Transmittal No. 11-22

Notice of Proposed Issuance of Letter of Offer
Pursuant to Section 36(b)(1)
of the Arms Export Control Act

Annex
Item No. vii

(vii) Sensitivity of Technology:

1. The AIM-120C-7 Advanced Medium Range Air-to-Air Missile (AMRAAM) is a new generation air-to-air missile. The AIM-120C-7 AMRAAM hardware, including the missile guidance section, is classified Confidential. State-of-the-art technology is used in the missile to provide it with unique beyond-visual-range capability. Significant AIM-120C-7 features include a target detection device with embedded electronic countermeasures, an electronics unit within the guidance section that performs all radar signal processing, mid-course and terminal guidance, flight control, target detection and warhead burst point determination. Anti-tampering security measures have been incorporated into the AIM-120C-7 to prevent exploitation of the AMRAAM software.

2. The AIM-120C-7 Air Vehicle-Instrumentation is an instrumented version of the missile where the warhead is replaced with a telemetry unit to capture missile data parameters during missile live-fire flight testing.

3. If a technologically advanced adversary were to obtain knowledge of the specific hardware and software elements, the information could be used to develop countermeasures which might reduce weapon system effectiveness or be used in the development of a system with similar or advanced capabilities.

[FR Doc. 2011–14942 Filed 6–15–11; 8:45 am]
**BILLING CODE 5001–06–C**

## DEPARTMENT OF DEFENSE

### Office of the Secretary

### Reserve Forces Policy Board (RFPB)

**AGENCY:** Department of Defense, Office of the Secretary of Defense Reserve Forces Policy Board.

**ACTION:** Notice of Advisory Committee meeting.

**SUMMARY:** Pursuant to the Federal Advisory Committee Act of 1972 (5 U.S.C. Appendix, as amended), the Sunshine in the Government Act of 1976 (5 U.S.C. 552b, as amended), and 41 CFR 102–3.150, the Department of Defense announces the following Federal advisory committee meeting of the Reserve Forces Policy Board (RFPB):

**DATES:** Tuesday, July 26, 2011 from 7:30 a.m. to 4:30 p.m. and Wednesday, July 27, 2011 from 7:30 a.m. to 4:30 p.m.

**ADDRESSES:** Meeting address is Pentagon, Conference Room 3E863, Arlington, VA. Mailing address is Reserve Forces Policy Board, 7300 Defense Pentagon, Washington, DC 20301–7300.

**FOR FURTHER INFORMATION CONTACT:** Lt. Col. Julie A. Small, Designated Federal Officer, (703) 697–4486 (Voice), (703) 693–5371 (Facsimile), RFPB@osd.mil. Mailing address is Reserve Forces Policy Board, 7300 Defense Pentagon, Washington, DC 20301–7300. Web site: http://ra.defense.gov/rfpb/.

**SUPPLEMENTARY INFORMATION:**

*Purpose of the Meeting:* An open meeting of the Reserve Forces Policy Board.

*Agenda:* Total Force Readiness, Care for Our People, and Culture of Relevance, Effectiveness, and Efficiency.

*Meeting Accessibility:* Pursuant to 5 U.S.C. 552b, as amended, and 41 CFR 102–3.140 through 102–3.165, and the availability of space, this meeting is open to the public. To request a seat, contact the Designated Federal Officer not later than 06/27/11 at 703–697–4486, or by e-mail, *RFPB@osd.mil.*

*Written Statements:* Pursuant to 41 CFR 102–3.105(j) and 102–3.140, the public or interested organizations may submit written statements to the membership of the Reserve Forces Policy Board at any time or in response to the stated agenda of a planned meeting. Written statements should be submitted to the Reserve Forces Policy Board's Designated Federal Officer. The Designated Federal Officer's contact information can be obtained from the GSA's FACA Database—*https://www.fido.gov/facadatabase/public.asp.*

Written statements that do not pertain to a scheduled meeting of the Reserve Forces Policy Board may be submitted at any time. However, if individual comments pertain to a specific topic being discussed at a planned meeting then these statements must be submitted no later than five business days prior to the meeting in question. The Designated Federal Officer will review all submitted written statements and provide copies to all the committee members.

Dated: June 8, 2011.

**Aaron Siegel,**

*Alternate OSD Federal Register Liaison Officer, Department of Defense.*

[FR Doc. 2011–14936 Filed 6–15–11; 8:45 am]
**BILLING CODE 5001–06–P**

## DEPARTMENT OF DEFENSE

### Office of the Secretary

**[Docket ID: DOD–2011–OS–0067]**

### Privacy Act of 1974; System of Records

**AGENCY:** Defense Intelligence Agency, DoD.

**ACTION:** Notice to alter a system of records.

**SUMMARY:** The Defense Intelligence Agency is proposing to alter a system to its existing inventory of records systems subject to the Privacy Act of 1974, (5 U.S.C. 552a), as amended.

**DATES:** This proposed action will be effective further notice on July 18, 2011 unless comments are received which in a contrary.

**ADDRESSES:** You may submit comments, identified by docket number and/ Regulatory Information Number (RIN) and title, by any of the following methods:

* *Federal Rulemaking Portal: http://www.regulations.gov*.

Follow the instructions for submitting comments.

* *Mail:* Federal Docket Management System Office, 1160 Defense Pentagon, Washington, DC 20301–1160.

*Instructions:* All submissions received must include the agency name and docket number or Regulatory Information Number (RIN) for this **Federal Register** document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at *http://www.regulations.gov* as they are received without change, including any personal identifiers or contact information.

**FOR FURTHER INFORMATION CONTACT:** Ms. Theresa Lowery, Defense Intelligence Agency, DAN 1–C, 600 McDill Blvd., Washington, DC 20340–0001 or by phone at (202) 231–1193.

**SUPPLEMENTARY INFORMATION:** The Defense Intelligence Agency system of records notices subject to the Privacy Act of 1974, (5 U.S.C. 552a), as amended, have been published in the Federal Register and are available from the address in **FOR FURTHER INFORMATION CONTACT**.

The proposed system report, as required by 5 U.S.C. 552a of the Privacy Act of 1974, as amended, was submitted on June 8, 2011 to the House Committee on Oversight and Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A–130, ''Federal Agency Responsibilities for Maintaining Records About Individuals, ''dated February 8, 1996 (February 20, 1996, 61 FR 6427).

Dated: June 9, 2011.

**Aaron Siegel,**

*Alternate OSD Federal Register Liaison Officer, Department of Defense.*

**LDIA 0660**

Security Files (July 24, 2006, 71 FR 41784)

* * * * *

**CHANGES:**

**SYSTEM NAME:**

Delete entry and replace with ''Security and Counterintelligence Records''.

* * * * *

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

Delete entry and replace with ''Current and former Defense Intelligence Agency (DIA) civilian, military and contractor personnel, nominees for employment with DIA, all persons with access to DIA facilities and infrastructure, all persons under the security cognizance of DIA. Persons about whom other U.S. government agencies have requested investigative assistance from DIA as part of lawful investigations by their agency. Individuals identified as the result of an administrative, security and/or investigative function who could pose a threat to DIA operations, data, personnel, facilities and systems.''

**CATEGORIES OF RECORDS IN THE SYSTEM:**

Delete entry and replace with ''Personnel: Name, date and place of birth, Social Security Number (SSN), gender, race, home address, family and dependent information, biometric data, medical/psychological information, financial, employment, training records, test results and education history, statements of personal history.

Administrative: Case control number, forms, documents and correspondence relating to security files, personnel security, investigative and employment records, personnel security functions, nomination notices, indoctrination/ debriefing memoranda, secrecy and nondisclosure agreements, certificates of clearance.

Adjudication memoranda and supporting documentation, in-house investigations, security violations, security threats and incidents, investigations and inquiries of criminal and counterintelligence matters, investigative referrals, counterintelligence reporting, foreign travel, foreign contacts, identification badge records, retrieval indices, clearance status records, facility and access control records.''

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

Delete entry and replace with ''National Security Act of 1947; Executive Order 12333, United States Intelligence Activities; DoDD 5105.21, Defense Intelligence Agency; DoDI 5240.06, Counterintelligence Awareness, Briefing, and Reporting Programs; DoDI 5200.08, Security of DoD Installations and Resources; DoD 5200.2.R, Personnel Security Program; DIA Directive 3020.400, DIA Critical Infrastructure Program; Intelligence Community Directive (ICD) 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Special Compartmented Information and Other Controlled Access Program Information; DIA Manual 50–8, Personnel Security Program; DIA Manual 50–14, Security Investigations; DIA Regulation 50–17, Reporting Foreign Contact and Foreign Travel; DIA Instruction 5200.002, Credibility Assessment Program and E.O. 9397 (SSN), as amended.''

**PURPOSE(S):**

Delete entry and replace with ''The system will manage records used to accomplish security and counterintelligence functions. Information is used to comply with regulatory requirements related to initial and continued employment, to determine eligibility for access to classified information, to protect the agency's operations, data, personnel, facilities and systems (by using administrative, security and investigative functions to detect actual or potential threats and risks) and to document training and education''.

* * * * *

**STORAGE:**

Delete entry and replace with ''Paper and Electronic storage media''.

**RETRIEVABILITY:**

Delete entry and replace with ''By last name, Social Security Number (SSN), and applicable case control number''.

**SAFEGUARDS:**

Delete entry and replace with ''Records are stored in office buildings protected by guards, controlled screenings, use of visitor registers, electronic access, and/or locks. Access to records is limited to individuals who are properly screened and cleared on a need-to-know basis in the performance of their duties. Passwords and User IDs are used to control access to the system data, and procedures are in place to deter and detect browsing and unauthorized access. Physical and electronic access are limited to persons responsible for servicing and authorized to use the system''.

**RETENTION AND DISPOSAL:**

Delete entry and replace with ''Security Files: Personnel Security Records. Case files documenting the processing of investigations on Federal employees or applicants for Federal employment, whether or not a security clearance is granted, and other persons, such as those performing work for a Federal agency under contract, who require an approval before having access to Government facilities or to sensitive data. These files include questionnaires, summaries of reports prepared by the

investigating agency, and other records reflecting the processing of the investigation and the status of the clearance, exclusive of copies of investigative reports furnished by the investigating agency. Temporary-Destroy upon notification of death or 5 years after separation or transfer of employee or no later than 5 years after contract relationship expires.

Security Files: Polygraph examinations, favorable examinations; Temporary-Destroy 90 days. Unfavorable Examinations; examinations considered as part of an investigation action necessary for security adjudicative purposes and includes the Medical/Psychiatric Condition Statement-Temporary-Destroy when 15 years old.

Medical and Psychiatric Condition Statement (Favorable), Temporary-Destroy when 1 year old; (Unfavorable), Temporary-Destroy when 15 years old.

Examinations considered records of major significance, congressional interest, national security or upon which significant action was taken (trial, courts-martial, employment termination). PERMANENT—Offer to National Archives and Records Administration (NARA) when 25–30 years old. Final disposition determinations of individual cases are made by NARA.

Security Violations: Temporary-Destroy 5 years after close of case. Files referred for prosecution determination; Temporary-Destroy 3 years after close of case.

Orientation and Training: Temporary-Destroy when no longer required for current operations (documents reflecting training, security orientation, and compliance with security regulations).

Non-Disclosure Agreements: Temporary-Destroy when 70 years old.

Logs and Registers: Temporary-Destroy 2 years after final entry.''

**SYSTEM MANAGER(S) AND ADDRESS:**

Delete entry and replace with ''Counterintelligence and Security Office, Defense Intelligence Agency, 200 MacDill Blvd, Washington DC 20340–5100''.

**NOTIFICATION PROCEDURE:**

Delete entry and replace with ''Individuals seeking to determine whether information about themselves is contained in this system of records should address written inquiries to the DIA Freedom of Information Office (DAN–1A), Defense Intelligence Agency, 200 MacDill Blvd, Washington, DC 20340–5100.

Request should contain the individual's full name, current address, and telephone number''.

**RECORD ACCESS PROCEDURES:**

Delete entry and replace with ''Individuals seeking access to information about themselves, contained in this system of records, should address written inquiries to the DIA Freedom of Information Office (DAN–1A), 200 MacDill Blvd, Washington, DC 20340–5100.

Request should contain the individual's full name, current address, and telephone number''.

**CONTESTING RECORD PROCEDURES:**

Delete entry and replace with ''DIA's rules for accessing records, for contesting contents and appealing initial agency determinations are published in DIA Instruction 5400.001 ''Defense Intelligence Agency Privacy Program''; or may be obtained from the system manager''.

**RECORD SOURCE CATEGORIES:**

Delete entry and replace with ''Subject individuals, agency and other government officials as well as open source information''.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

Delete entry and replace with ''Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C 552a(j)(2), may be exempt pursuant to 5 U.S.C 552(k)(2). However, if an individual is denied any right, privilege, or benefit for which he would otherwise be entitled by Federal law or which he would otherwise be eligible, as a result of maintenance of the information, the individual will be provided access to the information except to the extent that disclosure would reveal the identity of a confidential source. This exemption provides limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(k)(5) Investigatory material complied solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information but only to the extent such material would reveal the identity of a confidential source.

(k)(6) Testing or examination material used to determine individual qualifications for appointment or promotion in the Federal or military service, if the disclosure of such material would compromise the objectivity or fairness of the test or examination process.

An exemption rule for this system has been promulgated in accordance with the requirements of 5 U.S.C 553(b)(1),(2), and (3), (c) and (e) and published in 32 CFR part 319''.

* * * * *

**LDIA 0660**

**SYSTEM NAME:**

Security and Counterintelligence Records.

**SYSTEM LOCATION:**

Defense Intelligence Agency, 200 MacDill Boulevard, Washington, DC 20304–5100.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

Current and former Defense Intelligence Agency (DIA) civilian, military and contractor personnel, nominees for employment with DIA, all persons with access to DIA facilities and infrastructure, all persons under the security cognizance of DIA. Persons about whom other U.S. government agencies have requested investigative assistance from DIA as part of lawful investigations by their agency. Individuals identified as the result of an administrative, security and/or investigative function who could pose a threat to DIA operations, data, personnel, facilities and systems.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

Personnel: Name, date and place of birth, Social Security Number (SSN), gender, race, home address, family and dependent information, biometric data, medical/psychological information, financial, employment, training records, test results and education history, statements of personal history.

Administrative: Case control number, forms, documents and correspondence relating to security files, personnel security, investigative and employment records, personnel security functions, nomination notices, indoctrination/debriefing memoranda, secrecy and nondisclosure agreements, certificates of clearance.

Adjudication memoranda and supporting documentation, in-house investigations, security violations, security threats and incidents, investigations and inquiries of criminal and counterintelligence matters, investigative referrals, counterintelligence reporting, foreign travel, foreign contacts, identification badge records, retrieval indices, clearance status records, facility and access control records.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:**

National Security Act of 1947; Executive Order 12333; United States

Intelligence Activities; DoDD 5105.21, Defense Intelligence Agency; DoDI 5240.06, Counterintelligence Awareness, Briefing, and Reporting Programs; DoDI 5200.08, Security of DoD Installations and Resources; DoD 5200.2.R, Personnel Security Program; DIA Directive 3020.400, DIA Critical Infrastructure Program; Intelligence Community Directive (ICD) 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Special Compartmented Information and Other Controlled Access Program Information; DIA Manual 50–8, Personnel Security Program; DIA Manual 50–14, Security Investigations; DIA Regulation 50–17, Reporting Foreign Contact and Foreign Travel; DIA Instruction 5200.002, Credibility Assessment Program and E.O. 9397 (SSN), as amended.

**PURPOSE(S):**

The system will manage records used to accomplish security and counterintelligence functions. Information is used to comply with regulatory requirements related to initial and continued employment, to determine eligibility for access to classified information, to protect the agency's operations, data, personnel, facilities and systems (by using administrative, security and investigative functions to detect actual or potential threats and risks) and to document training and education.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:**

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, these records contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

Information may be disclosed to other Federal agencies, state and local governments, as may have an official need for such information and agree to apply appropriate safeguards to protect the data in a manner consistent with the conditions or expectations under which the information was provided, collected or obtained.

The DoD 'Blanket Routine Uses' set forth at the beginning of the Defense Intelligence Agency's compilation of systems records notices apply to this system.

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

**STORAGE:**

Paper and Electronic storage media.

**RETRIEVABILITY:**

By last name, Social Security Number (SSN), and applicable case control number.

**SAFEGUARDS:**

Records are stored in office buildings protected by guards, controlled screenings, use of visitor registers, electronic access, and/or locks. Access to records is limited to individuals who are properly screened and cleared on a need-to-know basis in the performance of their duties. Passwords and User IDs are used to control access to the system data, and procedures are in place to deter and detect browsing and unauthorized access. Physical and electronic access are limited to persons responsible for servicing and authorized to use the system.

**RETENTION AND DISPOSAL:**

Security Files: Personnel Security Records. Case files documenting the processing of investigations on Federal employees or applicants for Federal employment, whether or not a security clearance is granted, and other persons, such as those performing work for a Federal agency under contract, who require an approval before having access to Government facilities or to sensitive data. These files include questionnaires, summaries of reports prepared by the investigating agency, and other records reflecting the processing of the investigation and the status of the clearance, exclusive of copies of investigative reports furnished by the investigating agency; Temporary-Destroy upon notification of death or 5 years after separation or transfer of employee or no later than 5 years after contract relationship expires.

Security Files: Polygraph examinations, favorable examinations; Temporary-Destroy 90 days. Unfavorable Examinations; examinations considered as part of an investigation action necessary for security adjudicative purposes and includes the Medical/Psychiatric Condition Statement-Temporary-Destroy when 15 years old.

Medical and Psychiatric Condition Statement (Favorable), Temporary-Destroy when 1 year old; (Unfavorable), Temporary-Destroy when 15 years old.

Examinations considered records of major significance, congressional interest, national security or upon which significant action was taken (trial, courts-martial, employment termination). PERMANENT—Offer to National Archives and Records Administration (NARA) when 25–30 years old. Final disposition determinations of individual cases are made by NARA.

Security Violations: Temporary-Destroy 5 years after close of case. Files referred for prosecution determination; Temporary- Destroy 3 years after close of case.

Orientation and Training: Temporary-Destroy when no longer required for current operations (documents reflecting training, security orientation, and compliance with security regulations).

Non-Disclosure Agreements: Temporary—Destroy when 70 years old.

Logs and Registers: Temporary-Destroy 2 years after final entry.

**SYSTEM MANAGER(S) AND ADDRESS:**

Counterintelligence and Security Office, Defense Intelligence Agency, 200 MacDill Blvd., Washington, DC 20340–5100.

**NOTIFICATION PROCEDURE:**

Individuals seeking to determine whether information about themselves is contained in this system of records should address written inquiries to the DIA Freedom of Information Office (DAN–1A), Defense Intelligence Agency, 200 MacDill Blvd, Washington, DC 20340–5100.

Request should contain the individual's full name, current address, and telephone number.

**RECORD ACCESS PROCEDURES:**

Individuals seeking access to information about themselves, contained in this system of records, should address written inquiries to the DIA Freedom of Information Office (DAN–1A), 200 MacDill Blvd., Washington, DC 20340–5100.

Request should contain the individual's full name, current address, and telephone number.

**CONTESTING RECORD PROCEDURES:**

DIA's rules for accessing records, for contesting contents and appealing initial agency determinations are published in DIA Instruction 5400.001 ''Defense Intelligence Agency Privacy Program''; or may be obtained from the system manager.

**RECORD SOURCE CATEGORIES:**

Subject individuals, agency and other government officials as well as open source information.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

Investigatory material compiled for law enforcement purposes, other than material within the scope of subsection 5 U.S.C 552a(j)(2), may be exempt pursuant to 5 U.S.C 552(k)(2). However, if an individual is denied any right,

privilege, or benefit for which he would otherwise be entitled by Federal law or which he would otherwise be eligible, as a result of maintenance of the information, the individual will be provided access to the information except to the extent that disclosure would reveal the identity of a confidential source. This exemption provides limited protection of investigative reports maintained in a system of records used in personnel or administrative actions.

(k)(5) Investigatory material complied solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information but only to the extent such material would reveal the identity of a confidential source.

(k)(6) Testing or examination material used to determine individual qualifications for appointment or promotion in the Federal or military service, if the disclosure of such material would compromise the objectivity or fairness of the test or examination process.

An exemption rule for this system has been promulgated in accordance with the requirements of 5 U.S.C 553(b)(1), (2), and (3), (c) and (e) and published in 32 CFR part 319.

[FR Doc. 2011–14941 Filed 6–15–11; 8:45 am]

BILLING CODE 5001–06–P

## DEPARTMENT OF DEFENSE

### Department of the Air Force

**[Docket ID: USAF–2011–0016]**

### Privacy Act of 1974; System of Records

**AGENCY:** Department of the Air Force, DoD.

**ACTION:** Notice to Add a System of Records.

**SUMMARY:** The Department of the Air Force proposes to add a system of records to its inventory of record systems subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended.

**DATES:** The proposed action will be effective on July 18, 2011 unless comments are received that would result in a contrary determination.

**ADDRESSES:** You may submit comments, identified by dock number and/RIN number and title, by any of the following methods:

* *Federal Rulemaking Portal: http://www.regulations.gov* Follow the instructions for submitting comments.

* *Mail:* Federal Docket Management System Office, 1160 Defense Pentagon, Washington, DC 20301–1160.

*Instructions:* All submissions received must include the agency name and docket number or Regulatory Information Number (RIN) for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at *http://www.regulations.gov* as they are received without change, including any personal identifiers or contact information

**FOR FURTHER INFORMATION CONTACT:** Mr. Charles J. Shedrick, Department of the Air Force Privacy Office, Air Force Privacy Act Office, Office of Warfighting Integration and Chief Information officer, ATTN: SAF/XCPPI, 1800 Air Force Pentagon, Washington DC 20330–1800, or by phone at 703–696–6488.

**SUPPLEMENTARY INFORMATION:** The Department of the Air Force's notices for systems of records subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published in the **Federal Register** and are available from the address in **FOR FURTHER INFORMATION CONTACT**.

The proposed systems reports, as required by 5 U.S.C. 552a(r) of the Privacy Act, were submitted on June 8, 2011 to the House Committee on Oversight and Government Reform, the Senate Committee on Homeland Security and Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A–130, ''Federal Agency Responsibilities for Maintaining Records about Individuals,'' dated February 8, 1996, (February 20, 1996, 61 FR 6427).

Dated: June 8, 2011.

**Aaron Siegel,**

*Alternate OSD Federal Register Liaison Officer, Department of Defense.*

**F036 AFMC L**

**SYSTEM NAME:**

Air Force Integrated Personnel and Pay System (AF–IPPS).

**SYSTEM LOCATION:**

Command, Control, Communications and Computers Enterprise Integration Facility (CEIF), 15 Elgin St., Hanscom Air Force Base, MA 01731–3000.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:**

Active Duty Air Force, Air Force Reserve, and Air National Guard personnel.

**CATEGORIES OF RECORDS IN THE SYSTEM:**

Personal Information: Individual's name, rank/grade, address, date of birth, eye color, height, weight, place of birth, Social Security Number (SSN), and similar personal identifiers for beneficiary/dependant purposes; driver's license number, security clearance level, office location, assigned user name and security questions, local and home of record addresses, phone numbers and emergency contact information.

Personnel Information: Evaluation and review history, enrollment, participation, status and outcome information for personnel programs, service qualification and performance measures, types of orders, accomplishments, skills and competencies, career preferences, contract information related to accession and Oath of Office, enlistment and re-enlistment, and separation information, benefits eligibility, enrollment, designations and status information, Uniform Code of Military Justice (UCMJ) actions summarizing court martial, non-judicial punishments, and similar or related documents. Circumstances of an incident the member was involved in and whether he or she is in an injured, wounded, seriously wounded, or ill duty status from the incident.

Duty related information: Duty station, employment and job related information and history, deployment information, work title, work address and related work contact information (e.g., phone and fax numbers, E-mail address), supervisor's name and related contact information.

Education and training: Graduation dates and locations, highest level of education, other education, training and school information including courses and training completion dates.

Pay Entitlement and Allowances: Pay information including earnings and allowances, additional pay (bonuses, special, and incentive pays), payroll computation, balances and history with associated accounting elements, leave balances and leave history.

Deductions from Pay: Tax information (federal, state and local) based on withholding options, payroll deductions, garnishments, savings bond information including designated owner, deductions, and purchase dates, thrift savings plan participation.

Other pay-related information: Direct deposit information including financial institution name, routing number, and account information.