FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Division of Information Technology
Delivery Management Branch
Enterprise Document Management Service Center
Microsoft SharePoint 2013

Date Approved by Chief Privacy Officer (CPO)/Designee
1/28/2019

Section 1.0: Introduction

In accordance with federal regulations and mandates[1], the FDIC conducts Privacy Impact Assessments (PIAs) on systems, business processes, projects and rulemakings that involve an *electronic* collection, creation, maintenance or distribution of personally identifiable information (PII).[2] The objective of a Privacy Impact Assessment is to identify privacy risks and integrate privacy protections throughout the development life cycle of an information system or electronic collection of PII. A completed PIA also serves as a vehicle for building transparency and public trust in government operations by providing public notice to individuals regarding the collection, use and protection of their personal data.

To fulfill the commitment of the FDIC to protect personal data, the following requirements must be met:

- Use of the information must be controlled.
- Information may be used only for necessary and lawful purposes.
- Information collected for a particular purpose must not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.
- Information collected must be sufficiently accurate, relevant, timely, and complete to ensure the individual's privacy rights.

Given the vast amounts of stored information and the expanded capabilities of information systems to process the information, it is foreseeable that there will be increased requests, from both inside and outside the FDIC, to share sensitive personal information.

Upon completion of this questionnaire and prior to acquiring signatures, please email the form to the FDIC Privacy Program Staff at: privacy@fdic.gov, who will review your document, contact you with any questions, and notify you when the PIA is ready to be routed for signatures.

Section 2.0: System/Project Description

In this section of the Privacy Impact Assessment (PIA), describe the system/project and the method used to collect, process, and store information. Additionally, include information about the business functions the system/project supports.

SharePoint 2013 is a Microsoft product that provides an integrated enterprise environment where users can collaborate, share and manage electronic information within groups and subgroups. The Microsoft SharePoint 2013 architecture deployed at the FDIC provides a selection of functionalities to enhance business collaboration and communications, such as browser-based process management modules, a document/records management platform, enterprise search modules, personalization, blogs and wikis. SharePoint 2013 is primarily used by FDIC to host Division/Office websites, shared workspaces, information stores and documents. Provisioned users can manipulate proprietary controls called "web parts" or interact

[1] Section 208 of the E-Government Act of 2002 requires federal government agencies to conduct a Privacy Impact Assessment (PIA) for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII). Office of Management and Budget (OMB) Memorandum M-03-22 provides specific guidance on how Section 208 should be implemented within government agencies. The Privacy Act of 1974 imposes various requirements on federal agencies whenever they collect, create, maintain, and distribute records that can be retrieved by the name of an individual or other personal identifier, regardless of whether the records are in hardcopy or electronic format. Additionally, Section 522 of the 2005 Consolidated Appropriations Act requires certain Federal agencies to ensure that the use of technology sustains, and does not erode, privacy protections, and extends the PIA requirement to the rulemakings process.

[2] For additional guidance about FDIC rulemaking PIAs, visit the Privacy Program website or contact the FDIC Privacy Program Staff at privacy@fdic.gov.

with pieces of content, such as lists and document libraries. "Web Parts" allowed for data presentation and organization.

FDIC SharePoint 2013 sites, blogs, and wikis are the Corporation's secure workspace for collaboration on active documents and other content for business purposes. "Other Content" is comprised of data such as scanned information received from various external sources. Data stored on FDIC SharePoint 2013 sites has the potential to include agency-sensitive information (SI) and personally identifiable information (PII) about internal (FDIC) and external (non-FDIC) parties to accomplish authorized FDIC business needs. Users are prohibited from storing personal, non-business documents within any FDIC SharePoint 2013 site, and must identify documents containing SI or PII, in accord with the Corporation's SharePoint Governance Plan and associated policies and procedures.

SharePoint 2013 provides the ability for site owners to manage content and security for sites under their area of responsibility. Site Owners/Administrators, in coordination with Division/Office SharePoint Site Collection Administrators, are responsible for monitoring and maintaining the content of their respective sites, including ensuring the appropriateness of the information being collected, as well as the retention and access to that information, in line with FDIC data protection and retention policies.

SharePoint 2013 runs on the FDIC's secured internal servers. The SharePoint 2013 servers are a component of the FDIC WINSERV general support system (GSS), which has undergone its own Privacy Threshold Analysis (PTA).

Section 3.0: Data in the System/Project

The following questions address the type of data being collected and from whom (nature and source), why the data is being collected (purpose), the intended use of the data, and what opportunities individuals have to decline to provide information or to consent to particular uses of their information.

3.1 What personally identifiable information (PII) (e.g., name, social security number, date of birth, address, etc.) will be collected, used or maintained in the system? Explain.

In general, all electronically stored information found on SharePoint 2013 sites (e.g., Division/Office Sites, Bank Closings Site Collections, FDIC AboutMe) must be related to official FDIC business and, as such, may include agency SI and PII about internal (FDIC) and external (non-FDIC) parties as necessary to accomplish authorized FDIC business needs. The specific types of PII maintained within SharePoint 2013 sites will vary depending on the particular business purpose(s) for which each site was designed (e.g., examination and enforcement, resolution and receivership, legal, vendor/contract management, HR/personnel, etc.), but could include any and all forms of PII, including full name, social security number, date of birth, address, etc.

For example, FDIC AboutMe (MySite) is a work area in which FDIC employees and contractors can post a biography and other business-related information such as skills and interests about themselves for others within the organization to view. Users will be allowed to edit profile information that will be available to corporate users, based on access rights, to search and view.

Users are required to utilize the standard Document Library template, which requires users to specify a sensitivity level and privacy level for all documents stored in the SharePoint 2013 environment. While it is permissible to store business-related SI/PII in SharePoint 2013, users are strongly encouraged to store such records in the official System of Records (SOR) or other appropriate document repositories prescribed in the official business processes. Moreover, the FDIC SharePoint Governance Plan (version 4.9 approved/dated March 24, 2017) and associated FDIC policies prohibit users from storing personal (non-business) data in SharePoint 2013 sites.

3.2 What is the purpose and intended use of the information you described above in Question 3.1?

SharePoint 2013 is a document management solution that supports the storage, management, and collaboration of business information. Through SharePoint 2013 sites, it provides secure environments that site owners or site collection administrators can configure and manage business content and access. In the normal course of fulfilling its mission, FDIC regularly interacts with PII. The purpose of storing PII on SharePoint is to support the mission of FDIC.

3.3 If Social Security Numbers (SSNs) are collected, used, or maintained in the system, please answer the following:

a) Explain the business purpose/need requiring the collection of SSNs:
Data is either collected and/or saved into the SharePoint system for the purpose of supporting the mission of FDIC. Specifically, in the case of the FDIC Bank Closings Site Collections (FDICbcs) within the Division of Resolutions and Receiverships (DRR), banking information containing personal data are collected and saved onto SharePoint during the bank closing events.

b) Aside from 12 U.S.C. § 1819, which provides the general authority for the Corporation to collect SSNs, are there any other Federal statutes/authorities that justify the collection and/or use of SSNs?

☐ Yes List any additional legal authorities:
☒ No

c) Is the SSN is masked or otherwise truncated within the system?

☐ Yes. Explain:
☒ No. Is it possible to mask or otherwise truncate the SSN within the system?
☐ Yes. Explain how it may be masked or truncated and why this has not been implemented:
☒ No. Explain why it may not be masked or truncated:
SharePoint site is a collaboration site where data such as active documents are shared and being collaborated on by all authorized users. Within the site, there is no tool or feature where any information can be masked or truncated. The data truncation or masking must be done outside of the SharePoint system.

d) Is access to SSNs (and other sensitive PII) restricted in any way to specific groups of users of the system?

☒ Yes. Explain: Access is only authorized for users having the need to access the data.
☐ No. Is it possible to restrict access to specific groups of users within the system?
☐ Yes. Explain how access may be restricted and why this has not been implemented:
☐ No. Explain why access cannot be restricted:

3.4 Who/what are the sources of the information in the system? How are they derived?

Data maintained in the SharePoint 2013 sites is obtained and uploaded by authorized FDIC staff and contractors in connection with their various Corporate and receivership job responsibilities. For example, many documents and items maintained in FDICbcs SharePoint 2013 repositories are obtained from failed financial institutions as part of the DRR bank closing activities performed by FDIC staff and contractors.

Additionally, with regard to FDICMySite, the following types of business and organizational tree information are pulled from Microsoft Active Directory (AD) to populate individual users' My Site public profile pages: FDIC user name, work email address, work telephone number, title/division, supervisor, work groups All content posted by users to My Site must be business-appropriate and professional in nature. Users are not able to upload documents to their public profile sites; they may only enter/post business information within predefined text box fields on their respective page. This is defined in the approved SharePoint Governance Plan (v. 4.9 dated March 24, 2017).

3.5 What Federal, state, and/or local agencies are providing data for use in the system? What is the purpose for providing data and how is it used? Explain.

The FDIC SharePoint 2013 environment is accessible only to internal FDIC network users. As such, no Federal agencies are providing data directly to SharePoint. However, FDIC staff or contractors may collect or receive business data from Federal agencies as part of their official business functions and, as applicable, store this data in designated SharePoint 2013 repositories. In addition, FDIC network users may include authorized representatives from Federal agencies who require access to FDIC SharePoint 2013 sites in order to review or post data for any official business purpose. All network users must be authenticated in order to access or post documents to SharePoint.

3.6 What other third-party sources will be providing data to the system? Explain the data that will be provided, the purpose for it, and how will it be used.

No third parties are providing data directly to SharePoint 2013. However, as part of their official business functions, FDIC staff or contractors may obtain or receive business data from third-party sources, such as commercial databases (e.g., Lexis-Nexis), nonpublic investigatory databases, credit bureaus, and store this data in designated SharePoint repositories as necessary.

3.7 Do individuals have the opportunity to decline to provide personal information and/or consent only to a particular use of their data (e.g., allowing basic use of their personal information, but not sharing with other government agencies)?

☐ Yes Explain the issues and circumstances of being able to opt out (either for specific data elements or specific uses of the data):

☒ No Explain: For documents posted on SharePoint 2013 sites, the individuals whose PII is contained in these documents may or may not have been offered an opportunity to opt out of providing this personal information. For example, information posted to FDICbcs sites may be obtained from failed financial institutions, not directly from individuals, and the information is necessary to support the Corporation's resolution and receivership activities. In general, the specific circumstances under which individuals are offered an opt out is dependent on the source of the data and consistent with the provisions outlined in the FDIC System of Records Notices (SORNs) and Privacy Act Notices governing the original data collection.

Section 4.0: Data Access and Sharing

The following questions address who has access to the data, with whom the data will be shared, and the procedures and criteria for determining what data can be shared with other parties and systems.

4.1 Who will have access to the data in the system (internal and external parties)? Explain their purpose for having access to this information.

Table 4.1.1 below provides a taxonomy of key SharePoint 2013 administrator/user roles, their associated permissions, and their purpose for having access to SharePoint 2013 sites. In general, only authorized users who require access to SharePoint 2013 information in order to perform their official job responsibilities will be granted access to their respective SharePoint sites. Which users will have access to the information in any particular SharePoint site will depend on the particular business purpose for which the SharePoint 2013 site is set-up and is subject to the access approval process.

Table 4.1.1 General SharePoint Access Roles (derived from the Governance Plan v. 4.9 dated March 24, 2017) Role	**Responsibilities and Tasks**
Site Collection Administrator (SCA) – Full Control (Owner)	Site Collection Administrators (SCAs) are responsible for the overall administration of Division/Office SharePoint 2013 site collections including steps to: • Manage access rights, permission levels, and site requests for the collection of site data; • Add content, remove content, manage content, manage folders, and control the site hierarchy of the Division/Office site; • Configure and enforce FDIC site standards and policies; • Provision Division/Office Team sites and Divisional/Office Project Sites; • Periodically review Site Owners list to ensure that only Site Owners have "Full Control" access rights to their respective sites; • Collaborate with Subsite Owners and follow the guidelines as stated in the established site management process for site removal prior to deletion; • Provide support to users and Sub-Site Owners for any questions and issues relating to the Division/Office sites; and • Recommend approval of SharePoint customizations or custom applications (e.g., Web Parts) to the Enterprise Document Management

Table 4.1.1 General SharePoint Access Roles (derived from the Governance Plan v. 4.9 dated March 24, 2017) Role	**Responsibilities and Tasks**
	(EDM) Working Group and EDMSC Section Chief.
Site Owner (SO) – Full Control (Owner)	Site Owners are responsible for the overall administration of their Division/Office SharePoint 2013 sites including the responsibility to: • Manage access rights, permission levels, and site requests for the sites. Conduct an annual review with the use of SailPoint or other tool to manage site security and work in conjunction with Information Security Managers (ISMs) in response to security audit inquiry from the Government Accountability Office (GAO); • Add content, remove content, manage content, manage folders, and control the Division/Office subsites; • Collaborate with the SCAs to support and enforce FDIC site standards and policies; • Provision Division/Office Team subsites and Divisional/Office Project subsites; • Periodically review subsite Site Owners list to ensure that only subsite owners have "Full Control" access rights to their respective sites; • Provide support to SCAs in managing site access in accordance with the FDIC security policies; • Obtain "approval" from SCA and follow the guidelines as stated in the Division/Office's SharePoint policy for deleting a site; • Provide support to users/subsite Owners for any questions and issues relating to the Division/Office subsites; • Collaborate with SCAs and subsites SOs regarding the PII, sensitivity, and Controlled Unclassified Information (CUI) content types to ensure corporate Security and Privacy policy compliance; • Identify SharePoint business needs and requests to the respective SCOs and/or the EDM Working Group; • Recommend approval of SharePoint customizations or custom applications (e.g., Web Parts) to the SCA.
SharePoint Coordinator (SC) – Full Control (Owner)	The Division/Office SharePoint Coordinator is responsible for overall management of Division/Office SharePoint 2013 site collection including the following: • Ensure the Division/Office is in compliance with policy, procedures, standards, and guidelines governing SharePoint as documented in the FDIC SharePoint Governance Plan; • Brief their respective Division/Office on the appropriate operational procedures and policies for SharePoint sites; • Document the Division/Office escalation points of contact; • Document Division/Office policies for SharePoint usage and operation guidelines; • Establish the Division/Office SharePoint hierarchy; • Establish and document annual access and content reviews and periodic site review processes;and • Conduct and document annual access rights review of their Division/Office SharePoint sites in collaboration with the ISM.

Role	Responsibilities and Tasks	SharePoint Permissions
Contributor (Member)	Responsible for adding, editing, and collaborating with other contributors as follows: • Update, maintain, archive, and delete files/folders as needed; • Respond to questions regarding content as posted on SharePoint sites, if necessary; and • Adhere to internal Division/Office policies and procedures and FDIC policies, procedures, standards, and guidelines governing information resource management.	• Member (contribute) • Read permissions • Add items • Edit items • Delete Items • Delete versions • Browse directories • Edit personal user information
Reader (Visitor)	• Responsible for adhering to internal Division/Office procedures for acceptable use and organizational compliance with FDIC policies, procedures, standards, and guidelines governing information resource management	• Read-only access to content

The SharePoint Technical Team is charged with supporting the policies and procedures as noted in this plan. Participants of the following roles are DIT employees and contractors:

Role/Area Responsibility	Responsibilities and Tasks
Enterprise Document Management Service Center (EDMSC)	All technical roles as defined below report to the EDMSC Section Chief who has ultimate responsibility for the overall management, operation, and administration of the SharePoint 2013 environments.
Farm Administrator ***Note:*** *This role is limited to only a small number of EDMSC personnel.*	Farm Administrators are responsible for all servers in the SharePoint 2013 server farm and can perform all administrative tasks in the SharePoint Central Administration Web site for the server or server farm; responsible for global SharePoint configuration, shared services, policies, procedures, and SharePoint vision, including: • Configure SharePoint; • Audit indexing logs; • Search and index tuning; • Monitor usage analysis; • Assist in policy creation and enforcement; • Determine content crawling sites (data sources and crawl schedules); • Enforce blocked file types; • Perform routine releases and upgrades to the application; and • Provide usage and permission-level reports.
Operations Section	The Operations Section is responsible for the SharePoint 2013 infrastructure

Role/Area Responsibility	Responsibilities and Tasks
	(hardware, operating system, etc.) including: • Provision security and permissions at the servers and application layers to the EDMSC technical team members as authorized and directed by the EDMSC Section Chief and Assistant Director, Operations Section; • Perform nightly backups and restores; • Communicate and coordinate with the EDMSC Section on any major changes to the SharePoint environment that will impact production up-time (e.g., major upgrades) prior to implementation; • Assist with "how-to" accomplish tasks when not able to be answered through the normal support process or outside the purview of the EDMSC Section; • Provide day-to-day operation support; • Monitor the performance of VMHosts and all VMs; • Leverage automatic monitoring with Microsoft Operations Manager (MOM) and event notifications; • Perform maintenance of the servers (e.g., service packs and security updates; • Troubleshoot hardware, software (OS), and network connectivity issues; • Escalate issues as necessary; and • Work with the Infrastructure Services Branch team members to develop infrastructure and operation best practices.
Engineering Section	The Engineering Section is responsible for SharePoint 2013 initiatives and coordinating with the EDMSC Section to: • Provide day-to-day engineering and escalation support; • Review existing infrastructure setup; • Assist with setting up SharePoint to use Active Directory for authentication; • Assist in synchronization of SharePoint with Active Directory; • Document any changes to the SharePoint environment, including new hardware, new updates, and configuration changes; • Work in conjunction with EDMSC Section to gather business requirements and to optimize the performance and throughput; • Work with EDMSC Section to maintain SharePoint architecture; • Provide requested and periodic SharePoint reporting at the VMHosts; • Provide architectural guidance; • Lead consulting team throughout life cycle events (e.g., initial release and upgrades); • Work with the Infrastructure Services Branch team members to develop infrastructure and operation best practices; • Troubleshoot hardware, software (OS), and network connectivity issues; and • Escalate issues to proper vendor if necessary.
Enterprise Information Management (EIM)	The EIM DBAs are responsible for:

Role/Area Responsibility	Responsibilities and Tasks
Administrator/Database Administrator (DBA)	• Performing Structured Query Language (SQL) backups and restores; • Managing SQL databases and available storage space; • Monitoring SQL usage analysis and tuning SQL for peak performance; and • Reporting issues and making recommendations to the EDMSC.
Business-led Developers	Business-led Developers work under the technical direction and guidance from the EDMSC Section to: • Provide development-related support for the SharePoint environment; • Build new Web Parts; • Write SharePoint.Net/C# code; • Adhere to FDIC development standards; • Coordinate with EDMSC for any SharePoint development work and for system design review; • Manage development environment risks and escalate incidents to the EDMSC Section as necessary; • Participate in development and testing as needed; • Build the framework and features of the SharePoint sites; • Build the SharePoint look and feel; • Modify SharePoint templates as needed; and • Participate in development and testing as needed.

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

Division/Offices are responsible for managing user access and permissions within their Division/Office SharePoint 2013 site(s). All authorized users who have access to SharePoint must have the approval of the Division/Office Site Owner/Administrator before access is granted. All guidelines established in the Corporation's Access Control Policies and Procedures documents, as well as the SharePoint Governance Plan, are also followed.

Access to data within the FDIC SharePoint 2013 environment is based on business need and a user's "need-to-know." In addition, access is determined according to the principle of "least privilege," whereby user accounts are provided the minimal, most restrictive set of permissions required to perform their work.

To obtain access to a Division/Office SharePoint 2013 site, individuals must contact the Division/Office Site Owner listed on the site for which they are requesting access. Alternatively, if the site has an automated "Access Request" feature enabled, individuals electronically submit the access request when presented with that option. Once access to the site has been reviewed and approved by the Site Owner, the Site Owner or Administrator will grant access that is specific to the business needs and role of the user. Some Division/Office sites, such as FDICbcs sites, implement additional, granular levels of access control and security restrictions. For example, certain libraries and library sub-folders within FDICbcs sites utilize an additional layer of security restrictions to control access to PII and other sensitive materials.

With regard to FDICMySite, individual users have access to their respective public profile. Users do not have the ability to upload documents to their public profile sites or edit personal profile information. The public profile site properties and Web Part inclusion and positioning are managed by the DIT Farm Administrator.

4.3 Do other systems (internal or external) receive data or have access to the data in the system? If yes, explain.

☒ No
☐ Yes Explain.

There are no direct interconnections with other systems at this time, aside from business-related directory data provided by Microsoft Active Directory (AD) to FDIC AboutMe.

4.4 If other agencies or entities use data in the system, explain the purpose for sharing the data and what other policies, procedures, controls, and/or sharing agreements are in place for protecting the shared data.

In general, external entities do not have direct electronic access to SharePoint; authorized FDIC contractors with network IDs may be granted access on a "need to know" basis and as necessary to support FDIC employees in carrying out their official business duties and to support the proper functioning of the SharePoint environment.

4.5 Who is responsible for assuring proper use of data in the system and, if applicable, for determining what data can be shared with other parties and systems? Have policies and procedures been established for this responsibility and accountability? Explain.

The Division/Office Site Collection Administrators and Site Owners share overall responsibility for protecting data posted to SharePoint 2013. Authorized FDIC network users are responsible for protecting data in accordance with the Corporation's established policies and procedures for protecting PII and SI, including but not limited to FDIC Circular 1380.6, Managing SharePoint Collaboration Sites, FDIC Circular 1360.9, Protecting Sensitive Information, and FDIC Circular 1300.4, Acceptable Use Policy for FDIC Information Technology. All FDIC network users are informed of their responsibilities for protecting privacy in the FDIC's mandatory Information Security & Privacy Awareness training, which is required to be completed on an annual basis and includes the Corporate Rules of Behavior.

4.6 What involvement will a contractor have with the design and maintenance of the system? Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been developed for contractors who work on the system?

Any FDIC contractors that help design, install, configure, maintain, and/or test the FDIC SharePoint 2013 environment and/or its components will be required to sign Contractor Confidentiality Agreements and abide by FDIC Circular 1360.9, Protecting Sensitive Information, as well as complete FDIC's mandatory Information Security & Privacy Awareness training on an annual basis, which includes the Corporate Rules of Behavior.

Section 5.0: Data Integrity and Security

The following questions address how data security and integrity will be ensured for the system/project.

5.1 How is data in the system verified for accuracy, timeliness, and completeness?

It is the responsibility of individual users to ensure the completeness and accuracy of the data they post to SharePoint 2013 sites. The Document Library section of all Division/Office SharePoint 2013 sites must use the FDIC Document Library template which requires users to specify a sensitivity level and privacy level for all documents stored in SharePoint 2013. Further, each Division/Office is responsible for conducting annual access and content reviews, and periodic site reviews, of their site collections, in accord with the FDIC SharePoint Governance Plan.

5.2 **What administrative and technical controls are in place to protect the data from unauthorized access and misuse? Explain.**

Site Owners and Site Collection Administrators are required to take training and review and sign a Roles and Responsibilities document. Site Owners must review and sign the document titled Roles and Responsibilities for Site Owners and Site Collection Administrators are required to review and sign the document titled Roles and Responsibilities for Site Collection Administrators. In addition, on an annual basis, business owners and site owners are required to conduct a review of permission levels on all site collections, which is facilitated with FDIC's Access Request and Certification System.

Section 6.0: Data Maintenance and Retention

The following questions address the maintenance and retention of records, the creation of reports on individuals, and whether a system of records is being created under the Privacy Act, 5 U.S.C. 522a.

6.1 How is data retrieved in the system or as part of the project? Can it be retrieved by a personal identifier, such as name, social security number, etc.? If yes, explain, and list the identifiers that will be used to retrieve information on the individual.

The search functionality within SharePoint 2013 allows authorized users to search for documents posted to the respective SharePoint 2013 sites to which they have been granted access. Users may search by any term, including personal identifiers such as name, Social Security Number, address, etc., but they may only view documents to which they have been granted permission to access.

6.2 What kind of reports can be produced *on individuals*? What is the purpose of these reports, and who will have access to them? How long will the reports be maintained, and how will they be disposed of?

As part of their site maintenance duties, Division/Office Site Owners/Administrators have the ability to run and view reports about who has access to their respective sites and what type of access has been granted to these users. Only the DIT Farm Administrator and his/her designee have access to the SharePoint 2013 audit reporting tool in order to monitor all SharePoint 2013 sites and run reports regarding user access and activities (e.g., who viewed, deleted or downloaded what and at what time). These reports are shared with authorized FDIC OIG and/or Division/Office staff on a "need to know" basis in support of official business duties. Data contained within the reports may contain any information uploaded to SharePoint 2013, including PII. All data within SharePoint must be managed in accord with current policies set forth by the Record and Information Management Unit in FDIC Circular 1210.1, FDIC Records and Information Management Policy Manual.

6.3 What are the retention periods of data in this system? 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.

Project sites will remain only for 2 - 3 years after the project is closed, depending on the retention policy for that type of project. All data within SharePoint is required to be managed in accord with current policies set forth by the Record and Information Management Unit in FDIC Circular 1210.1, FDIC Records and Information Management Policy Manual.

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

The FDIC SharePoint 2013 environment does not operate as a Privacy Act Systems of Records, nor does its use require alteration to any existing system of records. The FDIC SharePoint 2013 environment may be used to process and store Privacy Act Records from existing FDIC Privacy Act Systems of Records by authorized contributors (FDIC staff and contractors) in connection with their various Corporate and Receivership job responsibilities. Contributors are responsible for ensuring there is coverage under the appropriate System of Records Notice for the data collected/maintained and ensuring that appropriate procedures are followed. For a listing of current FDIC Privacy Act Systems of Records, please visit: http://www.fdic.gov/regulations/laws/rules/2000-4000.html.

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

Not applicable.

Section 7.0: Business Processes and Technology

The following questions address the magnitude of harm if the system/project data is inadvertently disclosed, as well as the choices the Corporation made regarding business processes and technology.

7.1 Will the system aggregate or consolidate data in order to make privacy 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?

Not applicable.

7.2 Is the system/project using new technologies, such as monitoring software, SmartCards, Caller-ID, biometric collection devices, personal identification verification (PIV) cards, radio frequency identification devices (RFID), virtual data rooms (VDRs), social media, etc., to collect, maintain, or track information about individuals? If so, explain how the use of this technology may affect privacy.

SharePoint 2013 is not using new technologies, nor does SharePoint 2013 use existing technologies in a new way. However, SharePoint 2013 does have certain functionalities that, if enabled, may present potential privacy risks, such as blogs and wikis, and mobile access to SharePoint sites. To mitigate potential risks, governance is tightly controlled in areas where there is substantial public exposure in terms of readership or potential litigation or privacy issues, such as blogs and wikis. For instance, FDIC prohibits the use of the wikis/blogs functionality without prior authorization from Division and Office Directors, as well as restricts users to publishing information within the FDIC intranet SharePoint 2013 sites to which they have been given access. Moreover, general privacy risks, such as mobile access to SharePoint

2013 sites, are mitigated by hosting SharePoint 2013 on the FDIC's secured internal servers, limiting access to SharePoint 2013 sites to within the FDIC network, and disabling SharePoint 2013 features that would allow for the publishing or sharing of information outside of the FDIC environment.

7.3 Will the system/project provide the capability to monitor individuals or users? If yes, describe the data being collected. Additionally, describe the business need for the monitoring and explain how the information is protected.

Yes, SharePoint 2013 has the ability to run reports of usage built into the application architecture. The SharePoint 2013 auditing tool can run reports of usage, accessible only to the the DIT Farm Administrator and his designee. These reports detail users' access/activities and usage times on SharePoint 2013 sites.

7.4 Explain the magnitude of harm to the Corporation if privacy-related data in the system/project is disclosed, intentionally or unintentionally. Would the reputation of the Corporation be affected?

The unintentional compromise of SharePoint data could adversely affect FDIC's reputation. Therefore, appropriate safeguards are maintained in order to protect the privacy and security of information contained in FDIC SharePoint 2013 sites.

7.5 Did the completion of this PIA result in changes to business processes or technology? If yes, explain.

No, the completion of this PIA does not result in technology changes.