From: Mierzwa, Charles
Sent: Tuesday, January 23, 2007 3:39 PM
To: Matsuoka, Karen Y.
Subject: RE: 3220-0005 Employer Reporting

Karen,

To confirm our discussion earlier today, the RRB has the following responses to your E-mail of January 22, 2007.

Re: item 1, Program letter: e-mail submission of form BA-6a, BA-6 Address Report

- On page 2….
  The RRB agrees to add the OMB suggested language "and information should be protected in accordance with security controls outlined in NIST guidance 800-53."
- Are there any safeguarding procedures required by NIST guidance 800-53 that RRB is **not** implementing or has not described in this Program Letter?
  The RRB's Computer Security Official advises that," the RRB has met the safeguarding procedures required by NIST guidance 800-53 for personally identifiable information (PII). Further, the RRB has responded appropriately to OMB memoranda M-06-15 and M-06-16 on security controls for PII, and is working diligently to comply with FIPS 200 and FISMA requirements for testing and evaluating SP800-53 control procedures of the major applications and general support systems".

Re: Item 2: forms AA-12 and G-88A2

- in item #2, the request for "facsimile number" should be a little further down in the box to give the respondent more room to fill in name and address information.
  The RRB agrees to provide to provide additional space for name and address and to move the "facsimile number" down further on both forms.
- in "section 2: employer instructions," RRB should specify what it means by "within 10 days." Is this within 10 days of receiving this notice? Or within 10 days of retirement/death?
  The RRB means within **10 days of the date released** by the RRB, which is found in item 9 of the proposed AA-12 and item 3 of **the current G-88A.2** and item 12 of the proposed G-88A.2. We suggest amending the proposed language for both forms from "within 10 days" to "within 10 days of the date released ".

If RRB means within 10 days of receiving this notice, how will RRB know when the form was received in order to enforce this 10 day timeframe? See response to previous question.

If you need anything else clarified or have any other questions, please let me know.

Chuck Mierzwa

-----Original Message-----
From: Matsuoka, Karen Y.
Sent: Monday, January 22, 2007 12:34 PM
To: Mierzwa, Charles
Subject: 3220-0005 Employer Reporting

Hi Chuck. Here are OMB's questions regarding these forms:

1. Program Letter: "Email submission of form BA-6a, BA-6 Address Report"
   - On page 2, the following (in red text) should be added to the last sentence of the second paragraph: "To meet these security requirements all e-mail messages we

exchange must be encrypted and signed with a Digital ID, and information should be protected in accordance with security controls outlined in NIST guidance 800-53."

- Are there any safeguarding procedures required by NIST guidance 800-53 that RRB is **not** implementing or has not described in this Program Letter?

2. forms AA-12 and G-88A2

- in item #2, the request for "facsimile number" should be a little further down in the box to give the respondent more room to fill in name and address information
- in "section 2: employer instructions," RRB should specify what it means by "within 10 days." Is this within 10 days of receiving this notice? Or within 10 days of retirement/death?
- If RRB means within 10 days of receiving this notice, how will RRB know when the form was received in order to enforce this 10 day timeframe?

Can you please give me your responses by COB Wednesday? Thanks!

Karen