From: Edward Roback [edward.roback@nist.gov]
Sent: Wednesday, December 08, 2004 3:23 PM
To: DraftFips201@nist.gov
Subject: Fwd: Re: Comments on draft FIPS 201

```
Susan is on the ISPAB.  Here are her comments for the public record.  Ed


>X-Sieve: CMU Sieve 2.2
>To: edward.roback@nist.gov
>CC: reeder@bellatlantic.net, Elaine Frye <elaine.frye@nist.gov>
>Started-at: 2004.12.08-10:27:22
>From: Susan Landau <susan.landau@sun.com>
>Sender: Susan Landau <susan.landau@sun.com>
>Date: Wed,  8 Dec 2004 10:56:47 -0500
>Subject: Re: Comments on draft FIPS 201
>X-MailScanner:
>X-MailScanner-From: slandau@sunlabs-sr1.east.sun.com
>
>
>                                Wednesday  08 December 2004  at 10:27
>
>
>Ed,
>
>I won't be at the December meeting, so here are my comments.  I hope
>they are useful.
>
>Best,
>
>Susan
>
>Overall, a very good job on an impossible task.  You guys are to be
>congratulated for pulling this off.
>
>I have one major concern, and a number of small comments.  The major
>concern is something that came up during the September briefing.  As
>you guys are well aware, fingerprint ID is lousy.  I would like to see
>early in the document a discussion of the fact that fingerprints are
>currently used as the biometric identifiers but the expectation is that
>there will be a move in K years (K can be five) to more robust forms of
>biometrics even though the fingerprints will continue to be allowed for
>a period (to enable backwards compatibility).  I think this is
>important technically.  I think this is important for security.  And I think it is
important politically.
>You don't want to be seen endorsing a standard that uses a weak
>biometric identifier.  You have to do fingerprints now because the
>standard is due now.  But you don't have to endorse it as terrific ID technology.
>
>I have the following specific comments:
>
>page vi, section 10: I would add a comment here that security is only as
>    good as the weakest link the chain, and the PIV should not be viewed as
>    a substitute for the careful vetting of people getting the credential.
>    This issue is obvious but I think this point needs to be emphasized.
>
>page 1, introduction, paragraph 3: Similarly, I would change the order to
>    say "depending upon the process used to issue the credential, the type
>    of credential, and the authentication mechanism ..."  You want to make
>    clear that the vetting for the credential is absolutely crucial in
>    determining the value of the identity verification.
```

```
>
>page 10, 3.1, first paragraph: One threat not listed is the malfunction of
>    the system that results in preventing a legitimate owner of a credential
>    from using it (a denial-of-service attack, if you would).
>
>page 12, 3.3, paragraph beginning "There is another ...": "virtual" rather
>    than "logical"?
>
>page 17, 4.1.3: ICC? (This term may be known to readers of the
>document.)
>
>page 21, 4.1.4.3.b: Why is such private information on an ID card?
>
>page 30, 4.4: Here is where it is also appropriate to make a comment about
>    current standard versus what might be used at some later point.
>
>page 40, 5.1.2: Should there be recommendations here as to how long
>    authentication certificate lifetimes should be for various
>    agencies/security levels?
```