

INFORMATION SHEET

Project Title: ITL-16-0011 - Usable Cryptography a Survey

Key Researchers:

NIST Principal Investigators: Mary Theofanos, Phone: (301) 975-5889, Email: mary.theofanos@nist.gov
Simson Garfinkel, Phone (301) 975-8516, Email: Simson.garfinkel@nist.gov

RESEARCH DESCRIPTION

This study is being performed to understand how organizations design and implement crypto applications. It will investigate organization's use of cryptography by determining: sources of crypto implementations, testing and evaluation approaches, challenges when incorporating crypto in products, and standards used in developing products. The research is funded and conducted by the National Institute of Standards and Technology (NIST).

Requirements for Participation

In order to participate in this research project, you must be at least 18 years old and have experience in developing products that include cryptography.

Study Procedures

You will be given a survey consisting of 12 questions. All of your questionnaire responses will be recorded without any identifiers. The survey should take you no more than 20 to 30 minutes.

We expect to have approximately 1,000 participants complete this phase of the study.

Confidentiality:

You will be assigned a participant reference code that will be used for all data in this project. Your identity will be protected to the extent permitted by law, including the Freedom of Information Act. The Office for Human Research Protections (OHRP) of the U.S. Department of Health and Human Services, members of the NIST Institutional Review Board (IRB), appropriate NIST researchers, and other appropriate Federal employees may review the records of this study. The study data will be used by the research team to develop guidance on cybersecurity and privacy training and administration. All of the data from the survey will be recorded without identifiers. Your data will not be linked back to you in any way. NIST will not create or keep a list that links your reference code to your name or other identifying information. In the freeform questions of the questionnaire, do not include information that may identify you.

Voluntary Participation

Your participation is voluntary. Refusal to participate will involve no penalty or loss of benefits to which you are otherwise entitled. You are free to withdraw from the study at any time during the experiment, without penalty or loss of benefits to which you are otherwise entitled. If you withdraw from the study, your data will not be removed from the study.

Potential Risks and Benefits

The risks during performance of the study activities are minimal and not greater than those ordinarily encountered in daily life or in responding to a routine survey. You will not benefit directly by participating in the study. The long-term benefits of this study to society should be improved cryptographic implementations.

Contact Information:

For questions regarding this study, please contact Mary Theofanos at 301-975-5880, maryt@nist.gov or Simson Garfinkel, (301) 975-8516, simson.garfinkel@nist.gov. For questions regarding your rights as a human subject, please contact Anne Andrews, Director, NIST Human Subjects Protection Office, at (301) 975-5445 or anne.andrews@nist.gov, or Laura Baxter in the Office of the Chief Counsel for NIST, at 301-975-5622, or laura.baxter@nist.gov. Any research-related injury during the study should be reported to Mary Theofanos at 301-975-5880, maryt@nist.gov or Simson Garfinkel, (301) 975-8516, simson.garfinkel@nist.gov.