Internal Audit Department
NeighborWorks® America

# Review of Cybersecurity Protocols

Project Number: NW.ITS.CYBERSEC.2018

**Review of Cybersecurity Protocols**

## Table of Contents

October 5, 2018

To: NeighborWorks® America Audit Committee

Subject: **Review of Cybersecurity Protocols**

Attached is our draft audit report for the NWA's corporations Cybersecurity Protocols. Please contact me with any questions you might have.

Thank you.

Frederick Udochi
Chief Audit Executive

Attachment

cc: M. Rodriguez
T. Chabolla
R. Bond
R. Simmons

# Function Responsibility and Internal Control Assessment
# Review of Cybersecurity Protocols

| Business Function Responsibility | Report Date | Period Covered |
|---|---|---|
| Information Technology & Services | October 5, 2018 | January 1, 2018 to September 30, 2018 |
| **Assessment of Internal Control Structure** | | |
| Effectiveness and Efficiency of Operations | | **Generally Effective**[1] |
| Reliability of Financial Reporting | | **Not Applicable** |
| Compliance with Applicable Laws and Regulations | | **Not Applicable** |

This report was reissued February 15, 2024 in accordance with a recommendation by the Government Accountability Office (GAO-23-105944, June 14, 2023).

[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

| Summarized Observation Risk Rating | Management Agreement with Observation (Yes/ No) | Internal Audit Recommendation Summary | Accept IA Recommendation (Yes/ No) | Management's Response to IA Recommendation | Estimated Date of Implementation (Month/Year) | Internal Audit Comments on Management Response |
|---|---|---|---|---|---|---|
| **Observation 1**<br>(b) (5)<br>NeighborWorks® America has (b) (5) .<br>**Risk Rating**: (b) (5) | **Yes** | **Recommendation 1**<br>We recommend that NeighborWorks® (b) (5) that would also be in alignment with (b) (5) | **Yes** | IT&S will conduct research on (b) (5) that will best fits the organization's needs Estimated completion (b) (5) .<br>(b) (5) Estimated completion (b) (5) . | (b) (5) | Internal Audit Accept Management's Response |
| **Observation 2**<br>(b) (5)<br>NeighborWorks® America does not have in place (b) (5) . | **Yes** | **Recommendation 2**<br>We recommend that NeighborWorks® (b) (5) | **Yes** | IT&S intends to (b) (5) | (b) (5) | Internal Audit Accept Management's Response |

| Summarized Observation Risk Rating | Management Agreement with Observation (Yes/ No) | Internal Audit Recommendation Summary | Accept IA Recommendation (Yes/ No) | Management's Response to IA Recommendation | Estimated Date of Implementation (Month/Year) | Internal Audit Comments on Management Response |
|---|---|---|---|---|---|---|
| **Risk Rating**: (b) (5) | | | | | | |
| **Observation 3**<br>(b) (5)<br>(b) (5) are not in place to ensure consistency in the (b) (5) across the NeighborWorks® (b) (5).<br><br>**Risk Rating**: (b) (5) | **Yes** | **Recommendation 3**<br>We recommend that NeighborWorks® (b) (5) for System Administrators are communicated to these individuals and that follow-up is performed to (b) (5).<br><br>We also recommend that the Corporation institute an (b) (5) | **Yes** | IT&S will create a (b) (5) to use. This (b) (5).<br><br>Training for All Staff via Grovo: :03/22/2019<br><br>(b) (5) | (b) (5) | Internal Audit Accept Management's Response |

| Summarized Observation Risk Rating | Management Agreement with Observation (Yes/ No) | Internal Audit Recommendation Summary | Accept IA Recommendation (Yes/ No) | Management's Response to IA Recommendation | Estimated Date of Implementation (Month/Year) | Internal Audit Comments on Management Response |
|---|---|---|---|---|---|---|
| | | (b) (5) The Security Awareness training for all staff should also be continued to be administered on an annual basis. | | | | |

## 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 Responses to<br>The Review of:<br><br>Cybersecurity Program** | | |
|---|---|---|
| **# of Responses** | **Response** | **Recommendation #** |
| 3 | Agreement with the recommendation(s) | 3 |
| 0 | Disagreement with the recommendation(s) | 0 |

## Background

NeighborWorks® America is responsible for ensuring that adequate security and related support processes are in place to minimize risk associated with cyber threats. To accomplish this requirement, certain Cybersecurity measures have been put in place to prevent, detect and respond to recover a Cybersecurity incident.

## Objective

The objective of .this review was to determine whether the Cybersecurity Program met the program objectives of protecting the corporate environment through a series of preventive and detective protocols when responding to potential attacks in a formal and timely manner.

## Scope

The scope of these procedures included an evaluation of the processes and controls associated with the Cybersecurity Protocols at NeighborWorks®. Our procedures focused specifically on the following areas:

- Review processes and procedures in place to support the NeighborWorks® Cybersecurity program for each of the required components: Identify, Detect, Protect, Respond and Recover. The review was based on the NIST Cybersecurity framework.

- Review documentation that will support the maturity level (Ad-hoc, Defined, Consistently Implemented, Managed and Measurable or Optimize) for each of the 5 components of the Cybersecurity program listed above.

## Methodology

Procedures were performed to determine whether the Cybersecurity Protocols addressed the foundational areas of a Cybersecurity program. The framework used was based on the National Institute of Standards and Technology Cybersecurity (NIST) Cybersecurity Framework. These foundational areas are Identify, Protect, Detect, Respond and Recover. Testing, verification and validation of the aforementioned components were conducted against documentations provided by IT&S.

Below are the observations and recommendations that resulted from the testing performed.

## Observations and Recommendations

### Observation 1 – (b) (5)

NeighborWorks® America has (b) (5) . A framework would provide established guidelines for (b) (5) . NIST Publication

800-37[2] defines the objectives for having a Risk Management Framework for Information Systems. The objectives based on NIST 800-37 to be accomplished through a Risk Management Framework for Information Systems are as follows:

- Provides a repeatable process designed to promote the protection of information and information systems commensurate with risk;
- Emphasizes organization-wide preparation necessary to manage security and privacy risks;
- Facilitates the categorization of information and systems; the selection, implementation, assessment, and monitoring of controls; and the authorization of information systems and common controls;
- Promotes near real-time risk management and ongoing system and control authorization through the implementation of robust continuous monitoring processes;
- Encourages the use of automation to provide senior leaders with the necessary information to make cost-effective, risk-based decisions for information systems supporting their missions and business functions;
- Facilitates the seamless integration of security and privacy requirements and controls into enterprise architecture, Systems Development Life Cycle, acquisition processes, and systems engineering processes;
- Connects risk management processes at the organization and mission/business process levels to risk management processes at the information system level via a risk executive (function); and,
- Establishes responsibility and accountability for controls implemented within information systems and inherited by those systems.

Based on NIST 800-37, the Risk Management Framework provides a dynamic and flexible approach to effectively manage information security and privacy risks in diverse environments with complex and sophisticated threats, changing missions, and system vulnerabilities. In the absence of an established framework it would be difficult to benchmark and evaluate the current structures for effectiveness and efficiency.

**Recommendation 1**

We recommend that NeighborWorks® adopt and implement an IT&S Risk Management Framework modified and adapted to meet the scale, scope and sophistication of current IT&S activities which references best practice guidelines such as NIST 800-37, ISACA's The Risk IT

[2] NIST 800-37: Risk Management Framework for Information Systems and Organizations – A System Life Cycle Approach for Security and Privacy, was developed by National Institute of Standards and Technology (NIST) in May 2018 to provide minimum requirements for federal information systems.

Framework-based on COBIT[3]5, etc. This framework should be seamlessly aligned with the Corporations ERM framework.

**Observation 2 –** (b) (5)

NeighborWorks® America does not have in place (b) (5) . NeighborWorks® America has (b) (5) . These applications are (b) (5) .

The (b) (5) . Examples of outcome categories within this function include (b) (5)

**Recommendation 2**

We recommend that NeighborWorks® implement (b) (5) .

**Observation 3 –** (b) (5)

Assessment processes are (b) (5) NeighborWorks® operates the various (b) (5) Monitoring should include such functions as (b) (5) We also observed that specifically related to Information Security and Awareness Training, such training was last administered to all employees in 2017.

**Recommendation 3**

We recommend that NeighborWorks® implement a (b) (5) The (b) (5)

[3] COBIT (Control Objectives for Information and Related Technologies) is an IT management framework developed by ISACA. COBIT 5 focuses amongst other activities on security, risk management and information governance.

(b) (5) . This would ensure consistency in practice for all (b) (5) .

We also recommend that the Corporation institute an annual Security Awareness training for all System Administrators geared towards cybersecurity threats. The Security Awareness training for all staff should also be continued to be administered on an annual basis.

**Conclusion**

The table below provides the Internal Audit maturity level conclusion for each area of the NeighborWorks® Cybersecurity Program. The maturity levels defined according to the NIST Cybersecurity Framework are Ad-hoc, Defined, Consistently Implemented, Managed and Measurable or Optimize. We can conclude that overall the current maturity level is "Defined" which is good progress given that the protocols are less than 2 years old.

| Area | Maturity Level | Observation Identified |
|---|---|---|
| (b) (5) | Defined | 1 |
| | Defined | 3 |
| | Defined | 2 |
| | Defined | *Note 1 |
| | Defined | *Note 1 |

***Note 1: This area is impacted by all observations and cannot achieve another level of maturity until all observations are addressed.**

The review procedures and related recommendations should help NeighborWorks® enhance the processes and procedures supporting the Cybersecurity Program.