

Federal Computer Week

Personal data requirements raise eyebrows

Privacy advocates puzzled by DHS ID card

- By [Alice Lipowicz](#)
- Jul 10, 2009

Privacy advocates are puzzled and dismayed by the Homeland Security Department's recent addition of new categories of personal information it plans to collect and store for all employees, contractors and volunteers who regularly access DHS facilities. The new categories of information include mother's maiden name and financial history, according to a June 25 Federal Register notice.

Information to be collected

The Homeland Security department is expanding the personal data it gathers from employees and contractors in controlling access to buildings and systems.

New categories: Maiden name, mother's maiden name, clearance level, identifying physical information, financial history, duty date and weapons-bearer designation.

Existing categories: Date of birth, Social Security number, organizational and employee affiliations, fingerprints, digital color photograph, digital signature and phone numbers.

DHS is updating the Personal Identity Verification and Identity Management System to support measures in Homeland Security Presidential Directive 12 that pertain to who gets access to buildings and computer systems.

But the new categories of data are raising eyebrows, especially the ones requiring a mother's maiden name and financial history.

Asking for financial history information, for example, "could be benign, depending on what information is being requested. Or is bad credit now a security risk?" asked Christopher Calabrese, counsel for the American Civil Liberties Union's Technology and Liberty Program. "And why does DHS need to know [someone's] mother's maiden name? It seems strange."

Amy Kudwa, a DHS spokeswoman, said the "financial history" data element refers to a credit history check, which she says is standard for government employees. "We are simply moving forward with HSPD-12," Kudwa said.

Jim Dempsey, vice president of public policy at the Center for Democracy and Technology, agreed that requesting and storing data on mother's maiden name and financial history is risky and unusual. That kind of information would seem more appropriate for a background check or security clearance than a building access identification program, he said.

"This information collection is odd, particularly financial history," Dempsey said. "A general principle is that the [agency] collecting the information becomes responsible for protecting it. This is sensitive information, and it looks unnecessary. They have not justified why they need this information."

Sponsored by
Booz | Allen | Hamilton
delivering results that endure

**Instilling confidence
in Cloud confidentiality
and integrity.**

Click here for more information

Jim Harper, director of information policy studies at the Cato Institute, said the expanded data collection seems to increase the risks of possible identity theft and privacy loss for employees and contractors. Financial institutions often use mother's maiden name as an added layer of authentication for people trying to gain access to bank accounts or other financial holdings. If there were to be a data breach that allowed identity thieves to get the personal information that DHS is now requiring, knowing someone's mother's maiden name could give the thieves easier access to that person's accounts, he said.

A DHS Privacy Impact Assessment Update issued on the HSPD-12 program June 18 said the expanded amount of information collection presents no additional privacy risks. It states that all the information will be secured and protected under existing policies.

Dempsey said it appears the department has been collecting the additional categories of information in its hiring database but now will be storing it in its ID card database. Dempsey said that is troubling, because "this duplication creates another opportunity for data loss."

The HSPD-12 ID card system covers all DHS employees, contractors and their employees, consultants, and volunteers who require long-term access to DHS facilities and computer systems, the department said. The system also has been expanded to cover federal emergency responders, foreign nationals on assignment and other federal employees detailed to DHS.

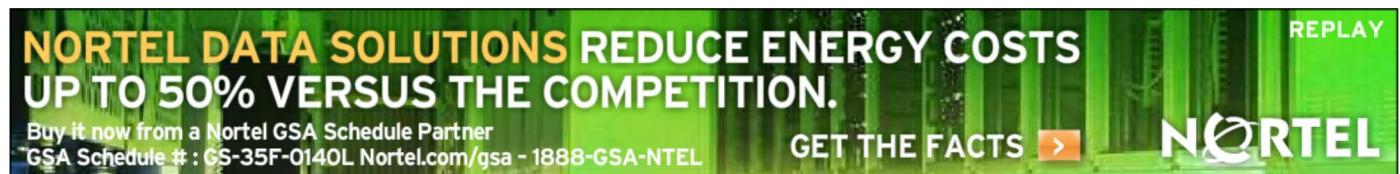
Personal information provided to DHS may be shared within DHS and with appropriate federal, state, local and tribal agencies on a need-to-know basis. The records on individuals are destroyed upon notification of death or five years after the individual leaves employment or is transferred, under National Archives and Records Administration guidance.

The new categories of data also include the employee or contractor's own maiden name, clearance level, identifying physical information, duty date and weapons-bearer designation.

DHS already collects date of birth, Social Security number, organizational and employee affiliation, fingerprints, digital color photograph, digital signature and telephone number.

About the Author

Alice Lipowicz is a staff writer for Federal Computer Week.



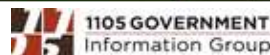
NORTEL DATA SOLUTIONS REDUCE ENERGY COSTS UP TO 50% VERSUS THE COMPETITION.

Buy it now from a Nortel GSA Schedule Partner
GSA Schedule #: GS-35F-0140L Nortel.com/gsa - 1888-GSA-NTEL

GET THE FACTS >

REPLAY

NORTEL



© 1996-2009 1105 Media, Inc. All Rights Reserved.