DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE OF DIRECTOR

ACTION REFERRAL

TO	DATE
Jacobs	1-13-11

DIRECTOR'S USE ONLY	ACTION REQUESTED
1. LOG NUMBER 10-306 306	[ ] Prepare reply for the Director's signature DATE DUE _____
2. DATE SIGNED BY DIRECTOR Cleared 1/28/11, letter attached.	[X] Prepare reply for appropriate signature DATE DUE 1-28-11 [ ] FOIA DATE DUE _____ [ ] Necessary Action

APPROVALS (Only when prepared for director's signature)	APPROVE	* DISAPPROVE (Note reason for disapproval and return to preparer.)	COMMENT
1.			
2.			
3.			
4.			

SOCIAL SECURITY

January 12, 2011

Ms. Emma Forkner, Director
South Carolina Department of
Health and Human Services
P.O. Box 8206
Columbia, SC 29202-8206

Dear Ms. Forkner:

On November 2, 2010, the Social Security Administration (SSA) conducted a remote review via telephone of the technical, procedural, and administrative controls implemented by the South Carolina Department of Health & Human Services (SC DHHS) to comply with the system security requirements included in the data exchange agreement between our agencies. Also on the call was the Data Exchange Coordinator from SSA's Atlanta Regional Office. The purpose of the review was to verify that sufficient security safeguards remain in place to protect the confidentiality of information supplied by SSA through the State Verification and Exchange System (SVES). Your agency receives SSA SVES information via the South Carolina Department of Social Services.

During the review, appropriate members of the SC DHHS staff involved in the protection and usage of SSA information were interviewed. In addition to the interview, agency documents pertaining to policies and procedures intended to safeguard SSA supplied information were examined. The review indicated that overall, the suite of security safeguards implemented by SC DHHS to protect SSA supplied information is well managed and in compliance with the security requirements of the data exchange agreement. However, the following is a list of findings and requirements that need immediate attention:

Finding #1:

SC DHHS Household Maintenance subsystem has one screen that contains SSA-provided data paired with verification indicators. No inquiry log exists on this screen.

Requirement #1:

5.4 Automated Audit Trail. . . .If SSA-supplied information is retained by the EIEP (e.g., Access database, Share Point, etc.), or if certain data elements within the EIEP's system will indicate to users that the information has been verified by SSA, the EIEP's system must also capture an audit trail record of any user who views SSA-provided information stored within the EIEP's system. The audit trail requirements for these inquiry transactions are the same as those outlined above for the EIEP's transactions requesting or accessing information directly from SSA. . . . .

Finding #2:

SSA provided data is being store as a separate file that sits inside a database file table as a file comprised solely of SSA-provided data. This practice is in violation of the CMPPA agreement signed between our agencies.

Requirement #2:

Article VII--Disposition and Records Retention of Matched Items

A. State agencies receiving data from SSA to administer programs governed by this CMPPA Agreement will retain all such data only for the required processing times for the applicable federally funded benefit programs and will then destroy all such data.

D. State agencies may not create separate files or records comprised solely of the data provided by SSA to administer programs governed by this CMPPA Agreement.

Finding #3:

Users on the Clemson mainframe are allowed 100 failed logon attempts in a 15-minute period before the system locks the ID. This is excessive and this practice allows brute force attacks and usage of password cracking software and does not follow industry best practices.

Requirement #3:

5.3 System Access Control. . . .Implementation of the control software must be in compliance with recognized industry standards. For example, password policies should enforce sufficient construction strength (length and complexity) to defeat or minimize risk-based identified vulnerabilities. . . . . also refer to NIST publication section 3
http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

Finding #4:

SC DHHS audit records can be altered and are not read only. Systems Security Requirements dictate that audit records must be unalterable, read only, and protected from being overwritten.

Requirement #4:

5.4 Automated Audit Trail. . . .Each entry in the audit file must be stored as a separate record, not overlaid by subsequent records.. . .Access to the audit file must be restricted to authorized users with a "need to know" and audit file data must be unalterable (read only) and maintained for a minimum of three (preferably seven) years.

Within 10 Business Days of Receipt of this Report

An authorized official of SC DHHS must submit a Plan of Action and Milestones (POA&M) detailing the implementation of compensating controls, intended as short-term solutions to the Finding Requirements, until a permanent control solution is in place. Importantly, the POA&M must provide detailed descriptions of the compensating control and permanent control solutions, as well as implementation timelines for each. Both the compensating control and permanent control solutions are subject to SSA's approval.

Within 25 Business Days of Receipt of This Report

SC DHHS must implement compensating controls as identified in the POA&M to address Finding Requirements.

Notice of Implementation of Permanent Control Solution to a Finding Requirement

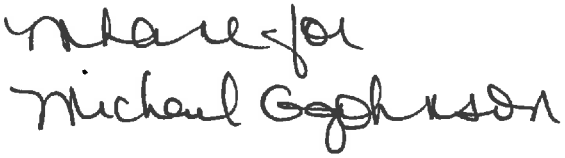
Pursuant to the CMPPA Agreement and the Information Exchange Agreement, failure to meet the Finding Requirements contained in this report may result in suspension of SSA-provided information and/or termination of these agreements.

SSA will continuously monitor the status of all Finding Requirements pending with SC DHHS. When appropriate, an authorized SC DHHS official must provide to SSA's lead security reviewer a formal written notice attesting to the implementation of a permanent control solution to the Finding Requirements.

Please provide the POA&M detailing implementation for the compensating controls, according to the timeline above to the lead review, Linda E. Rice at **DX.Compliance.OIS@ssa.gov**

On behalf of SSA, I would like to thank you and your staff for your dedication to protecting SSA information. If there are any questions on the review, please do not hesitate to contact Linda E. Rice at (410) 966-8952 or e-mail at linda.e.rice@ssa.gov.

Sincerely,



Michael G. Johnson, Director
Office of the Chief Information Officer
Office of Information Security
Division of Compliance and Oversight

cc:
Mr. Brooks Hansen
Social Security Administration
Atlanta Regional Office
BITT1200 Rev. Abraham Woods Jr. Blvd
Birmingham, AL 35285

Ms. Heather D. Dawkins
Social Security Administration
Atlanta Regional Office
BITT1200 Rev. Abraham Woods Jr. Blvd
Birmingham, AL 35285

Ms. Patricia Davis
South Carolina Department of Health and Human Services
P.O. Box 8206
Columbia, SC 29202-8206

Ms. Sharon O. King
Bureau of Eligibility Administration
Div. of MEDS Project & Support Management
South Carolina Department of Health and Human Services
P.O. Box 8206
Columbia, SC 29202-8206

Log # 306

South Carolina Department of Health & Human Services

Anthony E. Keck • Director
Nikki R. Haley • Governor

January 28, 2011

Linda E. Rice
Lead Reviewer
linda.e.rice@ssa.gov

Dear Ms. Rice:

The South Carolina Department of Health and Human Services (SCDHHS) received a letter from Michael G. Johnson, Director of the Office of the Chief Information Officer, dated January 12, 2011. This letter was advising SCDHHS of the results of the Social Security Administration (SSA) Security Review that was conducted in November 2010.

Your security audit of our State Data Exchange (SDX), BENDEX, and State Verification and Exchange System (SVE) subsystems was beneficial in that you identified four areas where our security did not meet the established guidelines.

SCDHHS has created the necessary system change documentation to provide to Clemson University, our Eligibility System contractor, to address three of the requirements (Requirements #1, #2 and #4). Requirement #3 dealt with system access control and Clemson University has created their necessary documentation and plans for developing a solution that will reduce the number of failed logins from 100 to 10. All of these changes have been presented to the necessary Change Control Boards and are tentatively scheduled to be implemented in March 2011.

Since SCDHHS and Clemson University are both planning for these deliverables to be implemented on March 2011, this letter is intending to serve as the Plan of Action and Milestones for addressing these requirements.

If you need additional information, please contact Michael Jones at 803-898-2987 or jonest@scdhhs.gov.

Sincerely,

Alicia Jacobs

Alicia Jacobs
SC DHHS Deputy Director
Medicaid Eligibility and Beneficiary Services

Office of Medicaid Eligibility & Beneficiary Services
P. O. Box 8206 Columbia South Carolina 29202-8206
(803) 898-2502 Fax (803) 255-8235

Monique Dabreu - Re: SC DHHS Response

From: Michael Jones
To: Monique Dabreu
Date: 1/31/2011 9:02 AM
Subject: Re: SC DHHS Response

Constituent Services should not be involved with this one. Its just for Alicia and myself. If you will just put it in my box that should suffice.

>>> Monique Dabreu 1/31/2011 8:46 AM >>>
Michael,

Should I put the log letter in your box and let constituent services know?

Monique

>>> Michael Jones 1/28/2011 5:08 PM >>>
Ms. Rice,

Please find attached a letter from our South Carolina Deputy Director of Medicaid Eligibility concerning our responses to the SSA security letter sent on January 12th.

Please let me know if you have any additional questions or concerns.

Thank you!

Michael L. Jones
Bureau Chief
Bureau of Eligibility Administration
803-898-2987
jonest@scdhhs.gov

Monique Dabreu - SC DHHS Response

From: Michael Jones
To: DX.Compliance.OIS@ssa.gov
Date: 1/28/2011 5:08 PM
Subject: SC DHHS Response
CC: Alicia Jacobs; Linda.E.Rice@ssa.gov; Monique Dabreu; Patricia Davis; Sharon KING
Attachments: Log Letter 0306 - Linda E Rice.pdf

Ms. Rice,

Please find attached a letter from our South Carolina Deputy Director of Medicaid Eligibility concerning our responses to the SSA security letter sent on January 12th.

Please let me know if you have any additional questions or concerns.

Thank you!

Michael L. Jones
Bureau Chief
Bureau of Eligibility Administration
803-898-2987
jonest@scdhhs.gov