Consular Task Force

1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

Date PIA was completed: September 25, 2009

Name of system: Consular Task Force

System acronym: CTF

IT Asset Baseline (ITAB) number: 4696

System description:

CTF is a collateral function of the Internet Based Registration System (IBRS), and is used by the Bureau of Consular Affairs, overseas Consular sections, and Consular Task Force volunteers. CTF imports IBRS subject data to have an awareness of any U.S. citizens who may be affected by the crisis. A separate privacy impact assessment (PIA) is published by the Department for IBRS. CTF associates U.S. citizen subject data with that of inquirers ("contacts") and allows overseas posts and the Bureau to maintain an awareness of the subjects' welfare, whereabouts, and needs. CTF is only used when a task force is established to track cases or inquiries about a crisis, or when a situation arises in which other overseas posts or the Department will likely receive multiple requests for assistance or information. CTF helps to keep informed (among others) concerned family members, friends, and members of Congress, who desire the status of the crisis situation and the welfare of affected U.S. citizens overseas. Its major functions are:

- Talking Points permits the task force coordinator to create and maintain informational documents related to the crisis for use by task force personnel in interacting with inquirers.
- Subjects is used to maintain knowledge of U.S. citizens who may be affected by the crisis.
- Contact permits collection of identifying information from a contact.

Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security re-certification

Explanation of modification: Not applicable

Date of previous PIA: April 16, 2008 (incorporated prior in IBRS)

3. Characterization of the Information

The system:

☐ does NOT contain PII.

☒ does contain PII.

What elements of PII are collected and maintained by the system? What are the sources of the information?

Information about subject U.S. citizens overseas who may be affected by a crisis is imported from IBRS. Information about individuals than U.S. citizens may be collected in the process of providing services. For example, information about a relative, contact, or service provider, who may not be a U.S. citizen, may be collected during the process of providing services to U.S. citizens overseas.

Information about a Consular employee, such as their assigned computer user name, is collected and stored with the applicant's record as it relates to the auditing of actions taken during the processing of the applicant's service request.

Information collected by CTF staff includes information about a crisis and facts relevant to a U.S. citizen who may be affected by the crisis; information about other individuals (either family or affiliation) related to the U.S. citizen; and information about a concerned relation (i.e., contact) who inquires about the U.S. citizen. The following information forms the basis for providing services in CTF:

- Subject U.S. citizen's last name
- Subject U.S. citizen's gender
- Subject U.S. citizen's last known whereabouts
- Name of the crisis event
- Beginning date of crisis event
- Talking points used to read to inquiring contacts

How is the information collected?

Information is recorded in CTF by CTF staff and managers through their direct interactions with a U.S. citizen or associated contacts.

Why is the information collected and maintained?

The minimum information required for CTF staff to provide statutorily mandated services is collected and maintained in CTF.

How will the information be checked for accuracy?

CTF case workers verify information accuracy during the course of their interaction with the subject U.S. citizens and authorized contacts. The crisis event is marked as inactive in CTF when the event is over, indicating the end of the useful life of all related information.

What specific legal authorities, arrangements, and/or agreements define the collection of information?

22 U.S.C. 2715 provides that in the case of a major disaster or incident abroad which affects the health and safety of U.S. citizens of the United States residing or traveling abroad, the Secretary of State shall provide prompt and thorough notification of all appropriate information concerning such disaster or incident and its effect on United States citizens to the next-of-kin of such individuals.

Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The elements of personal information collected about a U.S. citizen or any related contacts are limited to the extent that any potential harm from its exposure or misuse is considered negligible.

4. Uses of the Information

Describe all uses of the information.

The information in CTF is used only to monitor a crisis event and maintain an awareness of any U.S. citizens affected by the crisis. Consular staff can produce reports from CTF to assist in those uses.

What types of methods are used to analyze the data? What new information may be produced?

No new or previously unavailable personal data is created by means of derivation or aggregation.

If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

CTF does not use or incorporate information of these kinds.

Is the system a contractor used and owned system?

No. CTF is operated by the Department of State.

Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Policies and procedures governing the disclosure of U.S. citizen information are specified in the Foreign Affairs Manual. These policies and procedures mitigate against unauthorized uses of the information.

5. Retention

How long is information retained?

All information related to a particular crisis is marked as inactive in CTF when the event is over. Thereafter the information is not used by Consular staff. The disposition schedule for U.S. citizen records in CTF is contained in Department Records Disposition Schedule, Chapter 15, OCS Records.

Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Information about a past crisis is not accessed or edited once the crisis has been marked inactive. Privacy risk from any extended retention of the data is considered negligible.

6. Internal Sharing and Disclosure

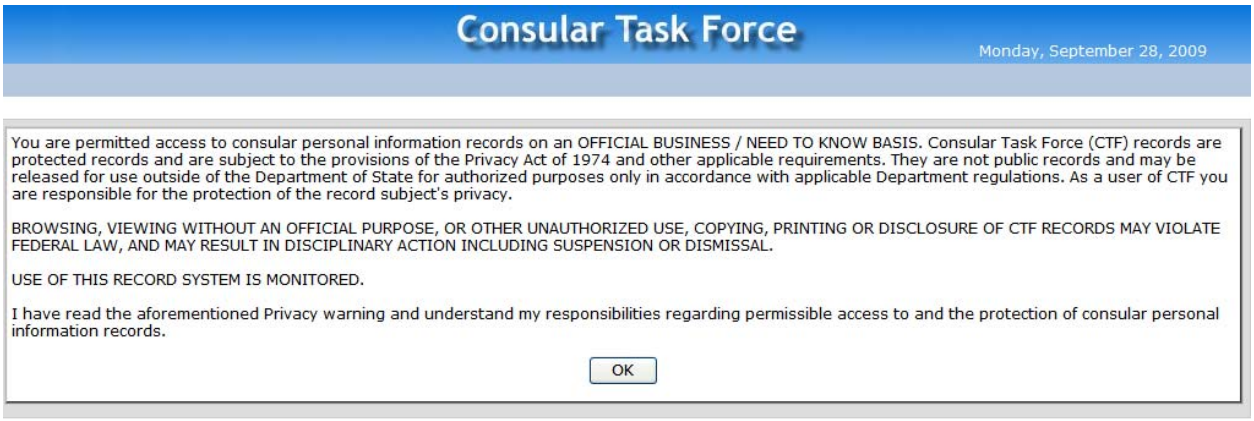
With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

CTF is accessed by the following categories of Department of State staff:

- Consular staff at overseas posts
- Domestic staff of the Bureau of Consular Affairs
- CTF staff and their managers

How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

All levels of access granted to task force staff are based on the concepts of least privilege and separation of duties. Information is shared by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. Consular staffs with access to CTF are presented with the following warning banner that describes the permissible use of the system.



Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

Personal information is shared solely within the Bureau of Consular Affairs among cleared employees with role-based access to the data. Sharing is done so via secure transmission methods. As such, the privacy risk from internal sharing is negligible.

7. External Sharing and Disclosure

With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

No agencies external to the Department of State have access to CTF.

How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Not Applicable

Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

CTF data is not shared with external sources; consequently, risk is negligible.

8. Notice

The system:

☒ constitutes a system of records covered by the Privacy Act.

(Reference Department of State Privacy Act System of Records State-05, Overseas Citizens Services Records)

☐ does not constitute a system of records covered by the Privacy Act.

Is notice provided to the individual prior to collection of their information?

Information about a U.S. citizen abroad who may be affected by a crisis is collected and maintained in IBRS, a collateral system. The Department publishes a separate PIA for IBRS that describes the notice provided by it to U.S. citizens who register.

Do individuals have the opportunity and/or right to decline to provide information?

Information about a U.S. citizen abroad who may be affected by a crisis is collected and maintained in IBRS, a collateral system. The Department publishes a separate PIA for IBRS that describes registrant options under IBRS.

Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Information about a U.S. citizen abroad who may be affected by a crisis is collected and maintained in IBRS, a collateral system. The Department publishes a separate PIA for IBRS that describes the consent options under IBRS.

Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The notice and consent mechanisms at point of collection offered to individuals are reasonable and adequate in relation to the system's purpose and uses. Therefore, this category of privacy risk is considered negligible.

9. Notification and Redress

What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

U.S. citizen subject information used by CTF is imported from IBRS. IBRS registrants must create a user account and logon in order to enter their information. They can then use their account logon information to gain access to their information to make changes and updates.

Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

U.S. citizen subject information used by CTF is imported from IBRS. Because IBRS is Privacy Act-covered, formal procedures for notification and redress exist and are published in the aforementioned Privacy Act System of Records Notice. Therefore, this category of privacy risk is appropriately mitigated.

10. Controls on Access

What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Internal access to CTF is limited to authorized Consular Affairs domestic and overseas staff having a need for the system in the performance of their official duties. All authorized users maintain a security clearance level at least commensurate with public trust positions. To access the system, the individual must first be an authorized user of the Department's unclassified computer network. Access to CTF requires a unique user account assigned by Consular Affairs.

What privacy orientation or training for the system is provided authorized users?

All internal Department personnel accessing CTF are required to receive security awareness briefings administered by the Bureau of Diplomatic Security and by Consular Affairs. Both presentations require signed acknowledgement of rules of behavior and include segments covering appropriate system usage and formal statements on the rules of behavior regarding Department computer systems.

Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Adequate controls to limit access and to regulate the behavior of authorized users are implemented in CTF. Therefore, this category of privacy risk is negligible. Access control lists, which define who can access the system and at what privilege level, are regularly reviewed; and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a user performed – or attempted to perform – on an information system.) As a result of these actions, the residual risk is low.

11. Technologies

What technologies are used in the system that involve privacy risk?

The system uses standard, commercially-available software products residing on a government-operated computing platforms not shared by other business applications or technologies. There are no technologies used which employ commonly identified vulnerabilities that might cause an elevation of overall privacy risks.

Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

The system does not use any technologies that are known to contain vulnerabilities that might cause undue privacy risk.

12. Security

What is the security certification and accreditation (C&A) status of the system?

CTF is within the accreditation boundary of the collateral system IBRS. Its certification and accreditation is conducted as part of that for IBRS. The Department of State operates IBRS (and CTF) in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls. The Department performs monitoring, testing, and evaluation of security controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act provision for the triennial recertification of this system, its most recent date of authorization to operate was August, 2007.