



**Privacy Impact Assessment (PIA)
for
FDIC Conferencing and
Content Sharing Technologies (FCCST)**



September 23, 2021

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 public-facing website,¹ which describes 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 FDIC's Division of Information Technology (DIT) operates FDIC's Conferencing and Content Sharing Technologies (FCCST) that facilitate electronic business conferencing and content sharing with the general public, throughout the agency, and between FDIC and FDIC's authorized business partners, which may include Financial Institutions, other Federal agencies, state regulators, and Technology Service Providers. Depending on the nature and purpose of a particular FCCST-supported event, there is a potential that any manner of sensitive information, including personally identifiable information (PII), could be shared if it is pertinent and necessary to carry out an FDIC authorized business activity.

FCCST is comprised of the following key components, which serve the purposes outlined below:

Collaborative Audio-Video Service – This service allows authorized users to hold virtual meetings in real time with audio-only and audio-video participants. Meetings are managed using an Internet browser or desktop application on which a suite of collaboration tools allow participants to share documents, applications, and presentations; to use remote desktop capabilities; and to chat. Participants can connect to meetings using their computers or telephones or video teleconferencing equipment. Information may be shared internally within FDIC, as well as with FDIC authorized business partners or select members of the public.

External Webcasting Service – This service enables the live webcast of FDIC sponsored events externally to the general public, and subsequent storage of the webcast for viewing by the public at a later date. For instance, FDIC Board Meetings and FDIC Quarterly Banking Profile meetings are broadcast via live video stream and recorded and subsequently made available on a public website for viewing at a later date by the general public. Webcast presenters and moderators may create polls, conduct and answer questions during their presentations and manage the access to the content of their presentations.

FDICTV – This is FDIC's on premise Enterprise Video Management system. FDICTV provides FDIC employees and contractors with FDIC-issued video-on-demand (VOD) content and live internally conducted FDIC webcasts covering a variety of topics, such as FDIC-sponsored conferences, town halls, and various awareness events, which may be recorded and made available for viewing by FDIC employees and contractors over the FDIC network. FDICTV is also used to maintain and provide authorized pre-recorded videos obtained from non-FDIC sources for viewing by internal FDIC users. Additionally, FDICTV provides Internet Protocol Television (IPTV) that delivers select digital television services, such as CSPAN, CNN, or MSNBC, to FDIC employees and contractors over the FDIC network.

Conference Room and Classroom Technology - FDIC's conference rooms and classrooms have been equipped with tools to seamlessly enable conferencing and content sharing between individuals participating in meetings, both virtually and physically. Such tools include a screen mirroring solution that works natively with mobile devices in FDIC classrooms to facilitate the wireless casting of mobile device screens to classroom displays, as well as hardware appliances located in FDIC meeting facilities that allow the meeting attendees in those facilities to seamlessly join collaborative audio-video meetings with audio and video content sharing functionality.

¹ www.fdic.gov/privacy

Virtual Outreach Center - FDIC's Virtual Outreach Center is a full-service video and audio production facility for recording, editing and distributing video and audio content internally and externally for web, broadcast, and social media purposes, and could include content such as live and recorded broadcast interviews, virtual town halls, webinars, and podcasts.

Coverage Requirements

The authority to collect information using the technologies described in this PIA lies within each program or project's legal authorities. All programs or projects covered under this FDIC-wide PIA must satisfy the following requirements:

1. FDIC projects and programs must work with the Privacy Section to ensure that the program or project meets all privacy requirements.
2. FDIC projects and programs must set limits on the utilization and sharing of PII.
3. FDIC projects and programs must be appropriately approved and operate within authorized FDIC system boundaries.

PRIVACY RISK SUMMARY

In conducting this PIA of FCCST, we 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 and Individual Participation
- Access and Amendment
- Data Minimization
- Data Quality and Integrity
- Purpose and Use Limitation

Transparency and Individual Participation Risk:

Privacy Risk: There is a risk that individuals, other than those that register to participate in FDIC-sponsored virtual events, are not aware that their data could be maintained and processed by FCCST, and that they are not provided with an opportunity to consent to or opt-out of the maintenance and processing of their information by FCCST.

Mitigation: In such instances, notice, in the form of a Privacy Act Statement or SORN, is not possible, however, in instances where FCCST processes PII obtained from other FDIC systems that operate as Privacy Act systems of records, notice is provided through the publication of FDIC's SORNs for those systems, which are available at: <https://www.fdic.gov/policies/privacy/index.html>. In instances where FCCST maintains or processes PII received from FDIC business partners, those entities are responsible for providing any applicable, required notices to the individuals from whom they collect the information. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information. Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII.

Access and Amendment Risk:

Privacy Risk: There is a risk that individuals, other than those that register to participate in FDIC-sponsored virtual events, do not have the opportunity to access their information or amend inaccurate information contained within FCCST.

Mitigation: In such instances, notice, in the form of a Privacy Act Statement or SORN, is not possible, however, in instances where FCCST processes PII obtained from other FDIC systems that operate as Privacy Act systems of records, information regarding how individuals may access and amend their information in those systems is provided through the publication of FDIC's SORNs for those systems, which are available at: <https://www.fdic.gov/policies/privacy/index.html>. In cases where FCCST maintains or processes PII

received from FDIC business partners, those entities are responsible for providing any applicable, required notices to the individuals from whom they collect the information. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information. Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII.

Data Minimization Risk:

Privacy Risk: There is a risk that the personally identifiable information maintained by FCCST may be unnecessary or excessive, or may be kept longer than is necessary to meet the business need for which it was collected.

Mitigation: This risk is mitigated by FCCST users being appropriately trained and FDIC policy regarding the collection, use, and retention of FDIC information. FDIC users are required to complete Annual Security and Privacy Training, which addresses the creation, maintenance and retention of FDIC records. Additionally, FDIC Directive 1360.9, Protecting Sensitive Information, requires that sensitive information only be collected and retained when it is necessary to satisfy an FDIC business requirement. Further, FDIC users are responsible for complying with FDIC Circular 1210.01, FDIC Records and Information Management Program, which is informed by the Federal Records Act and NARA regulations.

Data Quality and Integrity Risk:

Privacy Risk: There is a risk that the information maintained and processed by FCCST may not be accurate.

Mitigation: FDIC relies upon the individuals that register to attend FDIC-sponsored virtual events to provide contact information that is accurate. Otherwise, the accuracy of FCCST information is primarily dependent on end users who have responsibility for the content they maintain and process using FCCST. The collaborative nature of some FCCST components provide a platform where those involved in the collaboration may address inaccuracies identified. Information maintained and processed by FCCST that is used by the FDIC as part of its supervisory, examination, compliance, receivership, legal, administrative, and other legally authorized functions will be reviewed for accuracy and timeliness as required by the particular function, laws, and authorities (see Question 5.1), if any, applicable at the time the agency compiles the information.

Purpose and Use Limitation Risk:

Privacy Risk: There is a potential risk associated with purpose and use limitation for FCCST in that information, including PII, transmitted using FCCST could potentially be used or shared for a purpose not compatible with the original purpose for which the information was collected.

Mitigation: This risk is mitigated by FCCST users being appropriately trained. This risk is further mitigated by FDIC Directive 1360.9, Protecting Sensitive Information, which addresses the protection of sensitive information, including PII. Additionally, FDIC uses a combination of technical and operational controls to reduce the risk associated with the FCCST environment, such as encryption, passwords, audit logs, firewalls, malware identification, and a data loss prevention program.

Section 1.0: Information System

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

Generally, the information maintained and processed by FCCST may include any manner of information, including PII, that FCCST users deem pertinent and necessary to carry out FDIC authorized business activities, which include:

- Insuring deposits
- Examining and supervising financial institutions for safety and soundness and consumer protection

- Making large and complex financial institutions resolvable
- Managing receiverships
- Administering and managing FDIC's workforce

Additionally, PII, such as name and contact information, may be collected from meeting participants to document meeting attendance or to respond to a participant's request for additional information related to meeting content.

PII Element	Yes	No
Full Name	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Date of Birth (DOB)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Place of Birth	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Social Security Number (SSN)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Employment Status, History or Information	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Mother's Maiden Name	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Certificates (e.g., birth, death, naturalization, marriage, etc.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Home Address	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Phone Number(s)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Email Address	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Employee Identification Number (EIN)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Driver's License/State Identification Number	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Vehicle Identifiers (e.g., license plates)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Education Records	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Criminal Information	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Military Status and/or Records	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Investigation Report or Database	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Biometric Identifiers (e.g., fingerprint, voiceprint)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Photographic Identifiers (e.g., image, x-ray, video)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Other : Network ID	<input checked="" type="checkbox"/>	<input type="checkbox"/>

1.2 Who/what are the sources of the PII in the information system or project?

Data Source	Description of Information Provided by Source
Collaborative Audio-Video Service	The use of FDIC's collaborative audio-video service facilitates the sharing of information, including PII, that is necessary for fulfilling a legitimate FDIC business function (e.g., examination and enforcement data, resolution and receivership data, assessment data, legal documents, contract data, administrative data, etc.) as deemed appropriate by the users of the collaborative audio-video service. The service could also be used to capture images (both photo and video) and voice recordings of participants. The source of information shared via this service could be an FDIC employee/contractor, FDIC business partner, or a member of the public.
External Webcasting Service	External webcasts are intended to share information with the general public, but could share PII that is relevant and necessary for fulfilling a legitimate FDIC business function (e.g., examination and enforcement data, resolution and receivership data, assessment data, legal documents, contract data, administrative data, etc.) as deemed appropriate by the webcast participants. Webcasts also capture images (both photo and video) and voice recordings of the webcast participants. The source of information shared via these events could be an FDIC employee/contractor, FDIC business partner, or a member of the public.

Data Source	Description of Information Provided by Source
FDICTV	FDICTV videos and broadcasts are available to only FDIC employees and contractors over the FDIC network. FDICTV content could potentially include PII that is relevant and necessary for fulfilling a legitimate FDIC business function (e.g., examination and enforcement data, resolution and receivership data, assessment data, legal documents, contract data, administrative data, audit information, etc.). FDICTV also captures images (both photo and video) and voice recordings of video participants. The source of information shared via FDICTV could be an FDIC employee/contractor, FDIC business partner, or a member of the public.
Conference Room and Classroom Technology	Meetings conducted within FDIC conference rooms and classrooms using FDIC Conference Room and Classroom Technology (CRCT) could potentially transmit video renderings of any type of PII that is necessary for fulfilling a legitimate FDIC business function (e.g., examination and enforcement data, resolution and receivership data, assessment data, legal documents, contract data, audit information, etc.) as deemed appropriate by CRCT users. The source of information shared via CRCT could be an FDIC employee/contractor, FDIC business partner, or a member of the public.
Virtual Outreach Center	Virtual Outreach Center (VOC) productions could potentially share PII that is relevant and necessary for fulfilling a legitimate FDIC business function (e.g., examination and enforcement data, resolution and receivership data, assessment data, legal documents, contract data, audit information, administrative data, etc.) as deemed appropriate by the VOC production participants. VOC productions also capture images (both photo and video) and voice recordings of the production participants. The source of information shared via VOC content could be an FDIC employee/contractor, FDIC business partner, or a member of the public.

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

Yes, FCCST supports systems that have been granted ATOs and that are periodically reviewed as part of the FDIC ongoing authorization process.

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.

With respect to the contact information that may be collected from meeting participants to document meeting attendance or to respond to a participant’s request for additional information related to meeting content, FDIC Privacy Act SORN 30-64-0005, Consumer Complaint and Inquiry Records, provides SORN coverage.

FCCST may also be used to process, store, maintain, disseminate, or disclose information about individuals that is collected from other FDIC systems that operate as Privacy Act systems of records. A full inventory of FDIC's SORNs is available at: <https://www.fdic.gov/policies/privacy/index.html>.

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

No, the SORN does not require amendment or revision. Generally, the FDIC conducts reviews of its SORNs every three years or as needed.

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

With respect to the contact information that may be collected from meeting participants to document meeting attendance or to respond to a participant's request for additional information related to meeting content, a Privacy Act Statement is provided to them when they register to attend an FCCST meeting.

In cases where FCCST may be used to facilitate the transport, exchange, or sharing of information about individuals that is related to other FDIC systems that operate as Privacy Act systems of records, FDIC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.01, FDIC Forms Management Program.

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 contains policies and information related to SORNs, PIAs, FDIC's Privacy Policy, and contact information for the SAOP, the Privacy Program Manager, and the Privacy Program. See <https://www.fdic.gov/policies/privacy/index.html>.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: There is a risk that individuals, other than those that register to participate in FDIC-sponsored virtual events, are not aware that their data is maintained and processed by FCCST.

Mitigation: In such instances, notice, in the form of a Privacy Act Statement or SORN, is not possible, however, in instances where FCCST processes PII obtained from other FDIC systems that operate as Privacy Act systems of records, notice is provided through the publication of FDIC's SORNs for those systems, which are available at: <https://www.fdic.gov/policies/privacy/index.html>. In instances where FCCST maintains or processes PII received from FDIC business partners, those entities are responsible for providing any applicable, required notices to the individuals from whom they collect the information. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information. Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII.

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?

Individuals that register to attend FDIC-sponsored virtual events may contact the meeting organizer to access and make changes to their information.

In cases where FCCST may be used to facilitate the transport, exchange, or sharing of information about individuals that is related to other FDIC systems that operate as FDIC Privacy Act systems of records, the FDIC provides these individuals the ability to have access to their PII maintained in the respective source systems of records as specified by the Privacy Act and FDIC Circular 1031.1. The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1360.1. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public facing website. The FDIC adheres to Privacy Act requirements and Office of Management and Budget (OMB) policies and guidance for the proper processing of Privacy Act requests.

FCCST may also be used to receive, transmit, or share data provided by FDIC business partners that conduct business with the FDIC, which may include information about FI customers or FI employees collected in conjunction with FDIC's authorized business activities. Individuals should contact the appropriate FI directly for access to their personal information. The FDIC does not make decisions regarding individuals based on the PII received from FDIC business partners that conduct business with the FDIC.

This PIA serves as notice with respect to the collection, use, and disclosure of PII.

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

Individuals that register to attend FDIC-sponsored virtual events may contact the meeting organizer to access and make changes to their information.

In cases where FCCST may be used to facilitate the transport, exchange, or sharing of information related to other systems that operate as FDIC Privacy Act systems of records, the FDIC provides these individuals the ability to have access to their PII maintained in the respective source systems of records as specified by the Privacy Act and FDIC Circular 1031.1. The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1031.1. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public facing website. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

FCCST may also be used to receive, transmit, or share data provided by FDIC business partners that conduct business with the FDIC, which may include information about FI customers or FI employees collected in conjunction with FDIC's authorized business activities. Individuals should contact the appropriate FI directly for access to their personal information.

Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII. Further, the FDIC does not make decisions regarding individuals based on the PII received from FDIC business partners that conduct business with the FDIC.

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

Individuals that register to attend FDIC-sponsored virtual events may contact the meeting organizer to review and make changes to their information.

In cases where FCCST facilitates the transport, exchange, or sharing of information related to other systems that operate as FDIC Privacy Act systems of records, the FDIC provides these individuals with the procedures for correcting their PII maintained in the respective source systems of records as specified by the Privacy Act and FDIC Circular 1031.1. The FDIC publishes its SORNs on the FDIC public-facing website, which includes rules and regulations governing how individuals may request access to records maintained in each system of records, as specified by the Privacy Act and FDIC Circular 1031.1. The FDIC publishes access procedures in its SORNs, which are available on the FDIC public facing website. The FDIC adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.

FCCST also receives, transmits, or shares data provided by FDIC business partners that conduct business with the FDIC. Individuals should contact the appropriate FI directly to correct any inaccurate information. The FDIC does not make decisions regarding individuals based on the PII received from FDIC business partners that conduct business with the FDIC.

This PIA serves as notice with respect to the collection, use, and disclosure of PII.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: There is a risk that individuals, other than those that register to participate in FDIC-sponsored virtual events, do not have the opportunity to access their information or amend inaccurate information contained within FCCST.

Mitigation: In such instances, notice, in the form of a Privacy Act Statement or SORN, is not possible, however, in instances where FCCST processes PII obtained from other FDIC systems that operate as Privacy Act systems of records, information regarding how individuals may access and amend their information in those systems is provided through the publication of FDIC's SORNs for those systems, which are available at: <https://www.fdic.gov/policies/privacy/index.html>. In cases where FCCST maintains or processes PII received from FDIC business partners, those entities are responsible for providing any applicable, required notices to the individuals from whom they collect the information. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information. Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII.

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

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 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 1974², as amended; Section 208 of the E-Government Act of 2002³, Section 522 of the 2005 Consolidated Appropriations Act,⁴ the Federal Information Security Modernization Act of 2014,⁵ OMB privacy policies, and standards issued by the National Institute of Standards and Technology (NIST).

The FDIC's Privacy Section Staff supports the SAOP in carrying out those responsibilities through the management and execution of the FDIC's Privacy Program. The Privacy Program has been fully integrated throughout the agency and is supported on a part-time basis by divisional information security managers located within the agency's divisions and offices.

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 FDIC's Privacy program. Privacy risks for new and updated collections of PII are analyzed and documented in Privacy Threshold Analyses (PTAs) and PIAs. A PTA is used to determine whether a PIA is required under the E-Government Act of 2002 and the Consolidated Appropriations Act of 2005. A PIA is required for: (1) a new information technology (IT) system developed or procured by FDIC that collects or processes PII; (2) a substantially changed or modified system that may create a new privacy risk; (3) a new or updated rulemaking that may affect the privacy of PII in some manner; or (4) any other internal or external electronic collection activity or process that involves PII.

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?

Privacy risks posed by FCCST are captured in this PIA, which was conducted in accordance with applicable law, OMB policy, and FDIC policy (Circular 1360.19). PIAs are posted on FDIC's public-facing website, <https://www.fdic.gov/policies/privacy/index.html>.

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

Contractors may be responsible for configuring, operating, troubleshooting, applying corrections, and implementing enhancements for/to FCCST components based on evolving business requirements and the discovery of security vulnerabilities and system functionality defects.

Contractors are required to take mandatory annual information security and privacy training. Privacy and security related responsibilities are specified in contracts and associated Risk Level Designation documents.

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?

Yes, Confidentiality Agreements/Non-Disclosure Agreements have been completed and signed for contractors who support FCCST. Privacy and security requirements for contractors and service providers are mandated and are documented in relevant contracts.

² The Privacy Act of 1974, as amended, 5 U.S.C. § 552a.

³ Section 208 of the E-Government Act of 2002, Public Law No. 107-347, 44 U.S.C. Ch. 36.

⁴ Consolidated Appropriations Act, 2005, Public Law No. 108-447, Division H, Title V, Section 522.

⁵ The Federal Information Security Management Act of 2014, Public Law No: 113-283, 44 U.S.C. § 3554.

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 is currently in the process of implementing 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 Privacy Program maintains an ongoing Privacy Training Plan that documents the development, implementation, and update of a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and 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 staff as well.

Additionally, application-specific role-based training may be required for certain FCCST applications. For instance, FCCST network administrators are required to complete training annually that focuses on information security and privacy specific responsibilities in their roles as network administrators, while organizers of meetings conducted using FCCST collaborative audio-video tools are provided training related to the administration and control of meetings and the information that is shared in those meetings.

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 Section develops reports both for internal and external oversight bodies through several methods, including the following: Annual Senior Agency Official for Privacy Report (SAOP) as required by FISMA; weekly reports to the SAOP; bi-weekly reports to the CISO, monthly meetings with the SAOP and CISO; and Information Security Manager's Monthly meetings.

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

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

Breaches are handled in accord with FDIC's Breach Response Plan.

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 FDIC maintains an accurate accounting of disclosures of information held in each system of record under its control, as mandated by the Privacy Act of 1974 and FDIC Circular 1031.1.

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 FDIC retains the accounting of disclosures as specified by the Privacy Act of 1974 and FDIC Circular 1031.1.

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 FDIC makes the accounting of disclosures available to the person named in the record upon request as specified by the Privacy Act of 1974 and FDIC Circular 1031.1.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There are no identifiable risks associated with accountability for FCCST.

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. FCCST may collect, maintain, transmit or share PII in support of authorized business functions pursuant to the following laws:

- 12 USC 1819 states that FDIC can make examinations of and to require information and reports from depository institutions.
- 12 USC 1820 discusses examinations and the authority of FDIC to make and keep copies of information for FDIC's use.
- 12 USC 1821 deals with Deposit Insurance, the Deposit Insurance Fund and closing and resolving banks. The Corporation shall insure the deposits of all insured depository institutions as provided in this chapter.
- 12 USC 1822 deals with FDIC as a Receiver of failed banks.
- 12 CFR 330 clarifies the rules and define the terms necessary to afford deposit insurance coverage under the Act and provide rules for the recognition of deposit ownership in various circumstances.
- 12 CFR 366 deals with FDIC contractors.
- 5 CFR 720 deals with Affirmative Action.
- 5 U.S. Code § 7201 deals with antidiscrimination policy; minority recruitment program.

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable risks associated with authority for FCCST.

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 personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection?

The PII elements maintained, transmitted, or shared using FCCST are relevant and necessary, as deemed by FCCST users, to support various FDIC business functions, including ongoing examination, supervision, compliance, legal, and administrative activities, and are dictated on FDIC business requirements.

Additionally, through the conduct, evaluation and review of privacy artifacts,⁶ 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?

The PII elements maintained and processed by FCCST are relevant and necessary, as deemed by FCCST users, to support FDIC's business functions and activities. 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, including the minimizing the collection of PII and retention of PII. Additionally, through the conduct, evaluation and review of privacy artifacts, the FDIC ensures that the collection and retention of PII is limited to the PII that has been legally authorized to collect.

6.3 How often does the information system or project evaluate the PII holding 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?

FCCST may be used to process, maintain, or share information collected in conjunction with any of FDIC's systems. FDIC maintains an inventory of systems that contain PII. On an annual basis, FDIC does an evaluation of information in the system to ensure it is the same as in the PIA and not kept longer than its retention period. New collections are evaluated to see if they are part of the inventory.

6.4 What are the retention periods of 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.

FDIC records are retained in accordance with the FDIC Circular 1210.01, FDIC Records and Information Management Program, which is informed by the Federal Records Act and NARA regulations.

Due to the nature of records shared via FCCST Collaborative Audio-Video Services, there may be numerous records schedules with different retention requirements applicable to the records created and maintained by FCCST users. It is the responsibility of the respective FCCST users to maintain and dispose of the records they create in accordance with the appropriate records retention schedules applicable to their program area.

⁶ Privacy artifacts include Privacy Threshold Analyses (PTAs), Privacy Impact Assessments (PIAs), and System of Records Notices (SORNs).

With respect to videos and recordings capturing content that include FDIC activities, webinars, virtual training events, functions, and other uses for internal and external viewing, the videos and recordings may be destroyed one day after they have been superseded or when no longer needed.

With respect to information shared via Conference Room and Classroom Technology, the technology is used to transmit data, however, no data is recorded or stored.

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

PII maintained, transmitted or shared by FCCST is not used for testing, training, or research. The FDIC is in the process of developing an enterprise test data strategy to reinforce the need to mask or utilize 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. Additionally, the project team is required to consult the FDIC Privacy Program to identify PII and ensure it is adequately protected or transformed before it is used in test or lower environments.

Privacy Risk Analysis: Related to Minimization

Privacy Risk: There is a risk that the personally identifiable information maintained by FCCST may be unnecessary or excessive, or may be kept longer than is necessary to meet the business need for which it was collected.

Mitigation: This risk is mitigated by FCCST users being appropriately trained and FDIC policy regarding the collection, use, and retention of FDIC information. FDIC users are required to complete Annual Security and Privacy Training, which addresses the creation, maintenance and retention of FDIC records. Additionally, FDIC Directive 1360.9, Protecting Sensitive Information, requires that sensitive information only be collected and retained when it is necessary to satisfy an FDIC business requirement. Further, FDIC users are responsible for complying with FDIC Circular 1210.01, FDIC Records and Information Management Program, which is informed by the Federal Records Act and NARA regulations.

Privacy Risk: There is a potential risk that PII could be used in the test or lower environments beyond that which is necessary.

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

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.

It is the responsibility of FCCST users to ensure the accuracy, relevancy, timeliness, and completeness of data that they create, transmit or share using FCCST. Additionally, data may be provided by FDIC business partners that conduct business with FDIC. As such, the FDIC relies on them to provide data that is accurate, relevant, timely, and complete.

Information that is used by the FDIC as part of its supervisory, examination, compliance, receivership, legal, administrative, and other legally authorized functions will be reviewed for accuracy and

timeliness as required by the particular function, laws, and authorities (see Question 5.1), if any, applicable at the time the agency compiles the information.

Additionally, the FDIC reviews privacy artifacts for adequate measures 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?

Contact information, such as name and email address, may sometimes be collected from meeting participants to document meeting attendance or to respond to a participant's request for additional information related to meeting content. In those instances, the contact information is collected directly from the individual.

Otherwise, FCCST is not intended to collect PII directly from individuals. However, FCCST may maintain or process PII that was obtained from other FDIC systems or from FDIC business partners that conduct business with FDIC. In those instances where PII is collected by other FDIC systems, the FDIC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.01, FDIC Forms Management Program. In those instances where PII is obtained from FDIC business partners that conduct business with FDIC, the FDIC does not have the ability to provide privacy notices prior to the Agency's collection of individuals' PII. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information. 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.

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

It is the responsibility of FCCST users to ensure the data that they create, transmit or share using FCCST is not inaccurate or outdated. Additionally, data may be provided by FDIC business partners that conduct business with FDIC. As such, the FDIC relies on them to provide data that is not inaccurate or outdated.

The FDIC reviews privacy artifacts to ensure adequate measures are taken to check for and correct any inaccurate or outdated PII in its holdings.

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

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.

FDIC has technical security measures and controls in place to prevent the misuse of data maintained and processed by FCCST. Such security measures and controls consist of: user identification and authentication, network permissions, automatic session lockout after a period of inactivity, automatic account lockout after a specified number of failed logon attempts, strong password requirements, and the deployment of firewalls that protect network connections and prevent unauthorized access. Access to information within FCCST is controlled using role-based permissions that are dependent upon a person's need to know and the principle of least privilege. Further, FDIC employees must complete FDIC's Corporate Information Security and Privacy Awareness Training on an annual basis.

Additionally, application-specific role-based training may be required for certain FCCST applications. For instance, FCCST network administrators are required to complete training annually that focuses on information security and privacy specific responsibilities in their roles as network administrators,

while organizers of meetings conducted using FCCST collaborative audio-video tools are provided training related to the administration and control of meetings and the information that is shared in those meetings.

Through its PTA adjudication process, the FDIC Privacy Program utilizes the Federal Information Processing Standards Publication 199 (FIPS 199) methodology to determine the potential impact on the FDIC and individuals should there be a loss of confidentiality, integrity, or availability of the PII. The Office of the Chief Information Security Officer prescribes administrative and technical controls for the system or project based on the FIPS 199 determination.

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, and consequently does not have a need to establish a Data Integrity Board.

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: There is a risk that the information maintained and processed by FCCST may not be accurate.

Mitigation: FDIC relies upon the individuals that register to attend FDIC-sponsored virtual events to provide contact information that is accurate. Otherwise, the accuracy of FCCST information is primarily dependent on end users who have responsibility for the content they maintain and process using FCCST. The collaborative nature of some FCCST components provide a platform where those involved in the collaboration may address inaccuracies identified. Information maintained and processed by FCCST that is used by the FDIC as part of its supervisory, examination, compliance, receivership, legal, administrative, and other legally authorized functions will be reviewed for accuracy and timeliness as required by the particular function, laws, and authorities (see Question 5.1), if any, applicable at the time the agency compiles the information.

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, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection.

With respect to the contact information that may be collected from meeting participants to document meeting attendance or to respond to a participant's request for additional information related to meeting content, those individuals may choose not to provide their information in conjunction with the registration process, which would preclude them from participating in the event, as well as preclude their ability to request associated content.

Otherwise, FCCST is not intended to collect PII directly from individuals. However, FCCST may maintain or process PII that was obtained from other FDIC systems or from FDIC business partners that conduct business with FDIC. In those instances where PII is collected by other FDIC systems that operate as Privacy Act systems, the FDIC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.01, FDIC Forms Management Program. In those instances where PII is obtained from FDIC business partners that conduct business with FDIC, the FDIC does not have the ability to provide privacy notices prior to the Agency's collection of individuals' PII. Individuals

should review the relevant privacy notices that would have been presented to them by the entity collecting the information. 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.

With respect to the contact information that may be collected from meeting participants to document meeting attendance or to respond to a participant's request for additional information related to meeting content, those individuals may choose not to provide their information in conjunction with the registration process, which would preclude them from participating in the event, as well as preclude their ability to request associated content.

Otherwise, FCCST is not intended to collect PII directly from individuals. However, FCCST may maintain or process PII that was obtained from other FDIC systems or from FDIC business partners that conduct business with FDIC. In those instances where PII is collected by other FDIC systems that operate as Privacy Act systems, the FDIC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.01, FDIC Forms Management Program. In those instances where PII is obtained from FDIC business partners that conduct business with FDIC, the FDIC does not have the ability to provide privacy notices prior to the Agency's collection of individuals' PII. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information. 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.

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

It is not feasible or appropriate to obtain direct consent prior to any new use or disclosures of previously collected PII. If applicable, the FDIC Privacy Program will update this PIA as necessary.

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

With respect to the contact information that may be collected from meeting participants to document meeting attendance or to respond to a participant's request for additional information related to meeting content, FCCST only uses the PII referenced for that purpose.

Otherwise, FCCST is not intended to collect PII directly from individuals. However, FCCST may maintain or process PII that was obtained from other FDIC systems or from FDIC business partners that conduct business with FDIC. In those instances where PII is collected by other FDIC systems that operate as Privacy Act systems, the FDIC ensures that its forms, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.01, FDIC Forms Management Program. In those instances where PII is obtained from FDIC business partners that conduct business with FDIC, the FDIC does not have the ability to provide privacy notices prior to the Agency's collection of individuals' PII. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information. 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.

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

The FDIC Privacy Program website, <https://www.fdic.gov/policies/privacy/index.html>, instructs viewers 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: With the exception of contact information that is sometimes collected from meeting participants, the PII that could be maintained and shared using FCCST is not collected directly from individuals. As such, there is a risk that these individuals will not know how their data is being used or shared. Additionally, individuals are not provided with an opportunity to consent to or opt out of the FDIC's collection and use of their PII.

Mitigation: With the exception of contact information that is sometimes collected from meeting participants, the FDIC does not have the ability to provide privacy notices to individuals or provide the opportunity for individuals to consent or opt-out of FDIC's maintenance and processing of their PII using FCCST. In instances where PII is obtained from other FDIC systems that operate as Privacy Act systems of records, notice is provided through the publication of FDIC's SORNs for those systems which are available at: <https://www.fdic.gov/policies/privacy/index.html>. In instances where FCCST maintains or processes PII received from FDIC business partners, those entities are responsible for providing any applicable, required notices to the individuals from whom they collect the information. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information. Additionally, this PIA serves as notice with respect to the collection, use, and disclosure of PII.

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 PII maintained and processed by FCCST is pertinent and necessary, as deemed by the respective FCCST users, to carry out FDIC authorized business activities, which include:

- Insuring deposits,
- Examining and supervising financial institutions for safety and soundness and consumer protection,
- Making large and complex financial institutions resolvable,
- Managing receiverships, and
- Administering and managing FDIC's workforce

Contact information, such as name and email address, may sometimes be collected from meeting participants to document meeting attendance or to respond to a participant's request for additional information related to meeting content.

Otherwise, FCCST is not intended to collect PII directly from individuals. However, FCCST may maintain or process PII that was obtained from other FDIC systems or from FDIC business partners that conduct business with FDIC. In instances where PII is obtained from other FDIC systems that operate as Privacy Act systems of records, notice is provided through the publication of FDIC's SORNs for those systems which are available at: <https://www.fdic.gov/policies/privacy/index.html>. In instances where FCCST maintains or processes PII received from FDIC business partners, those entities are responsible for providing any applicable, required notices to the individuals from whom they collect the information. Individuals should review the relevant privacy notices that would have been presented to them by the entity collecting the information.

9.2 Describe how the information system or project uses personally identifiable information (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.

Through the conduct, evaluation and review of privacy artifacts, 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, with the use of various privacy controls. Additionally, annual Information Security and Privacy Awareness Training is mandatory for all staff 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.

Access to the data within FCCST is limited based on business need. All authorized users who have access to FCCST or its components must have the approval of their Manager/Supervisor and the pertinent Data Owner before access is granted. FCCST users are responsible for sharing only that information which is appropriate and ensuring that those with whom they are sharing the information are properly authorized. Further, all FDIC network users must annually complete the FDIC's Information Security and Privacy Awareness training, which includes the Corporation's general rules of behavior. Guidelines established in the Corporation's access control policies and procedures are also followed.

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, FCCST does not aggregate or consolidate data in order to make determinations or derive new data about individuals.

9.6 Does the information system or project share personally identifiable information (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.

Authorized FDIC users may use FCCST to share data external to FDIC, including PII that was obtained from other FDIC systems that operate as Privacy Act systems of records. FCCST users are responsible for ensuring that any sharing of information external to FDIC is in accord with the routine uses stipulated in FDIC's SORNs, which are available at: <https://www.fdic.gov/policies/privacy/index.html>.

Additionally, through the conduct, evaluation and review of PIAs and SORNs, the FDIC ensures that PII shared externally 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 1031.1, Administration of the Privacy Act, 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.

Annual Information Security and Privacy Awareness Training is mandatory for all staff and contractors, which includes information on rules and regulations regarding the sharing of PII with third parties.

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 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 Purpose and Use Limitation

Privacy Risk: There is a potential risk associated with purpose and use limitation for FCCST in that information, including PII, transmitted using FCCST could potentially be used or shared for a purpose not compatible with the original purpose for which the information was collected.

Mitigation: This risk is mitigated by FCCST users being appropriately trained. This risk is further mitigated by FDIC Directive 1360.9, Protecting Sensitive Information, which addresses the protection of sensitive information, including PII. Additionally, FDIC uses a combination of technical and operational controls to reduce the risk associated with the FCCST environment, such as encryption, passwords, audit logs, firewalls, malware identification, and a data loss prevention program.

Privacy Risk: There is a risk that non-authorized individuals may inadvertently gain access to FCCST content to which they should not have access.

Mitigation: FCCST users are responsible for ensuring that FCCST content is restricted to those having an authorized purpose, in accordance with FDIC Directive 1360.9, Protecting Sensitive Information. Additionally, FCCST users are required to complete annual Information Security and Privacy Awareness Training, which includes information on rules and regulations regarding the sharing of PII.

Privacy Risk: There is a risk that the individuals participating in an FCCST session may unknowingly be recorded without their consent.

Mitigation: FDIC restricts the use of recordings to specific, authorized purposes as stipulated in FDIC Directive 3100.5, Unauthorized Recording. Further, in instances where a recording is authorized, Directive 3100.5 requires that individuals be notified of a recording before the recording begins. FCCST collaborative audio-video tools display a banner that notifies meeting participants when a session is being recorded. Participants have the option of exiting, or may consent to the recording by participating in the meeting. Further, FCCST users can disable their cameras and microphones during calls.

Privacy Risk: There is a risk that individuals may take screenshots using phone cameras or snipping tools to capture FCCST content without notifying the individual sharing the content.

Mitigation: FCCST users are responsible for sharing only that content which is applicable to a particular FCCST session and for ensuring that those with whom they share information are appropriately authorized. FDIC users are responsible for complying with FDIC Circular 1360.9, Protecting Sensitive Information, and are required to complete annual Information Security and Privacy Awareness Training, which includes information on rules and regulations regarding the sharing of PII.

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 personally identifiable information (PII).

FDIC maintains an inventory of systems that contain PII. On a semi-annual basis, FDIC does an evaluation of information in the system to ensure it is the same as in the PIA and not kept longer than its retention period. New collections are evaluated to see if they are part of the inventory.

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?

The FDIC Privacy Program updates the Chief Information Security Officer (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?

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?

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 risks associated with security for FCCST.

Mitigation: No mitigation actions are recommended.