OMB Control No. – 0693-0043 – NIST Generic Clearance for Usability Data Collections

NIST, ITL, Use of Cryptography Data Collection

1. **Explain who will be surveyed and why the group is appropriate to survey.**

   As part of an in-depth interview study of how software developers use cryptography in the programs that they are developing, the Visualization and Usability Group (VUG), of the Information Technology Laboratory (ITL), of the National Institute of Standards and Technology (NIST) intends to recruit 25 participants. Participants will be individuals who have first-hand technical knowledge of the domain area. Participants will be recruited from several different sources: a list of developers who previously completed a NIST usable cryptography survey and expressed interest in being interviewed, NIST partner mailing lists, and recommendations from NIST personnel. The information being requested is not available from public sources, such as software documentation or an inspection of open source software code.

   The purpose of this project is to investigate how developers test cryptography in their software, the factors that are used to plan testing procedures, and the challenges experienced in testing cryptographic products. We believe that by collecting this data we can identify and describe the process by which cryptography is tested in software, which will assist NIST in creating recommendations for making it easier for developers to use encryption correctly and securely and robustly test cryptographic products.

2. **Explain how the survey was developed including consultation with interested parties, pretesting, and responses to suggestions for improvement.**

   The interview questions were developed and refined based on discussions with cryptography experts at the National Institute of Standards and Technology (NIST). This is the first interview of its kind that we are aware of.

3. **Explain how the survey will be conducted, how customers will be sampled if fewer than all customers will be surveyed, expected response rate, and actions your agency plans to take to improve the response rate.**

   Participants will be recruited via email. Once an individual agrees to participate, an interview appointment will be scheduled at either a particular location agreed upon by both the participant and researchers, or via video teleconference or phone. The data will be collected through semi-structured interviews. The interview includes 20 questions and will be at most 60 minutes in length. The audio of the interview will be recorded and transcribed.

   We expect the response rate to vary by recruitment group. We expect an 80% response rate from previous survey respondents who expressed their willingness to participate in the interviews, and a 50% response rate from NIST partners.

4. Describe how the results of the survey will be analyzed and used to generalize the results to the entire customer population.

We intend to use the qualitative data analysis technique of grounded theory to create a list of developer testing practices, concerns, and techniques. We will compare the qualitative responses across different kinds of developers and organizations to identify commonalities and differences. From these results, we will plan any subsequent phases of our research efforts.

There will be no collection, storage, access, use, or dissemination of personally identifiable information from the interviews. As stated in the provided Information Sheet, participants will be assigned a participant reference code that will be associated with their responses. Data will not be linked back to a respondent. NIST will not create or keep a list that links the participant reference code to a participant.