



Privacy Impact Assessment of the Community Advisory Council Systems (CAC Systems)

Program or application name: Community Advisory Council Systems

System Owner: Board of Governors of the Federal Reserve System's (Board) Division of Consumer and Community Affairs (DCCA)

Contact information:

System Manager: Joseph Firschein
Title: Associate Director and Community Affairs Officer
Division: Division of Consumer and Community Affairs
Address: 20th Street and Constitution Avenue, N.W.
Washington, D.C. 20551
Telephone: (202) 736-5531

IT System Manager: Chris Melvin
Title: Manager, Information Technology
Division: Division of Information Technology
Address: 20th Street and Constitution Avenue, N.W.
Washington, D.C. 20551
Telephone: (202) 452-3837

Description of the IT system:

The Board created the Community Advisory Council (CAC) as an advisory committee to the Board on issues affecting consumers and communities. The CAC is composed of a diverse group of experts and representatives of consumer and community development organizations and interests, including representatives from such fields as affordable housing, community and economic development, small business, and asset and wealth building. CAC members meet semiannually with the members of the Board in Washington, D.C. to provide a range of perspectives on the economic circumstances and financial services needs of consumers and communities, with a particular focus on the concerns of low-and moderate-income consumers and communities.

In its operation and management of the CAC, the Board relies on a variety of information technology systems and applications that collect and maintain information about individuals seeking membership on the CAC (CAC candidates) and members of the CAC. These systems and applications as are known as “CAC Systems.”

CAC Systems is comprised of the following components:

- (1) a web interface on the Board’s public website that allows CAC candidates to submit their application, resume, cover letter and other information;
- (2) a dedicated email account that collects application forms, resumes, and cover letters submitted by CAC candidates, collects any other data the CAC candidate chooses to provide, and allows Board staff to answer questions submitted by CAC candidates;
- (3) an internal collaboration site that contains information relating to the selection of candidates to the CAC (including information submitted through the website, the email account, and through postal mail) as well as documents prepared by Board staff;
- (4) a separate internal collaboration site that contains information relating to the CAC members; and
- (5) shared network folders that contain information relating to CAC candidates and CAC members.

1. Information concerning individuals that is being collected and/or maintained:

CAC Systems contains the following information about candidates and members of the CAC (hereinafter also collectively referred to as “individuals” and singularly as “individual”):

- The individual’s application that includes name and contact information (such as address, telephone number, and email address), organization and title, as well as organization type and expertise;
- Resume and cover letter explaining the individual’s interest in serving on the CAC and describing the individual’s qualifications and any other information the individual submits relating to the individual’s qualifications for membership on the CAC;
- Publicly available information regarding the CAC candidate independently obtained by Board staff; and

Once selected, as necessary, the Board may also collect information that facilitates the member’s service on the CAC or the work of the CAC. This includes information regarding CAC member travel to the Board to attend CAC meetings and honoraria provided by the Board to the CAC members. The payments information related to CAC member travel and honoraria is also transmitted to and retained in the System of Records entitled BGFRS-9, “FRB—Supplier Files.” The Board may also collect other information, such as contact information for staff assistants (including name, email, and phone number) and pictures (including “headshots”) of the CAC members.

2. Source(s) of each category of information listed in item 1:

Generally, the primary source of information is the individual who submits their information to the Board. However, CAC members may submit the contact information for their staff assistants on their behalf and staff assistants may submit information on behalf of the CAC member.

Board staff may also independently obtain publicly available information regarding the CAC candidate.

3. Purposes for which the information is being collected:

The Board collects the information to aid the Board in its operation and management of the CAC, including in the selection of members to the CAC. If a candidate is selected as a member, the Board may collect additional information (such as information for arranging or reimbursing travel, financial information to pay honoraria, headshots, mailing addresses, and staff assistant contact information) as necessary to facilitate the member's service on the CAC or the work of the CAC.

4. Individuals who will have access to the information:

Access to the information maintained in CAC Systems is limited to authorized Board staff who have a need for the information for official business purposes. In addition, the Board may disclose information in the CAC Systems for the purposes set forth in the Board's System of Records entitled BGFRS-39 "FRB—General File of the Community Advisory Council" and payment information for the purposes set forth in the Board's System of Records entitled BGFRS-9 "FRB—Supplier Files."

5. Whether the individuals to whom the information pertains will have an opportunity to decline to provide the information or consent to particular uses of the information (other than required or authorized uses):

CAC candidates voluntarily submit the information to the Board. If a CAC candidate is selected as a member, the Board may collect additional information (such as travel, honoraria, headshots, and staff contact information) as necessary to facilitate the member's service on the CAC or the work of the CAC. Once the information is submitted, individuals will not have an opportunity to consent to particular uses of the submitted information.

6. Procedure(s) for ensuring that the information maintained is accurate, complete and current:

The individual CAC candidate or member is responsible for ensuring the accuracy and completeness of any information they submit. Before Board staff enter into CAC Systems any publicly available information obtained during the vetting process, Board staff will verify the accuracy of the information.

7. The length of time the identifiable information will be retained and how it will be purged:

Pending establishment of an approved retention period, the CAC records will be retained indefinitely. Data submitted into the CAC Systems is sent to FIRMA, the Board's official recordkeeping system, on an annual basis.

8. The administrative and technological procedures used to secure the information against unauthorized access:

Data submitted through the Board's public website is protected by encryption. The CAC web interface encrypts the data on submission. The data is then transferred in an encrypted state from the public website to the Board's internal network, decrypted, and then moved to the internal section of CAC Systems. All incoming data whether submitted electronically through the Board's public website or the CAC email account is subject to appropriate safeguards, including virus scanning. The CAC Systems have the ability to track individual user actions within each system. The audit and accountability controls are based on NIST and Board standards, which in turn are based on applicable laws and regulations. The controls assist in detecting security violations and performance or other issues in the CAC Systems.

Access to the CAC Systems is restricted to authorized Board users who require access for official business purposes. Users are classified into different roles and common access and usage rights are established for each role. User roles are used to delineate between the different types of access requirements such that users are restricted to data that is required in the performance of their duties. Periodic audits and reviews are conducted to determine whether users still require access, have the appropriate role, and whether there have been any unauthorized changes in any information maintained in the CAC Systems.

9. Whether a new system of records under the Privacy Act can be created. (If the data is retrieved by name, unique number, or other identifier assigned to an individual, then a Privacy Act system of records may be created):

CAC Systems is covered by an existing System of Records Notice entitled BGFRS-39, "FRB—General File of the Community Advisory Council." Payment information in the CAC Systems is covered by an existing System of Records notice entitled BGFRS-9 "FRB—Supplier Files."

Reviewed:

/signed/
Sharon Mowry
Chief Information Officer and
Senior Agency Official for Privacy

3/25/22
Date