Audit Review of the NFMC Outsourced Data Collection System: Data Privacy

Project Number: NFMC.PRVCY.2012
Audit Review of the **NFMC Outsourced Data Collection System: Data Privacy**
Internal Audit Department Project # NFMC.PRVCY.2012

**Table of Contents**

- Project Completion Letter .................................................................................................. 2
- Function Responsibility and Internal Control Assessment .............................................. 3
- Executive Summary of Observations, Recommendations, and Management Responses .......................................................................................................................... 1
- Background ......................................................................................................................... 7
- Scope .................................................................................................................................. 9
- Methodology ........................................................................................................................ 10
- Observations and Recommendations ............................................................................ 11
- Conclusion ........................................................................................................................ 14
April 11, 2012

To: NeighborWorks® America Audit Committee

Subject: Audit Review of the NFMC Outsourced Data Collection System: Data Privacy
Internal Audit Department Project NFMC.PRVCY.2012

Enclosed is a copy of the recently concluded review of the policy, controls, and procedures in place to protect personally identifiable information in the NFMC program’s Data Collection System.

Please contact me with any questions you might have. Thank you.

Frederick Udochi
Director of Internal Audit

Attachment

cc: E. Fitzgerald
M. Forster
P. Kealey
J. Bryson
S. LeGrand
F. Mattos
J. Fekade-Sellassie
T. Sims
Function Responsibility and Internal Control Assessment
Audit Review of the NFMC Outsourced Data Collection System: Data Privacy

<table>
<thead>
<tr>
<th>Business Function Responsibility</th>
<th>Report Date</th>
<th>Period Covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Foreclosure Mitigation Counseling (NFMC)</td>
<td>April 11, 2012</td>
<td>October 2008 - February 2012</td>
</tr>
</tbody>
</table>

Assessment of Internal Control Structure

<table>
<thead>
<tr>
<th>Effectiveness and Efficiency of Operations</th>
<th>Generally Effective¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability of Financial Reporting</td>
<td>Generally Effective</td>
</tr>
<tr>
<td>Compliance with Applicable Laws and Regulations</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

¹ Legend for Assessment of Internal Control Structure: 1. Generally Effective: The level and quality of the process is satisfactory. Some areas still need improvement. 2. Inadequate: Level and quality of the process is insufficient for the processes or functions examined, and require improvement in several areas. 3. Significant Weakness: Level and quality of internal controls for the processes and functions reviewed are very low. Significant internal control improvements need to be made.

This report was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing.*

---

¹ Legend for Assessment of Internal Control Structure: 1. Generally Effective: The level and quality of the process is satisfactory. Some areas still need improvement. 2. Inadequate: Level and quality of the process is insufficient for the processes or functions examined, and require improvement in several areas. 3. Significant Weakness: Level and quality of internal controls for the processes and functions reviewed are very low. Significant internal control improvements need to be made.
### Executive Summary of Observations, Recommendations, and Management Responses

#### Summary of Observations and Recommendations:

<table>
<thead>
<tr>
<th>Summarized Observation; Risk Rating</th>
<th>Management Agreement with Observation (Yes/ No)</th>
<th>Internal Audit Recommendation Summary</th>
<th>Accept IA Recommendation (Yes/ No)</th>
<th>Management’s Response to IA Recommendation</th>
<th>Estimated Date of Implementation (Month/Year)</th>
<th>Internal Audit Comments on Management Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observation No. 1</td>
<td>Yes</td>
<td>We recommend that NeighborWorks’ management in conjunction with the Information Management department develop an information security plan that articulates the Corporation's practices relating to administrative, physical and technical controls that would ensure PII is adequately protected. This plan should amongst other information security issues address policies, standards and procedures relating to PII in the areas of data classification, record management, retention and destruction. In addition, an inventory of the laws and regulations that apply to the</td>
<td>Yes</td>
<td>Management agrees to have the Information Management Division, in conjunction with the Office of the General Counsel, and other divisions as required, develop an information security plan to document the Corporation’s policies and procedures for information security. Once a plan has been published, the NFMC team will work with IM and OGC to determine how those standards may apply to the program.</td>
<td>March 31, 2013</td>
<td>Internal Audit accepts Management response.</td>
</tr>
</tbody>
</table>

---

2 The observations and recommendations in this section are summarized at a high level for informational purposes. To obtain a full, detailed explanation of each, please refer to the “Observations and Recommendations” section. Management’s response is directly related to the detailed observations and recommendations noted in the “Observations and Recommendations” section.
<table>
<thead>
<tr>
<th>Summarized Observation; Risk Rating</th>
<th>Management Agreement with Observation (Yes/ No)</th>
<th>Internal Audit Recommendation Summary</th>
<th>Accept IA Recommendation (Yes/ No)</th>
<th>Management’s Response to IA Recommendation</th>
<th>Estimated Date of Implementation (Month/Year)</th>
<th>Internal Audit Comments on Management Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>corporation should be made available within the information security policy. In addition practices around the security and privacy issues associated with procuring cloud services should be indicated in such a policy. As a suggestion the corporation might want to consider adopting relevant sections of the National Institute of Standards and Technology (NIST) guidelines on security and privacy in public cloud computing (NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Summarized Observation; Risk Rating</td>
<td>Management Agreement with Observation (Yes/ No)</td>
<td>Internal Audit Recommendation Summary</td>
<td>Accept IA Recommendation (Yes/ No)</td>
<td>Management’s Response to IA Recommendation</td>
<td>Estimated Date of Implementation (Month/Year)</td>
<td>Internal Audit Comments on Management Response</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------</td>
<td>---------------------------------------</td>
<td>-------------------------------------</td>
<td>---------------------------------------------</td>
<td>----------------------------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Observation No. 2</td>
<td>Yes</td>
<td>We recommend that NFMC add a part of its internal control structure to request, obtain, and review the SSAE 16 Service Organization Control (SOC) Type 2 report at a minimum or Type 3 (if performed and available) report for [ ] and other service providers on at least an annual basis. Also we recommend NFMC follow up on any observations that may directly or indirectly impact the services and controls relied upon by the NFMC program. If a SOC Type 2 or 3 report are not available for review, we recommend that NFMC Management and the Information Management Department identify controls relied upon by the service provider and obtain assurance that the controls are in place and operating effectively during the period as well as consider exercising its right to audit (See Observation No. 3).</td>
<td>Yes</td>
<td>Management accepts the IA Recommendations with conditions: all IT functions are managed through the Information Management (IM) Division at NeighborWorks America, not any individual program or support division. Given the technical nature of the SSAE 16/ISAE 3402 documents, it is not the responsibility of NFMC to review the document. This should fall under the purview of the IT Security Expert, a position which management recently added and is currently under recruitment. Currently we are able to acquire the Type 2 report from our Vendor [ ] on an annual basis; however the NFMC may not be able to continue getting this report if the cost becomes restrictive.</td>
<td>01/2013 (file Acquisition or when annual release is available)</td>
<td>Internal Audit accepts management response and acknowledges that all IT functions should be managed through the Information Management Division. However, the absence of a Corporate information security plan that would provide the framework in this aspect was lacking during the recent review undertaken. Internal Audit notes that management has accepted both recommendations and we are of the opinion that the addition of an information security expert would greatly facilitate future</td>
</tr>
<tr>
<td>Observation No. 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------</td>
<td>-------------------</td>
<td>-------------------</td>
<td>-------------------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td><strong>Service Level Agreement Enhancements</strong></td>
<td><strong>Yes</strong></td>
<td><strong>We recommend an addendum to the existing agreement(s) and a revision all future agreements with</strong> NFMC’s Service Level Agreement <strong>noting the omission of several key and standard contract clauses given the nature of the business relationship. We note the following additions should be made to the agreement to formally document the expectations of the business relationship, expected deliverables, and improve the quality of the services provided:</strong></td>
<td><strong>Yes</strong></td>
<td><strong>Management agrees to have OGC and IM review the current agreement and consider appropriate addendums as per the recommendations by Sept 30th, 2012. The final language incorporated in the contracts as mutually agreed to by parties. OGC and IM will also review and evaluate publishing guidelines for hosting service provider agreements as part of the wider information security plan development.</strong></td>
<td><strong>March 31, 2013</strong></td>
<td><strong>Internal Audit accepts management response.</strong></td>
</tr>
</tbody>
</table>

We reviewed NFMC’s Service Level Agreement with **[redacted]** noting the omission of several key and standard contract clauses given the nature of the business relationship. We note the following additions should be made to the agreement to formally document the expectations of the business relationship, expected deliverables, and improve the quality of the services provided:

- Inclusion of records retention, destruction, and disposal guidance that is aligned with OMB Circular A-110 (e.g., similar to the requirements imposed...
<table>
<thead>
<tr>
<th>Summarized Observation; Risk Rating</th>
<th>Management Agreement with Observation (Yes/ No)</th>
<th>Internal Audit Recommendation Summary</th>
<th>Accept IA Recommendation (Yes/ No)</th>
<th>Management’s Response to IA Recommendation</th>
<th>Estimated Date of Implementation (Month/Year)</th>
<th>Internal Audit Comments on Management Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>upon Grantees;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Inclusion of data security and information transmission requirements/parameters when sharing DCS information with authorized third parties (i.e., and and)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Inclusion of a Right to Audit Clause (See Observation and Recommendation No. 2).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Rating:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Risk Rating Legend:**

**Risk Rating: HIGH**

A serious weakness which significantly impacts the Corporation from achieving its corporate objectives, financial results, statutory obligations or that may otherwise impair the Corporation’s reputation.

**Risk Rating: Moderate**

A control weakness which could potentially undermine the effectiveness of the existing system of internal controls and/or operational efficiency, integrity of reporting and should therefore be addressed.

**Risk Rating: Low**

A weakness identified which does not seriously detract from the system of internal control and or operational effectiveness/efficiency, integrity of reporting but which should nonetheless be addressed by management.

### Management Response to Audit Review Recommendations

**NFMC Outsourced DCS – Data Privacy**

<table>
<thead>
<tr>
<th># Of Responses</th>
<th>Response</th>
<th>Recommendation #</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Agreement with the recommendation(s)</td>
<td>1,2,3</td>
</tr>
<tr>
<td>N/A</td>
<td>Disagreement with the recommendation(s)</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Background

The National Foreclosure Mitigation Counseling (NFMC) program was created by the Consolidated Appropriations Act of 2008 to address the mortgage foreclosure crisis. Legislation was signed authorizing approximately $640 million for a National Foreclosure Mitigation Counseling (NFMC) program (Rounds 1 through 6). NeighborWorks America was elected to administer the NFMC program with the direction that funds be prioritized for use in “areas of greatest need” and for “owner occupied homes.”

The NFMC program seeks to help homeowners facing foreclosure by providing them with foreclosure prevention and loss mitigation counseling including counseling services, training, legal assistance, and program-related support. NeighborWorks distributes funds to about 179 competitively selected Grantee organizations, which in turn provide the counseling services, either directly or through Subgrantee organizations.

The Data Collection System (DCS) is a web-based data collection, validation and reporting system designed to support the monitoring and evaluation of NFMC operational activity. DCS was developed by [redacted] in 2008. The system is installed on servers that are hosted in [redacted] facility. Physical access to DCS is protected by key card (with PIN) and biometric finger scan.

The DCS application collects about 43 data points and the following five data points have been classified as Personally Identifiable Information (PII):

- Name
- Address
- Loan Number
- Race
- Ethnicity

Data within DCS is encrypted and viewing of PII is blocked to all users. Authorized NFMC personnel and NFMC Grantees have access to the DCS by using administered usernames and passwords. These users access DCS to upload and retrieve client level data. In addition, homeowners may be required to submit information to DCS and this is facilitated by the use of [redacted] which is a third-party vendor that provides cloud services for secure file share and transfer. [redacted] may also provide authorized parties (i.e., [redacted] or [redacted]) with DCS data via high level encryption with specific user keys, secure file transfer protocols (SFTP) or by using the file transfer vendor [redacted].
Privacy Initiatives Undertaken by NFMC

In May 2010, NFMC issued a memorandum to its Grantees that outlined program requirements on protection and disposal of clients’ personal information. NFMC requires Grantees to self-certify compliance with these guidelines. Grantees are also responsible for ensuring that their sub-grantees and branches are in compliance with the following:

1. National Industry Standards for Homeownership Counseling, especially these benchmarks for recordkeeping:
   a. Files should be maintained in secured file cabinets in order to protect client privacy. Scanned documents or electronic files should maintain the highest level of client security.
   b. At the time of disposal, files should be shredded or electronic copies should be deleted.

2. Housing and Urban Development (HUD)’s standards for approval of housing counseling

3. Applicable state and federal laws that involve protecting PII and preventing identity theft, including the Gramm-Leach-Bliley Act and accompanying regulations issued by FTC; specifically:
   a. The Safeguards Rule, which requires organizations to develop a written information security plan that describes their program to protect customer information. The plan must be appropriate to the company’s size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles.
   b. The Disposal Rule, which requires disposal practices that are reasonable and appropriate to prevent unauthorized access to, or use of, information in a consumer report.

In addition, the memo required Grantees and Sub grantees to certify compliance with the aforementioned privacy-related program requirements. Furthermore, the Office of General Counsel held its first privacy training and awareness meeting with NFMC management and staff on in February 2012. The training included an overview of PII, an FTC video on PII based on the five principles of data protection, and case studies highlighting the cost to companies that have lost PII.
Objective

This report examines and evaluates the policy, controls, and procedures in place to protect PII in the third party vendor managed DCS and the NFMC program’s internal privacy policies. The report seeks to provide objective assurance to NeighborWorks of the extent to which NFMC, subject to the scope of our audit, is complying with privacy best practices or generally accepted industry standards for protecting consumer information.

Access to PII enables collaboration and business productivity which is an asset, but it also places PII in constant danger of data breach. Federal government entities, state offices, and industry organizations have enacted tough legislation to force organizations to safeguard PII, but publicly-disclosed data breaches still occur. The growth in incidents of loss and unauthorized use of such information has led to increased concerns about protecting the privacy of clients’ and employees’ PII. As a result, there is the need to obtain assurance that any PII collected is protected and used only for the purposes that it was originally collected.

Scope

The engagement focuses solely on NFMC policies and controls for protecting PII; the thrust is to check and test the adequacy of the controls in place. This audit was limited to the NFMC Program and third-party outsourced vendor and was not extended to the Grantees and/or Sub-grantees of the NFMC Program. We understand that the NFMC DCS program operates with the assumption that Grantees, Sub Grantees, and third-parties that have access to DCS will implement their own internal security and data privacy controls and protocols that complement those NeighborWorks and NFMC may already have in place.

The engagement scope is to:

1. Identify and evaluate NeighborWorks and NFMC data classification standards;
2. To obtain assurance that appropriate controls have been identified and implemented for data classified as PII/confidential;
3. Identify and evaluate the privacy policies and controls put in place by the NFMC program and verify compliance with the established policies and procedures;
4. Review and evaluate the agreement between NeighborWorks and to ensure appropriate privacy and confidentiality related clauses are included and verify compliance;
5. Conduct an assessment of DCS authorization and authentication of users;
6. Identify all users (including organizations) and roles of persons with access to PII that results from the DCS; and
7. Obtain assurance that there are applicable privacy awareness trainings and training materials for NFMC employees and Grant recipients.
Methodology

The audit project was launched with an introductory meeting on February 8, 2012 to discuss the audit objective and obtain a preliminary overview of DCS, the controls over DCS, and access to PII within NFMC.

We undertook an assessment of the following primary areas for the purpose of this review:

- Data protection governance
- Staff data protection training and awareness
- Security of personal data (manual and/or electronic)
- Handling of requests for personal data
- Records management

In undertaking this assessment we conducted the following procedures:

- Desk-top review of NFMC policies, protocols and procedures for data protection
- Evaluation of Service Level Agreements (SLA) and protocols with third-party vendors and partners regarding security management and data privacy
- Review NFMC third party contracts for records management, storage, and/or destruction
- Review data sharing arrangements and policies and procedures for handling requests for personal data
- Assess operational guidance or manuals for staff processing PII
- Review data protection training and awareness for NFMC
- Interview NFMC team to establish the controls implemented to ensure compliance with its data protection responsibilities and to understand how staff process PII.
- Inspection of selected records
- Evaluate process and documents for compliance with generally accepted best practices for data privacy
Observations and Recommendations

**Observation No. 1: Corporate Wide Data Security Policy and Guidance**

Data protection governance has to do with policies, procedures, and governance structures related to corporate internal privacy practices and compliance. Governance implies control and oversight by NeighborWorks over NFMC policies, procedures, and standards for corporate internal privacy practices and compliance.

**Observation No. 1**

It is a best practice that any organization that has any assets that could be considered private, confidential, or proprietary has documented policies and procedures that govern how private, proprietary and confidential data/information is handled for the corporation as a whole. While we noted that the NFMC Program with input from Information Management, did put in place policies and procedures for the protection of PII and confidential data; those guidelines were not directly linked to any existing documented security policy regarding confidential/private/proprietary for NeighborWorks. It is best practice that base guidelines and parameters are established and maintained in a corporate information security plan that would provide a monitoring framework relating to administrative, physical and technical controls surrounding the protection of PII. This policy should also provide guidelines for outsourcing or hosting IT services especially in the new area involving the procurement of cloud services.

**Recommendation No. 1**

We recommend that the corporation’s management in conjunction with Information management develop an information security plan that articulates the Corporation’s practices relating to administrative, physical and technical controls that would ensure PII is adequately protected. This plan should address policies, standards and procedures relating to PII in the areas of data classification, record management, retention and destruction. In addition an inventory of the laws and regulations that apply to the corporation should be made available within the information security policy. In addition practices around the security and privacy issues associated with procuring cloud services should be indicated in such a policy.

As a suggestion the corporation might want to consider adopting relevant sections of the following National Institute of Standards and Technology guidelines on security and privacy in public cloud computing (NIST SP 800-144 *Guidelines on Security and Privacy in Public Cloud Computing*):

- Carefully plan the security and privacy aspects of cloud computing solutions before engaging them.
- Understand the public cloud computing environment of the cloud provider and ensure that a cloud computing solution satisfies or organizational security and privacy requirements.
- Ensure that the client-side computing environment meets organizational security and privacy requirements for cloud computing.
• Maintain accountability over the privacy and security of data and applications implemented and deployed in public cloud computing environments.

Observation No. 2: Review of Independent Audit Reports of Service Providers

Observation No. 2
NFMC relies on the internal control environment of its service provider to ensure PII is protected, safe, and remains confidential; however, NFMC Management does not include as part of its internal control framework to request, obtain, and review the Independent Service Auditor’s report of its service providers. At the request of Internal Audit, NFMC requested the Independent Service Auditors Reports issued for covering the period of 2009 – 2011, noting the following reports were received and reviewed by Internal Audit:

• 2009 SAS 70 report covering the period from October 1, 2008 – March 31, 2009
• 2011 S SAE 16 SOC I report covering the period from November 1, 2010 – October 31, 2011

The Independent Service Auditors report provides information about the controls at during the reporting period and enables some risk mitigation by confirming that physical, environmental, and logical (including network) security controls were in place for DCS during the reporting periods.

In addition, per review of the observations noted within the 2011 report we noted the following observation that may have had an impact on the protection and privacy of NFMC data within the DCS during the reporting period:

• No changes were made to the firewall configuration or rules in the period under review

We note that no additional follow up was made by NFMC Management to assess the risk and impact (if any) the observation noted may have had on the control environment for the DCS data.

Recommendation No. 2
We recommend that NFMC add a part of its internal control structure to request, obtain, and review the S SAE 16 Service Organization Control (SOC) Type 2 report at a minimum or Type 3 (if performed and available) report for other service providers on at least an annual basis. Also, we recommend NFMC follow up on any observations that may directly or indirectly impact the services and controls relied upon by the NFMC program. If a SOC Type 2 or 3 report is not available for review, we recommend that NFMC Management and the Information Management Department identify controls relied upon by the service provider and obtain assurance that they

---

3 Internal Audit notes that as of the report issuance date an Independent Service Auditors Report was not received for period covering April 2009 – October 2010
controls are in place and operating effectively during the period under assessment as well as consider exercising its right to audit (See Observation No. 3).

**Observation No. 3: Service Level Agreement Enhancements**

**Observation No. 3**

We reviewed NFMC’s Service Level Agreement with noting the omission of several key and standard contract clauses given the nature of the business relationship. We note the following additions should be made to the agreement to formally document the expectations of the business relationship, expected deliverables, and improve the quality of the services provided:

- Inclusion of records retention, destruction, and disposal guidance that is aligned with OMB Circular A-110 (e.g., similar to the requirements imposed upon Grantees);
- Inclusion of data security and information transmission requirements/parameters when sharing DCS information with authorized third parties (i.e., and ); and
- Inclusion of a Right to Audit Clause (See Observation and Recommendation No. 2).

The inclusion of the aforesaid would formally document NFMC’s expectations and would:

- Increase the assurance that information maintained by within the DCS is retained for the required time period and destroyed and disposed of in the proper manner;
- Increase the assurance that DCS data shared with authorized organizations and personnel will be done in a secure and acceptable manner; and
- Provide NFMC management with the right to review the internal controls in place to support privacy and data protection that may not be addressed in the Independent Service Auditors Report.

**Recommendation No. 3**

We recommend an addendum to the existing agreement(s) and a revision to all future agreements with and future service providers to include adequate language to support the following:

- Records retention, destruction, disposal guidance;
- Guidance and security parameters regarding how information may be shared with authorized third parties; and
- Inclusion of a Right to Audit Clause
**Conclusion**

Privacy addresses the confidentiality of data for specific entities, such as N FMC, or others, such as homeowners, whose information is processed in a system. Privacy carries legal and liability concerns, and should be viewed not only as a technical challenge but also as a legal and ethical concern. Protecting privacy in any computing system is a technical challenge; in a cloud setting this challenge is complicated by the distributed nature of clouds and the possible lack of subscriber awareness over where data is stored and who has or can have access.

Responsible privacy practices assure brand protection; customer trust and confidence; customer loyalty, responsible customer relationship management, business partner confidence, and differentiation from competitors. The absence of data privacy best practices includes litigation; reputational damage; interrupted data flows; breach of data; and unwanted attention.

The focus of this audit is to determine whether N FMC has implemented policies and procedures to regulate the processing of PII and that processing is carried out in accordance with such policies and procedures. When an organization complies with its requirements, it is effectively identifying and controlling risks to prevent a privacy breach.

The arrangements for data protection compliance with regard to governance and controls for governance structures, records management, and security of PII provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement to existing protocols.

We hope this report and the recommendations offered will provide additional guidance to management on what should be done to obtain additional assurance that PII is secure and protected when obtained, retained, stored, retrieved, shared, destroyed, and disposed of by NeighborWorks America and its third party service providers.