Slide 2:

Welcome, and thank you for standing by. I would like to inform all participants that today's call is being recorded. If you have any objections, you may disconnect. Go ahead, you may begin.

Hello, my name is Keith Marzullo. I am the division director for the division of computer network systems in the Directorate of computer and information science and Engineering.

I'd like to welcome everyone to this webinar on our new program in cybersecurity. In May 2009, President Obama gave an address on securing the nation's cyberinfrastructure. He released a report on a top-to-bottom review of the federal government's efforts on cybersecurity, and announced that his administration would pursue a new comprehensive approach to securing America's digital infrastructure. He observed, in his presentation, that America's economic prosperity in the 21st century will depend on cybersecurity.

One of the results of this address was a national-level focus on cybersecurity, and the realization of theneed to engage a broad set of researchers to maximize the impact of research and development on our cybersecurity posture. The new NSF program in cybersecurity, Secure and Trustworthy Cyberspace, is one part of this effort.

Slide 3:

The Secure and Trustworthy Cyberspace program, or "SaTC" for short, now includes support from more than just the one directorate of Computer and Information Science and Engineering. The directorate for Social, Behavioral and Economic Sciences has joined this program to support, for example, research in economic and behaviorial incentives. The Office of Cyberinfrastructure has joined to support transition to practice of research results, and the Directorate of Mathematical and Physical Sciences has joined to support the development of mathematical tools and methods in the area of cybersecurity. Today, you will hear from program directors in each of these directorates: Dr. Samuel Weber of CISE, Dr. Peter Muehlberger of SBE, Dr. Kevin Thompson of OCI and Dr. Andrew Pollington of MPS, who will describe this new program.

I hope you find this webinar informative, and please do feel free to ask questions after their presentation. I now would like to introduce to you Dr. Samuel Weber of CISE.

Slide 4:

Thank you for the introduction. As you can see from the agenda, after a brief overview of the program, we'll take an in-depth look at each of the program perspectives, and touch briefly on some of the submission procedures. Frontier awards are one of the new features of SaTC and deserve their own discussion. After that, we'll clarify some issues and finally take questions from you, our audience.

Slide 5:

To sum up the goals of our program succinctly, we fund research that aims to protect cyber-systems from malicious activity while preserving privacy. Furthermore, because it is pointless to have a secure system which nobody can operate, we also need to take usability into account.

Our field started with military applications, where the situation was very clear-cut: we were attempting to defend our computer systems against people who were explicitly our enemies and who were explicitly attempting to harm us. The solutions that we focused on at this time were primarily technological: building computer equivalents of better locks and gates.

The world now is very different and much more nuanced. Spammers, for instance, usually think of themselves as honest businesspeople who are selling useful products, even as they hire botnets to send us a flood of email. We find ourselves having to defend our privacy from companies that we are doing business with. Going to the websites of major reputable companies can result in your computer being attacked by malware. Even our cars and medical devices have been shown to be vulnerable to cyber-attacks. It is also clear that simple technological solutions cannot work: we have to consider not only whether end-users can safely use the systems that we build, but whether developers can successfully produce secure software.

What distinguishes our field from most others is that we are attempting to defend our systems from other humans, who are able to intelligently counter our actions. Physicists don't have to worry that subatomic particles are trying to deceive them, and traditional reliability engineering concerns itself against random environmental effects, not intelligently targeted actions. This means that we face a constantly changing field, as malware authors do read and respond to our conference papers.

Slide 6:

As you can see here, SaTC is our newest program in the long-standing NSF commitment to funding cyber-security research. Ten years ago, in the 2002 financial year, NSF started the "Trusted Computing Program". This program was limited to a single division in CISE, but after two years it was expanded into the "CyberTrust Program", and then into "Trustworthy Computing", which were cross-cutting programs throughout all of CISE. With SaTC, NSF is once-more widening the scope of the former Trustworthy Computing Program, and making it cross-directorate. The total NSF funding of cybersecurity is now over $100 million dollars across various programs including SaTC, and has increased significantly since 2002.

Slide 7:

Unlike most other federal research agencies, the National Science Foundation operates in a bottom-up rather than top-down fashion: we issue very broad solicitations and fund the best ideas that the research community generates. As a Program Director, I view our role as similar to that of a gardener: not only selecting the best plants, but applying extra fertilizer to sub-

fields which need assistance. We also know that academic research often has difficulty making it out of the ivory tower and into practice, and we wish to make this process easier.

Slide 8:

As I said earlier, past history has shown us that we cannot consider cybersecurity as simply a technical problem with technical solutions. Instead, we also have to consider human behaviour, both individually and socially, and take into account how research will impact and be impacted by practice.

Therefore, we have decided to make these aspects explicit, by defining three perspectives: Trustworthy Computing Systems, Social Behavioral & Economic, and Transition to Practice. A proposal to our program must belong to at least one of these perspectives, but may involve all three. By doing this, we don't, by any means, want to discourage proposals that target one particular perspective. Instead, we want to encourage researchers whose work crosses traditional disciplinary boundaries to engage with researchers with different backgrounds and expertise, and thereby enlarge and enrich the cybersecurity community.

Slide 9:

We strongly want to encourage this point: Trustworthy Computing aimed to foster long-term cybersecurity research, and that is still our key objective. What we are trying to do is to widen our research base. We also want to emphasize that, although we do want to encourage multi-disciplinary proposals, to be credible such a proposal will likely need a strong multi-disciplinary team: a perspective which appears to be simply "tacked-on" will detract from the proposal and reduce its chances of success.

Slide 10:

The first of the SaTC perspectives that we will discuss is the "Trustworthy Computing Systems Perspective". This perspective focuses on traditional Computer Science concerns, and is very similar to the former Trustworthy Computing Program. Despite the word "Systems" in the title, approaches ranging from theoretical to experimental are in-scope, as are the human-centric. Security, privacy and accountability are considered, as are theories, models, algorithms, programming languages, hardware and software architectures, and evaluation frameworks. We not only fund research that will directly result in improved defenses, but we also fund work that aims to understand or measure the problem, such as investigating security and privacy tradeoffs or the effectiveness of various development methods with respect to security.

Although work that in previous years would be submitted to the Trustworthy Computing program is still relevant to the Trustworthy Computing Systems Perspective, we think that a significant amount would be able to benefit by consideration of the other perspectives that are now available under SaTC.

And now I'll turn the presentation over to Peter Muhlberger, who will discuss the SBE perspective.

Slide 11:

The Social, Behavioral and Economic sciences or SBE perspective in SaTC seeks to fund proposals that have the potential to enhance the trustworthiness and security of cyberspace and which contribute to theory or methodology of basic social, behavioral or economic sciences.

NSF and prominent members of the cybersecurity community believe that cutting edge SBE research will make an important contribution to cybersecurity. We encourage PIs to incorporate SBE research, perhaps in collaboration with SBE scientists who are experts in issues relavant to the research topic.

The SBE perspective does not seek to fund research that simply applies existing SBE science research and methods to cybersecurity questions. Instead, research from the SBE perspective uses the domain of cybersecurity to explore, develop, or "push the boundaries" of SBE science. Proposals submitted to SBE will be evaluated based on their contribution to the SBE sciences and to cybersecurity. They will be reviewed by SBE scientists.

Proposals that apply rather than contribute to the SBE sciences, such as human factors research, may fit into the Trustworthy Computing Systems perspective. The new SaTC solicitation does not change or diminish what was possible under the old Trustworthy Computing solicitation.

Slide 12:

Good SBE science research contributes to the basic SBE sciences by identifying generalizable theories and regularities and pushing the boundaries of our understanding of social, behavioral, or economic phenomena. We seek research that generalizes to a variety of domains, identifies the conditions under which generalizations hold, or provides an advance in SBE science methods. More inductive or interpretative approaches may contribute to the SBE sciences as well, especially if they set the groundwork for generalizable research or reveal broad connections. SBE / SaTC proposals should clearly state and elaborate how the proposed research will contribute to SBE sciences.

The focus can be at any level or levels of analysis.

Also, any SBE methodology can be used, including field data, laboratory experiments, observational studies, simulations, and theoretical development, among others.

Slide 13:

Given the fledgling state of SBE science research in cybersecurity, we welcome proposals for workshops and other opportunities for intellectual engagements.

Such proposals, however, should clarify how the efforts are likely to enable future SBE science contributions to cybersecurity.

Infrastructure-oriented proposals should include components that also contribute directly to research.

Research outside the U.S. can be funded. SaTC / SBE is primarily concerned with creating knowledge. This knowledge could be garnered outside the U.S. as well as inside, and it need not be focused on specifically American examples of cybersecurity challenges.

If you have questions about the SBE perspective, feel free to contact me at pmuhlber@nsf.gov

And now for the Transition to Practice Perspective, allow me to introduce Kevin Thompson…

Slide 14:

Thank you Peter. Good afternoon. The Transition to Practice perspective supports later phases of a research and development lifecycle, including applied research, prototyping, experimental deployment and early adoption activities. Transition to Practice complements basic research activities and the broad research agenda represented by the rest of the program. A proposal targeted to this perspective may build off existing and successful research results, in further developing and realizing useable capabilities. Proposers interested in proposing into this persepective should carefully read the text found in the Transition to Practice Perspective section of the program description, as well as the review criteria. Proposed activities in the Transition to Practice perspective should address how the work will impact the networks, systems, and other cyberinfrastructure supporting the NSF research and education community. In this sense, there is an emphasis on viewing end users as part of and members of the NSF community. Note also from the program description that proposals into this perspective are expected to describe goals and milestones.

Other review criteria specific to this Perspective include:

- The expected impact on the deployed environment described in the proposal.
- The extent to which the value of the proposed cybersecurity research and development is described in the context of a needed capability required by science and engineering, and potential impact across a broader segment of the NSF community.
- The feasibility, utility, and interoperability of the capability in its proposed operational role.
- A project plan that addresses in its goals and milestones the demonstration and evaluation of a working system in the target environment.
- Tangible metrics described to evaluate the success of the capabilities developed, and the steps necessary to take the system from prototype status to potential production use.

Any software developed in this program area is required to be released under an open source license.

Slide 15:

For proposers planning to submit a small or medium proposal into one of the other two perspectives, there is also a supplemental funding opportunity available for these types of activities and this is described under the Transitions *Phase section. The same themes and types of activities in the Transition to Practice perspective are found in the Transitions Phase, but the Phase applies only to proposals in the other perspectives. The phase option allows a proposer to address an additional part of work that carries their activities into development and deployment activities. Such proposals can submit as part of their supplemental documents up to a 5 page description of this proposed phase. For such proposals, it is important to note that the material in the 5 page supplemental description will be evaluated and reviewed only for consideration for additional funding. Put another way, a proposal into the Trustworthy Computing Systems or Social, Behavioral and Economic perspectives will be evaluated and reviewed along with other similar proposals as normal. For those proposals containing a Transitions phase, that material will not factor into the primary review of the proposal and will not factor into the final determination of the overall proposal. For such proposals receiving awards, a separate decision will be made on whether to fund the supplemental Transitions phase.

If proposers have questions specific to the Transitions to Practice Perspective or the Transitions Phase, they are welcome to contact me directly at kthompso@nsf.gov
And now, back to Sam

Slide 16:

Thank you. SaTC as you probably are aware of, has three categories of awards: Small, Medium, and Frontiers. Those of you who are familiar with Trustworthy Computing Program, or the CISE Core solicitations are probably wondering what happened to the Larges. The answer is simple: we've decided to super-size them. In the CISE directorate, Large awards have a limit of 3 million dollars, and we've replaced them with "Frontiers", or "Extra-Larges" which go up to 10 million dollars. In other words, you can now propose projects that are more than three times the size of a Large.

Smalls and Mediums remain the same, with Small awards having a limit of three years and a half million dollars, and Mediums up to 4 years and 12 hundred thousand dollars.

As usual, a researcher is not allowed to be a PI or co-PI of more than two SaTC proposals per financial year.

Slide 17:

Let's talk more about Frontier awards, and what we want from them.

In previous years CISE funded what were called "Center-Scale" projects, which were, like Frontier awards, larger-than-Large awards. These awards are now ending or transitioning. We've been pleased with their success, and therefore wish to fund more sizable projects. Here are three examples of what can be accomplished by a comprehensive effort.

The CCIED project set out to investigate large-scale internet-based pathogens, such as botnets. They managed to passively monitor more than 1% of the routable internet address space, so they could detect and observe how malware is behaving. Some of the most interesting research results that have come out of this project were from an unanticipated direction: they have done significant work in understanding the economics of spam and how malware is monetized. This provides insights into the motivations and goals of the people behind current internet threats, and how we might reduce or avoid these conflicts.

The ACCURATE project investigated voting technology. They've had a large impact by discovering and preventing voting issues. Their work has necessarily been highly multi-disciplinary, as they've had to consider usability not only for traditional users of technology, but for the entire voting population. They've also had to consider legal issues across the many conflicting jurisdictions in the country.

The TCIPG project investigated the resilience of the power-grid to cyber-attacks, and included building a testbed for power grid hardware and software. This project has now transitioned to being funded by the Departments of Energy and Homeland Security, and serves as a nice example of how NSF seeds basic, long-term research that transitions into application-based work supported by other entities.

Slide 18:

So, what we'd like to see in Frontier proposals is a long-term vision, which requires a cohesive effort that is not simply a collection of smaller activities. Such research could be multidisciplinary, but does not need to be: a successful Frontier project could also be a deep, intensively focused effort on a single problem in a single discipline. However, Frontier projects should take into account NSF's educational mandates, and discuss how the proposed research results will be able to impact deployed systems.

There is one procedural matter that we should mention here: a Frontier proposal cannot be submitted solely to the SBE perspective. That is, although a Frontiers proposal can include the SBE perspective, the SBE perspective cannot be the only perspective.

Because of the magnitude and effort required to write a successful Frontiers proposal, we strongly advise researchers who are considering submitting such a proposal to consult with a Program Director before submitting.

And now, let's turn to Andrew Pollington, who will discuss the contribution of the Mathematical Sciences to the program.

Slide 19:

Thank you Sam. Good Afternoon

New mathematical and statistical methods offer possibilities of enhancing existing methods in security and the analysis and detection of threats.

The Division of Mathematical Sciences is interested in proposals in all of the SaTC perspectives.

Number Theory has been very successful in producing codes which, at least up to now, have proven difficult to break.

What mathematical and statistical tools might one employ to this end in the future? For example: Can one provide a secure environment if a quantum computer is built?

What mathematical and statistical tools would be useful in this area?

Mathematics and Statistics offer tools that can be employed in diverse areas where they were not previously considered to be of relevance.

For example, over the past ten years, topological methods have been employed to study the Statistics of large data sets (called Topological Data Analysis) introduced by Gunnar Carlson at Stanford, where the topology of point clouds at different scales is analyzed through the use of topological invariants. Such methods have found application in a number of areas.

Another place where one might look for tools is in the recent work done in Mathematical Biology, on large networks, random processes and stochastic modeling.

So we ask:

What statistical and mathematical tools can be brought to bear on the large data challenges of threat detection, in the modeling of networks, and in general in aiding the making of a Trustworthy Cyberspace? Thank you.

Back to you Sam.

Slide 20:

Thank you.

Since our solicitation was published, we have received a number of questions.

One of the most common questions is the relationship between SaTC and the various directorate core programs, and how a researcher should decide where to submit their

proposals. This is a natural question, because our research field naturally overlaps with many others.

What you should do, as a researcher, is to consider the research field that your work will impact, and not its motivation. For example, a secure networking proposal that uses standard security techniques but advances the field of networking should be submitted to the NeTS program, not SaTC. A secure networking proposal that is suitable for SaTC is one in which the security field itself is advanced. Similarly, a project that advances the field of program analysis to discover software bugs should not be submitted to SaTC just because some bugs happen to be security bugs. On the other hand, a project which used standard off-the-shelf program analysis techniques will be funded by SaTC if it uses these techniques to make new contributions to system security or privacy.

Now we know that deciding between programs can be difficult, and NSF program officers can share or transfer proposals between programs to ensure the best merit review. However, we recommend that researchers consider carefully their options, to ensure that their proposal does target the solicitation it is submitted to.

Slide 21:

Now, we've discovered that many proposals do not fare well in the review process because they have a common flaw: not making it clear what the problem they are attempting to solve actually is.

SaTC's aim is to protect cyber-systems. As I've already said, in the current world it is not always clear the aims or motivations of the people we are protecting our systems against, or even if said people consider themselves to be our opponents. This situation makes it even more important, not less, when writing your proposal to clearly state what problem you are attempting to solve.

Most proposed projects are attempting to defend systems against some threat, and it is important to make it clear what that threat actually is. What are the aims, motivations and abilities of the people behind the threat? Are you defending against a nation-state, or against asocial teenagers? Are you being attacked by people attempting to transfer money from your bank account, or to use your machine to send spam from? The traditional term for this is the "threat model", which is somewhat misleading since threat models are typically informal. The idea is that your proposed work can only be evaluated in relationship to the threats that you are considering. Making this clear to the reviewers is important.

Slide 22:

Another topic we wish to discuss is international cooperation. Not only do attackers not respect international boundaries, but for various reasons many centers of expertise are isolated

geographically, and this hinders research. SaTC, and NSF in general, support international collaboration.

Supplements are available that support international activities, such as travel, visitors and workshops. The situation is more complicated if a project needs co-funding with a non-US agency. Because we are a US federal governmental agency, the general rule is that NSF will fund the US participants and the other agency will fund participants from its own country. Arranging for proposals like this to be co-reviewed can be involved, so if you are thinking of submitting such a proposal, you should talk to a Program Officer about it as soon as possible.

Slide 23:

We've set up a mailing list for SaTC, which we will use to send infrequent notifications about events that might be useful to researchers in our community. In order to sign up to this list, you should send email to listserv@listserv.nsf.gov with the message shown on the slide.

Also shown here are the names and email addresses of all the SaTC Program Directors. If you have specific questions about the program, feel free to contact the Program Director whose research area is most relevant.

And now, we'll take questions from our audience.

Questions and Answers:

Facilitator: We will now begin the output -- we'll now begin the question and answer session. If you have a question, please press star one on your phone. Please unmute your phone and record your name at the pump. One moment please only wait for the first question.

Facilitator: Our first question comes from [Indiscernible name]. Go ahead, sir. Your line is open.

Question/Speaker 1: Yes, so my question concerns the…the question is about how the international Corp. and the interdisciplinary are allowed to be mixed with each other. So, is it advisable that one would have international collaborator who offers a perspective, for example, of social behavioral sciences while you space collaborator is, for example, offering a computer science perspective? Is that allowed or do the international collaborator would that have to be of the same discipline? That is my question.

Answer: Certainly, it is possible to do that. Once again, be aware that NSF generally is not able, by law to fund international operators directly. Therefore, if you have to arrange cooperation from another non-US agency. Please let us know even before you submit the proposal so that we can try to make the appropriate arraignments.

Speaker 1: Thank you.

Facilitator: Our next question comes from Michael Writer. Go ahead, your line is open.

Question/Speaker: Great. Do you anticipate allowing transition add-ons in years following the award of the proposal? For example, in the second year where it looks like there is a good opportunity to try to transition a technology to practice?

Answer response: Mike, was the question specific to the transition phase?

Question/Speaker: Right, for these transition addendums to proposals that you were suggesting--could you do those in later years?

Answer reply: Right, that is one option. Again, it will be considered for supplemental funding only.

Speaker reply: Thank you.

Facilitator: Our next question comes from Victor [Indiscernible last name].

Facilitator: Go ahead, your line is open.

Question/Speaker: Hi, this is a much more prosaic question. Is there a place where we can download the slides?

Answer reply: There will be.

Speaker response: Okay.

Answer reply: We will be posting it on the CISE website.

Speaker response: Thank you very much.

Answer reply: You are welcome.

Facilitator: Once again, if you have a question, it is a star one on your touch tone phone and record your name at the prompt. One moment for the next question, our next question comes from Gary [Indiscernible last name] line. Go ahead, sir. Your line is open.

Speaker question: Yes, can you say a little bit about the review process in terms of what sorts of backgrounds reviewers will have? Will the reviewers of the SBE proposals be primary from the social and behavioral sciences for example? Or what will they look like?

Answer reply: Yes, the reviewers for the SBE proposals would be from the SBE sciences. In general, each proposal must be submitted with an indication of what the primary area is for that proposal. And once we know that the primary area is, then we will definitely have people in that component. And also any subsidiary areas will also get reviewers for that as well.

Facilitator: Once again, if you have a question, please press star one on your touch tone phone and record your name at the prompt. One moment, we will see if we get any more questions in.

Facilitator: Once again, we have a question from Gary [Indiscernible last name]'s line. Go ahead, your line is open.

Speaker question: Thank you, I had understood that we were going to be receiving an FAQ (frequently asked questions) list. Maybe it has been sent and I just missed it? But has it been sent or is there one coming at some point?

Answer reply: There is one coming, it is currently going through the review process and so it should be posted shortly. And we will also send it to the SaTC mailing list.

Facilitator: Our next question comes from Victor-- [Indiscernible last name].

Speaker question: This question is a little less prosaic. How risk prone are you in terms of thinking about projects that could be very difficult to take out but aren't possible to test without resources?

Answer reply: Basically, NSF tries to fund transformative research. Basically, if a certain percentage of our projects do not fail, we probably have not done a good job of selecting them appropriately. So, as long as is the reward project is commenced with a risk, that is what we mostly look at.

Speaker response: Great, thanks.

Facilitator: Our next question comes from Bruce McMillan's line, go ahead, your line is open.

Speaker question: Hi, the slides talked about focusing on cyber security, but what about security in areas of cyber physical systems? Not cyber, not physical separately, but the combined aspect?

Answer reply: Certainly. In fact, issues such as the security of the power grid or medical devices or automobiles are fields in which we are actively hoping to receive submissions in.

Speaker reply: Thank you.

Facilitator: Our next question comes from [Indiscernible name]'s line.

Speaker question: Hi, you said that we could apply to multiple perspectives, yet we should pick one primary perspective? I guess this is a more mundane question, but can we indicate the secondary perspective to the title? By putting the appropriate keyword? How would we indicate it easily?

Answer response: I guess I got the privilege of looking really closely at that component of the proposal, so I will try to answer here. The title of the proposal is supposed to list the perspective from which that proposal comes. The first list of prospective, so, for example, if the proposal is an SBE perspective, you would put SBE first, and then a space, and then the next perspective. So let's say it is SBE and trustworthy computing. So, you're basically put both. The first one is the primary, and then anything after that is considered secondary. So, there is no explicit secondary for the second item, it is just all the rest are secondary to the primary prospective.

Speaker reply: Thank you.

Answer reply: You are welcome.

Facilitator: Our next question comes from [Indiscernible name]. Go ahead, your line is open.

Speaker question: Part of my question was answered in the last response. But, if we were to submit form -- for the trustworthy computing, which is DCISE should we also identified all three did you have listed that works in network systems, theory and foundations, human centric and artificial intelligence should we identify that too—which is the most closest to our proposal? [Indiscernible - heavy accent]

Answer reply: No, basically just say what prospective is sufficient. We don't really want to drill down any further--especially titles of proposals.

Facilitator: Our next question comes from Roy [Indiscernible last name].

Speaker reply: Yes, hi. I was a little bit confused by the due dates. So, for example, the small is due on January 11 according to your slides. But, I have some other announcements that says that something is due on January 4. What is it that I'm confused about?

Speaker reply: I have an announcement from NSF that says January 4.

Answer reply: I am not sure where you are seeing the January 4. The only thing that I could think of is that each of the types of proposals actually has a window. So, small projects you cannot submit before January 4 and the window closes on January 11. So, that might be where you see the date.

Speaker reply: Oh, I see. Okay, thank you.

Facilitator: Our next question comes from Dave Archer's line. Go ahead. Your line is open, sir.

Speaker reply: Hi, I have a follow-up question regarding proposal evaluation. For the submissions in the transitions to practice perspective, what can you tell me about the backgrounds of those evaluators will have and how they might go about evaluating such proposals?

Answer reply: I will give you a general answer. It is part of our job to bring experts in the community in as peer-reviewers, and I think in that context, you can expect NSF to have as part of their peer reviewed process people who have some level of experience and expertise as reflected in the review criteria for that perspective.

Facilitator: Once again, if you have a question, please press star one on your touchtone phones. Please [indiscernible] your phone and record your name at the prompt. Star one to ask a question. One moment, we will see if we get any more questions in.

Facilitator: Our next question comes from Andrew [Indiscernible last name]. Go ahead, sir. Your line is open.

Speaker question: Hello, this is a question again about the perspective in the CISE program. And that is, is there a relation between the multi-perspective approach and the size of program? Basically, the

question is, can we apply for the small type of program -- project, but using this multi-perspective approach? If our project has some kind of double [Pause] approach?

Answer reply: Okay, so let's understand the question you are asking whether a small proposal can have multiple perspectives?

Speaker reply: That is correct.

Answer reply: Certainly. The only thing you need to take into account is if you have multiple PI make sure that each of them has appropriate level of funding.

Speaker reply: Okay, thank you.

Facilitator: I am showing no further questions at this time.

Presenter: Okay, then in closing,thank you very much for joining this webinar. We look forward to your participation in the SaTC program. Thank you.

Facilitator: This concludes today's conference, thank you for your participation, you may now disconnect.

[Event Concluded]