

requirements of 5 U.S.C. 553 (b) (1), (2), and (3), (c) and (e) and published in 32 CFR part 312. For additional information contact the system manager. [FR Doc. 03-30397 Filed 12-8-03; 8:45 am]

BILLING CODE 5001-06-P

DEPARTMENT OF DEFENSE

Department of the Air Force

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 is proposing to add a system of records notice to its inventory of records systems subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended. The proposed system of records will be exempt to increase its value for law enforcement purposes.

DATES: The actions will be effective on January 8, 2004 unless comments are received that would result in a contrary determination.

ADDRESSES: Send comments to the Air Force FOIA/Privacy Manager, AF-CIO/P, 1155 Air Force Pentagon, Washington, DC 20330-1155.

FOR FURTHER INFORMATION CONTACT: Mrs. Anne P. Rollins at (703) 601-4043.

SUPPLEMENTARY INFORMATION: The Department of the Air Force's record system notices for records systems 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 above.

The proposed system report, as required by 5 U.S.C. 522a(r) of the Privacy Act of 1974, as amended, was submitted on November 17, 2003, to the House Committee on Government Reform, the Senate Committee on 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: November 20, 2003.

Patricia L. Toppings,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

F071 JTF A

SYSTEM NAME:

Computer Network Crime Case System.

SYSTEM LOCATION:

Law Enforcement and Counterintelligence Center, Joint Task Force—Computer Network Operations, 701 South Courthouse Road, Arlington, VA 22204-2164.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Active duty, retired or former military personnel; current, retired and former civilian employees; dependents of military personnel; and other Department of Defense employees and contractors, both current and former; United States citizens in the United States and abroad; legal aliens; and foreign nationals residing in the U.S. and abroad, who are suspected of violating some law, regulation or directive related to computer network crimes.

CATEGORIES OF RECORDS IN THE SYSTEM:

Reports of investigation, statements of individuals, correspondence, and other informational material pertaining to specific law enforcement and counterintelligence investigations of alleged violations of laws, regulations or directives related to computer network crimes. Name(s) or aliases of the subject, group affiliation (if any), civilian or military status, trusted status, and whether or not the individual is a juvenile.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

10 U.S.C. 8013, Secretary of the Air Force; E.O. 10450, Security Requirements for Government Employment; The Inspector General Act of 1978 (Pub. L. 95-452), as amended, and DoD Directive 5106.1 (32 CFR part 376); E.O. 13213, Critical Infrastructure Protection in the Information Age; DoD Instruction O-8530.2 Support to Computer Network Defense; DoD Directive 5240.2, DoD Counterintelligence; DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations not Affiliated with the Department of Defense.

PURPOSE(S):

To identify and assist in prevention and control of computer network crime and related computer network activity within DoD; aid in attribution of criminal activity; and assist in the development of DoD's network defensive posture.

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, these records

or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

To the Central Intelligence Agency, the Federal Bureau of Investigation, and other counterintelligence/intelligence agencies in matters pertaining to hostile intelligence and terrorist activities directed against the U.S., its installations, or personnel.

To Department of Justice officials to determine if judicial or administrative action is warranted.

To the U.S. Immigration and Naturalization Service in criminal matters, or matters pertaining to hostile intelligence and terrorist activities directed against the U.S., its allies, its installations, or personnel.

To defense and trial counsels for use in judicial and administrative actions.

To the U.S. Secret Service in conjunction with the protection of the President, Vice President, and other designated high-ranking officials.

To the Department of State and U.S. embassies overseas to provide criminal information affecting U.S. diplomatic relations with foreign nations.

To foreign law enforcement agencies where information sharing agreements exist in criminal matters, or matters pertaining to hostile intelligence and terrorist activities directed against the U.S., its allies, its installations, or personnel.

The DoD 'Blanket Routine Uses' published at the beginning of the Air Force's compilation of systems of records notices apply to this system.

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

STORAGE:

Maintained on computers and computer output products.

RETRIEVABILITY:

Records are retrieved by name or alias, group affiliation (if any), organization and case number, and/or "key-word" searches based on case information.

SAFEGUARDS:

Records are accessed by custodian of the record system and by person(s) responsible for servicing the record system in performance of their official duties who are properly screened and cleared for need-to-know. Records are stored in an approved automation system, with "password" protection. Records are controlled by personnel screening and are located in an office environment protected by a security alarm system.