

Comments in Response to
Homeland Security Presidential Directive 12 (HSPD-12)

By
The Village Group

Waltham, Massachusetts
village.com
wes@village.com
781-647-7178

Regarding FIPS 201, NIST 800-73 and NIST 800-76, we believe that various ideas from the **Quiet Enjoyment Infrastructure** would appear to be useful.

1. Credential Issuance

In response to concerns expressed in Response to Comments 1 and 2 in HHS Consolidated Comments for draft FIPS 201 and SP 800-73 by Will Liston, dated December 23, 2004 and other comments: The QEI argues for the creation of a foundational identity credential consisting of a digital certificate that attests to nothing more than attributes that bind an individual to an identity. Nothing is asserted by the foundational identity credential as to authorizations, clearances, character or, most importantly, relationships. It is, in effect, a *Digital Birth Certificate*.¹

A *Digital Birth Certificate* is “foundational” in that changeable attributes such as authorizations, clearances, and relationships may each be represented by an additional certificate that may be embedded in a token (smart card, USB token, cell phone, etc.) with each such attribute certificate being bound to the *Digital Birth Certificate*.

Such a *Digital Birth Certificate* would obviate the need for a temporary identity credential as attribute certificates representing such things as a completed NACI could be added at any time. A federal employee might have dozens of such attribute certificates bound to the *Digital Birth Certificate*, with attributes being added and removed from time to time. Such events do not affect the foundational *Digital Birth Certificate*. Indeed, it could be argued that a *Digital Birth Certificate* that is produced by a proper enrollment process, with multiple biometrics recorded at time of enrollment, becomes especially valuable in the event that the individual to whom it applies has been removed from a position for cause.

2. Privacy Concerns

Privacy concerns as expressed in Comment 6 in HHS Consolidated Comments for draft FIPS 201 and SP 800-73; in comments submitted by Pam Dixon on December 23, 2004 and in a presentation entitled *The New Federal ID Card: Privacy Implications* on behalf of the Electronic Frontier Foundation, PrivacyActivism, and the Privacy Rights Clearinghouse; and others raise a multitude of privacy concerns surrounding the use of any government-issued persona identifier; that avoidance of the use of SSN does not reduce those risks.

¹ “Digital Birth Certificate” is a trademark of The Village Group, Inc.

The authors call for a Privacy Impact Assessment to be performed immediately. But a Privacy Impact Assessment that assumes current approaches will only show a very difficult tradeoff, with security trumping privacy.

The notion that one must be sacrificed for the other must be challenged. It can be demonstrated that through proper process design and proper application of public authority, the unique identifier can be transformed from an eroder of personal privacy into a bulwark of personal privacy. When it comes to privacy and security, thoughtful engineering of identity solutions will allow us to have our cake and eat it too. A tradeoff is entirely unnecessary.

We believe we have outlined such proper process design and proper application of public authority in five of the twelve components of the Quiet Enjoyment Infrastructure. An abbreviated copy of the book entitled Quiet Enjoyment may be found at <http://www.village.com>.

3. In-Person Proofing

The Enrollment Infrastructure, one of the twelve components of the Quiet Enjoyment Infrastructure, outlines a complete process for economical and effective in-person identity verification and credential issuance. The Enrollment Infrastructure is described in the document identified in item 2 above.

Sincerely,

The Village Group
Wes Kussmaul
CEO