



Privacy Impact Assessment  
for

Combined Federal Campaign (CFC) Online Application  
and Donation System

November 7, 2019

**Program Office Point of Contact**  
Keith Willingham  
Office of Combined Federal Campaign

**Reviewing Official**  
Kellie Cosgrove Riley  
Chief Privacy Officer



## Abstract

The Combined Federal Campaign (CFC) Central Campaign Administrator (CCA) maintains the U.S. Office of Personnel Management (OPM) CFC Online Application and Donation Systems. The CCA also manages the systems under the auspices of the Merit System Accountability and Compliance (MSAC)/Office of CFC.

The mission of the CFC program is to promote and support philanthropy through a program that is employee-focused, cost-efficient, and effective in providing all federal employees the opportunity to improve the quality of life for all. The CFC Online Application and Donation System centralizes all aspects of CFC administration to a single point of entry for charities, donors, and payee systems. OPM conducted and updated this Privacy Impact Assessment because the CFC collects, maintains, and uses personally identifiable information about the individuals who participate in charitable giving through the CFC.

## Overview

The CFC is the largest workplace giving campaign in the world. Since its inception in 1961, Federal employees have pledged more than \$8 billion to thousands of qualified local, national, and international charities. Through 2016, more than 120 local campaigns administered the CFC across the country and overseas. Charities applied to participate, as either an independent charity or member of a federation, by submitting an application to either OPM or one of the local CFC campaigns.

Similarly, Federal, Postal, and military personnel donated through the CFC by submitting a completed paper or electronic pledge form to their payroll office and/or the administrator in their local campaign. The local administrators, known as Principal Combined Fund Organizations (PCFO), collected and maintained information about the donors, their contribution, and their designated charitable organizations to process and account for donor contributions. The PCFO collected cash, checks, and credit card contributions directly from the donors and the donors' payroll offices when donors had chosen to contribute via payroll deduction. The PCFO then made



payments directly to the individual charities or federations chosen by the donors.

OPM established a Federal Advisory Committee in 2011, known as the CFC 50 Commission. The CFC 50 Commission studied the campaign and recommended ways to streamline and improve the program. Following that report, OPM set out to centralize two core components of the CFC: a) The applications submitted by charities and federations that want to participate in the CFC; and b) The contributions from individuals who wish to support those charities. Accordingly, in 2017, the CFC Online Application and Donation System ([cfccharities.opm.gov](http://cfccharities.opm.gov) for charities applying to the CFC and [cfcgiving.opm.gov](http://cfcgiving.opm.gov) for individual donors) replaced the redundant paper processes and electronic systems that the PCFOs operated.

The new online system reduces administrative costs, increases transparency, and ensures that more of the contributions made by Federal, Postal and military personnel reach the people who need help the most. This new system also replaced electronic CFC modules in Employee Express and myPay, as well as a variety of local systems. The government benefits of the new system include:

- Universally available electronic giving. Prior systems only provided truly paperless giving to employees served by certain payroll providers.
- Increased transparency and accountability with fees disclosed upfront to the donor before they pledge. Charities, not just donors, share the cost of administering the campaign through application listing and distribution fees.
- A new avenue for recurring gifts by annuitants who could only make one-time pledges in the past;
- The ability to engage employees to give their money and their time; and
- An additional new feature that will enable newly hired employees who start working for the Federal service outside CFC "Open Season" to establish a pledge to their approved local, national or international charities.



Individuals now submit their donation information either electronically or by filling out a paper pledge form. If using paper forms, the CCA scans the form and enters the data into the electronic system. In addition to centralizing the CFC functions, OPM also expanded the donor pool by allowing civilian annuitants and military retirees to participate and by permitting Federal employees to pledge volunteer hours in addition to financial gifts.

The CFC Online Application and Donation System also collects and maintains the application information for charities applying to participate in the CFC and collects the charities' CFC application and listing fees. Once OPM approves a charity application for the annual campaign, the CCA updates the system to allow donors to pledge charitable contributions to the newly listed charity. Donors can set up payroll deductions or provide an unlimited number of one-time gifts using credit cards, electronic fund transfers, or checks. All donors who voluntarily provide needed information are registered and allowed to use the system to donate funds and/or volunteer time (to those charities accepting volunteer hours). The CFC donation process is similar to the deduction process for employees' other federal benefits.

The CCA also uses the system to submit requests for payroll deductions from an employee's payroll provider. Payroll providers then deduct those funds and transmit them electronically to the CCA. The CCA electronically disburses funds monthly or quarterly to charitable organizations in accordance with donors' wishes. Information on the donors and the disbursements are available to the charity system over secure web applications. The donor also can track disbursements in the transaction history of his or her web-based account.

## **Section 1.0 Authorities and Other Requirements**

### **1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?**

Executive Order (EO) 12353 (March 23, 1982), EO 12404 (February 10, 1983), and EO 13743 (October 13, 2016); 5 CFR Part 950; Pub. L. 100-202



and Pub. L. 102-393 (5 U.S.C. §1101 Note) require the creation of a centralized workplace giving campaign for the Federal government that is employee focused, cost-efficient, and effective in providing all federal employees the opportunity to improve the quality of life for all.

## **1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?**

The information is covered by the OPM/Central 20 National CFC System SORN.

## **1.3 Has a system security plan been completed for the information system(s) supporting the project?**

Yes. OPM completed an initial system security plan as a part of the Authority to Operate on November 26, 2016. The SSP was updated September 15, 2019 as a part of the ATO system recertification submission package. The program director of the Office of the CFC signed it October 7, 2019.

## **1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?**

Pursuant to 5 CFR § 950.604, OPM must retain CFC records for at least three completed campaign periods. OPM has submitted a records schedule to NARA and is awaiting its approval.

## **1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.**

OPM obtains the information in the CFC Online Application and Donation System via the following forms, listed with their corresponding OMB Control numbers (if applicable):



OPM Form Number	Form Name	OMB Control Number
1647-A	Application for Independent Organizations and Members of Federations	3206-9131
1647-B	Applications for Federations	3206-0131
1647-E	Application for Family Support and Youth Activities Organizations	3206-0131
1654-A	Standard Employee Pledge Form	PRA Not Applicable
1654-B	Standard Retiree Pledge Form	3206-0271

## Section 2.0 Characterization of the Information

### 2.1 Identify the information the project collects, uses, disseminates, or maintains.

The CFC Online Application and Donation System collects the following information from individual donors:

- a. Name;
- b. Social Security Number or other employee identification number used by a Federal payroll or retirement system;
- c. Work address;
- d. Home address;
- e. Phone number;
- f. Government e-mail address;
- g. Secondary e-mail address;
- h. Employment information (to include, but not limited to, Federal agency or military branch, department/unit, office, military service, commands, etc.);
- i. Charity or charities designated;
- j. Amount of donation, in dollars and/or hours;
- k. Credit card information, including credit card number and expiration date;



- l. Bank account number and bank routing number;
- m. Authorization to release name and other information to charities;
- n. Usernames and passwords created to access the system;
- o. Security questions and answers (for resetting passwords to access the online system);
- p. Help Desk ticket information; and
- q. Customer (donor and charity) satisfaction surveys.

The CFC Online Application and Donation System also obtains information from the charities that apply to participate in the CFC program. CFC regulations require the charity to demonstrate that it is qualified to participate under 5 CFR Part 950. This includes charity legal name, contact information (email, names of points of contact, business address), usernames and passwords created to access the system, tax identity number, CFC code, bank account information (including the routing number), public audit files (audited financials, Internal Revenue Service (IRS) Form 990, IRS letters of determination), *IRS Doing Business As* letters, base commander authorization letters, and other information as defined in the federal regulations for the application.

## **2.2 What are the sources of the information, and how is the information collected for the project?**

Individual donors provide their information by completing electronic forms on the public-facing CFC website ([cfcgiving.opm.gov](http://cfcgiving.opm.gov)). For the first five years that the system operates, donors may also submit paper forms, which the CCA then scans into the CFC Donation System for document retention. Trained and screened employees at the CCA manually enter the information from the form into the system. If any information on the paper form is illegible, the form includes a primary and secondary e-mail address, which the customer service team will use to get better instructions from the contributor.

Charities provide their information by completing a web-based form and uploading relevant documentation into the CFC Online Application and Donation System. Existing information systems will transfer historical charity data one time to the charity system, which will contain PII, such as contact information.



### **2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.**

The CFC Donation System does not use publicly available information or information from commercially available sources about individuals who make donations through the CFC. However, the CFC Online Application and Donation System does obtain information from the Internal Revenue Service's Exempt Organizations Business Master File (IRS EO BMF) to ensure that charities are eligible to participate in the CFC.

### **2.4 Discuss how the accuracy of the data is ensured.**

Individual donors provide their information by creating an account and typing their information directly into the public-facing CFC donor website. They can log into their accounts at any time to correct any errors in their information or cancel a pledge. The donors can log into their accounts to change the donation amounts only during an open solicitation or enrollment period (September through the following January). Therefore, the system relies upon the user's knowledge of their data to make sure it is valid. The system does not actively check the accuracy of the data.

The system has built-in features that contribute to the individual donors providing accurate information. For example, fields requesting donation amounts accept only numeric characters, and the field requesting social security number is limited to nine numeric characters. Entering too many or too few numbers in the social security field will invalidate the entry and the system will block the donor from saving the record.

Information that donors submit via paper forms contains a primary and secondary e-mail address, which the CCA's customer service team will use when information is illegible to contact the donor and obtain accurate information. Appropriate federal employees working on the CFC review the information provided by the charities who apply to participate in the CFC and review and reconcile the information submitted against information from the IRS before authorization.





## 2.5 Privacy Impact Analysis: Related to Characterization of the Information

**Privacy Risk:** There is a risk that the system will collect more information than is necessary to process individual donations.

**Mitigation:** This risk is mitigated by requesting only the information needed to process the individual donors' charitable contributions and by accepting only the designated donor form for those individuals who do not make use of the electronic system.

**Privacy Risk:** There is a risk that the system will collect Social Security numbers in situations where they are not needed.

**Mitigation:** This risk is present only for those individuals who make use of the paper pledge form and who are donating through a means other than payroll or annuity deduction. If those individuals provide SSN on the paper form, OPM partially mitigates the risk of over-collection of SSNs because the CCA will not manually enter the SSN into the system. However, the CCA scans the complete form, including SSN, for document retention and retains the SSN for as long as required.

**Privacy Risk:** There is a risk that the information collected is not accurate, and that the CCA cannot properly process an individual's charitable donations.

**Mitigation:** This risk is mitigated by collecting information directly from the individual donors, who have an interest in ensuring that the information they provide about themselves is accurate, and by structuring the electronic data fields to reduce the possibility that the donor will provide inaccurate information. The CCA manually enters data from paper pledge forms into the system at the CFC Processing Center in Madison, WI. If any information on the paper form is illegible, the form includes primary and secondary e-mail addresses, which the customer service team will use to get better instructions from the contributor. Should any PII be illegible, the customer service team will request that the donor submit a corrected pledge form or written instructions to make corrections. In instances where paper pledge forms are submitted in a batch by a campaign manager, the customer



service team may reach out to the official who submitted the batch if information such as the employees' department, agency, or office is not legible.

## **Section 3.0 Uses of the Information**

### **3.1 Describe how and why the project uses the information.**

OPM and the CCA use the information provided by the individual donors to receive, process, and account for their charitable donations; make payments to charitable organizations; and address inquiries from donors and other stakeholders, including Federal agencies, charitable organizations, and Congress, as necessary. In particular, OPM and the CCA provide Social Security numbers to payroll service providers to use to re-direct payment from the appropriate individual donor to the authorized charity accurately; and use and provide credit card and banking information to process one-time pledges made using a credit card or ACH.

OPM and the CCA may also use information obtained from individual donors to produce summary, de-identified descriptive statistics and analytical studies about the CFC program. OPM uses information obtained from the charitable organizations to approve or deny their applications to participate in the CFC and to adjudicate appeals by charities that OPM initially denies.

The CCA provides the names, home addresses, and personal email addresses of donors to the designated charitable organizations or their federations, where applicable, when the donor has so requested. The CCA and the federation may not make any other use of donors' names and contact information.

**3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.**



The system does not currently conduct data searches or analysis to locate predictive patterns or anomalies.

### **3.3 Are there other programs/offices with assigned roles and responsibilities within the system?**

Pursuant to the Inspector General Act, the system allows for an “auditor” role for OPM’s Office of the Inspector General to review transactions. Otherwise, only authorized users within OPM’s CFC Program Office and designated CCA personnel have access to the system.

### **3.4 Privacy Impact Analysis: Related to the Uses of Information**

**Privacy Risk:** There is a risk that the information will be used for a purpose other than that for which it was collected.

**Mitigation:** This risk is mitigated by allowing only authorized users from the program office, CCA, or OIG auditor to access data. OPM and the CCA monitor user activity on the system and generate security alerts if suspicious activity is noted. The system incorporates an Identity and Access Management service that automatically restricts access to data based on a user’s profile. For example, donors can view and edit their own records and can view a listing of approved charities; charities can view and edit their own records and can view the donations pledged to their organization. Charities cannot view any information on the donor, unless the donor allows the release of contact information and donation amount.

**Privacy Risk:** There is a risk that either an authorized or an unauthorized user may access the information for an unauthorized purpose.

**Mitigation:** This risk is reduced by auditing reports about the use of the system. We monitor user activity on the system and generate security alerts if we note suspicious activity. Also, clearly defined roles and access contribute to mitigating this risk. For example, system administrators do not have access to charities’ or donors’ data but Customer Service Representatives can view and edit both charities’ and donors’ information.



Project audit logging captures all changes made to a record, including the identity of the individual making changes.

## Section 4.0 Notice

### 4.1 How does the project provide individuals with notice before the collection of information? If notice is not provided, explain why not.

Individual donors are provided with a Privacy Act statement on the CFC website and the paper donor form when they provide their information. OPM also provides notice via the OPM/Central 20 National CFC System SORN and this PIA.

### 4.2 What opportunities are available for individuals to consent to uses, decline to provide information or opt-out of the project?

Participation in the CFC is voluntary. Those who participate cannot opt-out of OPM using their information for purposes related to processing their charitable donation, but that can opt-out of having their name and contact information released to the charity to which they are donating.

### 4.3 Privacy Impact Analysis: Related to Notice

**Privacy Risk:** There is a risk that individual donors will not have adequate notice concerning how the CFC program uses the information they provide and discloses such data to third parties.

**Mitigation:** This risk is mitigated by providing individual donors with a Privacy Act statement when they provide their information and by permitting them to opt-in to any disclosure of their information to the charity to which they donate.



## Section 5.0 Data Retention by the project

### 5.1 Explain how long and for what reason the information is retained.

Pursuant to 5 CFR § 950.604, OPM must retain CFC records for at least three completed campaign periods. A campaign period spans approximately 33 months, beginning with the CFC charity application process and ending with the completion of the audit of the campaign following the final disbursement of campaign funds. OPM developed and submitted a records schedule to NARA for approval. Until that records schedule is final, OPM shall retain all CFC records permanently.

### 5.2 Privacy Impact Analysis: Related to Retention

**Privacy Risk:** There is a risk that OPM will retain information for longer than the three completed campaign periods deemed necessary in the applicable regulation.

**Mitigation:** Without a records schedule in place, this risk is currently not mitigated. The CFC program is working to mitigate this risk and has developed a records schedule and has submitted it to NARA for approval. Until that records schedule is finalized and approved, NARA regulations require OPM to consider the record's status as permanent.

## Section 6.0 Information Sharing

### 6.1 Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Individual donors' information is provided to credit card companies, banks, and other financial institutions to process one-time or recurring donations. For those individual donors who choose to contribute to the CFC via payroll deduction, information is provided to their payroll service provider to facilitate accurate payroll deductions. For retirees/annuitants who choose to contribute to the CFC via annuity deduction, information is provided to their retirement service office to facilitate accurate annuity deductions. With the



consent of the individual donors, the CFC also shares name, address, donation amount, and volunteer hours committed with the applicable charity participant. This information allows the charities to send the donor letters of appreciation and to coordinate volunteer service projects. The CCA monitors user and sharing activity on the system and generates security alerts if it detects suspicious activity.

## **6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.**

The external sharing of information described in section 6.1 is consistent with the purposes stated in the OPM/Central 20 National CFC System SORN. In particular, the SORN's routine uses "h" and "i" specifically permit the disclosure of the information to credit card companies, banks, and other financial institutions as well as to payroll offices and retirement services, as appropriate.

## **6.3 Does the project place limitations on re-dissemination?**

Yes. Through CFC regulations, OPM prohibits the dissemination of any lists of donors or non-donors. In addition, by regulation, OPM restricts how charities can use any data authorized by the donor for release. Charities may not sell lists of donors who authorize the release of their name, address, or gift amount.

## **6.4 Describe how the project maintains a record of any disclosures outside of OPM.**

OPM retains and accesses transaction records that support donor and charity activities (e.g., registrations, donations). OPM can access these records as appropriate to document disclosures. In addition, OPM retains these transaction records following standards identified in section 5.1.



## 6.5 Privacy Impact Analysis: Related to Information Sharing

**Privacy Risk:** There is a risk that information will be shared with an external entity or re-disseminated with an external entity for a purpose other than the purpose for which the information was originally collected.

**Mitigation:** This risk is significantly reduced by monitoring data use. OPM and the CCA monitor user activity on the system and the CCA generates security alerts if it notes suspicious activity. The applicable regulation also limits the charity's ability to disseminate the information it receives through CFC.

## Section 7.0 Redress

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

Individual donors receive instructions to create login credentials when they first visit the CFC website to donate. Using these credentials, individuals may then access their records by logging into [cfcgiving.opm.gov](http://cfcgiving.opm.gov) (aka [www.opm.gov/showsomelovecfc](http://www.opm.gov/showsomelovecfc)) with their e-mail address, password, and a multi-factor authentication token (i.e., a one-time password or code sent to the user's email account or phone). Alternatively, individuals seeking notification of and access to their records in this system of records may submit a request in writing to the Office of Personnel Management, Office of the Combined Federal Campaign, 1900 E Street, NW, Washington, DC 20415. Individuals must furnish the following information so that OPM can locate their records:

1. Full name.
2. Date of birth.
3. Social Security Number.
4. Signature.
5. Available information regarding the type of information requested.
6. The reason why the individual believes this system contains information about him/her.
7. The address to which the requestor wants OPM to send the information.



Individuals requesting access must also comply with OPM's Privacy Act regulations, 5 CFR Part 297, regarding verification of identity and access to records.

Individuals may also contact the CCA Customer Care Center via telephone (Mon.-Fri. 8 am-6 pm CST) at (800)797-0098, or (608) 237-4898.

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

Individuals may modify or correct their own records by logging into [cfcgiving.opm.gov](http://cfcgiving.opm.gov) with their e-mail address, password, and a multi-factor authentication token (i.e., a one-time password or code sent to the user's email account or phone). Alternatively, individuals may request that records about them be amended by writing to the Office of Personnel Management, Office of the Combined Federal Campaign, 1900 E Street, NW, Washington, DC 20415 and furnishing the following information for their records to be located:

1. Full name.
2. Date of birth.
3. Social Security Number.
4. Local CFC name or city, state and zip code of their duty station
5. Signature.
6. Precise identification of the information they request OPM to amend.

Individuals requesting amendment must also follow OPM's Privacy Act regulations regarding verification of identity and amendment to records (5 CFR 297).

## **7.3 How does the project notify individuals about the procedures for correcting their information?**

Individuals are notified about the procedures for correcting their information through the User Manual at [cfcgiving.opm.gov](http://cfcgiving.opm.gov), the OPM/Central 20 National CFC System SORN, and this PIA. In addition, individual donors may contact the CFC Customer Care Center at (608)237-4898 (local/international) or (800)797-0098 (toll free) for assistance.





## **7.4 Privacy Impact Analysis: Related to Redress**

**Privacy Risk:** There is a risk that individuals will not understand how to access and amend their information in the CFC Online Donor System.

**Mitigation:** This risk is mitigated by providing information to the individuals at the CFC website, in the applicable SORN, and through this PIA.

## **Section 8.0 Auditing and Accountability**

### **8.1 How does the project ensure that the information is used per stated practices in this PIA?**

The CFC Online Application and Donation System generates audit logs. OPM and the CCA review these logs periodically to determine the appropriate handling of information. The relevant CCA contract also covers privacy requirements that aid in facilitating the appropriate of use information.

### **8.2 Describe what privacy training is provided to users, either generally or specifically relevant to the project.**

All OPM employees are required to take annual security and privacy awareness training. In addition, the MSAC/OCFC trains assigned employees on the Standard Operating Procedures that describe how to handle PII. All CCA personnel take security and privacy awareness training provided by their employers.

### **8.3 What procedures are in place to determine which users may access the information, and how does the project determine who has access?**

The system bases donor account creation on an e-mail/username and password combination. The donor receives a system-generated message to verify the account. A donor can log in to the system at any time during open season to enter or update a pledge to the local, national, and international charities approved to participate in the campaign. Federal employees, members of the military, retirees, or contractors may create accounts. Once a donor creates an account, the donor can search the list of approved



charities and make or edit a pledge at any time during open season and submit it for processing. Approved CFC charities obtain donor data by logging into the CFC Online Application and Donation System. The system limits the charity access only to information on its organization. In addition, the system records the log-on activity of the charity.

Payroll providers only have access to their own data, and the data exchange process with them has been heavily limited and secured. The system incorporates an Identity and Access Management service that automatically restricts access to data based on a user's profile.

Program office leadership determines who gets system administrator rights, and the program has identified unique types of users and their access by role. For example, donors can view and edit their own records and can view a listing of approved charities; charities can view and edit their own records and can view the donations made to them. However, charities cannot view any information on donors unless the donors specifically consent to the release of their name, address, and donation amount. Also, system administrators do not have access to charities' or donors' data, but Customer Service Representatives can view and edit both charities' and donors' information. Project audit logging captures all changes made to a record, including the identity of the individual making changes.

### **8.4 How does the project review, and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?**

The Chief Information Security Office will administer and maintain interconnection security agreements with Federal government entities about access and data transfers. OPM renews the agreements annually. Additionally, there is an OPM vendor tasked with administering the campaign and its subcontractors. Each subcontractor has agreements in place with all financial institutions that process payments. OPM updates the agreements when we create or maintain contracts.



## **Responsible Officials**

Keith Willingham  
Director, Office of Combined Federal Campaign  
Office of Personnel Management

## **Approval Signature**

---

Kellie Cosgrove Riley  
Chief Privacy Officer  
Office of Personnel Management