FDIC FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Social Media

August 8, 2022

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

An FDIC Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) the FDIC collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. The FDIC publishes its PIAs, as well as its System of Records Notices (SORNs), on the FDIC's public-facing website,[1] which describes the FDIC's activities that impact privacy, the authority for collecting PII, and the procedures to access and have PII amended or corrected if necessary.

SYSTEM OVERVIEW

The Federal Deposit Insurance Corporation (FDIC) uses social media to encourage greater participation, collaboration, and transparency with the public, enhance operations, and be more effective. The social media platforms the FDIC uses are provided by commercial third parties, and are governed by their own terms of service and privacy policies. Most social media platforms require users to provide personally identifiable information (PII) at the time of registration. The process varies by platform, and often users can provide more than is required for registration. For example, users can provide such information as his or her interests, birthday, religious and political views, family members and relationship status, education, occupation and employment, photographs, contact information, and hometown. The FDIC does not solicit, receive, or have access to user registration information, and whenever possible, the FDIC elects not to have non-public information made available to it. Moreover, the FDIC does not solicit, endorse, or control the comments or opinions provided by users of the platforms.

In accordance with the Office of Management and Budget's (OMB) M-17-06, *Policies for Federal Agency Public Websites and Digital Services*[2] and OMB M-10-06, *Open Government Directive,*[3] all FDIC uses of social media serve an intended purpose that is directly related to an agency function that supports its mission. Prior to its use of social media, the FDIC reviews the third-party privacy policies, identifies links to, and embedded applications from, third parties, and brands its usage in accordance with OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites.*[4] The FDIC's use of social media complies with applicable

[1] www.fdic.gov/privacy
[2] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-06.pdf
[3] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2010/m10-06.pdf
[4] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2010/m10-23.pdf

laws and statements, is described in the FDIC Privacy Policy, and follows FDIC Circular 1370.6 "Communicating on Social Media Sites" and standard operating procedures. The FDIC also provides instruction on distinguishing personal use from official FDIC use in FDIC Directive 1300.4 "Acceptable Use Policy for Information Technology Resources." The FDIC's use of social media covered by this PIA does not constitute web-based interactive technology, as outlined in OMB memorandum M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*,[5] or trigger Paperwork Reduction Act requirements.

The FDIC posts on social media platforms primarily as a way of driving public engagement back to FDIC.gov,[6] the official source of FDIC information. Social media posts include but are not limited to photos, news articles, short videos, podcast episodes and links to press releases, speeches, and information from the FDIC. Some FDIC posts may direct users back to information hosted online by other federal agencies whose activities support the FDIC mission. The FDIC uses a social media management solution (SMMS) to schedule, post, and manage content across multiple social media accounts. The SMMS also provides some analytical data to measure the overall number of followers, number of retweets, and similar statistical information to evaluate the effectiveness of the FDIC's social media usage.

The FDIC Office of Communications (OCOM) is the primary account holder for the following FDIC social media accounts and is responsible for ensuring that information posted and collected from these social media websites are appropriate:

- Twitter, https://www.twitter.com/fdicgov/;
- Facebook, https://www.facebook.com/fdicgov;
- Instagram, https://www.instagram.com/fdicgov/;
- Flickr, https://www.flickr.com/;
- LinkedIn, https://www.linkedin.com/company/fdic/;
- YouTube, https://www.youtube.com/user/FDICchannel; and
- Anchor.fm—FDIC podcast channel, https://anchor.fm/fdic.

Other Divisions and Offices within the FDIC may have limited access to information that individuals make publicly available via social media. For example, if individual users visit an FDIC page on a third-party site to view content but do not otherwise interact with the page (e.g., post comments, submit messages, "friend" or "follow" the FDIC), no PII about the users will be made available to the FDIC. If users choose to "follow," "friend," or take similar actions with respect to the FDIC's official page on these third-party sites, the fact that the user made that selection will often be publicly available, depending on the policies of the third-party site. If users choose to post information that is publicly available, the FDIC may review that information for potential impacts to Corporation activities in specific circumstances. For example, the FDIC may monitor FDIC-related keywords to track legislative developments; conduct official bank exam activities for banks that use social media tools themselves; search for cybersecurity threat indicators that may require the FDIC to implement enhanced security

[5] https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2010/m10-22.pdf
[6] https://www.fdic.gov/

controls; respond to messages or posts directed to the FDIC or its employees on an FDIC social media account managed are deemed as threatening or violent, or where the content may reveal some other potential law enforcement violation; or monitor for reputational risks to the FDIC and corroborate facts. Where possible, the FDIC does not allow users to post comments on its official pages on third-party sites and reserves the right to purge any postings or comments that contain PII or that do not meet FDIC posting standards. Further, the FDIC does not record or search for which users "follow," "friend," or take similar actions with respect to its official pages.

PRIVACY RISK SUMMARY

In conducting this PIA, the FDIC identified potential privacy risks, which are summarized below and detailed in the subsequent sections of this PIA. As indicated, recommendations to mitigate those risks were addressed with stakeholders during the assessment. The privacy risks for this system are categorized within the following privacy functional areas:

- Transparency;
- Minimization;
- Data Quality and Integrity; and
- Use Limitation.

Transparency

Privacy Risk: There is a risk that individuals may not understand how information related to their use of social media may be used by the FDIC, given social media is governed by third parties.

Mitigation: The FDIC complies with OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications,* as it relates to the use of social media platforms. The FDIC Privacy Policy and this PIA makes clear that social media platforms are third-party service providers and that the social media platforms are not governed by the FDIC or the FDIC Privacy Policy. Individuals who voluntarily choose to use social media are responsible for reviewing the social media platforms Privacy Policy and Terms of Service for how their information may be used and subsequently choosing to use those services. When embedding social media content into FDIC webpages, the FDIC attributes the social media site and, where it does not impede user experience, provides notice that users are being directed from the FDIC website.

Privacy Risk: There is a risk that individuals may be misled by social media accounts that claim to be official FDIC communications and receive inaccurate information or spam or unsolicited communications.

Mitigation: FDIC identifies ownership of its social media accounts in the account profile and uses the FDIC logo where possible to designate the account as the official account of the

FDIC. Consistent branding across social media platforms is designed to help the public identify FDIC accounts as a trustworthy source of information. The FDIC also obtains verification status from each social media platform when such verification is available.

Minimization

Privacy Risk: The FDIC official social media posts do not yet have an established records retention schedule.

Mitigation: The FDIC is currently engaged in a large effort to establish formal retention schedules for all systems. Also, the FDIC also reduces the privacy risk by only collecting PII that is relevant and necessary for legally authorized purposes and periodically evaluating and verifying PII that is collected.

Privacy Risk: : There is a risk that more PII may be collected, used, disclosed, or retained via social media than necessary for FDIC operations.

Mitigation: The risk of excessive collection, use, disclosure, or retention of PII is mitigated in four ways. One, the FDIC does not solicit, receive, or access user registration information from social media platforms. Two, in very limited circumstances, the FDIC may use the minimum amount of PII that it receives from social media posts if that information is necessary for the proper performance of agency functions and has practical utility. For example, if a user provides an e-mail address, which may or may not identify the individual, and requests the Corporation to respond, the FDIC may use the e-mail address to do so, but only for that purpose. Three, if user interactions with the FDIC via social media platforms includes PII, such as account information related to a failed bank, the FDIC may choose to hide or delete that user interaction to reduce any privacy risks that may result from such disclosure. Four, the FDIC provides individuals with alternatives mechanisms to engage with the FDIC so they are not required to use social media platforms. Finally, the FDIC is not responsible for what a user may post on social media platforms nor what is made available to the public by the user via the social media platform's privacy settings.

Data Quality and Integrity

Privacy Risk: There is a risk that a malicious third party may compromise the FDIC's corporate social media accounts or establish false social media accounts and claim to represent the FDIC.

Mitigation: To negate the impact of potential unauthorized social media accounts, FDIC maintains a single official account for each platform where it maintains a social media presence. Access to these accounts requires multi-factor authentication, where available, and is restricted to a small, approved group within FDIC OCOM. Consistent branding across social media platforms is designed to help the public identify FDIC accounts as a trustworthy source

of information. In addition, the FDIC also obtains verification status from each social media platform when such verification is available.

Use Limitation

Privacy Risk: Social media use necessarily involves interactions with other users and carries the risk that users may misrepresent themselves or their communications, resulting in spam, spyware, viruses, or other unsolicited communications.

Mitigation: Social media platforms are third-party service providers and are not governed by the FDIC or the FDIC Privacy Policy. Individuals who voluntarily choose to use social media are responsible for reviewing the social media platforms Privacy Policy and Terms of Service for how their information may be used and subsequently choosing to use those services. Individuals should be wary of other users with whom they interact on social media. They should avoid submitting PII, clicking on links, or downloading content from other users they do not know. To the extent possible, the FDIC provides individuals with alternatives mechanisms to engage with the FDIC so individuals are not required to use social media platforms.

Section 1.0: Information System

1.1 What information about individuals, including PII (e.g., name, Social Security number, date of birth, address) and non-PII, will be collected, used or maintained in the information system or project?

The system contains information made available to the FDIC by individuals and social media platforms.

PII Element	Yes
Full Name	☒
Date of Birth	☐
Place of Birth	☐
Social Security number (SSN)	☐
Employment Status, History or Information	☐
Mother's Maiden Name	☐
Certificates (e.g., birth, death, naturalization, marriage)	☐

Medical Information	☐
Address	☐
Phone Number(s)	☐
Email Address	☐
Employee Identification Number (EIN)	☐
Financial Information (e.g., checking account #/PINs/passwords, credit report)	☐
Driver's License/State Identification Number	☐
Vehicle Identifiers (e.g., license plates)	☐
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records)	☐
Education Records	☐
Criminal Information	☐
Military Status and/or Records	☐
Investigation Report or Database	☐
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐
Photographic Identifiers (e.g., image, video)	☐
User Information (e.g., User ID, password)	☐
Specify other: Screen name, content of public or private messages, comments, or other postings on the FDIC's social media accounts	☒

1.2 What are the sources of the PII in the information system or project?

Data Source	Description of Information Provided by Source
Members of the public	Members of the public may be the source of PII available to the FDIC, in the form of their screen name and the content of their public or private messages, comments, or other postings on the FDIC's social media accounts.
Social Media Management Solution	Measure the overall number of followers, number of retweets, and similar statistical information to evaluate the effectiveness of the FDIC's social media usage.

1.3 Has an Authority to Operate (ATO) been granted for the information system or project?

FDIC's use of social media does not require an ATO.

Section 2.0: Transparency

Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

2.1 How does the agency revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change?

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC ensures notices are revised to reflect changes in practice or policy that affect PII or changes in activities that may impact Privacy as soon as practicable.

2.2 In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this information system or project operate? Provide number and name.

The information collected, used, maintained, and disseminated by the system or project is not subject to the requirements of the Privacy Act of 1974 because the system or project does not retrieve information by personal identifier. Therefore, a SORN is not required.

2.3 If the information system or project is being modified, will the Privacy Act SORN require amendment or revision? Explain.

The information collected, used, maintained, and disseminated by the system or project is not subject to the requirements of the Privacy Act of 1974 because the system or project does not retrieve information by personal identifier. Therefore, a SORN is not required.

2.4 If a Privacy Act Statement[7] is required, how is the Privacy Act Statement provided to individuals before collecting their PII? Explain.

The information collected, used, maintained, and disseminated by the system or project is not subject to the requirements of the Privacy Act of 1974 because the

[7] *See* 5 U.S.C. §552a(e)(3). The Privacy Act Statement provides formal notice to individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.

system or project does not retrieve information by personal identifier. Therefore, a Privacy Act Statement is not required.

2.5 How does the information system or project ensure that its privacy practices are publicly available through organizational websites or otherwise? How does the information system or project ensure that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)? Explain.

The FDIC Privacy Program page provides access to agency SORNs, PIAs, Privacy Policy, and contact information for the SAOP, the Privacy Program Chief, and the Privacy Program (Privacy@fdic.gov). For more information on how the FDIC protects privacy, please visit www.fdic.gov/privacy.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: There is a risk that individuals may not understand how information related to their use of social media may be used by the FDIC, given social media is governed by third parties.

Mitigation: The FDIC complies with OMB Memorandum M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, as it relates to the use of social media platforms. The FDIC Privacy Policy and this PIA makes clear that social media platforms are third-party service providers and that the social media platforms are not governed by the FDIC or the FDIC Privacy Policy. Individuals who voluntarily choose to use social media are responsible for reviewing the social media platforms Privacy Policy and Terms of Service for how their information may be used and subsequently choosing to use those services. When embedding social media content into FDIC webpages, the FDIC attributes the social media site and, where it does not impede user experience, provides notice that users are being directed from the FDIC website.

Privacy Risk: There is a risk that individuals may be misled by social media accounts that claim to be official FDIC communications and receive inaccurate information or spam or unsolicited communications.

Mitigation: The FDIC identifies ownership of its social media accounts in the account profile and uses the FDIC logo where possible to designate the account as the official account of the FDIC. Consistent branding across social media platforms is designed to help the public identify FDIC accounts as a trustworthy source of information. The FDIC also obtains verification status from each social media platform when such verification is available.

Section 3.0: Access and Amendment

Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.

3.1 What are the procedures that allow individuals to access their information?

The system or project receives third-party data from social media platforms. The FDIC does not have the ability to implement procedures for individual access. Individuals should contact their social media platform directly for access to their personal information. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from the social media platforms.

3.2 What procedures are in place to allow the individuals to correct inaccurate or erroneous information?

The system or project receives third-party data from social media platforms. The FDIC does not have the ability to implement procedures to correct inaccurate or erroneous information. Individuals should contact their social media platforms directly to correct any erroneous or inaccurate information. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from the social media platforms.

3.3 How does the information system or project notify individuals about the procedures for correcting their information?

The system or project receives third-party data from social media platforms. The FDIC is unable to notify individuals about the procedures for correcting their information. Individuals should contact their social media platform directly to correct any inaccurate information. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from the social media platforms.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: There are no identifiable privacy risks related to access and amendment for the FDIC's use of social media.

Mitigation: No mitigation actions are recommended.

Section 4.0: Accountability

Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.

4.1 Describe how the FDIC's governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy.

The FDIC maintains a risk-based, enterprise-wide privacy program that is based upon sound privacy practices. The FDIC Privacy Program is compliant with all applicable laws and is designed to build and sustain public trust, protect and minimize the impacts on the privacy of individuals, while also achieving the FDIC's mission.

The FDIC Privacy Program is led by the FDIC's Chief Information Officer (CIO) and Chief Privacy Officer (CPO), who also has been designated as the FDIC's Senior Agency Official for Privacy (SAOP). The CIO/CPO reports directly to the FDIC Chairman, and is responsible for ensuring compliance with applicable federal privacy requirements, developing and evaluating privacy policy, and managing privacy risks. The program ensures compliance with federal privacy law, policy, and guidance. This includes the Privacy Act of 1974, as amended; Section 208 of the E-Government Act of 2002; Section 522 of the 2005 Consolidated Appropriations Act; Federal Information Security Modernization Act of 2014; OMB privacy policies; and standards issued by the National Institute of Standards and Technology (NIST).

The FDIC's Privacy Program supports the SAOP in the management and execution of the FDIC's Privacy Program.

4.2 Describe the FDIC privacy risk management process that assesses privacy risks to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

Risk analyses are an integral component of the FDIC's Privacy Program. Privacy risks for new and updated collections of PII are analyzed and documented in Privacy Threshold Analyses (PTAs) and Privacy Impact Assessments (PIAs). The Privacy Program looks across all FDIC systems and programs to identify potential areas of

privacy risk. The PTA is used to assess systems or sub-systems, determine privacy compliance requirements, categorize systems, and determine which privacy controls should be assessed for each system.

4.3 Does this PIA capture privacy risks posed by this information system or project in accordance with applicable law, OMB policy, or any existing organizational policies and procedures?

Yes, this PIA captures privacy risks posed by the FDIC's use of social media through the privacy risk analysis sections throughout the document. PIAs are posted on the FDIC's public-facing website, www.fdic.gov/privacy.

4.4 What roles, responsibilities and access will contractors have with the design and maintenance of the information system or project?

Contractors do not have any official access or responsibility to use social media on behalf of the FDIC. However, all contractors that have access to FDIC systems take mandatory annual information security and privacy training. Privacy and security-related responsibilities are specified in contracts and associated Risk Level Designation documents. Privacy-related roles, responsibilities, and access requirements are documented in relevant PIAs.

4.5 Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been completed and signed for contractors who work on the information system or project? Are privacy requirements included in the contract?

No, a Non-Disclosure Agreement or Confidentiality Agreement has not been completed by contractors because contractors do not have official access to use social media on behalf of the FDIC. However, contractors will not have access to individuals' PII. Additionally, privacy and security requirements for contractors and service providers are mandated and are documented in relevant contracts.

4.6 How is assurance obtained that the information in the information system or project is used in accordance with the practices described in this PIA and, if applicable, the associated Privacy Act System of Records Notice?

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC monitors and audits privacy controls. Internal privacy policies are reviewed and updated as required. The FDIC Privacy Program implements a Privacy Continuous Monitoring (PCM) program in accordance with OMB Circular A-130.

4.7 Describe any privacy-related training (general or specific) that is provided to users of this information system or project.

The FDIC provides guidelines to all employees regarding their use of social media on behalf of the FDIC in FDIC Directive 1370.6 "Communication on Social Media Sites" and provides instruction on distinguishing personal use from official FDIC use in FDIC Directive 1300.4 "Acceptable Use Policy for Information Technology Resources." Moreover, employees that use social media on behalf of the FDIC follow standard operating procedures.

Annual Security and Privacy Training is mandatory for all FDIC employees and contractors and they are required to electronically certify their acceptance of responsibilities for privacy requirements upon completion. Specified role-based privacy training sessions are planned and provided by the FDIC Privacy Program as well.

4.8 Describe how the FDIC develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

The FDIC Privacy Program develops reports both for internal and external oversight bodies through several methods, including the Annual Senior Agency Official for Privacy Report (SAOP) as required by FISMA, and regular reporting to the SAOP, the CISO, and the Information Technology Risk Advisory Committee.

4.9 Explain how this information system or project protects privacy by automating privacy controls?

The FDIC restricts access to social media websites and some functionality of social media websites for all FDIC employees and contractors using FDIC-issued equipment in order to mitigate against cybersecurity risks. The FDIC also restricts access to official FDIC social media accounts and applications to only federal employees with a role-based need. FDIC social media account passwords are maintained in accordance with FDIC Directive 1360.10 Corporate Password Standards and all FDIC social media posts must be issued from FDIC equipment.

Privacy has been integrated within the FDIC Systems Development Life Cycle (SDLC), ensuring that stakeholders are aware of, understand, and address Privacy requirements throughout the SDLC, including the automation of privacy controls

when possible. Additionally, the FDIC has implemented technologies to track, respond, remediate, and report on breaches, as well as to track and manage PII inventory.

4.10 Explain how this information system or project maintains an accounting of disclosures held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made?

The system or project is not a system of records under the Privacy Act, and the FDIC is therefore not required to maintain an accounting of disclosures.

4.11 Explain how the information system or project retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer?

The system or project is not a system of records under the Privacy Act, and the FDIC is therefore not required to maintain an accounting of disclosures.

4.12 Explain how the information system or project makes the accounting of disclosures available to the person named in the record upon request?

The system or project is not a system of records under the Privacy Act, and the FDIC is therefore not required to maintain an accounting of disclosures.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There are no identifiable privacy risks related to accountability for the FDIC's use of social media.

Mitigation: No mitigation actions are recommended.

Section 5.0: Authority

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.

5.1 Provide the legal authority that permits the creation, collection, use, processing, storage, maintenance, dissemination, disclosure and/or disposing of PII within

the information system or project. For example, Section 9 of the Federal Deposit Insurance Act (12 U.S.C. 1819).

The FDIC ensures that collections of PII are legally authorized through the conduct and documentation of PIAs and the development and review of SORNs. FDIC Circular 1360.20, "FDIC Privacy Program," mandates that the collection of PII be in accordance with Federal laws and guidance. This particular system or project collects PII pursuant to the following laws and regulations:

- 12 U.S.C. § 1819: establishes the FDIC as an independent federal agency

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable privacy risks related to authority for the FDIC's use of social media.

Mitigation: No mitigation actions are recommended.

Section 6.0: Minimization

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.

6.1 How does the information system or project ensure that it has identified the minimum PII that are relevant and necessary to accomplish the legally authorized purpose of collection?

Social media platforms are responsible for how information provided by a user is made available to the public. It is the responsibility of the users to review the privacy policies, terms of service, and privacy settings of the social media platforms prior to adopting their use. When individuals use social media platforms, they should understand that whatever they post or share is available to the public subject to the privacy settings they select.

The FDIC does not solicit, receive, or have access to user registration information, and whenever possible, the FDIC elects not to have non-public information made available to it. For example, if a member of the public posts a comment or message on one of the FDIC's social media accounts, the FDIC may access the content of that comment or

message from that social media account, including the screen name or other PII of that individual made available through the social media platform's privacy settings, such as sex, location, interests, and other handles the FDIC's followers follow. Where possible, the FDIC does not allow users to post comments on its official pages on third-party sites and reserves the right to purge any postings or comments that contain PII or that do not meet FDIC posting standards. Further, the FDIC does not record or search for which users "follow," "friend," or take similar actions with respect to its official pages.

Additionally, through the conduct, evaluation, and review of privacy artifacts, [8] the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected.

6.2 How does the information system or project ensure limits on the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent?

Social media platforms are responsible for how information provided by a user is made available to the public. It is the responsibility of the users to review the privacy policies, terms of service, and privacy settings of the social media platforms prior to adopting their use. When individuals use social media platforms, they should understand that whatever they post or share is available to the public subject to the privacy settings they select.

The FDIC provides notice to individuals regarding FDIC use of social media platforms and applications to enable individuals to understand what information they are making available to the FDIC via FDIC channels through the FDIC Privacy Policy and this PIA.

Additionally, through the conduct, evaluation, and review of privacy artifacts, the FDIC ensures that the collection of PII is relevant and necessary to accomplish the legally authorized purpose for which it is collected.

6.3 How often does the information system or project evaluate the PII contained in the information system or project to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose?

While social media platforms are not FDIC systems, the FDIC maintains an inventory of

[8] Privacy artifacts include Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), and System of Record Notices (SORN).

systems that contain PII. The Privacy Program reviews information in the systems at the frequency defined in the FDIC Information Security Continuous Monitoring Strategy. New collections are evaluated to determine if they should be added to the inventory.

6.4 What are the retention periods of the data in this information system or project? What are the procedures for disposition of the data at the end of the retention period? Under what guidelines are the retention and disposition procedures determined? Explain.

The FDIC is in the process of developing a records schedule for its official social media posts.

Procedures for disposition of the data at the end of the retention period are established in accordance with FDIC Records Schedules in conjunction with National Archives and Records Administration (NARA) guidance. For example, hard copies of any paper materials scanned into the system will be retained in accordance with FDIC Records Schedules or returned to the originating Division or Office for retention.

Additionally, records are retained in accordance with the FDIC Circular 1210.1 "Records and Information Management Program," which is informed by the Federal Records Act and NARA regulations Management Policy Manual and NARA-approved record retention schedule. Information related to the retention and disposition of data is captured and documented within the PIA process. The retention and disposition of records, including PII, is addressed in Circulars 1210.1 and 1360.9.

6.5 What are the policies and procedures that minimize the use of PII for testing, training, and research? Does the information system or project implement controls to protect PII used for testing, training, and research?

Social media platforms are responsible for how information provided by a user may be used for by the platforms themselves for testing, training, and research. The FDIC does not use information from social media for testing, training, or research on behalf of the FDIC.

Additionally, the FDIC is in the process of developing an enterprise test data strategy to reinforce the need to mask or use synthetic data in the lower environments whenever possible, and ensure all environments are secured appropriately based on the impact level of the information and the information system.

Privacy Risk Analysis: Related to Minimization

Privacy Risk: FDIC official social media posts do not yet have an established records retention schedule.

Mitigation: The FDIC is currently engaged in a large effort to establish formal retention schedules for all systems. Also, FDIC also reduces the privacy risk by only collecting PII that is relevant and necessary for legally authorized purposes and periodically evaluating and verifying PII that is collected.

Privacy Risk: : There is a risk that more PII may be collected, used, disclosed, or retained via social media than necessary for FDIC operations.

Mitigation: The risk of excessive collection, use, disclosure, or retention of PII is mitigated in four ways. One, the FDIC does not solicit, receive, or access user registration information from social media platforms. Two, in very limited circumstances, the FDIC may use the minimum amount of PII that it receives from social media posts if that information is necessary for the proper performance of agency functions and has practical utility. For example, if a user provides an e-mail address, which may or may not identify the individual, and requests the Corporation to respond, the FDIC may use the e-mail address to do so, but only for that purpose. Three, if user interactions with the FDIC via social media platforms includes PII, such as account information related to a failed bank, the FDIC may choose to hide or delete that user interaction to reduce any privacy risks that may result from such disclosure. Four, the FDIC provides individuals with alternative mechanisms to engage with the FDIC so they are not required to use social media platforms. Finally, the FDIC is not responsible for what a user may post on social media platforms nor what is made available to the public by the user via the social media platform's privacy settings.

Section 7.0: Data Quality and Integrity

Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

7.1 Describe any administrative and technical controls that have been established to ensure and maximize the quality, utility, and objectivity of PII, including its accuracy, relevancy, timeliness, and completeness.

Social media platforms are third-party service providers and are not governed by the FDIC or the FDIC Privacy Policy. Social media platforms are responsible for maximizing the quality, utility, and objectivity of PII that has been provided by a user. To the extent possible, the FDIC provides the public with alternative sources for information and avenues to seek assistance beyond the social media platforms, where the FDIC

has more control over the quality, utility, and objectivity of the PII. Most social media posts drive users back to FDIC.gov. The FDIC website is the official source of information for the Corporation and is managed in accordance with OMB's Guidance on Ensuring Information Quality and Accuracy, available at www.fdic.gov/policies. Any requests for FDIC assistance are directed to the FDIC Contact Information webpage and Customer Service at www.fdic.gov/contact. Links to other federal agency content must be consistent with FDIC authorities. Any uses of information made available to the FDIC via social media may be corroborated with other sources of information.

Additionally, the FDIC reviews privacy artifacts for adequate controls to ensure the accuracy, relevance, timeliness, and completeness of PII in each instance of collection or creation.

7.2 Does the information system or project collect PII directly from the individual to the greatest extent practicable?

The system or project receives third-party data from social media platforms. The FDIC does not have the ability to implement procedures to correct inaccurate or erroneous information. Individuals should contact their social media platforms directly to correct any erroneous or inaccurate information. Additionally, the FDIC does not make decisions regarding individuals based on the PII received from the social media platforms.

7.3 Describe any administrative and technical controls that have been established to detect and correct PII that is inaccurate or outdated.

Social media platforms are third-party service providers and are not governed by the FDIC or the FDIC Privacy Policy. Social media platforms are responsible for any administrative and technical controls to detect and correct PII that is inaccurate or outdated.

7.4 Describe the guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

Social media platforms are third-party service providers and are not governed by the FDIC or the FDIC Privacy Policy. The FDIC does not further disseminate the information it gathers from social media platforms.

To maximize the quality, utility, objectivity, and integrity of the information FDIC shares on social media, the FDIC implement security controls to maintain the integrity of its corporate social media accounts, and directs users back to FDIC assets where the FDIC has greater control over the information. Most FDIC social media posts direct

users back to fdic.gov. The FDIC website is the official source of information for the Corporation and is managed in accordance with OMB's Guidance on Ensuring Information Quality and Accuracy, available at www.fdic.gov/policies. Any requests for FDIC assistance are directed to the FDIC Contact Information webpage and Customer Service at www.fdic.gov/contact. Links to other federal agency content must be consistent with FDIC authorities.

The FDIC's guidelines for the disclosure of information subject to Privacy Act protections are found in Part 310 of the FDIC Rules and Regulations.

7.5 Describe any administrative and technical controls that have been established to ensure and maximize the integrity of PII through security controls.

Social media platforms are third-party service providers and are not governed by the FDIC or the FDIC Privacy Policy. The FDIC does not establish controls to maintain the integrity of PII on the social media platforms. The FDIC does, however, implement security controls to maintain the integrity of its corporate accounts on social media.

7.6 Does this information system or project necessitate the establishment of a Data Integrity Board to oversee a Computer Matching Agreements and ensure that such an agreement complies with the computer matching provisions of the Privacy Act?

The FDIC does not maintain any Computer Matching Agreements under the Privacy Act of 1974, as amended, by the Computer Matching and Privacy Protection Act of 1988. Consequently, the FDIC does not need to establish a Data Integrity Board.

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: There is a risk that a malicious third party may compromise the FDIC's corporate social media accounts or establish false social media accounts and claim to represent the FDIC.

Mitigation: To negate the impact of potential unauthorized social media accounts, FDIC maintains a single official account for each platform where it maintains a social media presence. Access to these accounts requires multi-factor authentication, where available, and is restricted to a small, approved group within FDIC OCOM. Consistent branding across social media platforms is designed to help the public identify FDIC accounts as a trustworthy source of information. In addition, the FDIC also obtains verification status from each social media platform when such verification is available.

Section 8.0: Individual Participation

Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

8.1 Explain how the information system or project provides means, when feasible and appropriate, for individuals to authorize the collection, use, maintenance, and sharing of PII prior to its collection.

The system or project receives data from third parties. The FDIC is unable to provide privacy notices prior to the Agency's processing of individuals' PII. Individuals should review the relevant third party's privacy notices. Additionally, this PIA serves as notice of the information collection. Lastly, the FDIC does not make decisions regarding individuals based on the PII received from third-parties.

8.2 Explain how the information system or project provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII.

The system or project receives data from third parties. The FDIC is unable to provide privacy notices prior to the Agency's processing of individuals' PII. Individuals should review the relevant third party's privacy notices. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. Lastly, the FDIC does not make decisions regarding individuals based on the PII received from third-parties.

8.3 Explain how the information system or project obtains consent, when feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.

It is not feasible or appropriate to get direct consent prior to any new use or disclosures of previously collected PII. If applicable, the FDIC Privacy Program will update the relevant SORN(s) as well as the relevant PIA.

8.4 Explain how the information system or project ensures that individuals are aware of and, when feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the FDIC collected the PII.

The system or project receives data from third parties. The FDIC is unable to provide privacy notices prior to the Agency's processing of individuals' PII. Individuals should review the relevant third party's privacy notices. Additionally, this PIA serves as notice and implicit consent with respect to the collection, use, and disclosure of PII. Lastly, the FDIC does not make decisions regarding individuals based on the PII received from third parties.

8.5 Describe the process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices?

The FDIC Privacy Program website, www.fdic.gov/privacy, instructs individuals to direct privacy questions to the FDIC Privacy Program through the Privacy@fdic.gov email address. Complaints and questions are handled on a case-by-case basis.

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: There are no identifiable privacy risks related to individual participation for the FDIC's use of social media.

Mitigation: No mitigation actions are recommended.

Section 9.0: Purpose and Use Limitation

Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

9.1 Describe the purpose(s) for which PII is collected, used, maintained, and shared as specified in the relevant privacy notices.

The FDIC uses social media to encourage greater participation, collaboration, and transparency with the public, and more effective operations. In accordance with OMB M-17-06, *Policies for Federal Agency Public Websites and Digital Services*, and OMB M-10-06, *Open Government Directive*, all FDIC uses serve an intended purpose that is directly related to an agency function that supports its mission.

Social media platforms are provided by commercial third parties, and are governed by their own terms of service and privacy policy. If users choose to "follow," "friend," or take similar actions with respect to the FDIC's official page on these third-party platforms, the fact that the user made that selection will often be publicly available, depending on the policies of the third-party platform. If users choose to post information is publicly available, the FDIC may review that information for potential impacts to Corporation activities in specific circumstances. For example, the FDIC may monitor FDIC-related keywords to track legislative developments; conduct official bank exam activities for banks that use social media tools themselves; search for cybersecurity threat indicators that may require the FDIC to implement enhanced security controls; respond to messages or posts directed to the FDIC or its employees on an FDIC social media account are deemed as threatening or violent, or where the content may reveal some other potential law enforcement violation; or monitor for reputational risks to the FDIC and corroborate facts. Where possible, the FDIC does not allow users to post comments on its official pages on third-party sites and reserves the right to purge any postings or comments that contain PII or that do not meet FDIC posting standards. Further, the FDIC does not record or search for which users "follow," "friend," or take similar actions with respect to its official pages.

9.2 Describe how the information system or project uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices? Who is responsible for assuring proper use of data in the information system or project and, if applicable, for determining what data can be shared with other parties and information systems? Have policies and procedures been established for this responsibility and accountability? Explain.

Social media platforms and applications are provided by commercial third parties, and are governed by their own terms of service and privacy policy.

Through the conduct, evaluation, and review of privacy artifacts, and in conjunction with the implementation of applicable privacy controls, the FDIC ensures that PII is only used for authorized uses internally in accordance with the Privacy Act and FDIC Circular 1360.9 "Protecting Sensitive Information." Additionally, annual Information Security and Privacy Awareness Training is mandatory for all employees and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

9.3 How is access to the data determined and by whom? Explain the criteria, procedures, security requirements, controls, and responsibilities for granting access.

The FDIC restricts access to social media websites and some functionality of social

media websites for all FDIC employees and contractors using FDIC-issued equipment in order to mitigate against cybersecurity risks. The FDIC also restricts access to official FDIC social media accounts and applications to only those with a role-based need. Access is managed through Active Directory group membership. The user profiles associated with social media are based on the user's job requirements and requires management approval, and is facilitated using the FDIC's Access Request and Certification System (ARCS). In the event that an employee misuses FDIC social media accounts, the Deputy to the Chairman for External Affairs and the Director, Office of Communications, consults with Labor and Employee Relations and the Legal Division about the appropriateness of changing the passwords and not sharing the passwords with the employee until disciplinary action is closed. In accordance with FDIC Directive 1360.10 "Corporate Password Standards," passwords to FDIC social media accounts are changed every 90 days or in the event that a concern is raised about the security of the social media channels.

9.4 Do other internal information systems receive data or have access to the data in the information system? If yes, explain.

☒ No
☐ Yes Explain.

9.5 Will the information system or project aggregate or consolidate data in order to make determinations or derive new data about individuals? If so, what controls are in place to protect the newly derived data from unauthorized access or use?

No, FDIC does not aggregate data to make program-level decisions.

9.6 Does the information system or project share PII externally? If so, is the sharing pursuant to a Memorandum of Understanding, Memorandum of Agreement, or similar agreement that specifically describes the PII covered and enumerates the purposes for which the PII may be used? Please explain.

The FDIC does not typically share the PII it obtains through social media third parties. In the rare occasion that messages or posts directed to or at the FDIC or its employees are deemed as threatening or violent, or indicates some other potential law violation, the FDIC Security Enterprise Programs Section (SEPS) may share this information with external law enforcement authorities for investigation. The sharing with law enforcement occurs in accordance with 29 CFR 1960.8(a) Basic Program Elements for Federal Employee Occupational Safety and Health Programs and Related Matters, and Executive Order 12977 Interagency Security Committee.

Additionally, through the conduct, evaluation, and review of PIAs and SORNs, the FDIC

ensures that PII shared with third parties is used only for the authorized purposes identified or for a purpose compatible with those purposes, in accordance with the Privacy Act of 1974, FDIC Circular 1360.20 "Privacy Program," and FDIC Circular 1360.17 "Information Technology Security Guidance for FDIC Procurements/Third-Party Products." The FDIC also ensures that agreements regarding the sharing of PII with third parties specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used, in accordance with FDIC Circular 1360.17 and FDIC Circular 1360.9.

9.7 Describe how the information system or project monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII.

The FDIC does not typically share the information it obtains through social media third parties. The sharing with law enforcement occurs under the purview of SEPS and roles and responsibilities established under FDIC Circular 1610.4 "Management Response Teams."

9.8 Explain how the information system or project evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

The FDIC does not typically share the information it obtains through social media third parties. The FDIC reviews privacy artifacts to evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Privacy Risk Analysis: Related to Use Limitation

Privacy Risk: Social media use necessarily involves interactions with other users and carries the risk that users may misrepresent themselves or their communications, resulting in spam, spyware, viruses, or other unsolicited communications.

Mitigation: Social media platforms are third-party service providers and are not governed by the FDIC or the FDIC Privacy Policy. Individuals who voluntarily choose to use social media are responsible for reviewing the social media platforms Privacy Policy and Terms of Service for how their information may be used and subsequently choosing to use those services. Individuals should be wary of other users with whom they interact on social media. They should avoid submitting PII, clicking on links, or downloading content from other users they do not know. To the extent possible, the FDIC provides individuals with alternatives mechanisms to engage with the FDIC so individuals are not required to use social media platforms.

Section 10.0: Security

Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

10.1 Describe the process that establishes, maintains, and updates an inventory that contains a listing of all information systems or projects identified as collecting, using, maintaining, or sharing PII.

While social media platforms are not FDIC systems, the FDIC Privacy Program maintains an inventory of all programs and information systems identified as collecting, using, maintaining, or sharing PII.

10.2 Describe the process that provides each update of the PII inventory to the CIO or information security official to support the establishment of information security requirements for all new or modified information systems or projects containing PII?

While social media platforms are not FDIC systems, the FDIC Privacy Program reviews new or modified uses of social media. The FDIC Privacy Program updates the CISO on PII holdings via the PTA adjudication process. As part of the PTA adjudication process, the FDIC Privacy Program reviews the system or project's FIPS 199 determination. The FDIC Privacy Program will recommend the appropriate determination to the CISO should the potential loss of confidentiality be expected to cause a serious adverse effect on individuals.

10.3 Has a Privacy Incident Response Plan been developed and implemented?

While social media platforms are not FDIC systems, the FDIC has developed and implemented a Breach Response Plan in accordance with OMB M-17-12.

10.4 How does the agency provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan?

While social media platforms are not FDIC systems, responses to privacy breaches are addressed in an organized and effective manner in accordance with the FDIC's Breach Response Plan.

Privacy Risk Analysis: Related to Security

Privacy Risk: There are no identifiable privacy risks related to security for the FDIC's use of social media.

Mitigation: No mitigation actions are recommended.