AFFIRST Contact Us

OMB CONTROL NUMBER: 0701-0070 OMB EXPIRATION DATE: 12/31/2024

## **Agency Disclosure Notice**

The public reporting burden for this collection of information, 0701-0070, is estimated to average 15 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or burden reduction suggestions to the Department of Defense, Washington Headquarters Services, at whs.mc-alex.esd.mbx.dd-dod-information-collections@mail.mil. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

## Site Login Disclaimer

Authority: 10 United States Code (U.S.C.) 8013, Secretary of the Air Force: powers and duties; delegation by; as implemented by Air Force Instruction 36-3009, Military and Family Readiness Centers; and Executive Order (E.O.) 9397 (Social Security Number - SSN), as amended.

**Purpose:** This system is a web-based application operated by the U.S. Air Force. It is used to maintain a record of customer service data determining the effectiveness of Military and Family Readiness Center (M&FRC) activities and services and provide reports reflecting impact of services on mission and family readiness to leadership. Also used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness, and conducting research.

Routine Use: Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

Data Breach Remediation Purposes Routine Use: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Disclosure: User disclosure of PII is voluntary. However, failure to furnish requested information may result in limited services being provided due to lack of requested information.

System of Records Notice: F036 AFPC Z - Air Force Family Integrated Results and Statistical Tracking (AFFIRST) (April 09, 2014, 79 FR 19592)

User Consent to Collection and Disclosure of Personally Identifiable Information (PII): AFFIRST collects Personally Identifiable Information (PII). By using this system, the user consents to the collection, use, maintenance, dissemination and retention of PII. All PII collected, used, maintained and retained by AFFIRST is used only for the purpose of providing, documenting and reporting M&FRC services delivery information. PII may be viewed by all roles involved in the stated purposes above, including system administrators and software developers within the capacity of troubleshooting and issue resolution. All PII is safeguarded in a manner consistent with the NIST.5P.800-53r4 and DoD Directive 5400.11, Privacy Program. Public disclosure of PII is in accordance with the Privacy Act of 1974.

AFFIRST Contact Us



## Welcome!

Log in with your Common Access Card

Log in with your CAC

## Mandatory notice and consent provisions for all DOD information system user agreements:

By accessing this application, you acknowledge and consent that you access Department of Defense (DOD) information systems.

You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.

You consent to the following conditions:

The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personal misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

At any time, the U.S. Government may inspect and seize data stored on this information system. Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

This information system includes security measures (e.g. authentication and access controls) to protect U.S. Government interests – not for your personal benefit or privacy.

Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching, or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operations, protection, or defense, or for communications security. This includes all communications.

The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and ata is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

Whether any particular communication or data qualifies for protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DOD direction. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

