Following are responses to requests from Daniel Shingledecker of BITS for clarification of items in the proposal submitted by ProvenSecure Solutions LLC

1. ***In the Technical Challenges and Risk Mitigation section, you discuss possible challenges in securing MFA systems. How will you mitigate these challenges using the MrE methodology, and how will you determine if it can be accomplished?***

   We will quantify multi-factor authentication risk and use that quantification to allow the minimization of false accept and false reject rates with the minimum authentication steps necessary. Factors are solicited and added to the model until the imposter or the correct user is sufficiently excluded. Any desired degree of risk mitigation can be achieved, provided sufficient factors are available. The improved risk assessment combining probabilistic factors over pass/fail factors for risk-based authentication will be analyzed. Comparison of authentication time with fixed factor risk-based authentication will be made. The benefits of using passive factors will be considered.

   MrE helps mitigate these challenges by looking at not only the risk, but the uncertainty or precision of our estimate as well. Since it can handle data as well as constraints (unlike Bayesian or Maximum entropy methods alone), it has the flexibility to make assessments with more information sources and in noisier environments than traditional MFA systems. MrE will be employed dynamically so as to estimate the best possible answers in a bounded amount of time. Comparison of accuracy between MrE and other methodologies will be made.

2. ***Can you please describe a typical use case where RMM would be beneficial to any authentication system?***

   Any multi-factor risk-based authentication system will benefit from more accurate risk assessment that also may take into account the quantity of uncertainty involved. The average authentication time can be reduced since only as many factors as are necessary will be solicited and additional factors may be solicited where the specific discrimination obtained by the “normal” number of factors proves insufficient to achieve the level of risk mitigation required by policy for the current access. Thus, the RMM is case independent.

3. ***During the test and evaluation process, CFT engineers will attempt to mimic the performer's environment as much as possible to facilitate accurate validation of exit criteria. Could you please elaborate on the development and test environment that you will be using? Could you please list various tools and platforms that you will leverage for performing testing?***

   We have determined that our development environment will be Microsoft .NET Framework based and will rely heavily on Microsoft’s Infer.NET (a probabilistic inference toolkit that is written in F#). The functionality in this SDK is not available in the Open Source world, and replicating it would be vastly beyond the scope of this effort. Programming will be done in

"C#" to facilitate access to Infer.NET.

We are investigating at this time whether we would be able to set up a linux-based environment that supports these tools. (We know .NET Framework is supported; we are still investigating whether Infer.NET is supported as well.) A linux environment would be our preference, but in the event the linux environment is not feasible, we will develop in a Windows environment. The selection of third-party authenticators may be influenced by this decision as well. We should be able to complete this determination within the next couple days, and will inform you as soon as we're sure which platform will be used.

The nature of the testing -- recording and analyzing attempts by humans to be authenticated (presumably for access to some asset) -- does not lend itself to automated testing, hence we do not anticipate the need for testing tools.

4. ***How will the white paper in Milestone 1 influence the remainder of the project? What impact will the research of Bayesian and MaxEnt methodologies have on developing the MrE tool?***

This new method, MrE, is capable of reproducing every aspect of orthodox Bayesian inference and proves the complete compatibility of Bayesian and Maximum Entropy methods. Therefore, we can use the best of both worlds in MrE. However, it also opens the door to tackling problems that could not be previously addressed by either the MaxEnt or orthodox Bayesian methods individually to provide a more complete tool for analysis. Even more significantly, MrE allows for a dynamic and continuous combination of the two approaches, to enhance inference and learning. However, MrE has not been applied to the security and authentication domains. The white paper in Milestone 1 will provide the foundation for the rest of the project in the design of RMM and the domain model. It will be shown how the MrE approach gets at least as reliable as other results in a bounded time.

5. ***You mention cloud services in your material costs. What cloud services are you planning to utilize and can you provide details as to how you will be using the services? Will MFA be available as a cloud service?***

We anticipated the need to contract for virtual machine and file-server capabilities to house the development environment. ProvenSecure Solutions, LLC does not have a physical data center. Our members are geographically dispersed; cloud-based virtual systems make the most sense for everything we do. It is our eventual aim to commercialize some form of multi-factor authentication with the MrE-based Risk Mitigation Measure (RMM) at its core. That may well be available as a cloud service, but delivery as a cloud service is not within this project's scope. Our intent here is to simply demonstrate the capabilities of an MrE-based Risk Mitigation Module within a multi-factor authentication package. We are currently determining which virtual services vendor will best fit our needs; we will provide details and quotes within the next couple of days.

6. ***Can you please provide a list of the commercially available authentication products that you intend to use during the course of your effort?***

   We anticipate utilizing the ATT VoiceVerification API now being made available in the ATT foundry and soon to be offered commercially. A number of other factors and authentication systems from various vendors are being considered, such as the offerings of Authentify, Mega AS, BioID, DigitalPersona, M2SYS, Betaface, PhoneFactor, DuoSytems, ATT Toggle, and many more. In addition, "simple" password, sms messaging and "knowledge factors" are available to us as potential authenticators, as are other commercial products (some of which ProvenSecure Solutions, LLC has relationships with). Final selection of one or two of these will be undertaken as part of the initial specification process in Milestone 2 of our revised schedule. If cost management is a significant issue, this can be taken into account when the final decisions are made during Milestone 2 work.

7. ***Regarding materials, please provide supporting quotes for the proposed material.***

   As indicated in our response to question 3, our preference is to develop in a linux environment utilizing .NET Framework and the Infer.NET SDK. These are no-cost technologies. If a suitable no-cost C# compiler can be identified, we will use that as well. We are in the process of finalizing the linux vs windows choice and subsequently the selection of specific development tools. We should be able to provide quotes for any purchases required within a day or two.

8. ***Travel costs will not be added to the agreement at this time. If Travel is required by DARPA, the appropriate funding will be added at that time. Please concur.***

   We understand and concur.

9. ***Vendor Registration. Please complete the attached and return along with response to the above.***

   Attached.

10. ***If you have any questions please let me know.***

    If you have more requirements we ought to be aware of, please let us know. Additionally, any specific information you can provide about authentication scenarios or use cases that might be of particular interest to DARPA would be useful in helping us fine tune our requirements as we begin development efforts.