COMMENTS ON NOTICE OF INFORMATION COLLECTION
Request for New Information Collection - Public Credentialing and Authentication Process
76 FR 31671
DOCUMENT NUMBER 2011-13409
U.S. SOCIAL SECURITY ADMINISTRATION
OFFICE OF MANAGEMENT AND BUDGET

RESPONSE FILED BY:
U.S. PUBLIC POLICY COUNCIL OF THE ASSOCIATION FOR COMPUTING MACHINERY

On behalf of the U.S. Public Policy Council (USACM) of the Association for Computing Machinery (ACM) we are submitting the following comments in response to the Notice of Information Collection by the Social Security Administration (SSA) for its public credentialing and authentication process.

With over 100,000 members, the Association for Computing Machinery (ACM) is the world's oldest and largest educational and scientific computing society. The ACM U.S. Public Policy Council (USACM) serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology. Our comments are informed by Congressional testimony from our Vice Chair, Annie Antón, connected to identity and authentication.[1] Should you have any questions or need additional information, please contact Cameron Wilson, our Director of Public Policy, at 202-659-9711 or at cameron.wilson@acm.org

Stronger authentication is an important part of ensuring trust in online transactions, for both the provider and recipient of services. The SSA should take measures to encourage this trust as it works to provide more services online. Stronger authentication measures should also include implementation of best practices in data collection and data management, as suggested by Fair Information Practice Principles. As the SSA moves forward with developing and implementing this new public credentialing and authentication process, we suggest that they keep the following things in mind.

Much personally identifiable information can be collected from other sources. While the information the SSA proposes to collect can help to better identify an individual, much of this information can be gathered from other sources. That makes it much easier for people to represent a different identity when registering online. The identity quiz referenced in the notice will be an important part of confirming identity. Unfortunately, some quizzes to confirm identity suffer from the same problem – asking for information that can by obtained via publicly available information. USACM checked the recently deployed E-Verify 'self-check' program when Dr. Antón was preparing her testimony (page 5). In testing this identity verification system we found:

> "In our experience, the self-check system requires an individual to submit his or her name, address, SSN and date of birth to access the system—information that is easily available to individuals wishing to verify someone else's employment eligibility. The secret questions cannot truly be considered "secret" given that the answers to these questions are available via public records: home addresses are available via whitepages.com; age range is available via whitepages.com; county or city in which one resides is available via Google maps; price paid for a home is available via local county tax records websites."

The SSA should take care to ensure that the components of its identity quiz do not rely on similar information that could be readily obtained by people besides the ones connected to this personally identifiable information.

The cell phone confirmation of activity is not a second factor of authentication. Authentication is a process of validating a claimed identifier and its association with the appropriate item or person. As described in the notice, people who opt for an enhanced account can receive a text message on their phone each time they log-in to the SSA

---

[1] Testimony of Ana I. Antón before the House Subcommittee on Social Secuirty, April 14, 2011, http://usacm.acm.org/images/documents/everify_Anton_USACM_testimony_final.pdf

website. This serves to notify people when their account is being accessed. But it does not serve as an additional means for SSA to validate that the person accessing the account is indeed the person associated with the account. If, for example, the text message provided a code or other phrase to enter into the SSA website (or text to another number) to allow access, then this would constitute a second factor of authentication. That would place an additional burden on visitors to the site, but not one related to information collection. Other things that could be used for a second factor of authentication fall into the following categories: something known by the person (password or other information only they would know), something possessed by the person (a token), or something about the person (a physical characteristic or location).

The above recommendations would apply to any information collection or other program that is connected to identification, credentialing, and authentication of identities. Many of our members address these issues in their work and research, and we would be happy to connect you with them to discuss these comments and any related issues.