acm
The Association for Computing Machinery

COMPUTER PRIVACY EXPERT WARNS OF GROWING RISKS TO SOCIAL SECURITY NUMBERS

USACM's Antón Proposes Actions to Prevent Identity Theft

NEW YORK, June 21, 2007 - At a Congressional hearing today on protecting the privacy of social security numbers, Ana I. Antón testified on behalf of the U.S. Public Policy Committee of the Association for Computing Machinery (USACM) that the theft of social security numbers has become the primary tool for stealing an individual's identity, enabling criminals to unlock access to credit, banking accounts, and other services. Dr. Antón, an advisor to the Department of Homeland Security's Data Privacy and Integrity Advisory Committee and a member of USACM, proposed policies that combine business procedures and information technology to help protect social security numbers (SSNs) and reduce the nation's reliance on them for personal identification. She urged Congress to strengthen the privacy of SSNs to prevent the resulting fraud that has become increasingly commonplace.

Dr. Antón, an associate professor of Software Engineering at North Carolina State University, noted that more than 36 million Americans have had their identities stolen since 2003. In addition, over 155 million personal records have been compromised since 2005, including the massive data breach in 2006 that resulted from stolen laptop computers containing the SSNs of 28 million veterans.

"Two key factors have enabled the explosion of identity theft in today's environment. One is the common use of SSNs as a de facto national identification number; the other is current computing technology that enables the collection, exchange, analysis, and use of personal information on a scale unprecedented in the history of civilization," said Dr. Antón, who is also director of ThePrivacyPlace.org, a privacy research center for North Carolina State University, Purdue University, and the Georgia Institute of Technology. She said that when paper records were used for personal information that included SSNs, they required some effort to find, copy, and disseminate, but the spread of inexpensive computing technology has made it much easier to find, use, and exploit such information for fraudulent purposes.

Dr. Antón noted that privacy problems with SSNs stem from their convenience for tracking individuals across public and private records, which leads them to be used as both an identifier and an authenticator. An identifier associates a label with something in a specific group - such as an individual's name, while an authenticator is used to verify that an identifier is valid - such as a password, fingerprint or password. She said using SSNs interchangeably confuses the role of these processes and makes SSNs much more valuable for stealing someone's identity. In addition, because SSNs are so readily available, they are not an adequate means of either identification or authentication, she testified.

Speaking before the Subcommittee on Social Security of the U.S. House of Representatives Committee on Ways and Means, Dr. Antón urged banks, credit agencies and government agencies to require strong proof of identity, such as passports, military IDs, or licenses with a photograph to verify personal identity. "Once that is established, a secondary authenticator, such as a secret shared password or PIN can be used for subsequent transactions. This approach provides extra layers of security, and should help assure the public that the security and privacy of their information is being taken seriously," she said.

To provide an incentive to move away from the SSN as an identifier, Dr. Antón added that there should be no penalty or discrimination for someone who will not provide this information when conducting business, unless required by law to disclose it. She said this approach is consistent with advice from the U.S. Federal Trade Commission on protecting against identity theft.

Dr. Antón also proposed prohibiting the display of SSNs in public records, and redacting them from these records. She offered several additional actions to reduce the use and exposure of SSNs including:

- Requiring transmission of records or documents containing SSNs and other personally identifiable information to be secure or encrypted
- Requiring electronic security for files and devices containing SSNs
- Eliminating SSNs as the primary key in databases, and substituting a unique number generated by the database management system.

Dr. Antón is a co-founder and co-director of the NC State University E-Commerce Studio, a lab for management and computer science graduate students to develop Web-based e-commerce applications for industrial partners. She is an associate editor for *IEEE Transactions on Software Engineering* and a member of the International Board of Referees for *Computers & Security*, published by Elsevier. She was named the "Woman of Influence in the Public Sector" in 2005 by CSO Magazine & the Executive Women's Forum.

The complete testimony from Dr. Antón for today's hearing is available on the USACM Web page at
http://www.acm.org/usacm/PDF/SSN_Anton_USACM_testimony.pdf

About ACM
ACM, the Association for Computing Machinery http://www.acm.org, is an educational and scientific society uniting the world's computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

About USACM
The ACM U.S. Public Policy Committee (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. Supported by ACM's Washington, D.C., Office of Public Policy, USACM responds to requests for information and technical expertise from U.S. government agencies and departments, seeks to influence relevant U.S. government policies on behalf of the computing community and the public, and provides information to ACM on relevant U.S. government activities. USACM also identifies potentially significant technical and public policy issues and brings them to the attention of ACM and the community.