Privacy Impact Assessment
for the

Citizen Corps Program

DHS/FEMA/PIA-029

June 28, 2013

Contact Point
Lynda Williams
Individual and Community Preparedness Division
Office of Protection and National Preparedness
Federal Emergency Management Agency
(202) 786-9472

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Federal Emergency Management Agency (FEMA), Office of Protection and National Preparedness (PNP), Individual and Community Preparedness Division (ICPD) administers the Citizen Corps Program, which also includes the Citizen Corps web-based application, and the Citizen Corps Database. Citizen Corps' mission is to strengthen the collaboration between government and community leaders from all sectors to encourage citizens' preparedness through education, training, and volunteer service to make communities safer, stronger, and better prepared to respond to all hazards and all threats. Through Citizen Corps, communities can establish and register Citizen Corps Councils (Councils) and Community Emergency Response Team (CERT) programs. This Privacy Impact Assessment (PIA) analyzes Citizen Corps' collection, use, maintenance, retrieval, and dissemination of personally identifiable information (PII) associated with points of contacts (POC) designated by Councils, CERTs, and other Citizen Corps partners.

Overview

Following the tragic events of September 11, 2001, federal, state, local, tribal, and territorial government officials have increased opportunities for citizens to become an integral part of protecting the homeland and supporting first responders. Officials determined that the formula for ensuring a more secure and safer homeland consists of preparedness, training, and citizen involvement in supporting first responders. On January 29, 2002, the President of the United States signed Executive Order 13254, "Establishing the USA Freedom Corps," which established the Citizen Corps Program, to capture the spirit of service that emerged throughout our communities following the terrorist attacks.

FEMA administers the Citizen Corps Program to strengthen collaborations with communities and better prepare them to respond to the threats of terrorism, crime, public health issues, and disasters of all kinds. Through Citizen Corps, communities can create and register their own Councils and CERT programs. Councils and CERT programs are sponsored by state, local, tribal, and territorial emergency management or elected leaders. Council and CERT members are members of the general public who volunteer time and resources to promote and assist with disaster preparedness, response, and recovery. The Councils' mission is to bring together diverse stakeholders in a community to plan for disasters. The CERT program offers training that prepares members of the public to help themselves, their families, and their neighbors in the event of a disaster in their community. Each state reviews and approves each program and registry submission and, upon approval, posts them on the Citizen Corps Program website (www.ready.gov/citizen-corps). FEMA then provides final approval for the program to be added into the national registry of Councils and CERTs. State approved registration of a Council or CERT program allows the program to: 1) be recognized at the federal level, thus providing the entity eligibility for Homeland Security grant funding; 2) coordinate preparedness and emergency management activities among other partners and groups associated with Citizen Corps; 3) promote its local Councils and CERTs to the public and become a part of the Citizen Corps national directory of Councils; and 4) receive important updates and messages from FEMA. In addition to the national registration of Councils and CERTs, several government-sponsored programs are recognized and known as Citizen Corps Partner Programs; including Fire Corps, Medical Reserve Corps, USA on Watch-Neighborhood Watch, and

Volunteers in Police Service. Citizen Corps and its partners promote whole community participation in disaster preparedness efforts and encourage citizens to take on active roles in preparing themselves, their families, and their communities to achieve greater community resiliency. Citizen Corps Partners provide FEMA with the POC information such as name, address, phone number, and email address of their programs to enhance public awareness of the various volunteer opportunities available nation-wide and within specific communities. Information provided by Citizen Corps Partners is not part of a FEMA registration process and is not verified by FEMA with state or local governments.

The Citizen Corps Application and Database was established to coordinate, track, and analyze Citizen Corps Councils nationally. The web-based application allows a Council or CERT POC to register the Council or CERT into the national Citizen Corps Database. The DHS/ALL-006 Citizen Corps Database System of Records Notice (SORN), 73 Fed. Reg. 77785, December 19, 2008, is being updated and published concurrently with this PIA to reflect FEMA's collection, use, and sharing of information within the Citizen Corps Application and Database.

To register his or her Council or CERT, a community POC uses www.ready.gov/citizen-corps and locates his or her state Council or CERT. The state Council or CERT POC approves a community Council or CERT through their state-governed process. Once the state has approved a community Council or CERT, the community Council or CERT registers its Council or CERT in the Citizen Corps Database using the Citizen Corps Application.

The Citizen Corps user provides the following PII about his or her Council or CERT POC: name, title, mailing address, and email address. FEMA provides notice on the registration page to the user that POC information will be displayed on the Citizen Corps website. The POC has the option of providing general POC information, such as a public phone number and email address for public use and separate contact information for internal access by Citizen Corps Application users. Additionally, the user enters information regarding his or her specific Council or CERT.

Once the registration is complete, an alert is sent to the Citizen Corps Database System Owner. The System Owner, or his or her designee, verifies with the state POC the Council's authority to operate within the stated jurisdiction. Post verification, the Council POC receives a Citizen Corps system generated message notifying the POC of his or her Council's registration status.

The Council and CERTs information, including the POC information, will then be viewable by the general public using the Citizen Corps Program website. FEMA will send Citizen Corps Program information, such as conferences and disaster assistance information to Councils and CERTs using the internal contact information provided at the time of registration or updated thereafter.

Once a Council or CERT has been approved, the POC can add additional members to the program and assign privileges to their accounts within the system. Within the Citizen Corps Application, appropriately privileged members can send email messages to other local members within their Council or CERT state jurisdiction. Similarly, appropriately privileged state Council or CERT POCs and members of the ICPD can send email messages to all members of the national database within the Citizen Corps Application. FEMA monitors all email messages, local or national, sent within the Citizen Corps Application.

The public can search for Councils, CERTs, and other partner programs by entering a ZIP code or interactively using a national map drill-down. Members of the public can view and access Council, CERT, and Citizen Corps Partners' POC contact information; links to Citizen Corps Partner's websites; and planned community preparedness events either nationally or on a state-by-state basis.

The Citizen Corps application provides limited analysis and management capabilities for authorized ICPD members and POCs of state Councils and CERTs. This includes the ability to view statistical reports, download mailing labels, and export data for further analysis.

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?

Pursuant to 31 U.S.C. § 1342 and Executive Order 13254, "Establishing the USA Freedom Corps" (Jan. 29, 2002), FEMA administers and supports Citizen Corps to advance individual and community preparedness.

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

Information Citizen Corps collects, maintains, uses, retrieves, and disseminates is covered by the DHS/ALL-006 Citizen Corps Database, 73 FR 77785, December 19, 2008, System of Records Notice. FEMA is updating and reissuing this SORN concurrently with this PIA as part of the SORN's biennial review.

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

The Citizen Corps Application and Database is expected to be awarded an Authority to Operate by September 30, 2013.

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

Yes, the records retention schedule for Citizen Corps Program records has been approved by the FEMA Records Officer and NARA as Authorities N1–311–86–1, Item 1B4 and N1–311–97–2, Item 1. 1) routine correspondence with state and local officials, as well as private citizens relating to Citizen Corps quantitative statistical data will be destroyed when no longer needed; and 2) records relating to external committees that are sponsored by FEMA, but have a membership including representatives from other federal agencies, states, local governments, and/or public citizens are transferred to Federal Records Center after 2 years from program cutoff and transferred to NARA 20 years after cutoff.

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.

The information that the Citizen Corps Program collects, uses, maintains, retrieves, and disseminates is collected through OMB No. 1660-0098.

Section 2.0 Characterization of the Information

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

General Point of Contact information for each Council or CERT includes:

- Program name;
- Individual name(s);
- Mailing address(es);
- Email address(es); and
- Telephone number(s).

Program related information includes:

- Program start date;
- CERT basic training and other course information;
- Program's participation in disaster and non-disaster exercises;
- Disaster/emergency response related information;
- Program participation in non-emergency related activities;
- Background checks performed by CERT on participants (Y/N);
- Amount of volunteer service hours donated;
- CERT program source funding information;
- CERT program coordinator pay status (paid or volunteer); and
- CERT mission statements and protocol information.

Account creation and user access information includes:

- User Name;
- Password;
- First name;
- Last name;
- Phone number;
- Personal email;
- User type; and
- Confirm email.

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

Citizen Corps collects information directly from the Council or CERT POC. FEMA collects Citizen Corps partners' information directly from the organization by way of regular uploads to the Citizen Corps Program website.

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

No, Citizen Corps does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

The state Council or CERT POC verifies the information with the requestor and approves the registration, based on its individual verification process. The state Council and CERT POC is usually a state official or his or her designee with emergency response responsibilities within his or her jurisdiction. FEMA updates the Citizen Corps Database and Application upon verification by the state Council POC or CERT program manager. Additionally, Council and CERT POCs have access to their information within the Citizen Corps Database and Application and can update their public and internal information as needed. Information collected from Citizen Corps partners is assumed accurate.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that the information collected, used, maintained, retrieved, and disseminated by Citizen Corps is inaccurate.

Mitigation: FEMA mitigates this risk by collecting information directly from the Council or CERT once it has been verified and approved through its state Council or CERT POC. Additionally, Council and CERT POCs can access their account information and update as needed.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Approved registration of a Council or CERT program allows the program to: 1) be recognized at the federal level, thus providing the entity eligibility for Homeland Security grant funding; 2) coordinate preparedness and emergency management activities among other partners and groups associated with Citizen Corps; 3) promote its local Councils or CERTs to the public and become a part of the Citizen Corps national directory of Councils; and 4) receive important updates and messages from FEMA. Council and CERT information is used to match the needs of disaster response and recovery with the skills and abilities of local volunteers during an incident The Council and CERT registries support the mission of FEMA's ICPD and Citizen Corps, to help achieve greater community resiliency nationwide.

FEMA also uses the Citizen Corps Program website to provide information to the public about approved Councils, CERTs, and other partner programs. The public can search for Councils, CERTs, and other partner programs by entering a ZIP code or interactively using a national map drill-down. Members of the public can also view and access Council, CERT, and Citizen Corps Partners' POC contact information; links to Citizen Corps Partner's websites; and planned community preparedness events either nationally or on a state-by-state basis.

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 DHS plans to use such results.

No, the Citizen Corps Application and Database is not designed to, nor does it conduct electronic searches, queries, or analyses to discover or locate a predictive pattern or anomaly.

3.3 Are there other components with assigned roles and responsibilities within the system?

No, there are no other components within DHS with assigned roles and responsibilities within the Citizen Corps Application and Database.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that information collected by the Citizen Corps Program may be used for purposes other than those for which it was originally collected.

Mitigation: FEMA mitigates this risk by restricting system access to authorized, trained ICPD users and the Council POC via secure login. FEMA does not allow administrative access to the system by other components within DHS who do not have a need to know of the information. ICPD staff members with access to the system are trained on the proper use and processing of information. Additionally, FEMA limits public access to a minimal amount of Council and CERT information voluntarily provided to enhance public awareness of volunteer and training opportunities community preparedness.

Section 4.0 Notice

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

Citizen Corps provides notice to the public by way of the Privacy Act Statement (PAS) accessible on the Citizen Corps Program website and separate notice at the beginning of the registration process that information will be accessible by the public. Additionally DHS/FEMA provides notice of this collection with the publication of this PIA, and the updated and reissued DHS/ALL-006 Citizen Corps Database, 73 FR 77785, December 19, 2008, SORN.

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

Registration into the national Council and CERT registry is voluntary; however, FEMA encourages all active Councils and CERTs to submit profiles and receive state approval in order to be eligible for DHS funding. Applicants that opt-out of the registration process will not be added to the national database or eligible for available Homeland Security grant funding. FEMA provides notice on the Citizen Corps Program website at the beginning of the registration process that Council and CERT POCs information provided will be made available to the public via the Citizen Corps website for outreach and contact purposes. Also, FEMA provides notice by way of the PAS accessible on the Citizen Corps Program website and this PIA of how it will use Council and CERT information collected during the application and registration process. Beyond general POC information, all questions asked during the registration process are required to successfully register the Council or CERT into the national database. By submitting the application, the POC is consenting to the use of his or her information. Once registered, Councils and CERTs can opt-out of the national database by accessing their Council or CERT profile and electing to deactivate the Council or CERT, remove or delete a POC, or adjust permissions.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that individuals are not provided notice of how the Citizen Corps Program uses information collected.

Mitigation: FEMA mitigates this risk by providing notice to the public by way of the PAS accessible on the Citizen Corps Program website and separate notice at the beginning of the registration process that information will be accessible to the public. Additionally DHS/FEMA provides notice of this collection with the publication of this PIA, and the updated and reissued DHS/ALL-006 Citizen Corps Database SORN, 73 FR 77785, December 19, 2008.

Section 5.0 Data Retention by the project

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

In accordance with Authorities N1-311-86-1, Item 1B4; and N1-311-97-2, Item 1, 1) routine correspondence with governors, mayors, and other state and local officials, as well as private citizens relating to Citizen Corps quantitative statistical data will be destroyed when no longer needed; and 2) records relating to establishment, organization, membership, and policy of external committees that are sponsored by FEMA, but have a membership including representatives from other federal agencies, states, local governments, and/or public citizens are transferred to Federal Records Center after 2 years from program cutoff and transferred to NARA 20 years after cutoff.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that information collected and used by the Citizen Corps Program will be retained for longer than needed or authorized.

Mitigation: FEMA mitigates this risk by maintaining Citizen Corps Program information according to the retention schedule set forth in Section 5.1 that has been approved by NARA and the FEMA Records Officer. Additionally, FEMA staff is required to take DHS records management training when granted access to DHS/FEMA information and facilities.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS 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.

FEMA shares Council and CERT contact information with the general public through the Citizen Corps Program website. Additional Council and CERT information regarding specific organizational information is available only to registered users of the Citizen Corps Application and Database. FEMA also shares statistical data regarding Council registration by way of an annual report to Congress for oversight purposes. These reports are accessible by the public at the Citizen Corps Program website.

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

Routine use I of the DHS/ALL-006 Citizen Corps Database SORN allows DHS to share contact and program information with Citizen Corps Application and Database registered users. This is compatible with the purpose for original collection because the Citizen Corps mission involves community outreach, awareness, and coordination.

Routine use H allows DHS to share national program information such as trends and statistical information with Congress. This is compatible with the purpose for original collection because the Congress has oversight of the DHS/FEMA mission and programs.

6.3 Does the project place limitations on re-dissemination?

There are no limitations on re-dissemination of information shared with the public for the purpose of community outreach.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

As described in the DHS/ALL-006 Citizen Corps Database SORN, individuals seeking information within the Citizen Corps Program request those records through the FEMA Disclosure Officer who maintains the accounting of what records are disclosed and to whom.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a privacy risk that individual's information may be inappropriately disclosed.

Mitigation: FEMA mitigates this risk by only sharing information with the public that is needed for Citizen Corps Program outreach and as permitted by the DHS/ALL-006 Citizen Corps Database SORN. Additionally, FEMA routinely shares only statistical information with Congress for program oversight purposes.

Section 7.0 Redress

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

All Citizen Corps Application and Database users have the ability to access and correct their contact information (name, phone, email address, etc.). Also, Citizen Corps Application and Database administrative users have the ability to create/update other users' information. Council and CERT POCs can email or call their sponsoring state Citizen Corps or CERT POC or FEMA POC to have a FEMA user with administrator rights within the Citizen Corps Application and Database access their records.

Alternatively, Council and CERT POCs can submit a Freedom of Information Act (FOIA) or Privacy Act (PA) request to the FEMA Disclosure Officer. All requests should be submitted to: Federal Emergency Management Agency, Attention Disclosure Officer, 500 C Street, S.W., Room 840, Washington, DC 20472.

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

Individuals may correct inaccurate or erroneous information using the same procedures mentioned above in Section 7.1.

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

Notice is provided through this PIA, the DHS/ALL-006 Citizen Corps Database SORN, and the Citizen Corps Program website.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a privacy risk that Council and CERT POCs are not able to access their information and correct any discrepancies.

Mitigation: FEMA mitigates this risk by allowing registered users of the Citizen Corps Application and Database to access their information and correct it as needed within the application and database. Additionally, individuals can access their information using the FEMA PA and FOIA process outlined above in Section 7.1.

Privacy Risk: There is a privacy risk that Council and CERT POCs are not aware of the process to access and correct their information.

Mitigation: FEMA mitigates this risk by providing notice to the public by way of this PIA, the DHS/ALL-006 Citizen Corps Database SORN, and the Citizen Corps Program website.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Citizen Corps Application and Database user's activity, including but not limited to failed login attempts, is recorded and tracked within the system's audit log files. A user's account is locked for twenty minutes following the last of three successive failed login attempts. Users may request that their password be reset by using "forgot password" option of the login screen. The system resets the password and sends a temporary password, to the email address on file. Users can contact the system's helpdesk to request password resets. Users who are identified as inappropriately accessing information within the Citizen Corps Application and Database may have their access privileges revoked and may face other disciplinary action.

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

FEMA employees and contractors are required to receive initial and annual Privacy Awareness training. Additionally, users of FEMA information technology must take Computer Security Awareness training before accessing FEMA information technology or other information.

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

Citizen Corps information that is stored within the Citizen Corps Application and Database is accessible by the general public and registered users of the system. For information that is not publicly accessible via the Citizen Corps Program website, Citizen Corps Application and Database uses role-based access. Users are categorized by areas of responsibility. The user groups associated with the Citizen Corps Application and Database includes:

- Administrator – has access to all information within the Application and Database.
- National – has access to all Council and CERT information.
- Regional – has access to state and local Councils and CERTs information in a specific region.
- State – has access to local Councils and CERTs information in a specific state.
- Local – has access to specific Council or CERT information.

A user group assignment is established by the high-level group user. For instance, a regional user can designate a state Council or CERT within his/her geographical area of responsibility as a state user group member. Within each user group, a user is assigned certain privileges. The following privileges are associated with each user group:

- Send email – allowed to send emails to subscribers within an assigned area.

- Manage users – allowed to add, edit, and delete users to one user group below the user in the designated area.
- Manage Councils/CERTs – allowed to create, approve, and delete Councils and CERTs in the designated area.
- View reports – allowed to view statistical reports.

FEMA staff members with assigned roles within the system are vetted through the System Owner or his or her designee. Assignment is based on need-to-know and operational needs. Additionally, the system's Information System Security Officer (ISSO) has access to the system to ensure security protocols are in place to prevent unauthorized access to the application and database.

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 DHS and outside?

Any MOU or Information Sharing and Access Agreement (ISAA) is reviewed by the System Steward, and will be fully vetted through the FEMA IT Security Branch, FEMA Privacy Officer, and Office of Chief Counsel prior to sending to DHS for a formal review.

Responsible Officials

Eric M. Leckey
Privacy Officer
Federal Emergency Management Agency
U.S. Department of Homeland Security

Approval Signature

Original signed and on file at the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security