DOC/NIST Generic Clearance for Program Evaluation Data Collections
OMB Control # 0693-0033
Expiration Date 10/31/2012

NIST/RTI Economic Analysis of the U.S. Cyber Security Infrastructure Supporting Statement

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

RTI International[1] (RTI) will field a survey designed to aid and inform the National Institute of Standards and Technology (NIST) and the broader government community in the planning of future investments in cyber security. This survey represents the second phase of an ongoing data collection phase for program evaluation (OMB Control #0693-0033). For this effort, RTI will field a survey to active professionals engaged in activities related to cyber security. This includes executives and managers that are decision-makers in any information security activity and are responsible for meeting governance requirements related to information security. These stakeholders manage information security policy, spending, and compliance/auditing.

Given the measurement and interoperability problems in cyber security, NIST can offer unique expertise in fostering increased standardization of cyber security technology characteristics and process attributes. For example, NIST currently develops Federal Information Processing Standards (FIPS) Publications and Special Publications Series documents that are compulsory for federal agencies and provide guidance to private-sector organizations. NIST is supporting this RTI data collection effort so that future government investments in cyber security can be made based on the estimated economic impact to the U.S.

In addition to NIST's role in cyber security, the White House has expressed a strong desire to improve cyber security by focusing and coordinating cross-agency investments. The White House report *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (2009) provided an explicit set of high-level, policy-oriented recommendations for improving cyber security, including improved coordination of government cyber security activities and increased collaboration between the government and private sector. This report identified as particularly important the finance and health care industries, critical infrastructure (e.g., public utilities), and any industry with valuable intellectual property. RTI's study and data collection efforts are aimed directly at these industries and several others, which were selected based on the potential economic impact of improved cyber security infrastructure.[2]

As described in the previous OMB submission, the survey that RTI will conduct will supplement a series of interviews with individuals who manage cyber security investments and operations at companies in the following industries: finance, health care, manufacturing, retail, telecommunications, and utilities. The information gather during these interviews helped to inform the development of the survey instrument that will seek to quantify the cost savings and quality benefits associated with an improved cyber security technology infrastructure.

The specific target population for these interviews will be individuals that represent the Information Technology Security staff at all U.S. organizations with more than 500 employees – i.e., medium to large

[1] RTI International is the trade name of the Research Triangle Institute.

[2] These industries were selected based on a combination of metrics including current spending on IT, reported and estimated IT security spending and losses, and systemic risk to the U.S. economy.

sized businesses. These employees were identified because they have the highest understanding of cyber security costs and risks, and they are most likely to understand the effectiveness and efficiency of cyber security policies. They will be able to enumerate quantitative data such as size of cyber security budget, specific areas and amounts of spending, and number of cyber security attacks; moreover, they will be able to quantify potential reductions of threats and improvements in spending efficiency in a counterfactual case. Smaller companies will not be surveyed as their needs are substantively different and would require a separate methodology, survey instrument, and analysis.

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

The survey was developed by a team of RTI technology economists and external technology consultants, including Dr. Douglas Reeve at North Carolina State University. The survey was constructed following a period of data collection via case study interviews. During these case studies, the team has spoken with a total of 25 professionals from private companies and industry consortia in the manufacturing, health care, retail, finance, telecommunications, and electric utilities industries. As mentioned in OMB Control #0693-0033, these informal interviews provided direct input in the development of the formal survey.

After a series of internal drafts, we developed a field survey which we pre-tested with interviewees from our case studies. During the pretesting phase, respondents answered all important questions and provided feedback regarding the ambiguity and difficulty of the questions. In addition to pretesting, we consulted with the client for additional feedback on the content of the survey.

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.

RTI will field an internet survey targeted to information security executives and managers in order to identify cybersecurity infrastructure needs. Customers will be identified and sampled with the aid of industry consortia and current contacts from the case study interviews. The team is working with industry groups and consortia in several IT intensive industries as well as several cross cutting groups in order to solicit respondents. Organizations with which we are in preliminary talks include Information Systems Audit and Control Association (ISACA), National Electrical Manufacturers Association (NEMA), National Association of Manufacturers (NAM), and North Carolina Healthcare Information & Communications Alliance (NCHICA), Internet Security Alliance (ISA), and the National Electric Sector Cyber Security Organization (NESCO).

We assume that most of the target respondents will be affiliated with industry consortia. Since many industry consortia have privacy and/or information security workgroups, we will have channels to reach information security executives and managers in those member organizations. There is no directory or list that provides a comprehensive list of this population. However, we assume that over 80% of information security decision-makers in our target company sizes are connected with one or more of our industry association partners. Therefore, we assume that soliciting participation via consortia will give us maximum exposure to information security professionals. All individuals notified will be allowed to participate in the web-based survey.

After receiving OMB approval, the finalized survey will be hosted on RTI's encrypted servers. Our security policy will ensure that information provided by respondents is secure. Ideally, the survey will be operational in mid-November. Thereafter we will ask industry associations and consortia to send information out through listserves and post on relevant websites. If our participation rates are not sufficiently high, we will request that additional follow-up emails be sent out to companies.

Total respondent time is estimated to be 20 minutes, including reviewing the survey instrument and directions. If the respondent indicates wiliness to be contacted, RTI may send follow-up questions by email. The survey and its results will be of great interest to respondents because of the potential effect on NIST's technology and standards investment activity.

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

The survey will include questions on industry, revenue, and number of employees in a respondent's organization. We will extrapolate survey data using total US employment or revenue by industry in firms with more than 500 employees. This way we can accurately "scale-up" the sum of the quantitative results to an estimation of the economic impact on all medium to large U.S. companies.