

NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

**AUDIT MEMORANDUM: ANALYSIS OF
REGION V 5300 CALL REPORT REFERRAL**

Report #OIG-05-01
January 10, 2005



A handwritten signature in black ink, appearing to read "William A. DeSarno".

**William A. DeSarno
Acting Inspector General**

Prepared by:

A handwritten signature in black ink, appearing to read "Tammy F. Rapp".

**Tammy F. Rapp, CPA, CISA
Sr. Information Technology Auditor**

TO: J. Leonard Skiles
Executive Director

FROM: William A. DeSarno
Acting Inspector General

DATE: January 10, 2005

SUBJECT: OIG Analysis of Call Report Referral
Report #OIG-05-01

NCUA's Region V Director requested that the OIG look into a matter involving a specific 5300 call report. Specifically, Region V was concerned about 5300 edit checks that may have been overridden by an examiner and whether this might have occurred with other call reports. Region V provided us with a report prepared by the Office of Examination and Insurance (E&I) regarding this particular call report which stated that the "examiner circumvented established controls and uploaded incorrect data."

OBJECTIVE

The objective of our work was to determine whether a preventive control in the 5300 call report upload process was circumvented and if this represents a systemic problem.

SCOPE AND METHODOLOGY

The scope of our work was limited to an isolated incident of a 5300 call report uploaded for one credit union located in Region V.

We interviewed the examiner who uploaded the subject call report, as well as staff from the E&I and Office of the Chief Information Officer (OCIO). We reviewed historical documentation relating to the incident including March and June 2004, 5300 data for this particular credit union. We reviewed the security plan and other documentation prepared by E&I and OCIO relating to this incident.

We also performed limited testing of the 5300EX application. Specifically, we tested whether the data could be modified outside of the application. We did not attempt to perform any transmission or uploads of the data to the server. We also did not determine the accuracy of the data presented in the March or June call reports.

Due to the limited scope of this project, we did not follow Yellow Book audit standards. Accordingly, our suggestions are not covered by NCUA's Audit Follow-up Instruction 1910.6.

5300 BACKGROUND ¹

Credit unions deliver the financial data to the examiner using one of several methods including a paper form physically delivered or faxed, verbal collection over the telephone, on-site collection, or electronic delivery via diskette or internet. Beyond the delivery format, NCUA has no control over the program used by the credit union to generate the data file. NCUA provides the agency developed 5300 Credit Union software program, for credit union use; however, the credit union is not obligated to use the program. The 5300 program provides credit union officials the ability to produce a file containing financial data. Credit unions transmit the file to the examiner either on a diskette or on-line through an NCUA server.

The examiner has an expanded version of the 5300 installed on the standard NCUA notebook computer. This version allows the examiner to load the data file provided by the credit union. This version also allows the examiner to upload verified data to the production SQL database.

The 5300 Call Report software contains edits that either stop the transmission or warn the user of potential erroneous data. Additional edits on the processing server recheck the data integrity upon receipt.

OBSERVATIONS

Our review of historical documentation shows the examiner attempted to upload at least five call reports for one credit union during the June 2004, call report cycle. Our review of the documentation and interviews of key staff also indicated that all but two of these uploads were rejected by the server. The first call report accepted by the server on July 25, 2004, appeared to represent March 2004, data with some adjustments. Although the file did not accurately reflect June 2004, data, it was in the correct format and appeared reasonable. The last call report accepted by the server on July 30, 2004, represented the credit union's June 2004, data.

We interviewed the examiner and learned that approximately 40 percent of her credit unions did not receive their 5300 package for the June 2004, cycle. The examiner advised the credit union that is the subject of this report to use its prior cycle software to input the data and then transmit the file. The examiner attempted to upload this data. However, the server rejected it since it had the wrong date. The examiner then opened the data file using notepad and changed the month from 03 to 06, saved the file, and imported this file into 5300EX. The data file did not have any warnings and passed all the edit checks. However, the server again rejected this file because it was in the short format. The short form is optional only during the March and September cycles for

¹ Source: NCUA Call Report System Security Plan, June 2, 2004

credit unions with total assets less than \$10,000,000. The examiner finally waited for the credit union to receive the June 2004, 5300 package and complete the proper form which was then transmitted successfully on July 30, 2004.

ANALYSIS & CONCLUSION

Controls were effective and prevented 5300 data from being accepted by the server that was in an unacceptable format. Although there were multiple attempts to upload 5300 data, the server rejected all but two. Although the data was an estimate, the first successful upload represented data in the correct format. The second upload that was accepted by the server represented actual data in the correct format. In addition to the server rejecting data in an unacceptable format, additional controls notified OCIO that there was a problem with this credit union's 5300 call report transmission by their examiner.

We learned that there is a well known back door to modifying data before uploading to the server. Examiners have the ability and sometimes use notepad to open the 5300 xml file to modify data prior to uploading.

SUGGESTION

The OIG suggests that E&I consider whether data modified outside of the 5300 program poses a material risk to 5300 data integrity. If E&I determines the risk is significant, they should work with OCIO to determine the best solution for preserving data integrity and preventing modification outside of the program.

Distribution:

Board Chairman, JoAnn M. Johnson
Board Member, Deborah Matz
Deputy Executive Director, J. Owen Cole, Jr.
Director, Office of Examination & Insurance, David M. Marquis
Director, Region V, Melinda Love
Chief Information Officer, Doug Verner