

LOPFI

LOCAL POLICE & FIRE RETIREMENT SYSTEM

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

LOPFI Audit Committee Meeting Agenda
Meeting to be held via Zoom (login details below)
Thursday, May 2, 2024
9:30 a.m.

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

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

Step 1 – Registration – Complete at any time prior to the meeting. Click this link to register for the meeting:
https://us06web.zoom.us/join/register/tZ0kc-GurjosGtE80-I9oJEkMsiG_naNCCcV

Step 2 – Join Meeting – Complete at least 10 minutes prior to the start time.

Once registration is completed an email from LOPFI 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.

LOPFI

LOCAL POLICE & FIRE RETIREMENT SYSTEM

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 LOPFI Audit Committee will hold a meeting on May 2, 2024 at 9:30 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,

LOPFI Staff

LOPFI

LOCAL POLICE & FIRE RETIREMENT SYSTEM

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: ltturner@abpg.com (2 pages)

Dear Ladies and Gentlemen:

The LOPFI Audit Committee will hold a meeting on May 2, 2024 at 9:30 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,

LOPFI Staff

FORVIS Report to the Board of Trustees

Arkansas Local Police and Fire Retirement System

Results of the 2023 Financial Statement Audit, Including Required Communications

December 31, 2023

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

Overview & Responsibilities

Matter	Discussion
Scope of Our Audit	<p>This report covers audit results related to your financial statements and supplementary information:</p> <ul style="list-style-type: none"> As of and for the year ended December 31, 2023 Conducted in accordance with our contract dated November 27, 2023
Our Responsibilities	<p>FORVIS is responsible for forming and expressing an opinion 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).</p>
Audit Scope & Inherent Limitations to Reasonable Assurance	<p>An audit performed in accordance with auditing standards generally accepted in the United States of America (GAAS) and <i>Government Auditing Standards</i> 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.</p>
Extent of Our Communication	<p>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.</p>
Independence	<p>The engagement team, others in our firm, as appropriate, and our firm have complied with all relevant ethical requirements regarding independence.</p>
Your Responsibilities	<p>Our audit does not relieve management or those charged with governance of your responsibilities. Your responsibilities and ours are further referenced in our contract.</p>



Matter	Discussion
Distribution Restriction	<p>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:</p> <ul style="list-style-type: none"> • The board of trustees • Others within the Entity

Qualitative Aspects of Significant Accounting Policies & Practices

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 topic:

- GASB Statement No. 96, *Subscription-Based Information Technology Arrangements*

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:

- Fair value of investments
- Actuarial methods and assumptions used in calculating amounts recorded or disclosed in the financial statements

Financial Statement Disclosures

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

- Fair value
- Net pension liability disclosures



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.

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.

Uncorrected Misstatement

An adjustment proposed was **not recorded** because its effect is not currently considered material. We request that all identified misstatements be corrected.

The uncorrected misstatements that was determined by management to be immaterial, but more than trivial to the financial statements as a whole is listed below.

While the uncorrected misstatement was deemed to be immaterial to the current-period financial statements, it is possible that the matters underlying the uncorrected misstatement, could potentially cause future-period financial statements to be materially misstated.

Current-Period Uncorrected Misstatements

- No matters are reportable.

Prior-Period Uncorrected Misstatements

- Updated estimated fair value of alternative investments.

Other Required Communication

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

- Management representation letter (see Attachment)



Representation of:
Arkansas Local Police and Fire Retirement System
620 W. Third Street, Suite 200
Little Rock, Arkansas 72201

Provided to:
FORVIS, LLP
Certified Public Accountants
111 Center St., 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.

Arkansas Local Police and Fire Retirement System
Page 2

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 directors' and committee of directors 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, deferred outflows of resources, liabilities, deferred inflows of resources, net position.

Arkansas Local Police and Fire Retirement System
Page 3

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, regulators, 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.

Ongoing Operations

15. We acknowledge the current economic volatility presents difficult circumstances and challenges for our industry. Entities are potentially facing declines in the fair values of investments and other assets. We understand the values of the assets and liabilities recorded in the financial statements could change rapidly, resulting in material future adjustments to asset values and allowances for accounts receivable.

We acknowledge that you have no responsibility for future changes caused by the current economic environment and the resulting impact on the entity's financial statements. Further, management and governance are solely responsible for all aspects of managing the entity, including questioning the quality and valuation of investments and other assets and reviewing allowance for uncollectible amounts.

Related Parties

16. 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.

17. We understand that the term related party refers to:
 - Affiliates.
 - 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.

Arkansas Local Police and Fire Retirement System
Page 4

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

18. We have disclosed to you all known actual or possible litigation and claims whose effects should be considered when preparing the financial statements. The effects of all known actual or possible litigation and claims have been accounted for and disclosed in accordance with accounting principles generally accepted in the United States of America.
19. 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.
20. 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.
21. 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.
22. 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

23. 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
 - Assisting with the adoption of GASB Statement No. 96
 - Assistance with year-end closing entries for investments
24. 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.

Arkansas Local Police and Fire Retirement System
Page 5

- 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

- 25. 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.
- 26. 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

- 27. All transactions have been recorded in the accounting records and are reflected in the financial statements.
- 28. We have everything we need to keep our books and records.
- 29. 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.
- 30. We believe the effects of the uncorrected financial statement misstatement summarized in the attached schedule is immaterial to the financial statements taken as a whole. This is not considered to be a material weakness, significant deficiency or deficiency in internal control over financial reporting.

Governmental Accounting & Disclosure Matters

- 31. Interfund, internal, and intra-entity activity and balances have been appropriately classified and reported.
- 32. With regard to deposit and investment activities:
 - a. All deposit, repurchase and reverse repurchase agreements, and investment transactions have been made in accordance with legal and contractual requirements.

Arkansas Local Police and Fire Retirement System
Page 6

- b. Investments, derivative instrument transactions, and land and other real estate held by endowments are properly valued.
 - c. Disclosures of deposit and investment balances and risks in the financial statements are consistent with our understanding of the applicable laws regarding enforceability of any pledges of collateral.
 - d. We understand that your audit does not represent an opinion regarding the enforceability of any collateral pledges.
33. Components of net position (net investment in capital assets, restricted, and unrestricted) are properly classified and, if applicable, approved.
34. Capital assets, including infrastructure and intangible assets, are properly capitalized, reported, and, if applicable, depreciated or amortized.
35. The supplementary information required by the Governmental Accounting Standards Board, consisting of management's discussion and analysis and pension information 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.
36. With regard to pension benefits:
- a. We believe the actuarial assumptions and methods used to measure pension liabilities and costs for financial accounting purposes are appropriate in the circumstances.
 - b. We have provided you with the entity's most current pension plan instrument for the audit period, including all plan amendments.
 - c. The participant data provided to you related to pension plans are true copies of the data submitted or electronically transmitted to the plan's actuary.
 - d. The participant data that we provided the plan's actuary for the purposes of determining the actuarial present value of accumulated plan benefits and other actuarially determined amounts in the financial statements were complete.

Accounting & Disclosures

37. 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.
38. Except as reflected in the financial statements, there are no:
- a. Plans or intentions that may materially affect carrying values or classifications of assets, deferred outflows of resources, liabilities, deferred inflows of resources, net position.
 - b. Material transactions omitted or improperly recorded in the financial records.

Arkansas Local Police and Fire Retirement System
Page 7

- 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.
 - h. Known or anticipated asset retirement obligations.
39. 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.

Revenue and Accounts Receivable

40. Adequate provisions and allowances have been accrued for any material losses from:
- a. Uncollectible receivables, of which there were none.

Estimates

41. 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.
42. 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.

Fair Value

43. With respect to the fair value measurements of financial and nonfinancial assets and liabilities, if any, recognized in the financial statements or disclosed in the notes thereto:
- a. The underlying assumptions are reasonable and they appropriately reflect management's intent and ability to carry out its stated course of action.

Arkansas Local Police and Fire Retirement System
Page 8

- b. The measurement methods and significant assumptions used in determining fair value are appropriate in the circumstances for financial statement measurement and disclosure purposes and have been consistently applied.
- c. The significant assumptions appropriately reflect market participant assumptions.
- d. The disclosures related to fair values are complete, adequate, and in conformity with U.S. GAAP.
- e. There are no subsequent events that require adjustments to the fair value measurements and disclosures included in the financial statements.

GASB Statement 96, Subscription-Based Information Technology Arrangements

44. In connection with the adoption of GASB Statement No. 96, *Subscription-Based Information Technology Arrangements*, (GASB 96), we represent the following:
- a. We have identified a complete population of potential subscription-based information technology arrangements (SBITAs) as of the implementation date.
 - b. We have reviewed all significant contracts to identify subscription and nonsubscription components as of the earliest date of adoption. Allocation of costs between subscription and nonsubscription components are based upon standalone prices or other reasonable factors.
 - c. Measurements of the subscription assets and liabilities are based upon facts and circumstances that existed at the beginning of the period of implementation.
 - d. The estimates related to any options to extend or terminate the SBITA terms within the measurement of subscription liability and an intangible right to use IT subscription asset agrees to management's plans for the SBITA.
 - e. The discount rates for each SBITA are based upon what would be obtained by the entity for similar payment amounts during the subscription term as an incremental rate.
 - f. We have adequate controls in place to prevent and/or detect errors in subscription assets and liabilities on a recurring basis.

DocuSigned by:



0403E73EA7574C5...

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

DocuSigned by:




BDF859E80A61470...

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

Arkansas Local Police and Fire Retirement System

Independent Auditor's Reports and Financial Statements

December 31, 2023 and 2022



Arkansas Local Police and Fire Retirement System
Contents
December 31, 2023 and 2022

Contents

Independent Auditor’s Report	1
Management’s Discussion and Analysis	4
Financial Statements	
Statements of Fiduciary Net Position	7
Statements of Changes in Fiduciary Net Position.....	9
Notes to Financial Statements	11
Required Supplementary Information	
Schedule of Changes in Net Pension Liability and Related Ratios	25
Schedule of Employer Contributions.....	26
Schedule of Investment Returns	27
Supplementary Information	
Schedule of Administrative Expenses.....	28
Schedule of Investment Expenses.....	29
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	30



111 Center Street, Suite 1600 / Little Rock, AR 72201

P 501.372.1040 / F 501.372.1250

forvis.com

Independent Auditor's Report

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

Report on the Audit of the Financial Statements

Opinions

We have audited the accompanying financial statements of the Arkansas Local Police and Fire Retirement System (System) as of and for the years ended December 31, 2023 and 2022, and the related notes to the financial statements, which collectively comprise the System'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 Local Police and Fire Retirement System as of December 31, 2023 and 2022, and the changes in financial position 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 System, 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 System'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 System'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 System'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 and pension information listed in the table of contents be presented to supplement the financial statements. Such information is the responsibility of management and, although not 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 basic financial statements and other knowledge we obtained during our audits 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.

Supplementary Information

Our audit was conducted for the purpose of forming an opinion on the financial statements that collectively comprise the System's basic financial statements. The schedule of administrative expenses and the schedule of investment expenses are presented for purposes of additional analysis and are not a required part of the basic financial statements. Such information is the responsibility of management and was derived from and relates directly to the underlying accounting and other records used to prepare the basic financial statements. The information has been subjected to the auditing procedures applied in the audit of the basic financial statements and certain additional procedures, including comparing and reconciling such information directly to the underlying accounting and other records used to prepare the basic financial statements or to the basic financial statements themselves, and other additional procedures in accordance with auditing standards generally accepted in the United States of America. In our opinion, the schedule of administrative expenses and the schedule of investment expenses are fairly stated, in all material respects, in relation to the basic financial statements as a whole.

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 System'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 System'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 System's internal control over financial reporting and compliance.

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

**Arkansas Local Police and Fire Retirement System
Management's Discussion and Analysis
December 31, 2023 and 2022**

This discussion and analysis of the Arkansas Local Police & Fire Retirement System (hereinafter referred to as LOPFI or System) is for the years ended December 31, 2023 and 2022. This analysis provides a summary of the financial position of LOPFI, including highlights and comparisons. For more detailed information regarding LOPFI financial activities, the reader should also review the actual financial statements, including notes and supplementary schedules.

The basic financial statements consist of:

The *Statement of Fiduciary Net Position*, which reports the pension fund assets, liabilities, deferred inflows of resources and net position restricted for pensions at the end of the calendar year. The *Statement of Fiduciary Net Position* is prepared on the accrual basis and, for the most part, the System's net position restricted for pensions is reported on a fair value basis.

The *Statement of Changes in Fiduciary Net Position*, which reports the pension fund transactions that occurred during the calendar year where additions minus deductions equal net increase (decrease) in fiduciary net position. It is an operating statement that reports the net increase or decrease in net position restricted for pensions from the beginning of the year until the end of the year.

The *Notes to Financial Statements* are an integral part of the above financial statements and include additional information not readily evident in the statements themselves.

The *Required Supplementary Information* and *Other Supplementary Information* following the *Notes to Financial Statements* provide added historical and detailed information considered useful in evaluating the condition of LOPFI.

The following pages contain summary comparative statements of LOPFI's pension trust fund for years 2023 and 2022.

**Arkansas Local Police and Fire Retirement System
Management's Discussion and Analysis
December 31, 2023 and 2022**

Summary Statements of Net Position Restricted for Pensions

	<u>2023</u>	<u>2022</u>	<u>2021</u>	<u>2023 Percentage Change</u>	<u>2022 Percentage Change</u>
Cash and cash equivalents	\$ 111,179,672	\$ 149,370,707	\$ 55,228,421	-25.57%	170.46%
Total receivables	12,588,740	12,674,869	10,592,081	-0.68%	19.66%
Prepaid expenses	15,777,924	14,625,139	14,035,674	7.88%	4.20%
Total investments, at fair value	3,054,545,531	2,594,527,517	3,186,230,192	17.73%	-18.57%
Property and equipment, net	3,840,265	3,347,590	3,605,971	14.72%	-7.17%
Other assets	178,402	88,811	123,362	100.88%	-28.01%
Total assets	<u>\$ 3,198,110,534</u>	<u>\$ 2,774,634,633</u>	<u>\$ 3,269,815,701</u>	<u>15.26%</u>	<u>-15.14%</u>
Accounts payable and accrued expenses	\$ 2,200,515	\$ 1,097,274	\$ 1,620,885	100.54%	-32.30%
Refunds payable	237,261	220,430	214,582	7.64%	2.73%
Due to Pension Review Board	394,966	352,372	416,560	12.09%	-15.41%
Total liabilities	<u>2,832,742</u>	<u>1,670,076</u>	<u>2,252,027</u>	<u>69.62%</u>	<u>-25.84%</u>
Total deferred inflows of resources	775,076	468,654	281,850	65.38%	66.28%
Net position restricted for pensions	<u>3,194,502,716</u>	<u>2,772,495,903</u>	<u>3,267,281,824</u>	<u>15.22%</u>	<u>-15.14%</u>
Total liabilities, deferred inflows of resources and net position	<u>\$ 3,198,110,534</u>	<u>\$ 2,774,634,633</u>	<u>\$ 3,269,815,701</u>	<u>15.26%</u>	<u>-15.14%</u>

December 31, 2023

There was growth in total investments as a result of the positive market conditions. The total investments at fair value increase reflects the strong performance of the financial markets in 2023 coupled with the transfer of cash and cash equivalents to investments.

December 31, 2022

There was decrease in total investments as a result of the negative market conditions. The total investments at fair value decrease reflects the weak performance of the financial markets in 2022 coupled with the transfer of investments to cash and cash equivalents.

**Arkansas Local Police and Fire Retirement System
Management's Discussion and Analysis
December 31, 2023 and 2022**

Summary Statements of Changes in Net Position Restricted for Pensions

	<u>2023</u>	<u>2022</u>	<u>2021</u>	<u>2023 Percentage Change</u>	<u>2022 Percentage Change</u>
Total contributions	\$ 197,034,202	\$ 171,619,209	\$ 165,689,468	14.81%	3.58%
Net investment income (loss)	429,484,614	(478,606,720)	467,050,885	-189.74%	-202.47%
Total additions	<u>626,518,816</u>	<u>(306,987,511)</u>	<u>632,740,353</u>	<u>-304.09%</u>	<u>-148.52%</u>
Benefit payments, including refunds and DROP distributions	200,916,498	184,653,916	176,064,754	8.81%	4.88%
Administrative expenses	<u>3,595,505</u>	<u>3,144,494</u>	<u>3,876,398</u>	<u>14.34%</u>	<u>-18.88%</u>
Total deductions	<u>204,512,003</u>	<u>187,798,410</u>	<u>179,941,152</u>	<u>8.90%</u>	<u>4.37%</u>
Net increase (decrease) in fiduciary net position	422,006,813	(494,785,921)	452,799,201	-185.29%	-209.27%
Net position restricted for pensions, beginning of year	<u>2,772,495,903</u>	<u>3,267,281,824</u>	<u>2,814,482,623</u>	<u>-15.14%</u>	<u>16.09%</u>
Net position restricted for pensions, end of year	<u>\$ 3,194,502,716</u>	<u>\$ 2,772,495,903</u>	<u>\$ 3,267,281,824</u>	<u>15.22%</u>	<u>-15.14%</u>

December 31, 2023

There was an increase to the total contributions, due to the increase in contributions from members and employers/departments into the System. The net investment income increased as a result of the portfolio producing a return of 15.90%, while 2022 had a return of -14.90%. An increase in benefits paid to participants is a combination of the growing number of retired LOPFI members as well as the addition of retirees from the consolidated Local Plans.

December 31, 2022

There was an increase to the total contributions, due to the increase in contributions from members and employers/departments into the System. The net investment income decreased as a result of the portfolio producing a return of -14.90%, while 2021 had a return of 17.45%. An increase in benefits paid to participants is a combination of the growing number of retired LOPFI members as well as the addition of retirees from the consolidated Local Plans.

Arkansas Local Police and Fire Retirement System
Statements of Fiduciary Net Position
December 31, 2023 and 2022

	2023		Total
	Cost-Sharing Multiple- Employer	Agent Multiple- Employer	
Assets			
Cash and cash equivalents	\$ 100,985,843	\$ 10,193,829	\$ 111,179,672
Contributions receivable	10,290,964	1,038,802	11,329,766
Interest receivable	420,403	42,437	462,840
Leases receivable	723,138	72,996	796,134
Total receivables	11,434,505	1,154,235	12,588,740
Prepaid expenses	14,331,280	1,446,644	15,777,924
Investments, at fair value			
Equity securities – U.S. companies	656,140,451	66,232,866	722,373,317
Equity securities – international companies	35,817,147	3,615,495	39,432,642
Mutual funds	1,498,752,003	151,288,709	1,650,040,712
U.S. Treasury securities	52,407,435	5,290,170	57,697,605
Corporate bonds	16,379,947	1,653,443	18,033,390
Mortgage-backed securities	73,375,916	7,406,794	80,782,710
Alternative investments	434,154,844	43,824,946	477,979,790
Real estate investment trusts	7,453,033	752,332	8,205,365
Total investments, at fair value	2,774,480,776	280,064,755	3,054,545,531
Property and equipment, net of accumulated depreciation	3,488,159	352,106	3,840,265
Other assets	162,045	16,357	178,402
Total assets	2,904,882,608	293,227,926	3,198,110,534
Liabilities			
Accounts payable and accrued expenses	1,998,754	201,761	2,200,515
Refunds payable	215,507	21,754	237,261
Due to Pension Review Board	358,752	36,214	394,966
Total liabilities	2,573,013	259,729	2,832,742
Deferred Inflows of Resources			
Deferred amounts for leases	704,011	71,065	775,076
Net Position Restricted for Pensions	<u>\$ 2,901,605,584</u>	<u>\$ 292,897,132</u>	<u>\$ 3,194,502,716</u>

Arkansas Local Police and Fire Retirement System
Statements of Fiduciary Net Position (Continued)
December 31, 2023 and 2022

	2022		Total
	Cost-Sharing Multiple- Employer	Agent Multiple- Employer	
Assets			
Cash and cash equivalents	\$ 135,108,466	\$ 14,262,241	\$ 149,370,707
Contributions receivable	10,605,824	1,119,566	11,725,390
Interest receivable	418,647	44,193	462,840
Leases receivable	440,174	46,465	486,639
Total receivables	11,464,645	1,210,224	12,674,869
Prepaid expenses	13,228,699	1,396,440	14,625,139
Investments, at fair value			
Equity securities – U.S. companies	567,570,636	59,913,558	627,484,194
Equity securities – international companies	25,234,039	2,663,741	27,897,780
Mutual funds	1,231,981,109	130,049,668	1,362,030,777
U.S. Treasury securities	36,285,612	3,830,361	40,115,973
Corporate bonds	22,404,250	2,365,024	24,769,274
Mortgage-backed securities	75,530,123	7,973,067	83,503,190
Alternative investments	381,038,437	40,222,956	421,261,393
Real estate investment trusts	6,752,168	712,768	7,464,936
Total investments, at fair value	2,346,796,374	247,731,143	2,594,527,517
Property and equipment, net of accumulated depreciation	3,027,955	319,635	3,347,590
Other assets	80,331	8,480	88,811
Total assets	2,509,706,470	264,928,163	2,774,634,633
Liabilities			
Accounts payable and accrued expenses	992,504	104,770	1,097,274
Refunds payable	199,383	21,047	220,430
Due to Pension Review Board	318,727	33,645	352,372
Total liabilities	1,510,614	159,462	1,670,076
Deferred Inflows of Resources			
Deferred amounts for leases	423,906	44,748	468,654
Net Position Restricted for Pensions	<u>\$ 2,507,771,950</u>	<u>\$ 264,723,953</u>	<u>\$ 2,772,495,903</u>

**Arkansas Local Police and Fire Retirement System
Statements of Changes in Fiduciary Net Position
Years Ended December 31, 2023 and 2022**

	2023		
	Cost-Sharing Multiple- Employer	Agent Multiple- Employer	Total
Additions			
Contributions			
Member contributions	\$ 33,268,911	\$ 10,420	\$ 33,279,331
Employer contributions	115,963,410	40,290,148	156,253,558
Local plan administrative mergers and paid military time	24,297	7,477,016	7,501,313
Total contributions	149,256,618	47,777,584	197,034,202
Investment Income			
Net depreciation in fair value of investments	354,354,563	37,381,903	391,736,466
Interest, dividends and other income	40,913,057	4,316,039	45,229,096
Less investment expenses	(6,767,070)	(713,878)	(7,480,948)
Net investment loss	388,500,550	40,984,064	429,484,614
Total additions	537,757,168	88,761,648	626,518,816
Deductions			
Benefit payments, including refunds and DROP distributions	140,671,453	60,245,045	200,916,498
Administrative expenses	3,252,081	343,424	3,595,505
Total deductions	143,923,534	60,588,469	204,512,003
Net Increase in Net Position Restricted for Pensions	393,833,634	28,173,179	422,006,813
Net Position Restricted for Pensions, Beginning of Year	2,507,771,950	264,723,953	2,772,495,903
Net Position Restricted for Pensions, End of Year	\$ 2,901,605,584	\$ 292,897,132	\$ 3,194,502,716

Arkansas Local Police and Fire Retirement System
Statements of Changes in Fiduciary Net Position (Continued)
Years Ended December 31, 2023 and 2022

	2022		
	Cost-Sharing Multiple- Employer	Agent Multiple- Employer	Total
Additions			
Contributions			
Member contributions	\$ 27,469,832	\$ 15,259	\$ 27,485,091
Employer contributions	102,227,296	39,148,323	141,375,619
Local plan administrative mergers and paid military time	49,566	2,708,933	2,758,499
Total contributions	<u>129,746,694</u>	<u>41,872,515</u>	<u>171,619,209</u>
Investment Income			
Net appreciation in fair value of investments	(453,522,283)	(51,439,695)	(504,961,978)
Interest, dividends and other income	30,927,895	3,507,924	34,435,819
Less investment expenses	<u>(7,257,407)</u>	<u>(823,154)</u>	<u>(8,080,561)</u>
Net investment income	<u>(429,851,795)</u>	<u>(48,754,925)</u>	<u>(478,606,720)</u>
Total additions	<u>(300,105,101)</u>	<u>(6,882,410)</u>	<u>(306,987,511)</u>
Deductions			
Benefit payments, including refunds and DROP distributions	125,265,453	59,388,463	184,653,916
Administrative expenses	<u>2,824,142</u>	<u>320,352</u>	<u>3,144,494</u>
Total deductions	<u>128,089,595</u>	<u>59,708,815</u>	<u>187,798,410</u>
Net Decrease in Net Position Restricted for Pensions	<u>(428,194,696)</u>	<u>(66,591,225)</u>	<u>(494,785,921)</u>
Net Position Restricted for Pensions, Beginning of Year	<u>2,935,966,646</u>	<u>331,315,178</u>	<u>3,267,281,824</u>
Net Position Restricted for Pensions, End of Year	<u>\$ 2,507,771,950</u>	<u>\$ 264,723,953</u>	<u>\$ 2,772,495,903</u>

Arkansas Local Police and Fire Retirement System
Notes to Financial Statements
December 31, 2023 and 2022

Note 1. Reporting Entity and Summary of Significant Accounting Policies

The Arkansas Local Police and Fire Retirement System (System or LOPFI) is a statewide retirement system for police officers and firefighters of political subdivisions of the State of Arkansas. It was established under the authority of Act 364 of 1981 and bears a fiduciary obligation to the participants of the System. LOPFI maintains a cost-sharing multiple-employer defined benefit pension plan (cost-sharing plan) for participants hired by the respective local government unit after January 1, 1983. All accumulated plan assets of the cost-sharing multiple-employer defined pension plan are available to pay any benefit (or to refund any contribution) to any plan member or beneficiary of the plan.

Political subdivisions that had a local pension and relief fund (local plan) for its police officers and firefighters prior to the establishment of LOPFI may transfer their local plan to LOPFI for administration. Local plans that are now being administered by LOPFI are included in the agent multiple-employers defined benefit pension plan for financial reporting purposes; however, the assets of the individual local plans can only be used to pay the benefit (or to refund any contribution) to plan members or beneficiaries of the individual local plan.

The assets of all plans are pooled for investment purposes.

Basis of Accounting

The accounting policies of the System 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 System is accounted for on an economic resources measurement focus using the accrual basis of accounting. Plan member and employer contributions are recognized as additions in the period in which plan member services are performed. Benefits and refunds are recognized when paid in accordance with the terms of the Plan. Deductions are recognized as incurred.

Cash Equivalents

The System considers all liquid investments with original maturities of three months or less to be cash equivalents. At December 31, 2023 and 2022, cash equivalents consisted primarily of money market accounts with brokers.

Valuation of Investments

Investments are stated at fair value in the accompanying statements of fiduciary net position. The fair value of marketable investments, including U.S. government securities, mutual funds, corporate bonds and stocks, is determined by the latest bid price or by the closing exchange price at statement of fiduciary net position dates. The fair values of private equities are based on management's valuation of estimates and assumptions from information and representations provided by the respective general partners, in the absence of readily ascertainable fair values.

Purchases and sales of securities are recorded on a trade-date basis. Interest income is recorded on the accrual basis. Dividends are recorded on the ex-dividend date.

Net increase in fair value of investments reflected in the accompanying statements of changes in fiduciary net position represents gains or losses realized during the year plus or minus the change in the net unrealized gains or losses on investments.

The change in net unrealized gains or losses on investments represents the change in the difference between the cost and fair value of investments at the beginning versus the end of the year.

Arkansas Local Police and Fire Retirement System
Notes to Financial Statements
December 31, 2023 and 2022

Deferred Inflows of Resources

The System reports an acquisition of net assets that is applicable to a future reporting period as deferred inflows of resources in a separate section of its statements of fiduciary net position.

Investment Income

Net investment income credited to each plan is allocated based on the plan's average balance of fiduciary net position.

Administrative Expenses

Administrative expenses are allocated to each plan based on the plan's average balance of fiduciary net position.

Use of Estimates

The preparation of financial statements in conformity with accounting principles generally accepted in the United States of America requires the System's management to make estimates and assumptions that affect reported amounts of asset, liabilities and deferred inflows of resources and disclosure of contingent assets and liabilities and the actuarial valuation of the System's benefits at the date of the financial statements and the reported changes in plan net position during the reporting period. Actual results may differ from those estimates.

Arkansas Local Police and Fire Retirement System
Notes to Financial Statements
December 31, 2023 and 2022

Plan Descriptions

As of December 31, 2023 and 2022, the number of participating political subdivisions was 555 and 554, respectively. At December 31, 2023 and 2022, the System's membership consisted of the following:

Membership Classification	Number of Employees	
	2023	2022
Retired plan members or beneficiaries currently receiving benefits:		
Local plan fire without Social Security	1,011	999
Local plan police with Social Security	168	173
Local plan police without Social Security	611	622
Local plan volunteer fire	1,280	1,280
Subtotal for agent multiple-employer plans	3,070	3,074
LOPFI fire benefit program 2 – with Social Security	24	33
LOPFI fire benefit program 2 – without Social Security	213	220
LOPFI fire with Social Security	73	55
LOPFI fire without Social Security	1,536	1,389
LOPFI police benefit program 2 – with Social Security	27	39
LOPFI police benefit program 2 – without Social Security	227	213
LOPFI police with Social Security	1,757	1,598
LOPFI police without Social Security	983	945
LOPFI volunteer police benefit 4 program	1	2
LOPFI staff	6	6
LOPFI volunteer fire benefit program 3	4,014	3,729
LOPFI volunteer fire benefit program 4	7	21
LOPFI volunteer police benefit program 3	328	301
Subtotal for cost-sharing multiple-employer plans	9,196	8,551
Subtotal for retirees and beneficiaries	12,266	11,625
Active plan members:		
Local plan fire without Social Security	1	1
Local plan fire with Social Security	1	1
Local plan part paid contributory fire	1	2
Local plan volunteer fire	4	5
Subtotal for agent multiple-employer plans	7	9
LOPFI fire benefit program 2 – with Social Security	73	60
LOPFI fire benefit program 2 – without Social Security	198	191
LOPFI fire with Social Security	128	132
LOPFI fire without Social Security	2,546	2,484
LOPFI police benefit program 2 – with Social Security	76	67
LOPFI police benefit program 2 – without Social Security	241	233
LOPFI police with Social Security	2,325	2,252
LOPFI police without Social Security	1,242	1,223
LOPFI staff	7	6
LOPFI volunteer fire	6,673	6,743
LOPFI volunteer police	446	451
LOPFI volunteer fire benefit program 4	52	53
LOPFI volunteer police benefit program 4	13	4
Subtotal for cost-sharing multiple-employer plans	14,020	13,899
Subtotal for active employees	14,027	13,908
Inactive plan members entitled to but not yet receiving benefits	10,266	9,962
Total membership	36,559	35,495

Arkansas Local Police and Fire Retirement System
Notes to Financial Statements
December 31, 2023 and 2022

Contributions: The employee contribution rate depends on the type of service being rendered and whether or not the service is also covered by Social Security. The different employee contribution rates are:

- a. Paid service not covered by Social Security: 9.5% of gross pay beginning July 1, 2023; 8.5% of gross pay beginning July 1, 2009; 6% prior to that date
- b. Paid service also covered by Social Security: 3.5% of gross pay beginning July 1, 2023; 2.5% of gross pay beginning July 1, 2009; no employee contributions prior to that date
- c. Paid service-benefit program 2: 9.5% of gross pay beginning July 1, 2023; 8.5% of gross pay beginning July 1, 2009; 6% prior to that date
- d. Volunteer service: no employee contribution

The employer contribution rate is adjusted automatically every year to reflect changes in the composition of the employee group and other factors which affect cost. Contributions are determined on an actuarial basis in order to ensure that the individual system employers can honor their benefit commitments to covered employees. The individual entry age actuarial cost method of valuation is used in determining normal cost.

Benefit Terms: The benefits terms for the cost-sharing plan are established in accordance with the provisions of the Arkansas Code.

Benefit Program 1: Pension benefits to a member with five or more years (10 or more years for members hired on or after July 1, 2013) of credited service in force who has attained his normal retirement age consist of an annuity equal to the following:

- a. For each year of paid service resulting from employment in a position not also covered by Social Security, 3% of his final average pay; plus
- b. For each year of paid service resulting from employment in a position also covered by Social Security, 2% of his final average pay. In addition, if such member is retiring and if such member's age at retirement is younger than Social Security's minimum age for an unreduced retirement benefit, then such member receives a temporary annuity equal to 1% of his final average pay for each such year of paid service. Such temporary annuity terminates at the end of the calendar month in which the earliest of the following events occur: such member's death; or his attainment of such Social Security minimum age for unreduced benefits.
- c. In no event will the total of *a.* plus *b.* exceed, at time of retirement, 100% of such final average pay; plus
- d. Effective July 1, 2023, for each year of volunteer service, \$8.09 per month, to a maximum of \$323.60 monthly.
- e. Before the date that the first payment of his annuity becomes due, but not thereafter, a member may elect in writing to receive his annuity as a life annuity or he may elect to have his life annuity reduced but not any temporary annuity which may be payable, and nominate a beneficiary in accordance with the provisions of one of four options. If a member does not elect an option, his annuity shall be paid to him as a life annuity.

Benefit Program 2: For each year of paid service rendered on or after the election date of Benefit Program 2 and resulting from employment in a position not also covered by Social Security, 3.34% of his or her final average pay beginning July 1, 2023, plus for each year of paid service rendered on or after the election date of Benefit Program 2 and resulting from employment in a position also covered by Social Security, 3% of his or her final average pay beginning July 1, 2023.

Arkansas Local Police and Fire Retirement System
Notes to Financial Statements
December 31, 2023 and 2022

A member will receive disability benefits computed in the same manner as normal retirement benefits if the member has five or more years of credited service (or 10 years of actual service if hired on or after July 1, 2013) and terminates employment because of becoming totally and permanently disabled from non-duty related causes. If the disability is determined to be duty related, the member will receive a benefit regardless of the total amount of credited service. The disability will be designated as Catastrophic Duty (as if the member accrued 28 years of paid service), Hazardous Duty (65% of final average pay), or Ordinary Duty (15% of final average pay).

Deferred Retirement Option Plan (DROP): During 1993, the Arkansas General Assembly passed legislation (Acts 757 and 1004) allowing paid policemen and firefighters to elect to continue working for a period of 10 years past normal retirement age if a member of a local plan. In 2003, the Arkansas General Assembly passed legislation (Act 1734) affording paid members of LOPFI the same opportunity to continue working past normal retirement age with the maximum term being five year. The maximum term was extended to ten years in 2023.

This DROP is only available to participants having at least 20 years of paid service. In addition, Act 829 of 2015 allows up to 36 months of actual LOPFI volunteer service credit to be used toward DROP eligibility. The DROP member continues his payroll withholding, the employee's contribution is credited according to law to the defined benefit pension plan and the DROP, and the monthly benefits that would have been payable had the member elected to cease employment and receive a service retirement shall be paid into a separate DROP account. At December 31, 2023 and 2022, the DROP accounts totaled \$46,594,913 and \$46,293,213, respectively.

Note 2. Leases Receivable

The System leases a portion of its office space to various third parties, the terms of which expire 2025 through 2030. Payments increase based on the terms of the lease agreements. The leases were measured based upon the timing and amount of these payments at lease commencement. There are no variable payments. Revenue recognized under lease contracts during the years ended December 31, 2023 and 2022 was approximately \$140,000 and \$120,000, respectively, which includes both lease revenue and interest.

Note 3. Net Pension Liability

The components of the net pension liability of all entities participating in the cost-sharing plan at December 31, 2023 and 2022 were as follows:

	<u>2023</u>	<u>2022</u>
Total pension liability	\$ 3,951,335,469	\$ 3,631,010,767
Plan's fiduciary net position	<u>2,901,605,584</u>	<u>2,507,771,950</u>
Net pension liability	<u>\$ 1,049,729,885</u>	<u>\$ 1,123,238,817</u>
Plan's fiduciary net position as a percentage of total pension liability	73.43%	69.07%

**Arkansas Local Police and Fire Retirement System
Notes to Financial Statements
December 31, 2023 and 2022**

Actuarial Assumptions

The total pension liability as of December 31, 2023 and 2022 was determined by actuarial valuations as of December 31, 2023 and 2022 using the following actuarial assumptions:

	<u>2023</u>	<u>2022</u>
Wage inflation	3.00%	3.00%
Price inflation	2.25%	2.25%
Investment rate of return	7.25%	7.25%

The mortality table used for the December 31, 2023 and 2022 valuations was the Pub-2010 Amount-Weighted General Below Median Income Healthy Retiree tables for males and females. The disability postretirement mortality table used was the Pub-2010 Disabled Retiree benefit-weighted generational mortality table for males and females.

The actuarial assumptions used in the December 31, 2023 and 2022 calculation were based on the results of an experience study of the period 2017 to 2020.

Arkansas Local Police and Fire Retirement System
Notes to Financial Statements
December 31, 2023 and 2022

The long-term expected rate of return on pension plan investments was determined using a building-block method in which expected future real rates of return (expected returns, net of pension plan investment expense and inflation) are developed for each major asset class.

2023		
Asset Class	Target Allocation	Long-Term Expected Real Rate of Return
U.S. Stock – Large Cap	21.00%	5.62%
U.S. Stock – Small Cap	21.00%	5.86%
International Equity	9.00%	6.92%
Emerging Markets	9.00%	8.95%
U.S. Corporate Bonds	25.00%	2.29%
Real Estate	5.00%	3.61%
Private Equity	10.00%	9.48%
Total	100.00%	

2022		
Asset Class	Target Allocation	Long-Term Expected Real Rate of Return
U.S. Stock – Large Cap	21.00%	4.05%
U.S. Stock – Small Cap	21.00%	4.65%
International Equity	9.00%	5.27%
Emerging Markets	9.00%	7.49%
U.S. Corporate Bonds	25.00%	-0.35%
Real Estate	5.00%	3.76%
Private Equity	10.00%	9.10%
Total	100.00%	

Single Discount Rate

The single discount rate used to measure the total pension liability was 7.25% for the years ended December 31, 2023 and 2022. The single discount rate was based on the expected rate of return on pension plan investments.

The projection of cash flows used to determine this single discount rate assumed that plan member contributions will be made at the current contribution rate and that employer contributions will be made at rates equal to the difference between actuarially determined contribution rates and the member rate. Based on these assumptions, the pension plan's fiduciary net position was projected to be available to make all projected future benefit payments of current plan members.

Arkansas Local Police and Fire Retirement System
Notes to Financial Statements
December 31, 2023 and 2022

Plan assets are expected to be invested using a strategy to achieve the expected rate of return. Therefore, the long-term expected rate of return on pension plan investments was applied to all periods of projected benefit payments to determine the total pension liability. Regarding the sensitivity of the net pension liability to changes in the single discount rate, the following presents the net pension liability as of December 31, 2023 calculated using a single discount rate of 7.25%, as well as what the net pension liability would be if it were calculated using a single discount rate that is 1% lower or 1% higher:

	2023		
	1% Decrease	Current Single Discount Rate	1% Increase
	6.25%	7.25%	8.25%
Net pension liability	\$ 1,645,880,133	\$ 1,049,729,885	\$ 567,746,158

	2022		
	1% Decrease	Current Single Discount Rate	1% Increase
	6.25%	7.25%	8.25%
Net pension liability	\$ 1,672,188,582	\$ 1,123,238,817	\$ 679,252,862

Note 4. Deposits and Investments

The System's deposits and investments are managed by various investment managers who have discretionary authority over the assets managed by them, within the investment guidelines established by LOPFI, under contracts with the System.

Custodial Credit Risk

Custodial credit risk is the risk that, in the event of the failure of the custodian, the System will not be able to recover the value of its investments or collateral securities that are in the possession of an outside party.

The System's deposits and investments are held by the System's custodian in the System's name. Investments are uninsured and generally consist of short-term securities, U.S. and foreign government securities, domestic and foreign corporate debt and equity securities, real estate and real estate trusts.

The state law requires collateralization of all deposits with federal depository insurance and other acceptable collateral in specific amounts. The System's investment policy does not directly address custodial credit risk. At December 31, 2023, all of the System's deposits were either insured or collateralized with securities pledged in the System's name.

Credit Risk

Credit risk is the risk that an issuer or other counterparty to an investment will not fulfill its obligations to the System. The System's investment policy does not allow for more than 10% of the current fair value of the Fixed Income Portfolio to be invested in securities rated less than BBB by Standard & Poor's, or the equivalent by a recognized rating agency. In addition, the minimum-security quality shall be B or better.

Arkansas Local Police and Fire Retirement System
Notes to Financial Statements
December 31, 2023 and 2022

The following table summarizes the System's fixed income portfolio exposure levels and credit qualities at December 31, 2023 and 2022:

	<u>2023</u>	<u>2022</u>
Fixed Income Security Type by S&P Rating		
Corporate and Foreign Bonds		
A	\$ 7,029,880	\$ 12,959,187
BBB	11,003,510	11,810,087
	<u>18,033,390</u>	<u>24,769,274</u>
Mortgage-Backed Securities		
Not rated	<u>80,782,710</u>	<u>83,503,190</u>
	<u>\$ 98,816,100</u>	<u>\$ 108,272,464</u>

Interest Rate Risk

Interest rate risk is the risk that changes in interest rates will adversely affect the fair value of an investment. The System's interest rate risk is controlled through duration management. Duration is a measure of the sensitivity of the price (the value of principal) of a fixed income investment to a change in interest rates and is expressed as a number of years. In accordance with its investment policy, the fixed income portfolio shall vary from the duration of the relative comparative indices by no more than +/-25%. As of December 31, 2023 and 2022, the System's effective duration by investment type was:

<u>Fixed Income Security Type</u>	<u>Duration</u>	
	<u>2023</u>	<u>2022</u>
U.S. Government and Government Related	1.65	1.85
U.S. Credit	1.18	1.33
Non-U.S. Credit	0.00	-0.07
Mortgage-Backed	2.56	2.29
Non-Agency Mortgage-Backed	0.02	0.04
Asset-Backed	0.03	0.02
Other	0.02	0.02
Cash	<u>0.00</u>	<u>0.00</u>
Total Duration	<u>5.46</u>	<u>5.48</u>

Rate of Return

For the years ended December 31, 2023 and 2022, the annual money-weighted rate of return on pension plan investments, net of pension plan investment expense, was 15.90% and -14.90%, respectively. The money-weighted rate of return expresses investment performance, net of investment expense, adjusted for the changing amounts actually invested.

Arkansas Local Police and Fire Retirement System
Notes to Financial Statements
December 31, 2023 and 2022

Investment Policies

The LOPFI Board (Board) has been appointed by the Governor to oversee the investments of LOPFI. The Board is responsible for establishing overall financial objectives and setting the investment policy. The Board will carry out its responsibilities by acting on recommendations made to it by the Investment Committee (Committee). The Committee shall consist of at least three trustees of the Board. An amendment to the investment policy first requires a majority approval of the Committee and then review and approval by the Board.

Note 5. Disclosures About Fair Value of Assets and Liabilities

Fair value is the price that would be received to sell an asset or paid to transfer a liability in an orderly transaction between market participants at the measurement date. Fair value measurements must maximize the use of observable inputs and minimize the use of unobservable inputs. There is a hierarchy of three levels of inputs that may be used to measure fair value:

- Level 1** Quoted prices in active markets for identical assets or liabilities
- Level 2** Observable inputs other than Level 1 prices, such as quoted prices for similar assets or liabilities; quoted prices in markets that are not active; or other inputs that are observable or can be corroborated by observable market data for substantially the full term of the assets or liabilities
- Level 3** Unobservable inputs supported by little or no market activity and are significant to the fair value of the assets or liabilities

Arkansas Local Police and Fire Retirement System
Notes to Financial Statements
December 31, 2023 and 2022

Recurring Measurements

The following tables present the fair value measurements of assets and liabilities recognized in the accompanying financial statements measured at fair value on a recurring basis and the level within the fair value hierarchy in which the fair value measurements fall at December 31, 2023 and 2022:

	<u>Fair Value</u>	<u>Quoted Prices in Active Markets for Identical Assets (Level 1)</u>	<u>Significant Other Observable Inputs (Level 2)</u>	<u>Significant Unobservable Inputs (Level 3)</u>
December 31, 2023				
Investments by Fair Value Level				
Equity securities – diversified	\$ 722,373,317	\$ 722,373,317	\$ -	\$ -
Equity securities – foreign	39,432,642	39,432,642	-	-
Equity mutual funds	1,376,997,459	169,973,193	1,207,024,266	-
International equity mutual funds	55,536,799	-	55,536,799	-
Fixed income mutual funds	217,506,454	-	100,926,562	116,579,892
Real estate investment trusts	8,205,365	8,205,365	-	-
U.S. government obligations	57,697,605	-	57,697,605	-
Corporate bonds	18,033,390	-	18,033,390	-
Mortgage-backed securities	80,782,710	-	80,782,710	-
	<u>2,576,565,741</u>	<u>939,984,517</u>	<u>1,520,001,332</u>	<u>116,579,892</u>
Total investments by fair value level	<u>2,576,565,741</u>	<u>939,984,517</u>	<u>1,520,001,332</u>	<u>116,579,892</u>
Investments Measured at the Net Asset Value (NAV) ^(A)				
Private equity funds	143,866,604			
Private debt funds	126,614,290			
Equity long/short hedge funds	41,370,412			
Real estate funds	50,604,011			
Bank recapitalization and value opportunities funds	25,898,854			
Energy funds	15,676,150			
Opportunistic credit funds	73,949,469			
	<u>477,979,790</u>			
Total investments measured at the NAV	<u>477,979,790</u>			
Total investments measured at fair value	<u>\$ 3,054,545,531</u>	<u>\$ 939,984,517</u>	<u>\$ 1,520,001,332</u>	<u>\$ 116,579,892</u>

Arkansas Local Police and Fire Retirement System
Notes to Financial Statements
December 31, 2023 and 2022

	<u>Fair Value</u>	<u>Quoted Prices in Active Markets for Identical Assets (Level 1)</u>	<u>Significant Other Observable Inputs (Level 2)</u>	<u>Significant Unobservable Inputs (Level 3)</u>
December 31, 2022				
Investments by Fair Value Level				
Equity securities – diversified	\$ 627,484,194	\$ 627,484,194	\$ -	\$ -
Equity securities – foreign	27,897,780	27,897,780	-	-
Equity mutual funds	1,107,686,420	159,896,929	541,708,790	406,080,701
International equity mutual funds	48,645,472	-	48,645,472	-
Fixed income mutual funds	205,698,885	-	95,566,766	110,132,119
Real estate investment trusts	7,464,936	7,464,936	-	-
U.S. government obligations	40,115,973	-	40,115,973	-
Corporate bonds	24,769,274	-	24,769,274	-
Mortgage-backed securities	83,503,190	-	83,503,190	-
	<u>2,173,266,124</u>	<u>822,743,839</u>	<u>834,309,465</u>	<u>516,212,820</u>
Investments Measured at the Net Asset Value (NAV) ^(A)				
Private equity funds	167,602,884			
Private debt funds	57,582,034			
Equity long/short hedge funds	37,188,703			
Real estate funds	59,438,960			
Bank recapitalization and value opportunities funds	28,116,178			
Energy funds	5,089,542			
Opportunistic credit funds	66,243,092			
	<u>421,261,393</u>			
Total investments measured at the NAV	<u>421,261,393</u>			
Total investments measured at fair value	<u>\$ 2,594,527,517</u>	<u>\$ 822,743,839</u>	<u>\$ 834,309,465</u>	<u>\$ 516,212,820</u>

(A) Certain investments that are measured using the NAV per share (or its equivalent) practical expedient have not been classified in the fair value hierarchy. The fair value amounts included above are intended to permit reconciliation of the fair value hierarchy to the amounts presented in the statements of fiduciary net position.

Arkansas Local Police and Fire Retirement System
Notes to Financial Statements
December 31, 2023 and 2022

Investments

The valuation method for investments measured at the NAV per share (or its equivalent) is presented below.

	December 31, 2023			
	Net Asset Value	Unfunded Commitments	Redemption Frequency	Redemption Notice Period
Private equity funds ^(A)	\$ 143,866,604	\$ 68,425,131		
Private debt funds ^(B)	107,339,724	32,953,557		
Private debt funds ^(B)	19,274,566	-	Quarterly	90 Days
Equity long/short hedge funds ^(C)	41,370,412	-	Quarterly	90 Days
Real estate funds ^(D)	29,202,064	-	Quarterly	45 Days
Real estate funds ^(D)	21,401,947	-	Semi-annually	5 Months
Bank recapitalization and value opportunistic funds ^(E)	25,898,854	2,000,000		
Energy funds ^(F)	15,676,150	21,618,982		
Opportunistic credit funds ^(G)	73,949,469	-	Annually	90 Days

	December 31, 2022			
	Net Asset Value	Unfunded Commitments	Redemption Frequency	Redemption Notice Period
Private equity funds ^(A)	\$ 158,731,454	\$ 69,977,392		
Private equity funds ^(A)	8,871,429	-	Semi-annually	5 Months
Private debt funds ^(B)	57,582,034	50,572,733		
Equity long/short hedge funds ^(C)	37,188,704	-	Quarterly	90 Days
Real estate funds ^(D)	59,438,960	-	Quarterly	45 Days
Bank recapitalization and value opportunistic funds ^(E)	28,116,178	2,000,000		
Energy funds ^(F)	5,089,542	600,983		
Opportunistic credit funds ^(G)	66,243,092	-	Annually	90 Days

(A) This category includes investments in several private companies. Most of these investments can never be redeemed with the funds. Distributions from each fund will be made as the underlying investments of the funds are liquidated.

(B) This category includes a diversified portfolio of private debt investments in transactions sponsored by private equity sponsors, including leverage buyouts, refinancing, acquisitions and growth capital. These investments can never be redeemed with the funds.

(C) This category includes investments in hedge funds that take both long and short positions in equities. Management of the funds has the ability to shift investments among differing investment strategies.

(D) This category includes several real estate funds that invest primarily in U.S. commercial real estate. Distributions from each fund will be made as the underlying investments of the funds are liquidated.

Arkansas Local Police and Fire Retirement System
Notes to Financial Statements
December 31, 2023 and 2022

- (E) This category invests primarily in performing, underperforming or nonperforming loans, asset-backed securities, residential and commercial real estate and other debt instruments. These investments can never be redeemed with the funds.
- (F) This fund invests primarily in oil and gas and minerals and royalties. These investments can never be redeemed with the funds.
- (G) This category includes a diversified portfolio of loans and bonds. These investments can be redeemed annually after a 90-day notice period.

Note 6. Risks and Uncertainties

The System invests in various investment securities. Investment securities are exposed to various risks, such as interest rate, market and credit risks. Due to the level of risk associated with certain investment securities, it is at least reasonably possible that changes in the values of investment securities will occur in the near term and that such changes could materially affect the amounts reported in the statements of fiduciary net position.

System contributions are made and the actuarial present value of accumulated plan benefits are reported based on certain assumptions pertaining to interest rates, inflation rates and employee demographics, all of which are subject to change. Due to uncertainties inherent in the estimation and assumption process, it is at least reasonably possible that changes in these estimates and assumptions in the near term would be material to the financial statements.

Required Supplementary Information

**Arkansas Local Police and Fire Retirement System
Required Supplementary Information
Schedule of Changes in Net Pension Liability and Related Ratios**

	2023	2022	2021	2020	2019	2018	2017	2016	2015	2014
Total Pension Liability										
Service cost	\$ 65,784,489	\$ 63,599,165	\$ 63,571,932	\$ 62,439,385	\$ 59,701,701	\$ 61,057,199	\$ 52,999,883	\$ 52,411,007	\$ 50,466,076	\$ 51,147,644
Interest on the total pension liability	260,533,628	240,576,582	224,826,211	210,227,380	194,307,497	182,428,731	170,545,435	157,522,879	146,226,976	134,748,677
Benefit changes	-	32,765,847	-	(2,985,529)	-	(24,831,215)	-	-	-	272,375
Differences between expected and actual experience	134,678,038	76,572,153	33,796,334	45,976,608	64,405,712	32,299,710	27,286,660	19,163,957	5,172,371	(1,779,051)
Assumption changes	-	(124,878,986)	24,271,181	-	-	-	219,939,183	-	53,731,281	-
Benefit payments, DROP Distributions and Refunds	(140,671,453)	(125,265,453)	(117,682,480)	(97,656,316)	(87,057,377)	(74,102,672)	(64,420,008)	(58,298,612)	(45,407,579)	(35,732,645)
Net Change in Total Pension Liability	320,324,702	163,369,308	228,783,178	218,001,528	231,357,533	176,851,753	406,351,153	170,799,231	210,189,125	148,657,000
Total Pension Liability, Beginning of Year	3,631,010,767	3,467,641,459	3,238,858,281	3,020,856,753	2,789,499,220	2,612,647,467	2,206,296,314	2,035,497,083	1,825,307,958	1,676,650,958
Total Pension Liability, End of Year	\$ 3,951,335,469	\$ 3,631,010,767	\$ 3,467,641,459	\$ 3,238,858,281	\$ 3,020,856,753	\$ 2,789,499,220	\$ 2,612,647,467	\$ 2,206,296,314	\$ 2,035,497,083	\$ 1,825,307,958
Plan Fiduciary Net Position										
Employer contributions	\$ 115,963,410	\$ 102,227,296	\$ 97,841,951	\$ 93,919,327	\$ 88,524,836	\$ 83,861,098	\$ 77,410,021	\$ 75,298,216	\$ 67,624,600	\$ 63,964,129
Employee contributions	33,268,911	27,469,832	25,896,170	26,577,992	25,157,606	24,456,628	23,351,970	21,816,086	21,187,024	21,844,747
Other contributions	24,297	49,566	66,481	98,204	180,761	87,759	54,467	38,872	34,066	56,744
Pension plan net investment income	388,500,550	(429,851,795)	417,518,996	290,325,750	345,816,336	(53,604,321)	227,213,213	88,592,090	1,642,306	95,052,926
Benefit payments, DROP distributions and refunds	(140,671,453)	(125,265,453)	(117,682,480)	(97,656,316)	(87,057,377)	(74,102,672)	(64,420,008)	(58,298,612)	(45,407,579)	(35,732,645)
Pension plan administrative expense	(3,252,081)	(2,824,142)	(3,465,297)	(3,590,651)	(3,041,397)	(3,553,631)	(2,950,772)	(2,665,399)	(2,482,123)	(2,258,660)
Net Change in Plan Fiduciary Net Position	393,833,634	(428,194,696)	420,175,821	309,674,306	369,580,765	(22,855,139)	260,658,891	124,781,253	42,598,294	142,927,241
Plan Fiduciary Net Position, Beginning of Year	2,507,771,950	2,935,966,646	2,515,790,825	2,206,116,519	1,836,535,754	1,859,390,893	1,598,732,002	1,473,950,749	1,431,352,455	1,288,425,214
Plan Fiduciary Net Position, End of Year	\$ 2,901,605,584	\$ 2,507,771,950	\$ 2,935,966,646	\$ 2,515,790,825	\$ 2,206,116,519	\$ 1,836,535,754	\$ 1,859,390,893	\$ 1,598,732,002	\$ 1,473,950,749	\$ 1,431,352,455
Net Pension Liability, End of Year	\$ 1,049,729,885	\$ 1,123,238,817	\$ 531,674,813	\$ 723,067,456	\$ 814,740,234	\$ 952,963,466	\$ 753,256,574	\$ 607,564,312	\$ 561,546,334	\$ 393,955,503
Plan's Fiduciary Net Position as a Percentage of the Total Pension Liability	73.43%	69.07%	84.67%	77.68%	73.03%	65.84%	71.17%	72.46%	72.41%	78.42%
Covered Payroll	\$ 459,976,329	\$ 414,280,752	\$ 392,522,925	\$ 386,909,993	\$ 371,574,513	\$ 356,157,157	\$ 339,098,676	\$ 329,344,355	\$ 320,487,331	\$ 310,870,608
Plan's Net Pension Liability as a Percentage of Covered Payroll	228.21%	271.13%	135.45%	186.88%	219.27%	267.57%	222.13%	184.48%	175.22%	126.73%

**Arkansas Local Police and Fire Retirement System
Required Supplementary Information
Schedule of Employer Contributions**

Fiscal Year Ending	Actuarially Determined Contribution	Actual Contribution	Contribution Deficiency (Excess)	Covered Payroll	Actual Contribution as a % of Covered Payroll
12/31/2014	63,964,129	63,964,129	-	\$ 310,870,608	20.58%
12/31/2015	67,624,600	67,624,600	-	320,487,331	21.10%
12/31/2016	75,298,216	75,298,216	-	329,344,355	22.86%
12/31/2017	77,410,021	77,410,021	-	339,098,676	22.83%
12/31/2018	83,861,098	83,861,098	-	356,157,157	23.55%
12/31/2019	88,524,836	88,524,836	-	371,574,513	23.82%
12/31/2020	93,919,327	93,919,327	-	386,909,993	24.27%
12/31/2021	97,841,951	97,841,951	-	392,522,925	24.93%
12/31/2022	102,227,296	102,227,296	-	414,280,752	24.68%
12/31/2023	115,963,410	115,963,410	-	459,976,329	25.21%

Valuation Date: Actuarially determined contribution rates are calculated as of December 31, 2020.

Methods and Assumptions Used to Determine Contribution Rates:

Actuarial Cost Method	Entry Age Normal
Amortization Method	Level Percentage of Payroll, Closed
Remaining Amortization Period	14 years beginning January 1, 2022
Asset Valuation Method	5-Year smoothed market, 20% corridor
Wage Inflation	3.25%
Price Inflation	2.50%
Salary Increases	3.75% to 18.25%, including inflation
Investment Rate of Return	7.50%, as adopted by the Board
Retirement Age	Experience-based table of rates that condition. Last updated for the 2017 study of the period 2012-2016.
Mortality	RP-2014 Healthy Annuitant, Disabled Retiree and Employee mortality tables for males and females. The tables applied credibility adjustments of 135% for males and 125% for females and were adjusted for fully generational mortality improvements using Scale MP-2016.

Other Information:

Notes There were no changes in benefits, methods or assumptions in the December 31, 2020 actuarial valuation. There were benefit provision changes for the December 31, 2020 actuarial valuation. They include Act 72 of 2021 related to duty disability benefits, Acts 374 of 2021 related to reciprocal service and final average pay and Act 344 of 2021 related to return to service for retirees.

**Arkansas Local Police and Fire Retirement System
Required Supplementary Information
Schedule of Investment Returns**

Fiscal Year Ending	Annual Money-Weighted Rate of Return, Net of Investment Expense
12/31/2014	6.80%
12/31/2015	-0.05%
12/31/2016	5.76%
12/31/2017	14.48%
12/31/2018	-2.59%
12/31/2019	19.00%
12/31/2020	13.19%
12/31/2021	17.45%
12/31/2022	-14.90%
12/31/2023	15.90%

Note: This schedule provides the returns for the cost-sharing multiple-employer defined benefit pension plan and the agent multiple-employers defined benefit pension plans.

Supplementary Information

Arkansas Local Police and Fire Retirement System
Schedule of Administrative Expenses
Years Ended December 31, 2023 and 2022

	<u>2023</u>	<u>2022</u>
Personal Services		
Staff expense	\$ 998,854	\$ 1,164,633
Professional Services		
Computer operations/process	1,501,443	999,963
Audit services	130,500	121,800
Actuarial services	373,000	357,848
Legal services	150,000	177,936
Medical advisor/related	31,139	31,762
Total professional services	<u>2,186,082</u>	<u>1,689,309</u>
General Operating Expense		
Insurance expense	123,851	56,886
Office equipment	34,693	48,762
Office supplies	18,430	7,925
Printing	43,364	24,951
Telephone	31,511	32,024
Postage	41,005	20,923
Publications	1,494	717
Travel/professional education/conferences	36,955	26,493
Miscellaneous	-	(1,073)
Board/kitchen supplies	2,642	3,072
Total general operating expense	<u>333,945</u>	<u>220,680</u>
Total expenses	<u>3,518,881</u>	<u>3,074,622</u>
Depreciation expense	<u>76,624</u>	<u>69,872</u>
Total Administrative Expenses	<u>\$ 3,595,505</u>	<u>\$ 3,144,494</u>

Arkansas Local Police and Fire Retirement System
Schedule of Investment Expenses
Years Ended December 31, 2023 and 2022

	<u>2023</u>	<u>2022</u>
Investment consulting fees	\$ 860,000	\$ 860,000
Money manager fees	6,106,498	6,741,111
Custodial fees	216,000	216,000
Investment monitor expenses	<u>298,450</u>	<u>263,450</u>
Total investment expenses	<u>\$ 7,480,948</u>	<u>\$ 8,080,561</u>



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 of Trustees
Arkansas Local Police and Fire Retirement System
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 Local Police and Fire Retirement System (System), which comprise the statement of fiduciary net position as of December 31, 2023, and the related statements of changes in fiduciary net position, 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 System'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 System's internal control. Accordingly, we do not express an opinion on the effectiveness of the System'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 System'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

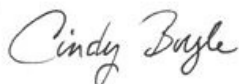
We believe our engagement is complete. This letter serves as a recap of the engagement.

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, CPA, CIA[®], CITP[®], CISA[®]
Partner, IT Risk & Compliance

CHB: edm

Enclosure

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	1
Definitions of Ratings	3
Findings & Recommendations	4
Scope of Services	6
Appendix A: NIST Framework	8

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

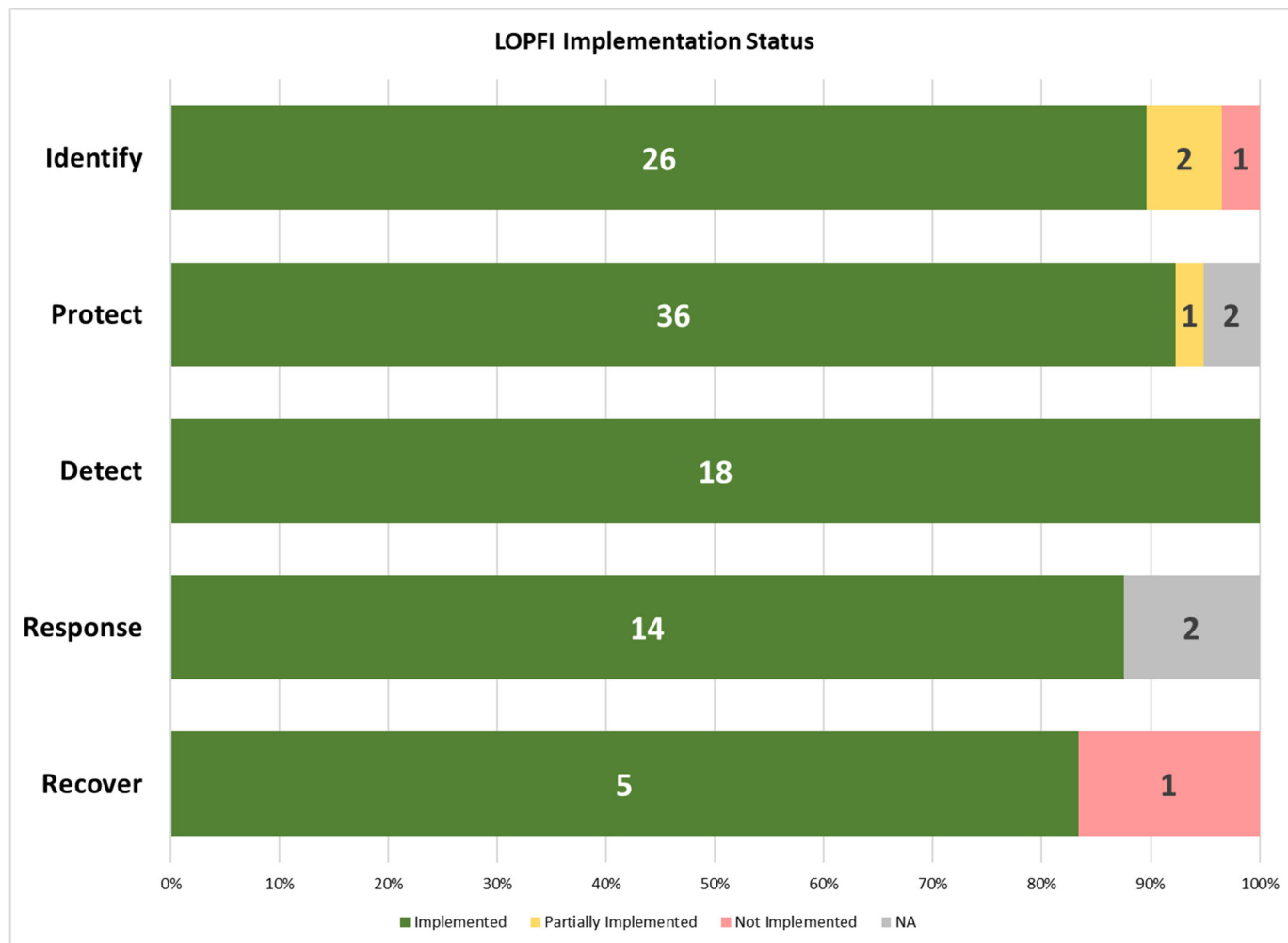
A finding is defined as a matter having a direct negative impact on internal control or indicates noncompliance with internal policy, procedure, applicable law, regulation, or guideline.

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	

The logo for FORVIS, consisting of the word "FORVIS" in a bold, white, sans-serif font with a registered trademark symbol (®) to the upper right. The background of the entire page is a pattern of diagonal red stripes of varying shades, creating a dynamic, geometric effect.

FORVIS®

069

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	1
Definitions of Ratings	4
Penetration Attack Summary	5
Findings & Recommendations	6
Scope of Services	10
Appendix A: Internet Profile	16
Appendix B: Details of External Vulnerability Scan Results	17
Appendix C: Details of Internal Vulnerability Scan Results	18

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
<i>Redacted due to sensitivity</i>
Internal IP Addresses or Range of Addresses
<i>Redacted due to sensitivity</i>

External Penetration Testing

External Penetration Test Findings

The Company had no findings.

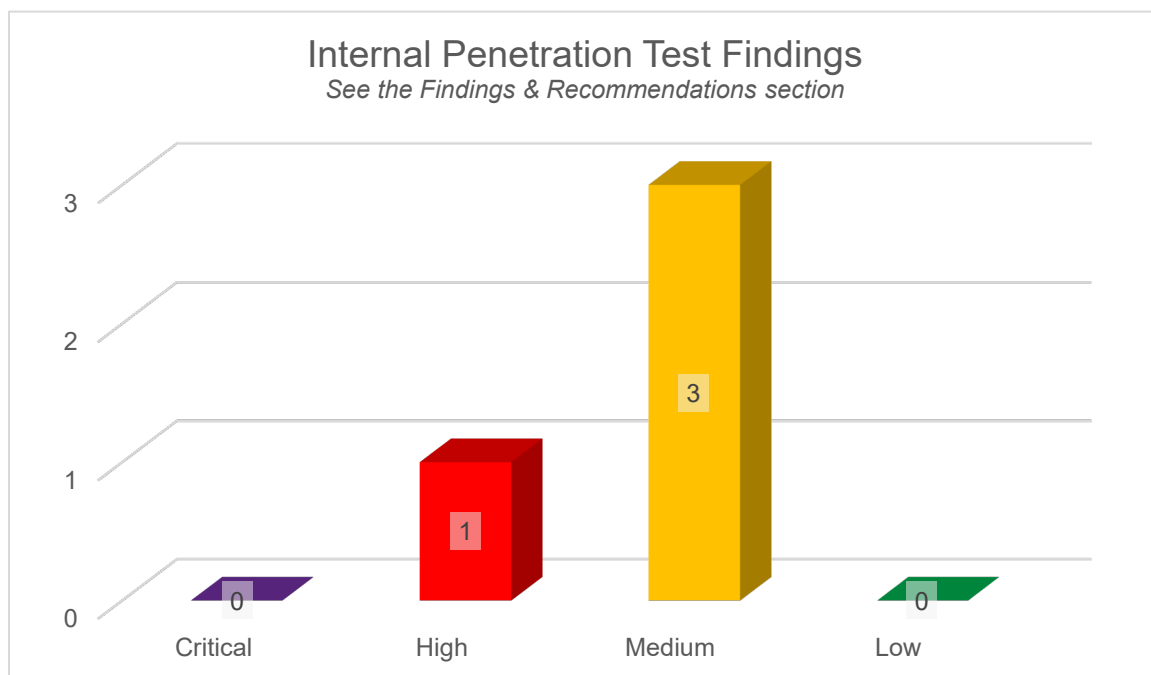
External Vulnerability Scan Results

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

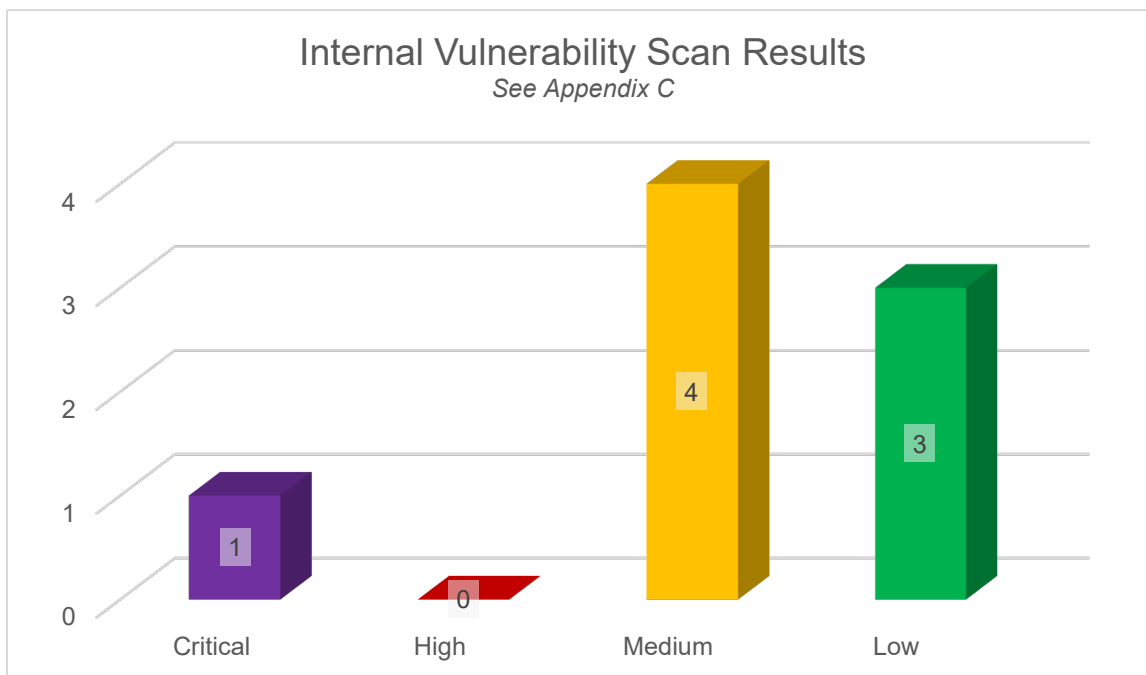
Internal Penetration Test Findings

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 unauthenticated 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 Linux Kernel 3.13 Linux Kernel 4.2 Linux Kernel 4.8	1
HP Integrated Lights-Out	1

Redacted due to sensitive information.