

X-Sieve: CMU Sieve 2.2

To: drafftips201@nist.gov

X-Mailer: Lotus Notes Release 6.5.2 June 01, 2004

From: timothy.p.ruland@census.gov

Date: Thu, 23 Dec 2004 13:37:29 -0500

X-MIMETrack: Serialize by Router on LNHQ08MTA/VHQ/BOC(Release 6.5.2|June 01, 2004) at 12/23/2004

01:37:30 PM

X-Spam-Status: No, hits=-4.5 required=4.0 tests=AWL,BAYES_00 autolearn=ham version=2.64-2004121301

X-Spam-Report:

* -0.5 BAYES_00 BODY: Bayesian spam probability is 0 to 1%

* [score: 0.0000]

* -4.0 AWL AWL: Auto-whitelist adjustment

X-Spam-Checker-Version: SpamAssassin 2.64-2004121301 (2004-01-11) on dispatch.tco.census.gov

X-MailScanner:

X-MailScanner-From: timothy.p.ruland@census.gov

Subject: Comments

Comments:

1. While the guidance as written seems fairly straight forward for most typical Federal network environments and systems, the Census Bureau faces some unique challenges in developing, fielding, and supporting its massive Decennial Census operations. We typically have approx. 500,000 temporary field enumerators that perform data collection efforts for periods of 6-8 weeks at a time during the Census operations. The requirements of HSPD-12 and FIPS 201 as written, particularly with no possibility of any kind of waivers will have a severe impact on our operations. Both in complexity and cost. We are looking at testing the feasibility of using hand held computing devices with encryption and specialized applications on them to perform these functions. With the large number of enumerators we are looking at, the short amount of time we have to complete the Census work under the time constraints of our Constitutional reporting deadlines I would respectfully recommend that some leeway in the form of modified guidance be addressed to meet specialized requirements. I understand you cannot write FIPS or Special Publications to address each unique situation, but with no possibility of relief from the letter of the guidance the Census Bureau will be face a severe impact on its most complex and important program, the Decennial 2010 Census, and the tests leading up to it.

2. There needs to be a better definition of what is logical access is meant to be controlled by the publication. As written, we interpret this to mean employees who access our email system (using the Internet) would require smartcard readers. We developed our Lotus Notes environment to support users accessing iNotes from the Internet. This allows flexibility for users on travel or at conferences. FIPS 201 as written seems to take

this capability away from our employees.

3. As written, the term logical access to a system could also mean access to devices like Blackberry systems, etc. Is this the intent? That any IT resource must have logical access control through the smartcard in place?

Thank you for the opportunity to provide my comments/concerns.

Timothy P. Ruland, CISM, CISSP
Chief, IT Security Office
US Census Bureau
301-763-2869
301-457-4504 (fax)

"Any man worth his salt will stick up for what he believes right, but it takes a slightly better man to acknowledge instantly and without reservation that he is in error" - Andrew Jackson