March 13, 2020

Re: FHLBI Member Due Diligence

Ladies and Gentlemen,

This letter is in response to your due diligence request for information relating to the Federal Home Loan Bank of Indianapolis' ("Bank") information security, disaster recovery efforts, and financial status.

Information Security and Privacy Policies

The Bank has implemented an Information Security Program designed to protect our information assets, information systems and sensitive data from internal, external, vendor and third-party security risks. The Information Security Program includes identification processes for monitoring existing, emerging and imminent threats as well as cyber-attacks affecting our industry in order to develop appropriate risk management strategies. Protective security controls are in place for critical infrastructure services including access controls, awareness and training, boundary defense, data security, local administrator restrictions, maintenance, physical security, secure configurations, and secure network engineering. Detective controls including continuous security monitoring and intrusion detection are used to identify cyber risk events. Responsive and recovery controls are part of our Business Continuity Plan and Information Security Incident Response Plan to ensure we can implement appropriate activities when an information security event is detected. The Bank complies with state laws in determining its disclosure responsibilities relating to information security events. Annually, we engage external third parties to assess our Information Security Program and perform Vulnerability and Penetration testing to validate the effectiveness of the program. For security reasons, we will not disclose the Bank's assessment and vulnerability test results.

The Bank acknowledges that in the course of its relationship with its members, the Bank may come into possession of certain "nonpublic personal information" as that term is defined under the Gramm-Leach-Bliley Act and various federal regulations promulgated

thereunder, as well as information which may be deemed to be private and/or confidential as defined under various state data security and/or privacy statutes, including, but not limited to, relevant Michigan and Indiana privacy laws and the California Consumer Privacy Act. Accordingly, the Bank agrees that, except where

disclosure is required for legal, accounting or regulatory purposes, the Bank will not disclose or use such information, except in the ordinary course of business of performing services on behalf of the member. The Bank agrees to maintain the confidentiality of such information with the same level of security that the Bank uses to maintain the confidentiality of its own business records and shall take all reasonable steps necessary to prevent unauthorized access to or use of such information. Further information about our privacy policies may be found on our public website, currently at https://www.fhlbi.com/privacy-notice.

Business Continuity Management Policy and Plan

The Bank maintains a Board-approved Business Continuity Management Policy, along with departmental Business Continuity Plans ("BCP") which are reviewed and updated on a regularly scheduled basis. The BCP provides procedures to ensure personnel safety and welfare, to safeguard the Bank's assets, including physical property and information, and to permit the continued operations of the Bank in the event of a short-term disruption or long-term catastrophic event. The BCP contains operating procedures for all departmental-level critical functions and identifies resources and staff required for each critical function. The BCP also details procedures for recovering and resuming critical functions based on criticality and achieving certain target service levels within specified recovery time objectives. For a declared disaster, the Crisis Management Plan manages the coordination, outlines the appropriate flow of information both internally and externally, including communicating with specified external parties, such as members, regulators, and vendors.

The Bank has established a dedicated business resumption facility in another city outside of Indianapolis, Indiana for the Bank to relocate its main office operations should the main facility become uninhabitable. The Bank has established a disaster recovery data center in a city outside of Indiana where we have the ability to restore operations within four hours after a disaster is declared. The Bank annually performs Disaster Recovery Tests at the recovery facilities as well as table-top exercises at the primary location to walk-through structured disaster scenarios and other unplanned incidents.

In addition, the Bank maintains a master backup support agreement with another Federal Home Loan Bank that provides a mechanism for the Bank to conduct certain critical business operations through the assisting bank. Under this agreement, if the Bank were unable to fully implement its disaster recovery plan for a period of time following a disruption, the other FHLBank would serve as the Bank's agent by facilitating advances to members, servicing principal and interest obligations on consolidated obligations for which the Bank is liable, and payment of any other obligations of the Bank.

Financial Information

The Bank is part of the Federal Home Loan Bank System, chartered by Congress in 1932 via the Federal Home Loan Bank Act (12 U.S.C. § 1421). We do not (and are not required to) have a state or federal business license/registration. Copies of the Bank's

March 13, 2020

SEC filings, including quarterly financial statements, and annual reports can be found on the Bank's website at www.fhlbi.com or on the SEC website at www.sec.gov. A copy of the Bank's insurance certificate and the Bank's W-9 are attached.

If you have any further questions, please do not hesitate to contact me at rpapalko@fhlbi.com or 317.465.0502.

Sincerely,

Rebecca L. Papalko
Assistant Vice President-Compliance Risk Manager

cc: Kristina Cunningham, First Vice President-Senior Director of Compliance and Operational Risk Analysis
Ron Duplessis, First Vice President-Chief Information Security Officer