PRB

ARKANSAS FIRE & POLICE PENSION REVIEW BOARD

620 W. 3rd Street, Suite 200
Little Rock, Arkansas 72201-2223
Telephone: (501) 682-1745
email: info@lopfi-prb.com
website: www.lopfi-prb.com

# PRB Audit Committee Meeting Agenda

Meeting to be held via Zoom (login details below)
Thursday, May 2, 2024
10:15 a.m.

| | | |
|---|---|---|
| 1. | Call to Order<br>Recognition of news media notification | Chairman Ledford |
| 2. | Review December 31, 2023 Financial Audit Report and IT Assessment Report | Chairman Ledford |
| 3. | Adjourn | Chairman Ledford |

To attend the meeting via the Zoom platform, follow the two (2) step process:

***Step 1 – Registration – Complete any time prior to the meeting.*** Click this link to register for the meeting:
https://us06web.zoom.us/meeting/register/tZIkcuGsrzgqGtcbUNAQQhhBVqo8bkOp9eC4

***Step 2 – Join Meeting – Complete at least 10 minutes prior to the start time.***
Once registration is completed an email from PRB staff at no-reply@zoom.us will be sent to you. The email will have a *Click Here to Join* button to select to join the meeting. If you are using the Zoom app on a mobile device, the email will also provide the Meeting ID number.

PRB

ARKANSAS FIRE & POLICE PENSION REVIEW BOARD

620 W. 3rd Street, Suite 200
Little Rock, Arkansas 72201-2223
Telephone: (501) 682-1745
email: info@lopfi-prb.com
website: www.lopfi-prb.com

April 18, 2024

Arkansas Democrat-Gazette
PO Box 2221
Little Rock, AR 72203

Via Email: mwickline@arkansasonline.com (2 pages)

Dear Ladies and Gentlemen:

The PRB Audit Committee will hold a meeting on May 2, 2024 at 10:15 am. The purpose of the meeting is to review the December 31, 2023 audit report. The meeting will be held at 620 W. 3rd Street, Suite 200 in Little Rock. An agenda is included with this notice.

Respectfully,

PRB Staff

**PRB**

ARKANSAS FIRE & POLICE PENSION REVIEW BOARD

620 W. 3rd Street, Suite 200
Little Rock, Arkansas 72201-2223
Telephone: (501) 682-1745
email: info@lopfi-prb.com
website: www.lopfi-prb.com

April 18, 2024

Arkansas Business
PO Box 3686
Little Rock, AR 72203

Via Email: lturner@abpg.com (2 pages)

Dear Ladies and Gentlemen:

The PRB Audit Committee will hold a meeting on May 2, 2024 at 10:15 am. The purpose of the meeting is to review the December 31, 2023 audit report. The meeting will be held at 620 W. 3rd Street, Suite 200 in Little Rock. An agenda is included with this notice.

Respectfully,

PRB Staff

FORVIS®

# Report to the Board

## Arkansas Fire and Police Pension Review Board

## Results of the 2023 Financial Statement Audit, Including Required Communications

Little Rock, Arkansas
December 31, 2023

# Required Communications Regarding Our Audit Strategy & Approach (AU-C 260)

The following matters are required communications we must make to you, including these responsibilities:

## Overview & Responsibilities

| Matter | Discussion |
|---|---|
| **Scope of Our Audit** | This report covers audit results related to your financial statements and supplementary information:<br>• As of and for the year ended December 31, 2023<br>• Conducted in accordance with our contract dated November 22, 2023. |
| **Our Responsibilities** | FORVIS is responsible for forming and expressing an opinion/opinions about whether the financial statements that have been prepared by management, with the oversight of those charged with governance, are prepared in accordance with accounting principles generally accepted in the United States of America (GAAP). |
| **Audit Scope & Inherent Limitations to *Reasonable Assurance*** | An audit performed in accordance with auditing standards generally accepted in the United States of America (GAAS) and *Government Auditing Standards* issued by the Comptroller General of the United States (GAGAS) is designed to obtain reasonable, rather than absolute, assurance about the financial statements. The scope of our audit tests was established in relation to the financial statements taken as a whole and did not include a detailed audit of all transactions. |

| Matter | Discussion |
|---|---|
| **Extent of Our Communication** | In addition to areas of interest and noting prior communications made during other phases of the engagement, this report includes communications required in accordance with GAAS that are relevant to the responsibilities of those charged with governance in overseeing the financial reporting process, including audit approach, results, and internal control. The standards do not require the auditor to design procedures for the purpose of identifying other matters to be communicated with those charged with governance. |
| **Independence** | The engagement team, others in our firm, as appropriate, and our firm have complied with all relevant ethical requirements regarding independence. |
| **Your Responsibilities** | Our audit does not relieve management or those charged with governance of your responsibilities. Your responsibilities and ours are further referenced in our contract. |
| **Distribution Restriction** | This communication is intended solely for the information and use of the following and is not intended to be, and should not be, used by anyone other than these specified parties:<br>• The board members<br>• Others within the Entity |

## Qualitative Aspects of Significant Accounting Policies & Practices

The following matters are detailed in the following pages and included in our assessment:

### Significant Accounting Policies

Significant accounting policies are described in Note 1 of the audited financial statements.

With respect to new accounting standards adopted during the year, we call to your attention the following topics detailed in the following pages:

- No matters are reportable.

### Unusual Policies or Methods

With respect to significant unusual accounting policies or accounting methods used for significant unusual transactions (significant transactions outside the normal course of business or that otherwise appear to be unusual due to their timing, size, or nature), we noted the following:

- No matters are reportable.

### Alternative Accounting Treatments

We had discussions with management regarding alternative accounting treatments within GAAP for policies and practices for material items, including recognition, measurement, and disclosure considerations related to the accounting for specific transactions as well as general accounting policies, as follows:

- No matters are reportable.

## Management Judgments & Accounting Estimates

Accounting estimates are an integral part of financial statement preparation by management, based on its judgments. Significant areas of such estimates for which we are prepared to discuss management's estimation process and our procedures for testing the reasonableness of those estimates include:

- Allocation of expense between the PRB and Arkansas Local Police and Fire Retirement System

## Financial Statement Disclosures

The following area involves particularly sensitive financial statement disclosures for which we are prepared to discuss the issues involved and related judgments made in formulating those disclosures:

- Related-party transactions

## Our Judgment About the Quality of the Entity's Accounting Principles

During the course of the audit, we made the following observations regarding the Entity's application of accounting principles:

- No matters are reportable.

FORVIS

## Adjustments Identified by Audit

During the course of any audit, an auditor may propose adjustments to financial statement amounts. Management evaluates our proposals and records those adjustments that, in its judgment, are required to prevent the financial statements from being materially misstated.

A misstatement is a difference between the amount, classification, presentation, or disclosure of a reported financial statement item and that which is required for the item to be presented fairly in accordance with the applicable financial reporting framework.

## Proposed & Recorded Adjustments

Auditor-proposed and management-recorded entries include the following:

- No matters are reportable.

## Other Required Communication

### Other Material Communication

Listed below is another material communication between management and us related to the audit:

- Management representation letter (see attached)

FORVIS

Representation of:
Arkansas Fire and Police Pension Review Board
620 W. Third Street, Suite 200
Little Rock, Arkansas 72201

*Provided to:*
**FORVIS, LLP**
Certified Public Accountants
111 Center Street, Suite 1600
Little Rock, Arkansas 72201

The undersigned ("We") are providing this letter in connection with FORVIS' audits of our financial statements as of and for the years ended December 31, 2023 and 2022.

Our representations are current and effective as of the date of FORVIS' report: April 15, 2024.

Our engagement with FORVIS is based on our contract for services dated: November 27, 2023.

## Our Responsibility & Consideration of Material Matters

We confirm that we are responsible for the fair presentation of the financial statements subject to FORVIS' report in conformity with accounting principles generally accepted in the United States of America.

We are also responsible for adopting sound accounting policies; establishing and maintaining effective internal control over financial reporting, operations, and compliance; and preventing and detecting fraud.

Certain representations in this letter are described as being limited to matters that are material. Items are considered material, regardless of size, if they involve an omission or misstatement of accounting information that, in light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would be changed or influenced by the omission or misstatement. An omission or misstatement that is monetarily small in amount could be considered material as a result of qualitative factors.

## Confirmation of Matters Specific to the Subject Matter of FORVIS' Report

We confirm, to the best of our knowledge and belief, the following:

***Broad Matters***

1. We have fulfilled our responsibilities, as set out in the terms of our contract, for the preparation and fair presentation of the financial statements in accordance with accounting principles generally accepted in the United States of America.

2. We acknowledge our responsibility for the design, implementation, and maintenance of:

   a. Internal control relevant to the preparation and fair presentation of the financial statements that are free from material misstatement, whether due to fraud or error.

   b. Internal control to prevent and detect fraud.

3. We have provided you with:

   a. Access to all information of which we are aware that is relevant to the preparation and fair presentation of the financial statements, such as financial records and related data, documentation, and other matters.

   b. Additional information that you have requested from us for the purpose of the audit.

   c. Unrestricted access to persons within the entity from whom you determined it necessary to obtain audit evidence.

   d. All minutes of governing body meetings held through the date of this letter or summaries of actions of recent meetings for which minutes have not yet been prepared. All unsigned copies of minutes provided to you are copies of our original minutes approved by the board, if applicable, and maintained as part of our records.

   e. All significant contracts.

4. We have responded fully and truthfully to all your inquiries.

***Government Auditing Standards***

5. We acknowledge that we are responsible for compliance with applicable laws, regulations and provisions of contracts and grant agreements.

6. We have identified and disclosed to you all laws, regulations, and provisions of contracts and grant agreements that have a direct and material effect on the determination of amounts in our financial statements or other financial data significant to the audit objectives.

7. We have identified and disclosed to you any violations or possible violations of laws, regulations, and provisions of contracts and grant agreements, tax or debt limits and any related debt covenants whose effects should be considered for recognition and/or disclosure in the financial statements or for your reporting on noncompliance.

8. We have taken or will take timely and appropriate steps to remedy any fraud, abuse, illegal acts, or violations of provisions of contracts or grant agreements that you or other auditors report.

9. We have a process to track the status of audit findings and recommendations.

10. We have identified to you any previous financial audits, attestation engagements, performance audits, or other studies related to the objectives of your audit and the corrective actions taken to address any significant findings and recommendations made in such audits, attestation engagements, or other studies.

***Misappropriation, Misstatements, & Fraud***

11. We have informed you of all current risks of a material amount that are not adequately prevented or detected by our procedures with respect to:

    a. Misappropriation of assets.

    b. Misrepresented or misstated assets or liabilities.

12. We have no knowledge of fraud or suspected fraud affecting the entity involving:

    a. Management or employees who have significant roles in internal control over financial reporting, or

    b. Others when the fraud could have a material effect on the financial statements.

13. We have no knowledge of any allegations of fraud or suspected fraud affecting the entity received in communications from employees, former employees, customers, analysts, SEC or other regulators, citizens, short-sellers, suppliers, or others.

14. We have assessed the risk that the financial statements may be materially misstated as a result of fraud and disclosed to you any such risk identified.

***Related Parties***

15. We have disclosed to you the identity of all of the entity's related parties and all the related-party relationships of which we are aware.

    In addition, we have disclosed to you all related-party transactions and amounts receivable from or payable to related parties of which we are aware, including any modifications during the year that were made to related-party transaction agreements which existed prior to the beginning of the year under audit, as well as new related-party transaction agreements that were executed during the year under audit.

    Related-party relationships and transactions have been appropriately accounted for and disclosed in accordance with accounting principles generally accepted in the United States of America.

16. We understand that the term related party refers to:

    - Affiliates.
    - Board members and members of their immediate families.
    - Management and members of their immediate families.
    - Any other party with which the entity may deal if one party can significantly influence the management or operating policies of the other to an extent that one of the transacting parties might be prevented from fully pursuing its own separate interests.

    Another party is also a related party if it can significantly influence the management or operating policies of the transacting parties or if it has an ownership interest in one of the transacting parties and can significantly influence the other to an extent that one or more of the transacting parties might be prevented from fully pursuing its own separate interests.

    The term affiliate refers to a party that directly or indirectly controls, or is controlled by, or is under common control with, the entity.

***Litigation, Laws, Rulings & Regulations***

17. We are not aware of any pending or threatened litigation or claims whose effects should be considered when preparing the financial statements. We have not sought or received attorney's services related to pending or threatened litigation or claims during or subsequent to the audit period. Also, we are not aware of any litigation or claims, pending or threatened, for which legal counsel should be sought.

18. We have no knowledge of communications, other than those specifically disclosed, from regulatory agencies, governmental representatives, employees, or others concerning investigations or allegations of noncompliance with laws and regulations, deficiencies in financial reporting practices, or other matters that could have a material adverse effect on the financial statements.

19. We have disclosed to you all known instances of violations or noncompliance or possible violations or suspected noncompliance with laws and regulations whose effects should be considered when preparing financial statements or as a basis for recording a loss contingency, of which there were none.

20. We have no reason to believe the entity owes any penalties or payments under the Employer Shared Responsibility Provisions of the *Patient Protection and Affordable Care Act* nor have we received any correspondence from the IRS or other agencies indicating such payments may be due.

21. We have not been designated as a potentially responsible party (PRP or equivalent status) by the Environmental Protection Agency (EPA) or other cognizant regulatory agency with authority to enforce environmental laws and regulations:

***Nonattest Services***

22. You have provided nonattest services, including the following, during the period of this engagement:

    - Preparing a draft of the financial statements and related notes and supplementary information and supplementary information
    - Assistance with year-end closing entries and outsourcing certain account reconciliations

23. With respect to these services:

    a. We have designated a qualified management-level individual to be responsible and accountable for overseeing the nonattest services.

    b. We have established and monitored the performance of the nonattest services to ensure they meet our objectives.

    c. We have made any and all decisions involving management functions with respect to the nonattest services and accept full responsibility for such decisions.

    d. We have evaluated the adequacy of the services performed and any findings that resulted.

    e. Established and maintained internal controls, including monitoring ongoing activities.

    f. When we receive final deliverables from you we will store those deliverables in information systems controlled by us. We have taken responsibility for maintaining internal control over these deliverables.

***Financial Statements & Reports***

24. We have reviewed and approved a draft of the financial statements and related notes referred to above, which you prepared in connection with your audit of our financial statements. We acknowledge that we are responsible for the fair presentation of the financial statements and related notes.

25. With regard to supplementary information:

    a. We acknowledge our responsibility for the presentation of the supplementary information in accordance with the applicable criteria.

    b. We believe the supplementary information is fairly presented, both in form and content, in accordance with the applicable criteria.

    c. The methods of measurement and presentation of the supplementary information are unchanged from those used in the prior period, and we have disclosed to you any significant assumptions or interpretations underlying the measurement and presentation of the supplementary information.

    d. We believe the significant assumptions or interpretations underlying the measurement and/or presentation of the supplementary information are reasonable and appropriate.

***Transactions, Records & Adjustments***

26. All transactions have been recorded in the accounting records and are reflected in the financial statements.

27. We have everything we need to keep our books and records.

28. We have disclosed any significant unusual transactions the entity has entered into during the period, including the nature, terms, and business purpose of those transactions.

29. We are in agreement with the adjusting journal entries you have proposed, and they have been posted to the entity's accounts.

***Governmental Accounting & Disclosure Matters***

30. Interfund, internal, and intra-entity activity and balances have been appropriately classified and reported.

31. The supplementary information required by the Governmental Accounting Standards Board, consisting of management's discussion and analysis, has been prepared and is measured and presented in conformity with the applicable GASB pronouncements, and we acknowledge our responsibility for the information. The information contained therein is based on all facts, decisions, and conditions currently known to us and is measured using the same methods and assumptions as were used in the preparation of the financial statements. We believe the significant assumptions underlying the measurement and/or presentation of the information are reasonable and appropriate. There has been no change from the preceding period in the methods of measurement and presentation.

***Accounting & Disclosures***

32. All transactions entered into by the entity are final. We are not aware of any unrecorded transactions, side agreements or other arrangements (either written or oral) that are in place.

33. Except as reflected in the financial statements, there are no:

    a. Plans or intentions that may materially affect carrying values or classifications of assets or liabilities.

    b. Material transactions omitted or improperly recorded in the financial records.

c. Material unasserted claims or assessments that are probable of assertion or other gain/loss contingencies requiring accrual or disclosure, including those arising from environmental remediation obligations.

d. Events occurring subsequent to the balance sheet date through the date of this letter, which is the date the financial statements were available to be issued, requiring adjustment or disclosure in the financial statements.

e. Agreements to purchase assets previously sold.

f. Arrangements with financial institutions involving compensating balances or other arrangements involving restrictions on cash balances, lines of credit or similar arrangements.

g. Guarantees, whether written or oral, under which the entity is contingently liable.

34. Except as disclosed in the financial statements, the entity has:

a. Satisfactory title to all recorded assets, and those assets are not subject to any liens, pledges, or other encumbrances.

b. Complied with all aspects of contractual agreements, for which noncompliance would materially affect the financial statements.

***Estimates***

35. We have identified all accounting estimates that could be material to the financial statements and we confirm the appropriateness of the methods and the consistency in their application, the accuracy and completeness of data and the reasonableness of significant assumptions used by us in making the accounting estimates, including those measured at fair value reported in the financial statements.

36. Significant estimates that may be subject to a material change in the near term have been properly disclosed in the financial statements. We understand that "near term" means the period within one year of the date of the financial statements. In addition we have no knowledge of concentrations, which refer to volumes of business, investments, or deposits, existing at the date of the financial statements that would make the entity vulnerable to the risk of severe impact in the near term that have not been properly disclosed in the financial statements.

DocuSigned by:
[redacted]
0403E73FA7574C5...

David B. Clark, Executive Director
dclark@lopfi-prb.com

DocuSigned by:
[redacted]
BDF859E80A51479...

Jen Sines, Chief Financial Officer
jsines@lopfi-prb.com

# Arkansas Fire and Police Pension Review Board

## Independent Auditor's Report and Financial Statements

December 31, 2023 and 2022

**Arkansas Fire and Police Pension Review Board**
**Contents**
**December 31, 2023 and 2022**

## Contents

FORVIS

111 Center Street, Suite 1600 / Little Rock, AR 72201
P 501.372.1040 / F 501.372.1250
forvis.com

# Independent Auditor's Report

Board Members
Arkansas Fire and Police Pension Review Board
Little Rock, Arkansas

## Report on the Audit of the Financial Statements

### *Opinions*

We have audited the accompanying financial statements of the Arkansas Fire and Police Pension Review Board (PRB) as of and for the years ended December 31, 2023 and 2022, and the related notes to the financial statements, which collectively comprise the PRB's basic financial statements as listed in the table of contents.

In our opinion, the accompanying financial statements referred to above present fairly, in all material respects, the financial position of the Arkansas Fire and Police Pension Review Board as of December 31, 2023 and 2022, and the changes in financial position and its cash flows for the years then ended in accordance with accounting principles generally accepted in the United States of America.

### *Basis for Opinions*

We conducted our audit in accordance with auditing standards generally accepted in the United States of America (GAAS) and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States (*Government Auditing Standards*). Our responsibilities under those standards are further described in the "Auditor's Responsibilities for the Audit of the Financial Statements" section of our report. We are required to be independent of the PRB, and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements relating to our audits. We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

### *Responsibilities of Management for the Financial Statements*

Management is responsible for the preparation and fair presentation of these financial statements in accordance with accounting principles generally accepted in the United States of America, and for the design, implementation and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error.

In preparing the financial statements, management is required to evaluate whether there are conditions or events, considered in the aggregate, that raise substantial doubt about the PRB's ability to continue as a going concern for 12 months beyond the financial statement date, including any currently known information that may raise substantial doubt shortly thereafter.

### *Auditor's Responsibilities for the Audit of the Financial Statements*

Our objectives are to obtain reasonable assurance about whether the financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinion. Reasonable assurance is a high level of assurance but is not absolute assurance and therefore is not a guarantee that an audit conducted in accordance with GAAS and *Government Auditing Standards* will always detect a material misstatement when it exists. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control. Misstatements are considered material if there is a substantial likelihood that, individually or in the aggregate, they would influence the judgment made by a reasonable user based on the financial statements.

In performing an audit in accordance with GAAS and *Government Auditing Standards*, we:

- Exercise professional judgment and maintain professional skepticism throughout the audit.
- Identify and assess the risks of material misstatement of the financial statements, whether due to fraud or error, and design and perform audit procedures responsive to those risks. Such procedures include examining, on a test basis, evidence regarding the amounts and disclosures in the financial statements.
- Obtain an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the PRB's internal control. Accordingly, no such opinion is expressed.
- Evaluate the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluate the overall presentation of the financial statements.
- Conclude whether, in our judgment, there are conditions or events, considered in the aggregate, that raise substantial doubt about the PRB's ability to continue as a going concern for a reasonable period of time.

We are required to communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit, significant audit findings, and certain internal control-related matters that we identified during the audit.

### *Required Supplementary Information*

Accounting principles generally accepted in the United States of America require that the management's discussion and analysis as listed in the table of contents be presented to supplement the basic financial statements. Such information is the responsibility of management and, although not a part of the basic financial statements, is required by the Governmental Accounting Standards Board, who considers it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America, which consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the financial statements and other knowledge we obtained during our audit of the financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

## Other Reporting Required by *Government Auditing Standards*

In accordance with *Government Auditing Standards*, we also have issued our report dated April 15, 2024, on our consideration of the PRB's internal control over financial reporting and on our tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements and other matters. The purpose of that report is solely to describe the scope of our testing of internal control over financial reporting and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the PRB's internal control over financial reporting or on compliance. That report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the PRB's internal control over financial reporting and compliance.

FORVIS, LLP

**Little Rock, Arkansas**
**April 15, 2024**

The management's discussion and analysis (MD&A) of the Arkansas Fire and Police Pension Review Board (hereafter referred to as the PRB) provides an overview of the financial activities for the years ended December 31, 2023 and 2022. For more detailed information regarding PRB financial activities, the reader should review the actual financial statements, including all notes.

The executive director and staff of Arkansas Local Police and Fire Retirement System (LOPFI) serve as executive director and staff for the PRB. LOPFI receives all revenue and pays all expenses for the PRB. The allocation of expenses is determined by each respective board through the use of an Administrative Services Committee composed of members of both boards.

The basic financial statements consist of:

The *Balance Sheet* reports the assets liabilities and net position at the end of the calendar year. The *Balance Sheet* is prepared on the accrual basis.

The *Statement of Revenues, Expenses and Changes in Net Position* reports the PRB's operating revenues, operating expenses and net position at the end of the calendar year. The PRB is entitled to receive up to one percent (1%) of the total premium tax revenues for its administrative and premium tax allocation expenses. The net position, beginning of year, reflects the net position reported on the prior year's balance sheet as of the end of that fiscal year.

The *Statement of Cash Flows* shows there is no cash generated by operating activities. The revenues and expenses attributable to the PRB are allocated to the PRB account on the LOPFI books. Due to this arrangement, the major asset of the PRB is a receivable from LOPFI.

The *Notes to Financial Statements* are an integral part of the PRB's financial statements and can be found on Page 10.

## Summary Balance Sheets

| | 2023 | 2022 | 2021 | 2023 Percent Change | 2022 Percent Change |
|---|---|---|---|---|---|
| Receivable from Arkansas Local Police and Fire Retirement System (LOPFI) | $ 394,967 | $ 352,372 | $ 416,560 | 12.09% | -15.41% |
| Total assets | $ 394,967 | $ 352,372 | $ 416,560 | 12.09% | -15.41% |
| Accrued expenses | $ 6,379 | $ 3,828 | $ 4,313 | 66.64% | -11.25% |
| Total liabilities | 6,379 | 3,828 | 4,313 | 66.64% | -11.25% |
| Total net position | 388,588 | 348,544 | 412,247 | 11.49% | -15.45% |
| Total liabilities and net position | $ 394,967 | $ 352,372 | $ 416,560 | 12.09% | -15.41% |

## December 31, 2023

LOPFI receives all revenue and pays all expenses for the PRB. For the year ended December 31, 2023, LOPFI paid more in expenses for PRB than was received in revenue. This resulted in the receivable from LOPFI increasing by $42,595 in 2023.

## December 31, 2022

LOPFI receives all revenue and pays all expenses for the PRB. For the year ended December 31, 2022, LOPFI paid more in expenses for PRB than was received in revenue. This resulted in the receivable from LOPFI decreasing by $64,188 in 2022.

## Summary Statement of Revenues, Expenses and Changes in Net Position

| | 2023 | 2022 | 2021 | 2023 Percent Change | 2022 Percent Change |
|---|---|---|---|---|---|
| State Insurance Commission tax turnback – PRB operations | $ 473,000 | $ 340,000 | $ 426,000 | 39.12% | -20.19% |
| State Insurance Commission tax turnback – UALR mapping project | 131,512 | 131,512 | 131,512 | 0.00% | 0.00% |
| State Insurance Commission tax turnback – allocation report | 54,000 | 54,000 | 52,000 | 0.00% | 3.85% |
| Operating revenue | 658,512 | 525,512 | 609,512 | 25.31% | -13.78% |
| UALR mapping program | 131,512 | 131,512 | 131,512 | 0.00% | 0.00% |
| Salaries | 239,074 | 229,615 | 220,755 | 4.12% | 4.01% |
| Actuarial expense | 101,825 | 107,950 | 113,420 | -5.67% | -4.82% |
| Office supplies | 16,591 | 7,881 | 20,315 | 110.52% | -61.21% |
| Office equipment maintenance | 57,729 | 48,596 | 33,006 | 18.79% | 47.23% |
| Other expenses | 71,737 | 63,661 | 57,285 | 12.69% | 11.13% |
| Operating expenses | 618,468 | 589,215 | 576,293 | 4.96% | 2.24% |
| Change in net position | $ 40,044 | $ (63,703) | $ 33,219 | -162.86% | -291.77% |

## December 31, 2023

The PRB is entitled to receive a portion of insurance premium tax monies for administrative expenses as defined in ACA 24-11-203. Based on the 2023 budget, the PRB requested and received $473,000 for PRB operations and $54,000 for the premium tax allocation report during 2023. In addition, the PRB received $131,512 for the UALR mapping project. The increase in expenses for the year ended December 31, 2023 was primarily due to an increase in salary expenses, office supplies and office equipment maintenance expense.

## December 31, 2022

The PRB is entitled to receive a portion of insurance premium tax monies for administrative expenses as defined in ACA 24-11-203. Based on the 2022 budget, the PRB requested and received $340,000 for PRB operations and $54,000 for the premium tax allocation report during 2022. In addition, the PRB received $131,512 for the UALR mapping project. The increase in expenses for the year ended December 31, 2022 was primarily due to an increase in salary expense and office equipment maintenance expense.

# Arkansas Fire and Police Pension Review Board
## Balance Sheets
## December 31, 2023 and 2022

| | 2023 | 2022 |
|---|---|---|
| **Assets** | | |
| Receivable from Arkansas Local Police and Fire Retirement System (LOPFI) | $ 394,967 | $ 352,372 |
| Total current assets | 394,967 | 352,372 |
| Total assets | $ 394,967 | $ 352,372 |
| **Liabilities** | | |
| Accrued expenses | $ 6,379 | $ 3,828 |
| Total current liabilities | 6,379 | 3,828 |
| Total liabilities | 6,379 | 3,828 |
| **Net Position** | | |
| Net position | 388,588 | 348,544 |
| Total net position | 388,588 | 348,544 |
| Total liabilities and net position | $ 394,967 | $ 352,372 |

# Arkansas Fire and Police Pension Review Board
## Statements of Revenues, Expenses and Changes in Net Position
## Years Ended December 31, 2023 and 2022

| | 2023 | 2022 |
|---|---|---|
| **Operating Revenues** | | |
| State Insurance Commission tax turnback – PRB operations | $ 473,000 | $ 340,000 |
| State Insurance Commission tax turnback – UALR mapping project | 131,512 | 131,512 |
| State Insurance Commission tax turnback – allocation report | 54,000 | 54,000 |
| Operating revenues | 658,512 | 525,512 |
| **Operating Expenses** | | |
| UALR mapping program | 131,512 | 131,512 |
| Salaries | 239,074 | 229,615 |
| Office supplies | 16,591 | 7,881 |
| Office equipment maintenance | 57,729 | 48,596 |
| Postage | 4,365 | 5,044 |
| Telephone | 31,510 | 30,086 |
| Publications | 1,215 | 717 |
| Travel/professional/education/conference | 15,932 | 9,077 |
| Board supplies | 1,676 | 1,509 |
| Actuarial expense | 101,825 | 107,950 |
| Insurance | 1,789 | 2,328 |
| Audit fee | 15,250 | 14,900 |
| Operating expenses | 618,468 | 589,215 |
| **Change in Net Position** | 40,044 | (63,703) |
| **Net Position, Beginning of Year** | 348,544 | 412,247 |
| **Net Position, End of Year** | $ 388,588 | $ 348,544 |

*See Notes to Financial Statements*

## Arkansas Fire and Police Pension Review Board
## Statements of Cash Flows
## Years Ended December 31, 2023 and 2022

| | 2023 | 2022 |
|---|---|---|
| **Operating Activities** | | |
| Cash flows from operating activities | $ - | $ - |
| **Noncapital Financing Activities** | | |
| Cash flows from noncapital financing activities | - | - |
| **Capital and Related Financing Activities** | | |
| Cash flows from financing activities | - | - |
| **Investing Activities** | | |
| Cash flows from investing activities | - | - |
| **Change in Cash and Cash Equivalents** | - | - |
| **Cash and Cash Equivalents, Beginning of Year** | - | - |
| **Cash and Cash Equivalents, End of Year** | $ - | $ - |

| | 2023 | 2022 |
|---|---|---|
| **Reconciliation of Change in Net Position to Net Cash Provided by Operating Activities** | | |
| Change in net position | $ 40,044 | $ (63,703) |
| Adjustments to reconcile change in net assets to cash provided by operating activities: | | |
| Changes in | | |
| Accrued expenses | 2,551 | (485) |
| Receivable from LOPFI | (42,595) | 64,188 |
| Net cash provided by operating activities | $ - | $ - |

## Note 1. Reporting Entity and Summary of Significant Accounting Policies

The Arkansas Fire and Police Pension Review Board (PRB) was created by the State of Arkansas to establish a state pension review board for all municipal fire and police pension funds established under Act 1921, No.491 and Act 1937, No. 250, which shall oversee all requests for benefit increases and review the annual accountant's reports and annual actuarial valuations required by the enacting legislation.

### *Basis of Accounting*

The accounting policies of the PRB have been established to conform to generally accepted accounting principles for state and local governments as promulgated by authoritative pronouncements issued by the Governmental Accounting Standards Board. The PRB is accounted for on an economic resources measurement focus using the accrual basis of accounting.

## Note 2. Related Party Transactions

The executive director and staff of Arkansas Local Police and Fire Retirement System (LOPFI) serve as executive director and staff for the PRB; LOPFI receives all revenue and pays all expenses for the PRB. The portion of revenues and expenses attributable to the PRB is allocated to the PRB account on the LOPFI books; due to this arrangement, the major asset of the PRB is a receivable from LOPFI, which amounted to $394,967 and $352,372 at December 31, 2023 and 2022, respectively. The allocation of expenses is determined by each respective board through the use of an administrative committee composed of members of both boards.

## Note 3. Commitments and Contingencies

### *Geographic Information Systems Mapping Project*

The PRB has entered into a contract with the University of Arkansas at Little Rock to provide demographic and mapping data through its Geographic Information Systems Applications Laboratory to ensure compliance with Acts 1570 and 1288 of the 82nd General Assembly of the State of Arkansas. The acts require the drawing of new fire district boundaries following physical features of the land. Per the 2000 Census data, a population assessment for each district has been tabulated for the purpose of allocating State Insurance Department Turnback Funds. The Arkansas Insurance Department has awarded the PRB $131,512 for each of the years ended December 31, 2023 and 2022 for funding of the project.

FORVIS

111 Center Street, Suite 1600 / Little Rock, AR 72201
P 501.372.1040 / F 501.372.1250
forvis.com

# Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards*

## Independent Auditor's Report

Board Members
Arkansas Fire and Police Pension Review Board
Little Rock, Arkansas

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States (*Government Auditing Standards*), the financial statements of Arkansas Fire and Police Pension Review Board (PRB), which comprise the balance sheets as of December 31, 2023, and the related statements of revenues, expenses and changes in net position and cash flows for the year then ended, and the related notes to the financial statements, and have issued our report thereon dated April 15, 2024.

## Report on Internal Control over Financial Reporting

In planning and performing our audit of the financial statements, we considered the PRB's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the PRB's internal control. Accordingly, we do not express an opinion on the effectiveness of the PRB's internal control.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A *material weakness* is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A *significant deficiency* is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified.

## Report on Compliance and Other Matters

As part of obtaining reasonable assurance about whether the PRB's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards.*

## Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

FORVIS, LLP

**Little Rock, Arkansas**
**April 15, 2024**

FORVIS®

111 Center Street, Suite 1600 / Little Rock, AR 72201
**P** 501.372.1040 / **F** 501.372.1250
forvis.com

April 12, 2024

Board of Trustees
Arkansas Local Police & Fire Retirement System
Attn: Mr. David Clark, Executive Director
620 West 3rd, Suite 200
Little Rock, AR 72201

Dear Mr. Clark:

Attached is the following final report of the NIST Cybersecurity Framework Assessment for Arkansas Local Police & Fire Retirement System.

- One PDF version of the NIST Cybersecurity Framework Assessment Report

We believe our engagement is complete. This letter serves as a recap of the engagement.

The scope of this engagement was established in our contract dated October 27, 2021. We have worked closely with you throughout this engagement and have kept you informed about the status of the engagement.

If you agree that we have completed the engagement requirements as outlined in our contract, no response is necessary. Your feedback on the delivery of this engagement is important to the success of our relationship with you and is appreciated.

We will communicate separately regarding any final billing and collection matters. We appreciate and value you and the staff of Arkansas Local Police & Fire Retirement System as a **FORVIS, LLP** client. Thank you for all the help and cooperation received during the completion of this engagement. Please do not hesitate to contact Cy Sturdivant at 615.988.3596 or cy.sturdivant@forvis.com should you have any questions or need anything.

Sincerely,

Cindy Boyle

Cindy Boyle, CPA, CIA®, CITP®, CISA®
Partner, IT Risk & Compliance

CHB: edm

Enclosure

FORVIS

# NIST CYBERSECURITY FRAMEWORK ASSESSMENT REPORT / **ARKANSAS LOCAL POLICE & FIRE RETIREMENT SYSTEM**

AS OF MARCH 28, 2024

FORVIS®

111 Center Street, Suite 1600 / Little Rock, AR 72201
P 501.372.1040 / F 501.372.1250
forvis.com

March 28, 2024

Board of Trustees
Arkansas Local Police & Fire Retirement System
Little Rock, AR

Dear Mr. Clark:

We have performed the procedures enumerated in this report, which were agreed to by management of Arkansas Local Police & Fire Retirement System (LOPFI) pursuant to our contract dated October 27, 2021, solely to assist you with respect to evaluating LOPFI's cybersecurity maturity. Our procedures were consistent with the National Institute of Standards and Technology (NIST) Cybersecurity Framework version 1.1 as well as industry best practices.

Neither our services nor our reports shall in any way guarantee that the LOPFI will not have a security incident, data breach, identity theft, network hacking, ransomware, etc. While our services and reports may contain findings, recommendations, and identify potential risks and threats, the sufficiency of policies, procedures, and practices to secure the IT environment is solely the responsibility of management. Management is also responsible for identifying and ensuring compliance with all laws and regulations applicable to its activities.

Our engagement did not include a detailed examination of all transactions and was not designed, and cannot be relied upon, to discover all errors, irregularities, or illegal acts, including fraud or defalcations, that may exist. Had we performed additional procedures, other findings of significance may have been reported to you. The sufficiency of the procedures is solely the responsibility of the parties specified in this report. Consequently, we make no representation regarding the sufficiency of the procedures described in this report for the purpose for which this report has been requested or for any other purpose.

The engagement was performed in accordance with consulting standards established by the American Institute of Certified Public Accountants (AICPA). We were not engaged to, and did not, conduct an examination, the objective of which would be the expression of an opinion on the internal control systems management has in place. Accordingly, we do not express such an opinion.

Our report is intended for use only by LOPFI's Board of Trustees and management solely for reporting findings with respect to the procedures performed by us. This report is not intended to be, and should not be, used by anyone other than these specified parties unless express written consent is obtained from FORVIS, LLP.

FORVIS, LLP

FORVIS, LLP

# Table of Contents

# Executive Summary

**Forward Vision Drives Our Unmatched Client Experiences™**

We are pleased to provide our report on the NIST Cybersecurity Framework Assessment procedures performed by FORVIS, LLP (FORVIS) for Arkansas Local Police & Fire Retirement System (LOPFI) as of March 28, 2024. This engagement is a point-in-time assessment. LOPFI is responsible for continuously monitoring cybersecurity risks and their IT systems.

Management approved the procedures we performed, which are included in the Scope of Services section. The results of our procedures were discussed with management at the conclusion of our engagement and are included in the Findings & Recommendations section.

## Engagement Summary

This engagement was performed to assist LOPFI in identifying compliance for managing cyberthreats and vulnerabilities and for protecting information and information systems by identifying, defending against, responding to, and recovering from attacks. We assessed the controls that LOPFI has in place in accordance with the framework identified below. The assessment consisted of inspecting policies and procedures, evaluating controls, and making inquiries. FORVIS mapped the existing environment against the applicable framework to identify the gaps between the current state and the framework.

This engagement was based on the following framework:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) version 1.1

This framework is voluntary guidance based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk.

## Findings

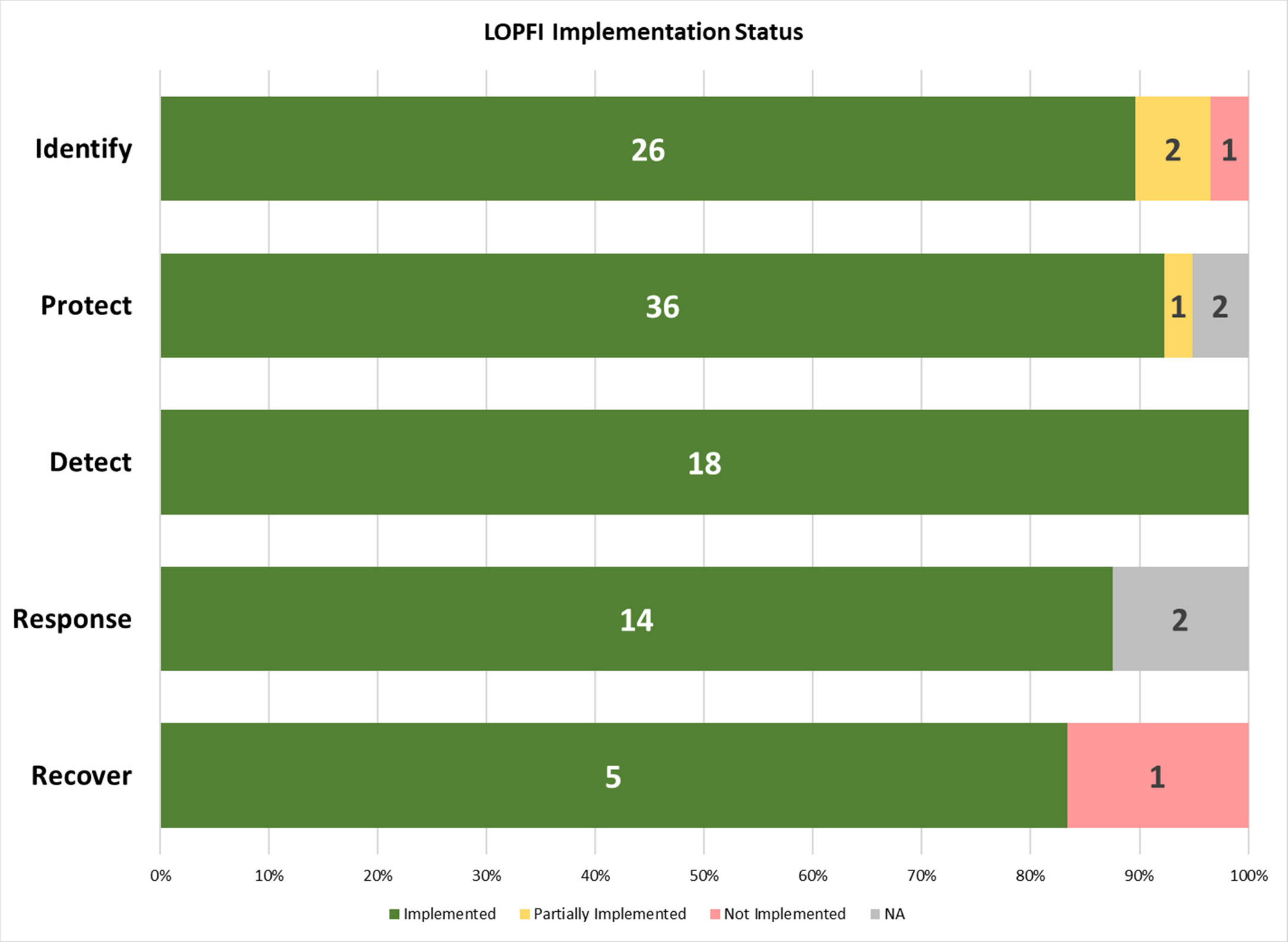
A finding is defined as a matter having a direct negative impact on internal control or indicates noncompliance with internal policy, procedure, applicable law, regulation, or guideline.

The risk ratings applied to the findings in this report are based on our experiences performing similar procedures at other organizations, NIST standards, and assistance from LOPFI. These ratings are intended to assist management with prioritizing the importance of acting on the findings identified. We believe all findings, regardless of the risk ratings assigned, if not addressed, could eventually lead to significant issues. We recommend management track the resolution of findings identified. The definitions of these ratings appear in the Definitions of Ratings section.

## Overall Ratings

The assessment of LOPFI's implementation of the NIST CSF requirements by function is shown below. Definitions of maturity ratings of information security controls (implementation status) are included in the Definitions of Ratings section below.

The following represents the Assessment Action Status by Section:



## Management Responses

Management's responses were not subjected to the procedures we applied and, accordingly, we express no opinion on the responses.

# Definitions of Ratings

## Maturity Ratings of Information Security Controls

The information security control maturity ratings were based solely on the procedures performed and related only to the items tested. Had we performed additional procedures, other matters might have come to our attention that could have changed an internal IT control area’s rating. Refer to Appendix A for additional detail.

- **Implemented –** Controls are designed to meet the objective of the requirement.
- **Partially Implemented –** Some of the requirement's objectives have been met, but there are multiple opportunities for improvement.
- **Not Implemented –** Controls are absent to support the requirement's objectives.
- **Not Applicable –** Requirement does not apply to the organization and/or the underlying technology is not utilized.

# Findings & Recommendations

The following table reflects findings and recommendations for management that may affect LOPFI's risk exposure.

| Finding ID | Finding | Recommendations | CSF Framework Control References | Management Response |
|---|---|---|---|---|
| 01 | The Organization does not have an asset-based Information Security Risk Assessment. | We recommend management establish a formalized, asset-based Information Security Risk Assessment. This Risk Assessment should encompass any perceivable cybersecurity threat to the organization that includes the likelihood, impact, inherent risk, mitigating controls, and residual risk. This Risk Assessment should be updated, reviewed, and approved at least annually. | ID.GV-4, ID.RA-5 | See below* |
| 02 | Although management has performed a tabletop disaster recovery test, it was noted that management has not performed a backup and restoration test to validate the ability to restore the data in the event of a disaster. | We recommend management perform a disaster recovery test as soon as possible as well as test annually thereafter. The results of the test should be documented, including who participated in the test, the nature of the test, as well as validating that recovery time objectives and recovery point objectives have been met. Lessons learned from this exercise should be added to the Disaster Recovery Plan. | ID.SC-5, RC.IM-1 | LOPFI's IT Professionals, PCA, has scheduled a disaster recovery test and implemented annual backup/restoration tests. |
| 03 | Although management has created a network and data flow diagram, it was noted that the diagrams do not contain a last reviewed/updated date. | We recommend management add a last reviewed/updated and signoff date to the network and data flow diagrams each year to account for any potential changes made and to verify a review has taken place. | PR.AC-5 | Dates have been added to each diagram and will be updated, when necessary, as recommended. |

## *Management Response for Finding ID 01:

After a lengthy conversation with FORVIS, and review of the sample documents provided, management has concluded that this exercise will not add value to LOPFI's IT security. LOPFI's IT professionals have outlined the protocols in place for the various areas detailed in the sample documents. Based on the protocols in place management does not feel that creating an Information Security Risk Assessment at this time is warranted.

- Ransomware
  - Workstations and servers are protected using SentinelOne's EDR platform. Endpoint Detection and Response leverages Behavior Monitoring to better protect our systems as well as allows for Forensics Analysis and Ransomware Rollback. In the event that any sort of malware or ransomware was deployed within the environment, it will mitigate the application/process and then restore any changes back to their original configuration.
- Business Email Compromise
  - Business Email Compromise is protected via conditional access, multifactor authentication, and SIEM monitoring for suspicious activity.
- Denial of Service Attacks
  - Denial of Service attacks are mitigated at the firewall level leveraging drop UDP flood attack methods. This is also monitored by the SIEM.
- Supply Chain Attack (third-party compromised)
  - Only approved hardware/software is currently installed, and any changes must be approved by LOPFI management and LOPFI's IT vendor before implementation.
  - Strict controls are already in place that limit vendor access. The protocols allow for an audit of all vendor access sessions and vulnerability scanning is in place. The IT administrators have security controls in place to protect from unauthorized access to systems.
- Exfiltration of Sensitive/Important Data
  - Data loss prevention has not been configured for LOPFI at this time. LOPFI's IT professionals are reaching out to security vendors for recommendations and anticipate this being implemented throughout the second quarter.
- Phishing Attacks
  - Advanced Email Threat Protection (AETP), an email cloud solution that provides multi-layered filtering that allows legitimate email while blocking malicious threats such as phishing, impersonation, malware, ransomware, and spam-type messages automatically, is in place.
  - Additionally, regular phishing tests are completed by staff, and end user education is provided on how to identify security risks.

# Scope of Services

Our cybersecurity assessment engagement was based on NIST's *Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework)*, version 1.1. The framework provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today. Our assessment procedures included evaluating existing policies, controls, and observing procedures to assess LOPFI's controls over IT as recommended by this framework. Our approach included:

## Discovery

During the discovery phase, our primary objective was to understand your business environment, technologies, and processes. We conducted planning discussions to finalize the overall assessment timeline, establish our on-site interviews, and request preliminary documents.

Interviews covered critical areas, including:

- Business and technology overviews
- Governance
- Risk management practices
- Asset management
- Data protection
- Security maintenance
- Security awareness
- Access management
- Security monitoring
- Security event detection
- Incident and breach response
- Business continuity
- Third-party risks (vendor management)

## Analysis

Based on the technologies and processes identified during our on-site interviews and inspection of supplemental documentation, we performed a high-level gap assessment using the NIST Cybersecurity Framework (CSF).

We discussed the initial gap assessment results with management, helped management identify their organization's acceptable level of risk, and reviewed our recommendations and how those relate to the underlying framework and best practices.

# Appendix

# Appendix A: NIST Framework

| Category | Subcategory | Description | Control Implementation Status | Report Finding |
|---|---|---|---|---|
| Asset Management | ID.AM-1 | Physical devices and systems within the organization are inventoried | Implemented | |
| Asset Management | ID.AM-2 | Software platforms and applications within the organization are inventoried | Implemented | |
| Asset Management | ID.AM-3 | Organizational communication and data flows are mapped | Implemented | |
| Asset Management | ID.AM-4 | External information systems are catalogued | Implemented | |
| Asset Management | ID.AM-5 | Resources (*e.g.*, hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value | Implemented | |
| Asset Management | ID.AM-6 | Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (*e.g.*, suppliers, customers, partners) are established | Implemented | |
| Business Environment | ID.BE-1 | The organization’s role in the supply chain is identified and communicated | Implemented | |
| Business Environment | ID.BE-2 | The organization’s place in critical infrastructure and its industry sector is identified and communicated | Implemented | |
| Business Environment | ID.BE-3 | Priorities for organizational mission, objectives, and activities are established and communicated | Implemented | |
| Business Environment | ID.BE-4 | Dependencies and critical functions for delivery of critical services are established | Implemented | |
| Business Environment | ID.BE-5 | Resilience requirements to support delivery of critical services are established | Implemented | |
| Governance | ID.GV-1 | Organizational information security policy is established | Implemented | |

| Category | Subcategory | Description | Control Implementation Status | Report Finding |
|---|---|---|---|---|
| Governance | ID.GV-2 | Information security roles and responsibilities are coordinated and aligned with internal roles and external partners | Implemented | |
| Governance | ID.GV-3 | Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed | Implemented | |
| Governance | ID.GV-4 | Governance and risk management processes address cybersecurity risks | Partially Implemented | 01 |
| Risk Assessment | ID.RA-1 | Asset vulnerabilities are identified and documented | Implemented | |
| Risk Assessment | ID.RA-2 | Threat and vulnerability information is received from information sharing forums and sources | Implemented | |
| Risk Assessment | ID.RA-3 | Threats, both internal and external, are identified and documented | Implemented | |
| Risk Assessment | ID.RA-4 | Potential business impacts and likelihoods are identified | Implemented | |
| Risk Assessment | ID.RA-5 | Threats, vulnerabilities, likelihoods, and impacts are used to determine risk | Not Implemented | 01 |
| Risk Assessment | ID.RA-6 | Risk responses are identified and prioritized | Implemented | |
| Risk Management | ID.RM-1 | Risk management processes are established, managed, and agreed to by organizational stakeholders | Implemented | |
| Risk Management | ID.RM-2 | Organizational risk tolerance is determined and clearly expressed | Implemented | |
| Risk Management | ID.RM-3 | The organization’s determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis | Implemented | |
| Supply Chain | ID.SC-1 | Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders | Implemented | |

| Category | Subcategory | Description | Control Implementation Status | Report Finding |
|---|---|---|---|---|
| Supply Chain | ID.SC-2 | Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process | Implemented | |
| Supply Chain | ID.SC-3 | Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan | Implemented | |
| Supply Chain | ID.SC-4 | Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. | Implemented | |
| Supply Chain | ID.SC-5 | Response and recovery planning and testing are conducted with suppliers and third-party providers | Partially Implemented | 02 |
| Access Control | PR.AC-1 | Identities and credentials are managed for authorized devices and users | Implemented | |
| Access Control | PR.AC-2 | Physical access to assets is managed and protected | Implemented | |
| Access Control | PR.AC-3 | Remote access is managed | Implemented | |
| Access Control | PR.AC-4 | Access permissions are managed, incorporating the principles of least privilege and separation of duties | Implemented | |
| Access Control | PR.AC-5 | Network integrity is protected, incorporating network segregation where appropriate | Partially Implemented | 03 |
| Access Control | PR.AC-6 | Identities are proofed and bound to credentials and asserted in interactions | Implemented | |
| Access Control | PR.AC-7 | Users, devices, and other assets are authenticated (*e.g.*, single-factor, multi-factor) commensurate with the risk of the transaction (*e.g.*, individuals' security and privacy risks and other organizational risks) | Implemented | |
| Awareness and Training | PR.AT-1 | All users are informed and trained | Implemented | |

| Category | Subcategory | Description | Control Implementation Status | Report Finding |
|---|---|---|---|---|
| Awareness and Training | PR.AT-2 | Privileged users understand roles and responsibilities | Implemented | |
| Awareness and Training | PR.AT-3 | Third-party stakeholders (*e.g.*, suppliers, customers, partners) understand roles and responsibilities | Implemented | |
| Awareness and Training | PR.AT-4 | Senior executives understand roles and responsibilities | Implemented | |
| Awareness and Training | PR.AT-5 | Physical and information security personnel understand roles and responsibilities | Implemented | |
| Data Security | PR.DS-1 | Data-at-rest is protected | Implemented | |
| Data Security | PR.DS-2 | Data-in-transit is protected | Implemented | |
| Data Security | PR.DS-3 | Assets are formally managed throughout removal, transfers, and disposition | Implemented | |
| Data Security | PR.DS-4 | Adequate capacity to ensure availability is maintained | Implemented | |
| Data Security | PR.DS-5 | Protections against data leaks are implemented | Implemented | |
| Data Security | PR.DS-6 | Integrity checking mechanisms are used to verify software, firmware, and information integrity | Implemented | |
| Data Security | PR.DS-7 | The development and testing environment(s) are separate from the production environment | NA | |
| Data Security | PR.DS-8 | Integrity checking mechanisms are used to verify hardware integrity | Implemented | |
| Information Protection | PR.IP-1 | A baseline configuration of information technology/industrial control systems is created and maintained | Implemented | |
| Information Protection | PR.IP-2 | A System Development Life Cycle to manage systems is implemented | Implemented | |
| Information Protection | PR.IP-3 | Configuration change control processes are in place | NA | |

| Category | Subcategory | Description | Control Implementation Status | Report Finding |
|---|---|---|---|---|
| Information Protection | PR.IP-4 | Backups of information are conducted, maintained, and tested periodically | Implemented | |
| Information Protection | PR.IP-5 | Policy and regulations regarding the physical operating environment for organizational assets are met | Implemented | |
| Information Protection | PR.IP-6 | Data is destroyed according to policy | Implemented | |
| Information Protection | PR.IP-7 | Protection processes are continuously improved | Implemented | |
| Information Protection | PR.IP-8 | Effectiveness of protection technologies is shared with appropriate parties | Implemented | |
| Information Protection | PR.IP-9 | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed | Implemented | |
| Information Protection | PR.IP-10 | Response and recovery plans are tested | Implemented | |
| Information Protection | PR.IP-11 | Cybersecurity is included in human resources practices (*e.g.*, deprovisioning, personnel screening) | Implemented | |
| Information Protection | PR.IP-12 | A vulnerability management plan is developed and implemented | Implemented | |
| Maintenance | PR.MA-1 | Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools | Implemented | |
| Maintenance | PR.MA-2 | Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | Implemented | |
| Protective Technology | PR.PT-1 | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy | Implemented | |
| Protective Technology | PR.PT-2 | Removable media is protected and its use restricted according to policy | Implemented | |
| Protective Technology | PR.PT-3 | Access to systems and assets is controlled, incorporating the principle of least functionality | Implemented | |

| Category | Subcategory | Description | Control Implementation Status | Report Finding |
|---|---|---|---|---|
| Protective Technology | PR.PT-4 | Communications and control networks are protected | Implemented | |
| Protective Technology | PR.PT-5 | Mechanisms (*e.g.*, failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | Implemented | |
| Anomalies and Events | DE.AE-1 | A baseline of network operations and expected data flows for users and systems is established and managed | Implemented | |
| Anomalies and Events | DE.AE-2 | Detected events are analyzed to understand attack targets and methods | Implemented | |
| Anomalies and Events | DE.AE-3 | Event data are aggregated and correlated from multiple sources and sensors | Implemented | |
| Anomalies and Events | DE.AE-4 | Impact of events is determined | Implemented | |
| Anomalies and Events | DE.AE-5 | Incident alert thresholds are established | Implemented | |
| Continuous Monitoring | DE.CM-1 | The network is monitored to detect potential cybersecurity events | Implemented | |
| Continuous Monitoring | DE.CM-2 | The physical environment is monitored to detect potential cybersecurity events | Implemented | |
| Continuous Monitoring | DE.CM-3 | Personnel activity is monitored to detect potential cybersecurity events | Implemented | |
| Continuous Monitoring | DE.CM-4 | Malicious code is detected | Implemented | |
| Continuous Monitoring | DE.CM-5 | Unauthorized mobile code is detected | Implemented | |
| Continuous Monitoring | DE.CM-6 | External service provider activity is monitored to detect potential cybersecurity events | Implemented | |
| Continuous Monitoring | DE.CM-7 | Monitoring for unauthorized personnel, connections, devices, and software is performed | Implemented | |
| Continuous Monitoring | DE.CM-8 | Vulnerability scans are performed | Implemented | |
| Detection Processes | DE.DP-1 | Roles and responsibilities for detection are well defined to ensure accountability | Implemented | |

| Category | Subcategory | Description | Control Implementation Status | Report Finding |
|---|---|---|---|---|
| Detection Processes | DE.DP-2 | Detection activities comply with all applicable requirements | Implemented | |
| Detection Processes | DE.DP-3 | Detection processes are tested | Implemented | |
| Detection Processes | DE.DP-4 | Event detection information is communicated to appropriate parties | Implemented | |
| Detection Processes | DE.DP-5 | Detection processes are continuously improved | Implemented | |
| Response Planning | RS.RP-1 | Response plan is executed during or after an event | Implemented | |
| Communication | RS.CO-1 | Personnel know their roles and order of operations when a response is needed | Implemented | |
| Communication | RS.CO-2 | Events are reported consistent with established criteria | Implemented | |
| Communication | RS.CO-3 | Information is shared consistent with response plans | Implemented | |
| Communication | RS.CO-4 | Coordination with stakeholders occurs consistent with response plans | Implemented | |
| Communication | RS.CO-5 | Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | NA | |
| Analysis | RS.AN-1 | Notifications from detection systems are investigated | Implemented | |
| Analysis | RS.AN-2 | The impact of the incident is understood | Implemented | |
| Analysis | RS.AN-3 | Forensics are performed | Implemented | |
| Analysis | RS.AN-4 | Incidents are categorized consistent with response plans | Implemented | |
| Analysis | RS.AN-5 | Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (*e.g.* internal testing, security bulletins, or security researchers) | NA | |

| Category | Subcategory | Description | Control Implementation Status | Report Finding |
|---|---|---|---|---|
| Mitigation | RS.MI-1 | Incidents are contained | Implemented | |
| Mitigation | RS.MI-2 | Incidents are mitigated | Implemented | |
| Mitigation | RS.MI-3 | Newly identified vulnerabilities are mitigated or documented as accepted risks | Implemented | |
| Improvement | RS.IM-1 | Response plans incorporate lessons learned | Implemented | |
| Improvement | RS.IM-2 | Response strategies are updated | Implemented | |
| Recovery Planning | RC.RP-1 | Recovery plan is executed during or after an event | Implemented | |
| Improvement | RC.IM-1 | Recovery plans incorporate lessons learned | Not Implemented | 02 |
| Improvement | RC.IM-2 | Recovery strategies are updated | Implemented | |
| Communication | RC.CO-1 | Public relations are managed | Implemented | |
| Communication | RC.CO-2 | Reputation after an event is repaired | Implemented | |
| Communication | RC.CO-3 | Recovery activities are communicated to internal stakeholders and executive and management teams | Implemented | |

FORVIS®

# PENETRATION TESTING REPORT / **ARKANSAS LOCAL POLICE & FIRE RETIREMENT SYSTEM**

AS OF MARCH 15, 2024

March 15, 2024

Board of Trustees
Arkansas Local Police & Fire Retirement System
Little Rock, AR

Dear Mr. Clark:

We have performed the procedures enumerated in this report, which were agreed to by management of Arkansas Local Police & Fire Retirement System (the Company) pursuant to our contract dated October 19, 2023, solely to assist you with respect to evaluating the Company's internal and external network security. Our procedures were consistent with frameworks published by the Open Worldwide Application Security Project (OWASP), pentest-standard.org, MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK), Payment Card Industry (PCI) Penetration Testing Guide, as well as industry best practices.

Neither our services nor our reports shall in any way guarantee that the Company will not have a security incident, data breach, identity theft, network hacking, ransomware, etc. While our services and reports may contain findings or results, recommendations, and identify potential risks and threats, the sufficiency of policies, procedures, and practices to secure the IT environment is solely the responsibility of management. Management is also responsible for identifying and ensuring compliance with all laws and regulations applicable to its activities.

Our engagement did not include a detailed examination of all transactions and was not designed, and cannot be relied upon, to discover all errors, irregularities, or illegal acts, including fraud or defalcations, that may exist. Had we performed additional procedures, other findings or results of significance may have been reported to you. The sufficiency of the procedures is solely the responsibility of the parties specified in this report. Consequently, we make no representation regarding the sufficiency of the procedures described in this report for the purpose for which this report has been requested or for any other purpose.

The engagement was performed in accordance with consulting standards established by the American Institute of Certified Public Accountants (AICPA). We were not engaged to, and did not, conduct an examination, the objective of which would be the expression of an opinion on the internal control systems management has in place. Accordingly, we do not express such an opinion.

Our report is intended for use only by the Company's Board of Trustees and management solely for reporting findings and results with respect to the procedures performed by us. This report is not intended to be, and should not be, used by anyone other than these specified parties unless express written consent is obtained from FORVIS, LLP.

FORVIS, LLP

# Table of Contents

# Executive Summary

**Forward Vision Drives Our Unmatched Client Experiences™**

We are pleased to provide our report on the penetration testing procedures performed by FORVIS, LLP (FORVIS) for the Company as of March 15, 2024. The overall objective of this engagement is to assist the Board of Trustees with assessing the confidentiality, integrity, and availability of their information and systems.

Our penetration testing procedures included:

- External Penetration Testing
- Internal Penetration Testing

The procedures we developed, management approved, and we performed are included in the Scope of Services section. The results of our procedures were discussed with management at the conclusion of our engagement and are included in the Findings & Recommendations section.

Prior to the start of external testing, the Company's external IP addresses and domain name were verified by Jen Sines, Chief Financial Officer. External network and domain name information was provided to the tester; however, no credentials were provided for the purpose of executing the engagement from the agreed-upon simulation. External testing began remotely on March 11, 2024, with the tester utilizing an IP locator tool to validate the geolocation of the provided IP address followed by port and vulnerability scans to identify key systems, ports, and services that were available externally.

Internal testing began on March 11, 2024. A penetration testing device was shipped to the Company and connected to the internal network for the purpose of executing the engagement from the agreed-upon simulation. The provided device was connected to the network by the Company's IT Coordinator. Remote access to the device was granted to the tester; however, no network or domain credentials were provided to the tester.

The scope of work included external and internal penetration testing of the internet protocol (IP) addresses associated with the Company. The table below identifies the IP addresses and domains included and were verified by Jen Sines, Chief Financial Officer.

| Environment Details |
|---|
| **External IP Addresses or Range of Addresses** |
| *Redacted due to sensitivity* |
| **Internal IP Addresses or Range of Addresses** |
| *Redacted due to sensitivity* |

# External Penetration Testing

## External Penetration Test Findings

The Company had no findings.

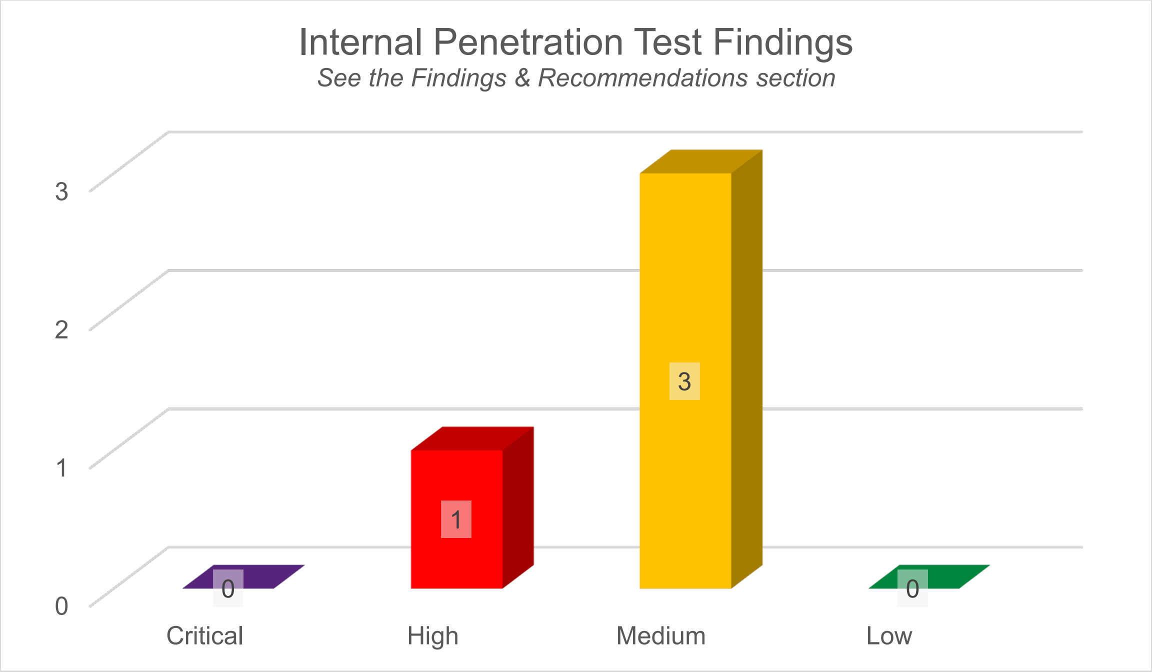
## External Vulnerability Scan Results

The Company had no unique results ranked Low to Critical based on the Common Vulnerability Scoring System (CVSS). Detailed information can be found in Appendix B.

# Internal Penetration Testing

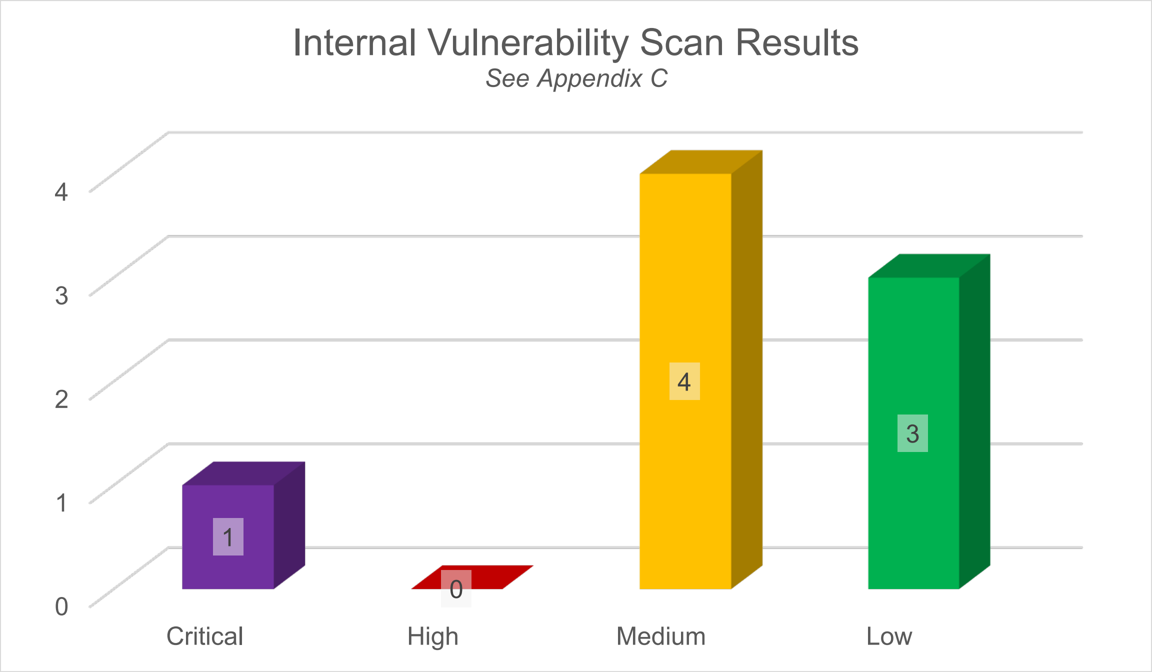
## Internal Penetration Test Findings

The Company had four findings based on probability and impact, which are defined in the Definitions of Ratings section. The graph below shows the number of findings by rating. Detailed information can be found in the Findings & Recommendations section and is intended to assist management with prioritizing corrective action.



### Internal Vulnerability Scan Results

The Company had eight unique results ranked Low to Critical based on the Common Vulnerability Scoring System (CVSS), which is defined in the Definitions of Ratings section. The graph below shows the number of results by CVSS rating. Detailed information can be found in Appendix C and is intended to assist management with prioritizing corrective action.



## Management Responses

We believe any findings, regardless of the risk ratings assigned, if not addressed, could lead to significant issues. Findings based on probability and impact are viewed as an immediate risk because they often lead to a breach of the Company's network and systems.

We recommend management track and report resolution status to the Board of Trustees or designated committee.

Management's responses were not subjected to the procedures we applied and, accordingly, we express no opinion on the responses.

# Definitions of Ratings

## Ratings of External & Internal Penetration Tests Findings

We use a rating based upon the probability and impact of exploiting the vulnerability being leveraged in an attack. These ratings are for all findings across all tests including External and Internal. These findings are viewed as an immediate risk because they often lead to a breach of the Company's network and systems. The following ratings define the risk associated with identified findings:

| Risk Rating | Definition |
|---|---|
| Critical | Indicates a matter requiring immediate remediation. |
| High | Indicates a matter requiring higher priority remediation. |
| Medium | Indicates a matter to be given priority for remediation. |
| Low | Indicates a matter to be remediated in the normal course of business. |

## Ratings of External & Internal Vulnerability Scan Results

The tools we use for vulnerability scanning utilize the industry standard Common Vulnerability Scoring System (CVSS) to ascertain the criticality of identified vulnerabilities. The CVSS is based on either Version 2 (v2) or Version 3 (v3) and utilizes the scoring system indicated in the table below. Not all vulnerabilities have a v3 score and will default to the v2 score, which applies to older systems and vulnerabilities, and may not be available in v3. Scores have been provided for both v2 and v3 when available. FORVIS may also include an informational finding that does not have a CVSS score but is still deemed relevant in regard to security best practices.

| Common Vulnerability Scoring System | | |
|---|---|---|
| **Vulnerability Score** | **v3 Definition** | **v2 Definition** |
| Critical | Base Score of 9.0 to 10.0 | N/A |
| High | Base Score of 7.0 to 8.9 | Base Score of 7.0 to 10.0 |
| Medium | Base Score of 4.0 to 6.9 | Base Score of 4.0 to 6.9 |
| Low | Base Score of 0.1 to 3.9 | Base Score of 0.0 to 3.9 |
| Informational | No CVSS score but security best practice | No CVSS score but security best practice |

More information can be found in regard to CVSS scoring and calculations by accessing the National Vulnerabilities Database hosted by the National Institute of Standards and Technology (NIST) at https://nvd.nist.gov.

# Penetration Attack Summary

## Summary of Attacks & Testing

### External Penetration Testing

Using a vulnerability scanning application, Tenable Nessus Professional, an external vulnerability scan was performed on the in-scope IP addresses. Based on the CVSSv3 ratings scale, no vulnerabilities were discovered.

Port scanning of network devices was performed using a tool named Network Mapper (NMAP) to discover IP addresses with open ports and services available externally. No exploitable ports or services were discovered during the port scan.

Throughout footprinting and organizational reconnaissance, the tester utilized tools to discover information from the Company's domain name. Using the query and response protocol, WHOIS, as well as the open-source tool, DNSRecon, the tester was able to verify the Company's Domain Name System (DNS) records, Mail Exchange Servers, and associated domain contact information which was set to private. The output of these tools can be seen in Appendix A.

The Company's domain name was also used to gather additional information in an attempt to discover sub-domains, employee names, emails, and relevant hosts. A tool named the Harvester, which gathers publicly available Open-Source Intelligence (OSINT) information, was used. None of the information gathered could be leveraged to gain external access.

External access was not obtained on the test and no sensitive information or personally identifiable information (PII) were obtained from the Company during the test.

### Internal Penetration Testing

Network broadcast traffic and network analysis began during the first day of testing using a data packet capture utility named Wireshark. Also, port scanning of the network devices using a tool named NMAP was performed to identify key systems, ports, and services running on network devices. Broadcast name resolution poisoning also began during the first day of testing using a tool named Responder. Broadcast name resolution poisoning abuses features of the Link-Local Multicast Name Resolution (LLMNR), Network Basic Input/Output System (NetBIOS), and Multicast DNS (mDNS) name resolution protocols allowing attackers to capture network account password hashes.

*Section redacted due to sensitivity*

A scan of the network servers and workstations using a tool named SMBClient was also used in an attempt to find open network file shares containing sensitive files. No open file shares containing sensitive data were discovered.

A search for default manufacturer logins was performed against internal devices and management web pages. No default manufacturer logins were discovered.

An uncredentialed vulnerability scan was performed on the internal IP subnets to discover weaknesses on systems with out-of-date or unpatched software. One unique critical vulnerability, four unique medium rated vulnerabilities, and three unique low vulnerabilities were reported. The results of the vulnerability scan may be seen in Appendix C.

No sensitive information or personally identifiable information (PII) were removed from the Company during the test and domain administrative access was not achieved during the test.

# Findings & Recommendations

## External Penetration Testing

The Company had no findings.

## Internal Penetration Testing

### Finding #1

**Risk Rating:** High

**Probability:** High

**Impact:** Medium

Systems on the network are currently utilizing an outdated authentication protocol, which is recognized for its inadequate security standards. *Redacted due to sensitivity.*

**Affected Devices:**
*Redacted due to sensitivity*

**Recommendation:**

We recommend management enable up-to-date authentication hashes on the network and, if possible, disable the use of dated protocols.

**Management Response:**

New protocol was enabled on the network and old was disabled as recommended.

## Finding #2

| | |
|---|---|
| **Risk Rating:** | **Medium** |

**Probability:** High

**Impact:** Low

Some devices within the environment were vulnerable to various types of broadcast name resolution poisoning attacks using the Responder tool. Spoofed responses to legitimate Link-Local Multicast Name Resolution (LLMNR) requests caused internal systems to connect back to the tester's machine. An attacker can intercept traffic on a network and impersonate the identity of legitimate systems. *Redacted due to sensitivity.*

During testing, two password hashes were obtained using this method. The passwords were not compromised and were not able to be used in any further attacks.

**IP Addresses:**
*Redacted due to sensitivity*

**Recommendation:**

LLMNR is not typically needed on modern networks and can often be disabled via Group Policy.

**Management Response:**

LOPFI's IT professionals have disabled LLMNR via Group Policy as recommended.

## Finding #3

| **Risk Rating:** | **Medium** |
|---|---|

**Probability:** Medium

**Impact:** Low

Systems on the network were found to have Server Message Block (SMB) signing disabled. This allowed the tester to perform relay attacks against servers and workstations in an attempt to gain unauthenticated access without requiring a password.

**IP Addresses:**
*Redacted due to sensitivity*

**Recommendation:**

We recommend enforcing message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'.

**Management Response:**

Server Message Block (SMB) signing has been enabled on the network systems as recommended.

## Finding #4

| | |
|---|---|
| **Risk Rating:** | **Medium** |

**Probability:** Medium

**Impact:** Low

IPv6 is enabled in the environment. Some devices within the environment were vulnerable to various types of IPv6 poisoning attacks. An attacker can perform man-in-the-middle attacks against IPv6 DHCP requests. The tester acted as a DNS server for IPv6 DHCP traffic spoofing DNS requests sending replies to the targets. Spoofed responses to legitimate Domain Name Service (DNS) requests caused internal systems to connect back to the tester's machine. An attacker can intercept traffic on a network and impersonate the identity of legitimate systems.

**IP Addresses:**
*Redacted due to sensitivity*

**Recommendation:**

We recommend management review devices with IPv6 enabled and determine if IPv6 is needed for the devices functionality.

If IPv6 is used, management should either configure routers to operate via IPv6 and use IPv6 addressing, or Dynamic Host Configuration Protocol version 6 (DHCPv6) and IPv6 router advertisements should be blocked and IPv6 disabled on all hosts in the Windows Firewall via Group Policy.

**Management Response:**

IPv4 has been configured to be prioritized over IPv6 as recommended.

# Scope of Services

The scope of procedures performed by FORVIS for the Company are as of March 15, 2024.

## External Penetration Testing

The testing was conducted from a “limited knowledge” standpoint, based on the assumption we had very limited knowledge of what is contained on the network or what there is to discover. We obtained the internet protocol (IP) network addresses from Company personnel and followed the methodology described below from our offices across the internet. The testing methodology included the following steps.

### Footprinting

- Organizational Reconnaissance

  Organization reconnaissance is primarily concerned with discovering information related to the target organization, its employees, partners, contractors, suppliers, etc.

- Network Reconnaissance

  The network reconnaissance phase is the identification of the testing network and the associated IP addresses including internet domain name(s) owned, IP addresses owned or associated with target organization and through domain registry examination, pinpoint web servers, mail servers, domain name system (DNS) servers, and identify operating system running on those servers. In many cases, an organization may have multiple departments or even companies that utilize the same network. It is important to correctly identify the network and devices to test.

### Scanning

- Ping Sweeps/Address Resolution Protocol (ARP) Requests

  Ping sweeps are used to send an internet control message protocol (ICMP) ECHO packet to a range of addresses or a network block in expectation of receiving an ICMP ECHO_REPLY from a live system. Any address that returns an ICMP ECHO_REPLY verifies a device is at that address. In addition, ARP requests across the network will help identify unknown devices.

- Transmission Control Protocol (TCP) and User Data Protocol (UDP) Port Scanning

  Port scanning is similar to ping sweeps in the discovery of unknown systems. TCP and UDP port scanning is the process of locating specific open ports. Open ports give the ability to attempt to identify systems and services that may be possible to exploit to gain unauthorized access to a system.

### Enumeration

- Hardware Device Identification

  Hardware device identification is used to attempt to map the devices on the network. Once able to determine what the hardware is, one can attempt to discern what firmware or operating system it may be running. An evaluation of open ports may reveal a vendor-specific port. There are exploits that are vendor specific, so positively identifying hardware may point you to a possible exploit or vulnerability.

- Services Identification

  This is the identification of what services are running on a device. The services are usually identified via the ports they run on. An evaluation of the open ports found from the TCP/UDP scan can identify the services running.

- Operating System Identification

  Operating system identification is an important step. Vulnerabilities may exist in the form of improperly coded programs or improperly configured services. By correctly identifying the firmware or operating system running, known exploits may be attempted, as well as attempts to take advantage of improperly configured systems/devices.

- Application Identification

  Application identification is similar to operating system identification except you are trying to determine what applications are being utilized. These may be database programs, mail programs, websites for e-commerce, etc.

- Account Identification

  Account identification is attempting to find information about the organization’s individual employees and the accounts they may use to access the network. To locate accounts, network research is utilized. It is possible the organization may have an employee index on their site listing all employees, telephone numbers, and email addresses. The user portion of the email address is usually (not always) the account name.

  After the services, applications, and operating systems have been identified, also research for default accounts that may be created by or used by the application/service. Vulnerabilities may take advantage of default configurations or misconfiguration.

## Penetration

- Vulnerability Identification on Target Devices (Router, Firewall, DNS, Mail, Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), etc.)

  Vulnerability identification utilizes the information gathered from the enumeration process to search out exploits and vulnerabilities for the specified device, operating system, service, and/or application. Beyond scanning tools, internet research is one of the fastest ways to locate information regarding exploits and vulnerabilities on a certain product.

- Attempt to Exploit Vulnerabilities

  The exploitation of vulnerabilities is a step-by-step process. Once an exploit has been found, it is important to read all information regarding the exploit, and possible continued research on the exploit may be required.

- Password Guessing/Brute Force Guessing

  Password/brute force guessing is an attempt to access a system or device by guessing the correct password for a given account. Before beginning this phase, it is important to correctly identify the password policy on the system you are attacking. Failing to do so may cause the lockout of multiple accounts. All password guesses should be performed manually first, to try known accounts/passwords or common passwords such as “admin,” “password,” etc. After manual attempts fail, there are a variety of tools available to automate the process of password guessing. These programs use dictionary files to try usernames and passwords. Some programs can perform a brute force attack where the program generates passwords via criterion entered into program (lowercase, alphanumeric, mixed case, etc.).

## Privilege Escalation

- Password Cracking

  Password cracking is attempting to decipher encrypted passwords for utilization against the network being tested. Once a password file has been retrieved (there are a variety of ways to gather encrypted/unencrypted passwords), the passwords must be unencrypted for use.

### Seek Information

- Pilfer

  Once the network has been breached, attempt to locate password files (in the case of escalation required to access other servers), log files or applications, such as databases, that may hold sensitive information and such.

### Begin Footprinting Again from New Access Point

From the penetrated system, attempts are made to footprint the internal network to locate the next targets/servers. Attempts are made to locate any shares and note all accounts in use. Attempts are made to sniff network for authorization requests and replies, as well as monitor internal simple network management protocol (SNMP) traffic.

## Internal Penetration Testing

The objective of internal penetration testing was to obtain access to as many resources as possible within the testing period to evaluate network controls and identify potential vulnerabilities. The results can be used to help determine the effectiveness of network controls and indicate areas where additional controls may be necessary. The testing methodology included the following steps.

### Footprinting

- Network Reconnaissance

  The network reconnaissance phase is the identification of the testing network and the associated internet protocol (IP) addresses. In many cases, an organization may have multiple departments or even companies that utilize the same network. It is important to correctly identify the network and devices to test.

### Scanning

- Ping Sweeps/Address Resolution Protocol (ARP) Requests

  Ping sweeps are used to send an internet control message protocol (ICMP) ECHO packet to a range of addresses or a network block in expectation of receiving an ICMP ECHO_REPLY from a live system. Any address that returns an ICMP ECHO_REPLY verifies a device is at that address. In addition, ARP requests across the network will help identify unknown devices.

- Transmission Control Protocol (TCP) and User Data Protocol (UDP) Port Scanning

  Port scanning is similar to ping sweeps in the discovery of unknown systems. TCP and UDP port scanning is the process of locating specific open ports. Open ports give the ability to attempt to identify systems and services that may be possible to exploit to gain unauthorized access to a system.

### Enumeration

- Hardware Device Identification

  Hardware device identification is used to attempt to map the devices on the network. Once able to determine what the hardware is, one can attempt to discern what firmware or operating system it may be running. An evaluation of open ports may reveal a vendor-specific port. There are exploits that are vendor specific, so positively identifying hardware may point you to a possible exploit or vulnerability.

- Services Identification

  This is the identification of what services are running on a device. The services are usually identified via the ports they run on. An evaluation of the open ports found from the TCP/UDP scan can identify the services running.

- Operating System Identification

  Operating system identification is an important step. Vulnerabilities may exist in the form of improperly coded programs or improperly configured services. By correctly identifying the firmware or operating system running, known exploits may be attempted, as well as attempts to take advantage of improperly configured systems/devices.

- Application Identification

  Application identification is similar to operating system identification except you are trying to determine what applications are being utilized. These may be database programs, mail programs, websites for e-commerce, etc.

- Account Identification

  Account identification is attempting to find information about the organization's individual employees and the accounts they may use to access the network. To locate accounts, network research is utilized. It is possible the organization may have an employee index on their site listing all employees, telephone numbers, and email addresses. The user portion of the email address is usually (not always) the account name.

  After the services, applications, and operating systems have been identified, also research for default accounts that may be created by or used by the application/service. Vulnerabilities may take advantage of default configurations or misconfiguration.

## Penetration

- Vulnerability Identification on Target Devices (Router, Firewall, Domain Name Server (DNS), Mail, Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), etc.)

  Vulnerability identification utilizes the information gathered from the enumeration process to search out exploits and vulnerabilities for the specified device, operating system, service, and/or application. Beyond scanning tools, internet research is one of the fastest ways to locate information regarding exploits and vulnerabilities on a certain product.

- Attempt to Exploit Vulnerabilities

  The exploitation of vulnerabilities is a step-by-step process. Once an exploit has been found, it is important to read all information regarding the exploit, and possible continued research on the exploit may be required.

- Password Guessing/Brute Force Guessing

  Password/brute force guessing is an attempt to access a system or device by guessing the correct password for a given account. Before beginning this phase, it is important to correctly identify the password policy on the system you are attacking. Failing to do so may cause the lockout of multiple accounts. All password guesses should be performed manually first, to try known accounts/passwords or common passwords such as “admin,” “password,” etc. After manual attempts fail, there are a variety of tools available to automate the process of password guessing. These programs use dictionary files to try usernames and passwords. Some programs can perform a brute force attack where the program generates passwords via criterion entered into program (lowercase, alphanumeric, mixed case, etc.).

## Privilege Escalation

- System Privilege

  In many cases, unprotected and unpatched systems are vulnerable to buffer overflow exploits. These exploits many times grant system-level access.

- Password Cracking

  Password cracking is attempting to decipher encrypted passwords for utilization against the network being tested. Once a password file has been retrieved (there are a variety of ways to gather encrypted/unencrypted passwords), the passwords must be unencrypted for use.

## Seek Information

- Pilfer

  Once the network has been breached, attempt to locate password files (in the case of escalation required to access other servers), log files, or applications, such as databases, that may hold sensitive information and such.

# Appendix

# Appendix A: Internet Profile

This information is gathered from publicly available data sources to assist management in verifying that the information is correct. No management responses are expected in this section since this additional technical information is supplementary.

## Internet Profile

Information about the Company’s domain gathered from publicly available information.

### lopfi-prb.com

### DNS Server Information

| | |
|---|---|
| dbru.br.ns.els-gms.att.net | 68.94.156.134 |
| dbru.br.ns.els-gms.att.net | 2001:1890:1ff:9f0:68:94:156:134 |
| dmtu.mt.ns.els-gms.att.net | 99.99.99.134 |
| dmtu.mt.ns.els-gms.att.net | 2001:1890:1ff:9f1:99:99:99:134 |

### Mail Server Information

| | |
|---|---|
| lopfi--prb-com.mx1.arsmtp.com | 8.31.233.233 |
| lopfi--prb-com.mx2.arsmtp.com | 8.19.118.211 |

### Contact Information

| | |
|---|---|
| Registrant Name | PERFECT PRIVACY, LLC |
| Registrant Email | cg6px8dp93x@networksolutionsprivateregistration.com |
| Admin Name | PERFECT PRIVACY, LLC |
| Admin Email | cg6px8dp93x@networksolutionsprivateregistration.com |
| Tech Name | PERFECT PRIVACY, LLC |
| Tech Email | cg6px8dp93x@networksolutionsprivateregistration.com |

# Appendix B: Details of External Vulnerability Scan Results

Appendix B is provided to assist the Company in prioritizing remediation of identified vulnerabilities. No management responses are expected in this section since this additional technical information is supplementary to our detailed testing and may assist in the technical resolution.

In total, 16 hosts were identified during the scan.

## Hosts with Most Vulnerabilities

Presents the hosts with the greatest number of critical and high vulnerabilities. Hosts are ordered by the sum of critical and high vulnerabilities.

| Host | FQDN | Critical Vulns | High Vulns |
|---|---|---|---|
| NA | NA | NA | NA |

## Hosts with Exploitable Vulnerabilities

Presents the 10 most common remediations for vulnerabilities of critical or high severity.

| Host | FQDN | Exploitable Critical Vulns | Exploitable High Vulns |
|---|---|---|---|
| NA | NA | NA | NA |

## Open Ports

| Host IP | Open TCP Ports | Open UDP Ports |
|---|---|---|
| **Removed** | Removed | |

## Statistics

### Vulnerability Total Count

| Severity | Vulnerabilities | Unique |
|---|---|---|
| None | 0 | 0 |

# Appendix C: Details of Internal Vulnerability Scan Results

Appendix C is provided to assist the Company in prioritizing corrective action of the vulnerabilities identified. No management responses are expected in this section since this additional technical information is supplementary to our detailed testing and may assist in the technical resolution.

In total, 36 hosts were identified during the scan.

## Top Operating Systems

Displays the 10 most common operating systems identified.

| Operating System | Count |
|---|---|
| Windows 11 | 7 |
| Linux Kernel 2.6 | 4 |
| Microsoft Windows Server 2019 Standard 17763 | 2 |
| Microsoft Windows Server 2016 Standard 14393 | 1 |
| Microsoft Windows | 1 |
| Linux Kernel 3.10<br>Linux Kernel 3.13<br>Linux Kernel 4.2<br>Linux Kernel 4.8 | 1 |
| HP Integrated Lights-Out | 1 |

*Redacted due to sensitive information.*