Audit Review of the EHLP Hope LoanPort and Data Collection System Interfaces

Project Number: EHLP.LPDCS.2012
Audit Review of the Hope LoanPort and Data Collection System Interfaces  
Internal Audit Department Project #EHLPLPDCS.2012

Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Completion Letter</td>
<td>2</td>
</tr>
<tr>
<td>Function Responsibility and Internal Control Assessment</td>
<td>3</td>
</tr>
<tr>
<td>Executive Summary of Observations, Recommendations and Management Responses</td>
<td>4</td>
</tr>
<tr>
<td>Risk Rating Legend</td>
<td>5</td>
</tr>
<tr>
<td>Background</td>
<td>6</td>
</tr>
<tr>
<td>Objectives</td>
<td>7</td>
</tr>
<tr>
<td>Scope and Limitations</td>
<td>7</td>
</tr>
<tr>
<td>Methodology</td>
<td>8</td>
</tr>
<tr>
<td>Observations and Recommendations</td>
<td>9</td>
</tr>
<tr>
<td>Appendix A</td>
<td>11</td>
</tr>
<tr>
<td>Appendix B</td>
<td>12</td>
</tr>
</tbody>
</table>
To: NeighborWorks America Audit Committee

Subject: EHLP Hope LoanPort and Data Collection System Interfaces

The Internal Audit Department conducted a review of EHLP Hope LoanPort and Data System Interfaces as part of the 2012 EHLP Audit Plan. Enclosed is a copy of the recently concluded review of the processes assessed.

Please review and let me know if you have any comments or questions.

Frederick Udochi
Director of Internal Audit

Attachment

cc: E. Fitzgerald
M. Forster
C. Wehrwein
J. Bryson
J. Fekade-Sellassie
P. Biby
N. Harmon
S. LeGrand
F. Mattos
# Function Responsibility and Internal Control Assessment

## Audit Review of the Hope LoanPort and Data Collection System Interfaces

<table>
<thead>
<tr>
<th>Business Function Responsibility</th>
<th>Report Date</th>
<th>Period Covered</th>
</tr>
</thead>
</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>Not Applicable</td>
</tr>
<tr>
<td>Compliance with Applicable Laws and Regulations</td>
<td>Generally Effective</td>
</tr>
</tbody>
</table>

This report was conducted in accordance with the [International Standards for the Professional Practice of Internal Auditing](https://www.aicpa.org).

---

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

<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</th>
<th>Internal Audit Comments on Management Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observation No. 1</td>
<td>Yes</td>
<td>Recommendation No. 1:</td>
<td>Yes</td>
<td>NeighborWorks has obtained the IT Security Checklist from Hope Loan Port and forwarded it to Internal Audit on 9/28/12. NeighborWorks has reviewed it for completeness, and will ask HLP to review each year to ensure their responses to the items on the checklist remain accurate.</td>
<td>Completed: NFMC has received the checklist and reviewed for completeness and accuracy. Sept. 2013 and Sept. 2014: NFMC will request that HLP confirm the accuracy of their responses to the Checklist items.</td>
<td>Internal Audit accepts Management’s Response.</td>
</tr>
</tbody>
</table>

**Completed IT Security Checklist**

The Agreement, between NeighborWorks and HLP, under Paragraph 4, states the contractor may show compliance with mandated Federal statute, regulations, policies and procedures governing the security of systems, listed in Paragraph 3, by providing a “Completed IT Security Checklist”. During the assessment of Hope LoanPort compliance with the Agreement listed above, no evidence was provided to substantiate the completion of an IT Security Checklist.

**Risk Rating:**

- Yes

---

**Internal Audit**

- NeighborWorks has obtained the IT Security Checklist from Hope Loan Port and forwarded it to Internal Audit on 9/28/12. NeighborWorks has reviewed it for completeness, and will ask HLP to review each year to ensure their responses to the items on the checklist remain accurate.

- Completed: NFMC has received the checklist and reviewed for completeness and accuracy. Sept. 2013 and Sept. 2014: NFMC will request that HLP confirm the accuracy of their responses to the Checklist items.
**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.

<table>
<thead>
<tr>
<th># Of Responses</th>
<th>Response</th>
<th>Recommendation #</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Agreement with the recommendation(s)</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>Disagreement with the recommendation(s)</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Background

The Dodd-Frank Wall Street Reform and Consumer Protection Act provided $1 billion for the Emergency Homeowners’ Loan Program (EHLP) to the Department of Housing and Urban Development (HUD). The program offers a declining balance, deferred payment “bridge loan” (non-recourse, subordinate loan with zero interest) for up to $50,000 to assist eligible homeowners who have become unemployed or underemployed due to the economic downturn or a medical condition.

Through a Cooperative Agreement signed May 5, 2011 and amended on September 23, 2011, the U.S. Department of Housing and Urban Development (HUD) contracted with NeighborWorks America to perform several functions for the Emergency Homeowners’ Loan Program (EHLP).

The Cooperative Agreement gave NeighborWorks America (NeighborWorks) responsibility for developing and maintaining a system through which counseling agencies could submit applications to the Bank of New York Mellon, the Fiscal Agent. NeighborWorks contracted with HOPE LoanPort (HLP) for the development and maintenance of this system.

An interface with HUD’s systems is required as part of the Agreement. Nonetheless, Internal Audit noted that system’s communication is limited to documentation exchange and that HLP does not have a direct interface with HUD’s information systems. However NeighborWorks provided an environment that allowed for the independent sharing and documentation of information without the direct interface, which met with the contractual intent and satisfaction of HUD requirements. Task Order Phase One - System Functionality states - “the contractor must develop and maintain adequate system functionality that allows two-way sharing and flow of documentation and information between EHLP agencies, housing counselors and the Fiscal Agent including but not limited to:

- Provide a secure platform to submit to HUD conditionally approved submissions and process HUD’s response,
- Provide reporting capability to HUD, and
- Provide secure system interfaces for the Fiscal Agent, HUD and Corporation to perform duties necessary for program completion.”

Hope LoanPort® (HLP) is a focal system for EHLP loan application submission, processing, and tracking. It is used for two primary purposes:

1) First, the counseling agencies use HLP to capture data on clients served. They then manually export the data and upload it in comma separate value (CSV) format to the data collection system (DCS).

2) Second, HLP transfers data to a secure server which the DCS later downloads to determine payments to counseling agencies. EHLP CSV specification states the DCS will use data from HLP to verify EHLP’s client IDs submitted by grantees in their

---

2 For IT security requirements, please see pg. 13 of the agreement between (NeighborWorks & HLP) under Appendix A.
3 CSV files are often used as a simple way to transfer a large volume of spreadsheet or database information between programs.
activity records, and to verify that the submitted counseling level is plausible given
the client’s status in HLP. HLP will export a data file containing information about all
EHLP clients on a daily basis. Data is made available with internet protocol security
(IPSEC)\(^4\) (for access control) and is transferred via secure file transfer protocol
(SFTP)\(^5\) to an external server. The DCS then retrieves this data file from the SFTP
server at [redacted] Time daily. The data retrieved by the DCS is limited to the
three essential items that are used to confirm the status and report ability of the
client: Client ID (a 5 digit number), client zip code, and current status. No other
information, and no Personally-Identifiable Information, is sent to the external server
for import into the DCS from HLP.

Data Collection System (DCS) was conceived at project launch to support monitoring and
evaluation of National Foreclosure Mitigation Counseling (NFMC) operational activity. The
system application was developed in [redacted], leveraging the [redacted] database
management system and the [redacted] operating system platform. The system is based
on servers that are hosted in [redacted] facility. The DCS
does not manage, interact, or have access to files/data/accounts on HLP’s system.

Objectives

The engagement objective of this interface internal security control assessment was to:

- Evaluate the implementation of the HLP/DCS interface and requirements as defined
  by EHLP enhancements,
- Evaluate compliance with the NeighborWorks America and Hope LoanPort Inc.
  Agreement dated May 20, 2011, and
- Review of security, change, and business cycle controls in order to assess the
  operating effectiveness of DCS/HLP interface in those areas.

Scope and Limitations

The scope of the assessment included a review of the risks and controls surrounding:

- Contractor compliance with the Agreement between NeighborWorks America and
  Hope LoanPort, Inc. dated May 20, 2011 including a:
  a. Completed IT Security Checklist,
  b. Review of SAS-70 Certificates, and
  c. Signed Memorandum of Understanding
- HLP and DCS systems architectural design and interfaces,
- Policies and procedures related to access control and outsourced service providers,

\(\text{IPSEC}\) is a protocol suite for securing Internet Protocol (IP) communications by
authenticating and encrypting each IP packet of a communication session.
\(\text{SFTP}\) is a network protocol designed to provide secure file transfer.
\(\text{Java}\) is a general-purpose, interpreted high-level programming language whose design philosophy emphasizes code readability.
\(\text{MySQL}\) is an object-relational database management system available for many platforms.
• Application development and maintenance, and
• Database support

High level NIST SP 800-53 control mapping to CobiT controls.

This engagement did not include a review of NeighborWorks IT operations and security infrastructure, information systems strategy, and business continuity planning as they were not within the scope of this project. Internal Audit has either undertaken reviews in each of these areas in previous years or has scheduled future audit reviews on the aforementioned areas. HLP and DCS interface security control assessment artifacts were limited to the responses contained within the NeighborWorks Technical Questionnaire.

**Methodology**

The DCS/HLP interface assessment project was launched with an introductory meeting to:

• Discuss the audit objectives,
• Acquire a preliminary understanding of the processes underlying the interface between DCS and HLP,
• Identify outsourced service provider requirements,
• Verify existence of service level agreements (SLA), review management SLA responsibilities,
• Identify contractual agreements, and
• Answer any questions pertaining to the assessment.

The Cooperative Agreement between NeighborWorks and HLP was provided to Internal Audit after the initial meeting and explained to be regarded as an extract of the original agreement between HUD and NeighborWorks in terms of compliance requirements. The agreement states under Article XXV, Security of Confidential Information that the contractor shall comply with applicable Federal regulation including the Federal Information Security Management Act (FISMA) which, in turn, refers to the use of National Institute of Standards and Technology (NIST) security framework. The areas and the assessment procedures used in this assessment were drawn from NIST, Special Publication (SP) 800-53 Revision 3, and “Recommended Security Controls for Federal Information Systems and Organizations” framework for information security management.

Based on the recommended NIST SP 800-53 Revision 3 internal control assessment guidance, a Technical Questionnaire was developed and distributed. This was followed by the NeighborWorks Security Documentation Request Matrix for all policies and procedures pertaining to DCS and HLP interface operation. In addition, a high level NIST SP 800-53 control mapping to CobiT controls, which is the security framework adopted by NeighborWorks, was developed and assessed based upon available IT security control information, Service Level Agreements (SLA), and previous DCS audit results provided.

Lastly, assessment procedures and timeline were developed based on initial meetings, preliminary interviews with key NeighborWorks personnel, and review of all operational and technical information provided.
Observations and Recommendations

Positive Observations - Based on the steps performed on the aforementioned methodology, Internal Audit had positive observations regarding internal security controls surrounding the DCS and HLP interface:

- Physical & Logical Access Controls – The “Audit Review: Data Collection System (DCS)” dated 02 September 2009, provides reasonable assurance that physical access to the servers are secure and remote access to DCS is well controlled through the use of and the use of both public and private keys to authenticate remote computers / users.

- Internal Controls, HLP and DCS Electronic Data Processing – based on a review of the HLP and DCS Electronic Data Processing answers provided, internal controls appear to be in place and operating effectively pertaining to:
  - Relationship with Outsourced Vendors
  - Application Development and Maintenance
  - Database Support

Observations

Observation No 1: Completed IT Security Checklist

The Agreement between NeighborWorks America (corporation) and Hope LoanPort Inc. (contractor) dated May 20th, 2011, states in Section 15, Article XXV, Paragraph 39, “Contractor shall comply with Federal status, regulations, policies and procedures governing the security of system(s) to which contractor has access by providing the Corporation with the following:”

- Completed IT Security Checklist
- Copy of a SAS-70 Certification completed in the last 24 months from the HOPE LoanPort and maintaining such certification during the life of the agreement and
- Signed Memorandum of Understanding mutually agreeable between both parties on the data security procedures being used

Internal audit was able to obtain a copy of a SAS-70 and signed Memorandum of Understanding but there was no evidence provided to substantiate compliance with a completed IT Security Checklist during the performance of this audit review.

A completed IT Security Checklist from HOPE LoanPort® provides the corporation with a greater level of assurance that full compliance has been achieved and that IT Security Controls provided by the contractor are documented based upon an accepted Federal IT

\[\text{SHA-256} \text{ is a cryptographic network protocol for secure data communication, remote shell services or command execution and other secure network services between two networked computers that it connects via a secure channel over an insecure network: a server and a client (running SSH server and SSH client programs, respectively).}
\]

9 See appendix A for more details on IT security requirements on the agreement
Security Control framework. In addition, the checklist provides an audit trail that would enable and adequately facilitate third-party oversight over the governance of systems.

**Recommendation No 1**

We recommend that Management obtain a completed IT Security Checklist from Hope LoanPort® in order to have a greater level of assurance that appropriate security controls are in place at Hope LoanPort® to meet contractual requirements and provide an audit trail. In addition, management should review the accuracy and completeness of the IT Security Checklist annually. As an alternative, in case the third-party service provider utilizes a different security framework from what is required in the agreement, NeighborWorks should ask the service provider to map questions on HUD’s IT Security Checklist to the IT security framework being utilized.

**Conclusion**

Based on the scope of this review, information provided, and information gathered from previous reviews, Internal Audit obtained reasonable assurance that the EHLP program and Contractor(s) have developed a comprehensive set of controls to protect client’s information as well as information systems utilized.
Appendix A
Excerpt of agreement between NeighborWorks® and Hope Loan Port (pg 13).

from another source. The Contractor, must undertake customary and industry standard efforts so that neither they nor its systems vendors disclose any Pre-Applicant, Applicant, Approved Applicant, or Borrower’s (each as defined under the HUD Agreement) personal or financial information to anyone except for authorized personnel in accordance with this Agreement.

Contractor acknowledges: (1) that its systems used in the performance of its respective obligations hereunder, HOPE LoanPort®, CMAX and GrantWorks are systems external to HUD, and will not be connected to, or have access to HUD information systems, and (2) that neither of the foregoing systems is a HUD information system.

Contractor shall comply with applicable Federal statutes, regulations, policies and procedures governing the security of the system(s) to which the Corporation, Sub-grantees, Fiscal Agent and Contractor have access, including, but not limited to:

(i) Federal Information Security Management Act (FISMA) of 2002;


(iii) HUD Handbook 2400.25, Information Security Policy;

(iv) HUD Handbook 732.3, Personnel Security/Suitability;

(v) Federal Information Processing Standards 201 (FIPS 201), Sections 2.1 and 2.2;

(vi) Homeland Security Presidential Directive 12 (HSPD-12); and

(vii) OMB Memorandum M-05-24, Implementing Guidance for HSPD-12.

Contractor may demonstrate compliance with applicable Federal statutes, regulations, policies and procedures governing the security of the system(s) to which Contractor has access by providing the Corporation with the following:

- Completed IT Security Checklist (attached to this Agreement);
- Copy of a SAS-70 Certification completed in the last 24 months from HOPE LoanPort® and maintaining such certification during the life of the agreement; and
- Signed Memorandum of Understanding mutually agreeable between both parties on the data security procedures being used.

ARTICLE XXVI – WORK PRODUCT AS GOVERNMENT PROPERTY

Notwithstanding any other provision of this Agreement, Contractor agrees that all Work
Appendix B

(i) Federal Information Security Management Act (FISMA) of 2002  

http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii

(iii) HUD Handbook 2400.25, Information Security Policy  
(http://www.hud.gov/offices/adm/hudclips/handbooks/admh/2400.25/index.cfm)

(iv) HUD Handbook 732.3, Personnel Security/Suitability  

(v) Federal Information Processing Standards 201 (FIPS 201), Section 2.1 and 2.2  

(vi) Homeland Security Presidential Directive 12 (HSPD-12)  
http://www.dhs.gov/homeland-security-presidential-directive-12

(vii) OMB Memorandum M-05-24, Implementing Guidelines for HSPD-12  