing challenge to understand remediation options. And so hopefully this will be an opportunity to provide you those options.

So just want to talk a little bit about objectives. So a few objectives for this particular presentation will be, what is the purpose of a remediation? So what’s the remediation guidance purpose and its objectives. Also, remediation scope. What is unapproved software remediation scope? Also CRISP overview. So we’ll talk about what the CRISP roles are. We’ll talk about TRM’s role as well and their process. We’ll talk about remediation solutions, which this one will be key in understanding what are some of your options.

We’ll talk about roles and responsibilities does include business owners, it includes ISOs, it includes the CRISP team, the TRM team as well. So we’ll talk a little bit about those roles and responsibilities. And then we’ll talk about frequently asked questions. So some of the questions we were able to derive from our meetings with our research stakeholders that we thought would be really critical for the community to have answers to. So we’ve included those as part of this presentation and also as part of the guidance document. So most everything that has come…that is in this presentation has come from the guidance document that was recently published on this same topic. And all the things including the guidance document link is included in this presentation as well and will be made available for you.

Okay, so let’s talk a little bit about our purpose and objectives. So the purpose and objectives here is really to ensure compliance with CRISP. And CRISP is Continuous Readiness and Information Security Program. That is the team who manages the remedial actions associated with unapproved software in TRM. So our goal is to really ensure compliance to that, and also provide VA research stakeholders, which include investigators, R&D stakeholders, ISOs, system owners, business owners, IRB board with best practices for remediation of that unauthorized unapproved software. Because we do use those terms interchangeably. TRM does use those terms interchangeably. So we’ll make you familiar with the new memorandum that was published as well.

And then our third objective is to provide awareness of recommendation remediation options and solutions to ensure only authorized research software applications are installed on VA systems in accordance with VA policy. So it’s really all about managing risk and we’ll help you in that process. Okay, so in terms of compliance overview, just wanted to acclimate you with the memo published in October 1, 2020, and that memo, TRM unapproved technologies memorandum does rescind and supersedes the other memo in November of 2018, which was the STAT waiver memo. Many of you are familiar with that Strategic Technology Alignment Team. And I know many of you work with them in terms of trying to get assistance with applications that were deemed unapproved by TRM.

So that memo, the old STAT memo has been replaced by the new TRM Unapproved Technologies Memorandum. And so we’ll talk a little bit about what those solutions involve. And I’ll tell you that…and the link is there. It will be available for you. You can look at the memo. It does talk specifically about POAM process. But what I wanted to share with you in this presentation and in the guidance is that there are other remediation options available outside of the POAM. Because many, many times many of know when you open a POAM, it does require some level of tracking. And so we’ll talk about all the remediation options, and we will also talk about POAM as well. So the goal is again to support the NIST 800-37, which talks about the risk management framework.

So from a remediation scope perspective, we have so many different processes within the VA in terms of application approval processed, and what applications are authorized for use on the VA network. And so I just really wanted to be really clear about the scope of this particular presentation. The scope of this presentation and the subsequent guidance document includes only those applications managed by TRM, because the other application processes have other management processes. Have other approval processes. GFE mobile apps, non-GFE mobile apps were not in scope for applications for medical devices.

Well, we say special-purpose just to sum it all up, which include medical devices, SPS/special-purpose systems and research scientific computing devices. And also SaaS applications. So there’s a \_\_\_\_\_ [00:10:35] process available for that. So I just wanted to be clear about the purpose of this particular guidance and it is specific to TRM applications and those software that has been deemed unapproved by TRM. Now there are other unauthorized software by TRM that fall in the prohibited and divested category. We are talking about unapproved only. The scope for this presentation.

Okay, so we talked about CRISP, the Continuous Readiness and Information Security Program. So there is a process outline for remediation of TRM unapproved software. So the roadmap is listed there. The decision is made into TRM, so the \_\_\_\_\_ [00:11:31] published the TRM decision unauthorized incidents located on the network, so there’s the scanning process that’s performed. And then the application’s inversions vetted by the working groups. And then once it’s been determined what applications…what software will be put on the list or be deemed unapproved, then the bulletin is published. And many of you may have seen this bulletin. And it will list the software that is deemed unapproved.

And in there, it will give you…users have 30 days to make the changes or make remediation. And then in the second 30-day period, remaining applications submitted to TRM for RS, which is removal script for review. So that is the CRISP process. But I wanted to take some points out of this bulletin to just highlight. So part of the bulletin does indicate that the VA Technical Reference Model/TRM was established to identify approved software for use within the VA. So it’s important that we’re compliant with that to ensure VA software systems use on the network are approved. Currently TRM has three categories of unauthorized software as I mentioned. It’s prohibited, unapproved, and divested. But we’re talking about unapproved only. So remediation associated with unapproved software.

So unapproved software may only be installed if the product has gone through the proper review channels. Including having the application or versions undergo a reviewed by the technical reference…technical review and analysis team. And those can be submitted through the site that I’ve indicated there. But I’ll show you another way in which those can be submitted to us. So just keep that in mind, but we’ll show you some other options in terms of reevaluation of software. So unauthorized software installation on VA systems violate both VA policy and put the enterprise at risk.

So basically in a nutshell, this particular statement is saying that you have 30 days to remediate, and then potentially another 30 days or in some cases it can be removed immediately. And so once it’s been deemed unapproved, it’s considered a risk. So at that point, it can be removed immediately. But in most cases, there is that timeframe of 30 days, and then another 30 days once it’s been put on the list before it’s actually removed via the other removal script. But he goal really is once it’s been identified as unapproved from a business owner perspective, you definitely want to start the remediation process right away.

And what are some of those remediation solutions? What are some of those remediation process? So we’ll talk a little bit about software upgrade as an option. We’ll talk about alternative TRM unapproved software. TRM approved software. And then we’ll talk about request for TRM reconsideration. And we’ll talk about the plan of action and milestones. And we will talk about data backup and recovery because that basically is a more proactive approach to ensuring your retention of your data in the event that the application is removed.

So we’ll talk about software upgrade. VA TRM compliant software includes the following. So many of you have been into TRM, you’ve seen the list of approved applications and you’ve seen a list of those that are approved or approved with constraints. So it’s very easy to tell in TRM what software is approved and what isn’t. And oftentimes with approved with constraints, of course it does tell you to work with your local ISO to ensure that those constraints are met. So I’m sure many of you have seen that.

So the TRM entry contains guidance along with any known applicable constraints on the permissible range of technologies or standards that a VA users or IT administrator support team or project development team may select or shall use. So FAQ 10 will show you how to search for technologies and standards in TRM. So you’re really just looking to upgrade from the unapproved version to the new version of the same software. And you can look into TRM to see what has been an approved version for use and/or approved with constraints and satisfy those constraints for the continued use of that software. That same software just a different version.

So alternative TRM approved software. So research stakeholders, business owners are encouraged to review the TRM VA categorization framework to determine if there are similar technologies by specific categories that meet a research technology requirement. So what this is really saying and I’m not sure how many have been in this particular link, but this link does provide you with more of a holistic look at satisfying your needs. So if you have a specific category that you’re using software for, you can actually go to this link and get a list of different categories and as you drill down on those categories, then the end result is that you will have a variety of software to select from for that particular category.

So an example of that may be information management technology. So then you can drill down to business intelligence and data warehouse platforms. And then you can further drill down to data mining and or data warehouse or web reporting apps. And then once you make that final selection, so let’s say for instance you’re looking at web reporting tools and you click on that hierarchy of characterization, then it’ll give you all the software that’s been approved by TRM for web reporting apps. So you can look at it from a category perspective and see if there are applications or software that’s approved within TRM based on the category that you have to satisfy your need. So that is another option if you have to now look for an alternative software to use. So we talked about upgrading. That doesn’t work, then you have to now look for an alternative solution and an alternative software, that’s one way to do it.

So the other consideration here is that you can request TR reconsideration for the same software. And so how do you do that? So the business owner and end users can request reconsideration of TRM decisions through the submit a request for evaluation from the TRM homepage. And again, links will be provided for you. You can review the common reasons for unapproved technologies and to request an update to an existing TRM entry, continue to the consent form—it’s really at the bottom of the form­­—and select the radio button labeled update an existing entry. So TRM will reach out to you once that entry has been published for reconsideration. However, it is still a risk there is still a vulnerability and likely a POAM will still be required. Because keep in mind, a POAM is meant to track the risk until it is mitigated. So that is not an exception for continued use because again, it still creates levels of vulnerability, but it is to track the risk until it is resolved.

So now let’s talk about the POAM. The Plan Of Action and Milestones. And there are many different roles and responsibilities associated with the POAM. For many of you if you’ve been involved in that process of reviewing a POAM. In this particular case, the goal, and the objective for a POAM is to obtain and authorizing official risk-based determination. So if you make a decision that that software is critical to your research and needs continued use, then a POAM is required. And when I say continued use, it means continued use until you have remediated that vulnerability. So the POAM is to get that risk acceptance from the authorizing official. And this is done in our eMASS system.

So the POAM can be submitted for any software application or any technology that has been identified into TRM as a status of divested or unapproved. And again, we’re only talking about unapproved in this particular instance. So a POAM assists VA system owners, authorizing officials, designated representatives, and authorizing officials in reducing risk to VA systems by identifying whether similar VA approved technologies are available, alternate solutions are available to minimize the impact in a research project. So that’s important. And so the POAM Management Guide is available if many of you already familiar with it. If not, the link is available there for your review.

Really kind of digs deep into what the roles and responsibilities are and the purpose of a POAM, the requirement for review and so forth and so on. So as I mentioned, once you open up POAM, it does require tracking. So the goal is to remediate and to reduce the risk on the VA network and there are many ways to do that, and we’ll talk a little bit about what some of those activities may be in supporting this tracking of the POAM and having the ability to close that POAM. Because at the end of the day, oftentimes there’s a POAM open and you just don’t really know how do I close it? How do I remediate? And so we’ll talk little bit about that.

So to be more proactive, of course data backup and recovery is important. So effective backup procedures ensure the ability to recover data if the application is removed from the VA network. The following steps should be considered during installation and setup of TRM approved application to ensure appropriate data backup. So you have an application that was approved by the VA, now it’s unapproved. But now you have all of this data that you’ve been using for your research studies, and you didn’t get the notice that…you didn’t get the 30 or the 60 days and the application processed and removed through the removal strip. So many of your local facilities have local shared drives just designated for research. And that is important that your research that is being conducted on behalf of the VA, that information and that data are saved on that local shared drive. Because it does meet specific contingency planning. It’s outlined in our control CP-9.

So that’s important. Now the local IT is responsible as administrators for installing software on VA devices to be on the VA network. And typically, that is the location…that shared drive is the location that is pointing to that software. Now there may have been other cases and use cases that we may not be familiar with where data is being saved somewhere else and then subsequently is lost and unrecoverable. But to avoid that, ensure that you’re using that local shared drive for research at your local facility so that will ensure that the data is backed up on a cadence that is approved by the VA and consistent with CP-9 controls.

So the TRM script removal as I mentioned that process after 30 days titles will be subject to change order unless the title has undergone a new TRM review or if the software has gone through the proper review process. Which is plan of action and milestone or reconsideration or some of those areas that I mentioned early on. So after an additional 30 days of being subject to the title…subject to the change order, titles will then be added to the TRM removal script. So I did place a link there that takes you to some of the basics of unauthorized software, which would include unapproved software for TRM.

So just want to talk a little bit about some use cases here that we had an opportunity to receive from research stakeholders. One was NVivo, which is really a big one for us that really helped us to get this off and running. Oftentimes you feel that if you complain about something, than that’s just it. But what we did was, we took those complaints and we wanted to create a solution, an enterprise solution and that’s how this guidance has come about. So NVivo scenario, the software Windows is newly unapproved because it requires SQL Server Express Local Database 2017 and Windows Management Framework 4.0 to be loaded. And these have been deemed unapproved. End-of-life with the VA. So it appears that the SQL Server Express which is not used by business owners, but does present security vulnerability, so it is not used by VA business owners. But it is part of the software, and it does create security vulnerabilities.

So a possible compliance remediation plan could include three of the following. Well, it could also include an upgrade to a different version if that’s allowed. But these three options business owner coordinates with a vendor to recommend a package with a newer compliant version with either an updated SQL Server or simply omitting that. That SQL Server Express that’s causing the vulnerability. Or the business owners can coordinate with vendors to determine if software can be reconfigured to access a compliant database application. Or the business owner develops a mitigation plan to move to an alternate and compliant software application. So this is just an example, but this is the activity that you would be performing in support of a POAM.

So you’re not able to really manage this activity within a timely manner based on the TRM remediation timeline, so you open a POAM. These remedial actions here will be in support of updating your POAM. So these are just an example here, but it does kind of give you an example of when you would be using it. You could follow these actions before 30 days and hopefully be successful before the 60 days as well. But in case if you’re not and a POAM is required, you can use these remedial action plans or steps to help facilitate risk and removal and then also closing of the POAM. So

Blaise scenario is the next one. So there was a version 4.8, and I was actually part of this one, which was unapproved. Version five or higher was approved and there were three studies that had version 4.8 was using for version 4.8 for Blaise. And so that possible compliance remediation plan that…I say a possible remediation plan, but this is actually a specific use case. And this is the actual remediation plan. The business owner decided to remove the three studies from the old version and then was able to only enroll patients on the newest version five or higher for Blaise, and that is how it was remediated.

One thing I will tell you, many researchers use the same application across the enterprise. They use the same software across the enterprise. And while it can sometimes…it’s not mandatory that you collaborate with other researchers on your remediation steps, it sure would help the community to remediate activities and share best practices with each other for remediation. In the guidance document—and again, I will provide you the presentation and links are there—there are reports that you can run to see who else is using the applications or using that software within the VA. And so that collaboration can certainly be of great benefit to other researchers scrambling to find alternative solutions.

So the roles and responsibilities just want to talk briefly about this because the POAM Management Guide really gives clear roles and responsibilities for the POAM. But I just wanted to set some expectations around who does what and from a remediation perspective. So some examples of that given the audience and I’m just jumping down. Develop a mitigation plan to move the alternative and compliant software application. So that’s a real collaborative effort there in terms of those involved. Requires TRM support, requires the business owner support, requires the ISO’s support. So across-the-board, that is important.

Review each POAM item and correctly document the current situation. This is done with the ISOs. They do receive POAMs on an ongoing basis. I believe it’s quarterly that they do quarterly reviews of POAMs. I could be wrong, but it’s in the POAM Management Guide. So if I’m wrong, that’s your reference. And so just keep in mind again, opening those POAMs, it does require that level of tracking to ensure that there are steps being complete to move you into a compliant state. Can disapprove and still move the workflow forward in the POAM workflow diagram…in the workflow process.

That’s a collaborative effort in terms of TRM being consulted, business owners being informed there, and ISOs reviewing that POAM on a regular basis. Once it’s created and moving it to the appropriate workflow, they are part of that workflow as well from a POAM perspective. And then responsible \_\_\_\_\_ [00:33:45] last one responsible for the development of remediation and mitigation of software that has been deemed prohibited and unapproved by TRM. And that is also collaborative effort as well. And ultimately, the goal is…the role I play for Blaise was the ISO role in helping them come up with remediation solutions. And so that included talking with the vendor for some of those possible solutions as well. And again, the goal is to remove that risk.

So just some frequently asked questions. And again, these are questions that we received as a result of our communications and meetings with research stakeholders, and hopefully these questions will be helpful. But in the actual guidance document itself there are many more. So we pulled a few out. So how can users be proactive in tracking a technology if it is scheduled to be put on the TRM unapproved list, and where can they locate a complete list of unapproved applications? So users can be added to the TRM email distribution list for an application. You can going to TRM for an application and be added to an email distribution list that will give you updates anytime there’s a change made. And then additionally, users can search for existing technology assessments on the unapproved application report and all TRM unapproved application reports as well. So there are links available there for you.

So who is included in the email notification for CRISP remediation of unauthorized software? Our understanding at this point is that the email is currently being sent to the system owners, which are typically the area managers and those in the OIT community. However, we are in the process of trying to resolve this issue and add the research community to that distribution list. So can software with licenses owned by research affiliates be installed on VA computers if the license is owned by an affiliate, but the software is approved in TRM? Application would apply also to those devices that come with package software approved in TRM, but the affiliate owns the license. This is a big question. And so what we determine through our research is that service now—and then the knowledge base article link is there—does not include requirements for licensed ownership prior to installation.

So as long as the software is on the TRM unapproved list…on the TRM approved list, then irrespective of the owner of that license, that software can be used on the VA network as long as they have approved it. And that is the knowledge-based article link there that will take you to how to submit request for an application. Alright, so the references that I provided as I indicated to you the CRISP analysis process, I’ve also indicated the first reference we made in the 6500 on risk management framework, also TRM links and some FAQs that are located there.

The POAM Management Guide is also located there. And then the, all TRM unapproved application report, those are links that you can get to. The memo is also there. I think I put both memos there. Oh, and then the knowledge base article for request a temporary approval to use on approved tools. And technologies is also there for you. The link to the TRM bulletins or the CRISP bulletins I should say for TRM unapproved software or unauthorized actually is the full scope of those bulletins that you can read the information specific to unapproved.

And then the eMASS boundary categorization in terms of who’s the…who is actually the system owner is there. And then the actual guidance document itself. Again, everything mentioned in this presentation comes from the actual guidance document developed by the team, the Research Cyber Security Team. And so you will be able to click on that link and get the full document and any additional references and FAQs that you will find helpful there as well. So at this moment, that is the last slide. We can open it up for questions and answers Parker.

Parker Cunneen: We don’t have any questions yet in the Q&A, but we’ll give folks a moment to put that in there. As a reminder to everyone, if you have any questions for our panelists, you’re going to go down to the bottom right-hand corner of your screen and enter them in the Q&A box. And just make sure you’re addressing them to all panelists. So we’ll just give folks a minute or two here. Seeing one pop-up, so it should be up on your screen in a moment Carol.

Carol Johnson: Okay, I’ll read the question. There is an enterprise endpoint management and reporting for TRM unapproved reports that is in Power BI dashboard. What is the integration with TRM and/or is it external product to TRM? So I’m not sure about that particular reporting and I will have to access that link to just get a visual of what that link is. Power BI. It’s in Power BI. So it could certainly be…it could be the link that we’re sharing with you in terms of all the list of applications that are deemed unapproved through TRM. But I would have to actually look at it to confirm that to be the case.

Okay, next question, is if you’re affiliate is a university which are most cases, are you allowed to put educational software on VA PCs and laptops? Only if it is approved through TRM for install on VA equipment. Okay, have you considered allowing add packs to be included on the list that shows when software…when their software has changed? So you as an individual can add your name to an email distribution list for a particular software. So I think the question is more has TRM considered the ability to add groups to that distribution. And I think that would be more of a question for TRM. But you can certainly add yourself to the list to be notified when there is a change to a specific software. But because we don’t own the process, we don’t own the TRM process, that question would be more a TRM question in terms of adding a group. Because add packs are those that have a zero-account administration level access to the network if I remember correctly in my days with the ISO facility as ISO. Yes, that would be….

Terry Peters: Carol.

Carol Johnson: Yes.

Terry Peters: One thing we can recommend to, if you do have an add pack that you’d like to be included, you can follow those instructions in the slides to have that individual add it. So that’s an option as well.

Carol Johnson: That’s an option yes. At the individual level, yes. I mean, it’s a good question. It’s a question to have a group added. But definitely TRM \_\_\_\_\_ [00:44:26]. Okay, so I have run into where software is approved in TRM, but CRISP contractor states it’s unapproved in an IT ticket. So a number of things could be happening there. There could be a timing issue. So it may be on a nonapproved list and there may have been communication that is in the process. So a number of things could be happening there. My recommendation is that you do have the option within TRM because what you’re getting is you’re getting one thing in TRM and you’re getting the IT contract representative telling you something different. You can make a request or an inquiry directly within TRM for that particular software to get a direct answer in terms of whether it’s approved or not. But you can also look at the list of unapproved software to see if it is on there. And that link is provided in slides as well.

Okay, is there research software and library for affiliates and research departments to request the latest product as to trying to purchase something oh, outside the scope of VA security standard. We do understand that that is all…procurement, when that happens it’s really critical within your project…your research project of the VA. Please look at TRM for those of through software. That is your reference. That is your library. The TRM is your software library for determining what’s approved for use. And we run into the same situation with devices. So often times devices are purchased and want to be used at the VA and in the list hasn’t been reviewed to make sure that it’s an approved device for use at the VA, and so there’s always a lot of procurement waste there. So TRM is your software library. Oh, okay. That is going to be…so I apologize if I missed it. But where is the report that will tell you who is utilizing a software that has been approved in TRM? It is in the reference section of the slide presentation.

Terry Peters: I’m sorry Carol I was muted a second ago. I wanted to add something to that previous one about the research library. One thing that is going to be forthcoming that we’re in the process of finalizing right now is within TRM, you got the software listed, we’re in the process of tagging that software for research. Software that’s commonly used in research. And what we’re that as well besides that tag of research, running additional tags where maybe it was a software that’s used in precision ontology. Or a software that’s used for data collection. And that is going to be forthcoming. But that’ll help you a lot when you go in TRM, you’ll be able to see what software is recommended for research and then kind of those subareas that it would really be beneficial in. So that’ll be forthcoming here soon.

Carol Johnson: Good point. Thank you. And also to the question earlier, I just wanted to take a double check on the presentation slides. Go into the link in the reference section and actually click on the last tile, and in that last tile it’ll show you where the guidance document is located, and it will definitely be included. It is included in the guidance documents itself. That’s where you can find out who else is utilizing software. Okay, thank you for that Terry.

Terry Peters: Yes, ma’am.

Carol Johnson: Yes, as a matter-of-fact…okay, so the question is, where would I add my name to the list? You’re talking about the software notification list. So the guidance document will give you step-by-step on where you can actually add your name to the list.

Parker Cunneen: This appears to be the last question in the box. I don’t see any more coming through at the moment.

Parker Cunneen: Carol, would you like to give folks another minute or two \_\_\_\_\_ [00:50:49] here?

Carol Johnson: Okay, yes, I think if that is the last question, I think we’re in good shape to end.

Parker Cunneen: Fantastic. Well, Carol I want to thank you and your fellow panelists for having this presentation today and we look forward to hearing more from you in the future. To our attendees, as mentioned, if you could take a moment or two just to fill out that post-webinar survey. Especially as this is going to be a new ongoing webinar, we would really appreciate that feedback. And with that, we’ll give you all 11 minutes back and hope you have a good afternoon. Thanks.

Carol Johnson: Thank you,