

BY ORDER OF THE COMMANDER
OFFUTT AIR FORCE BASE

AIR FORCE INSTRUCTION 33-332



OFFUTT AFB
Supplement

19 OCTOBER 2007

Communications and Information

PRIVACY ACT PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: The official version of this publication is available electronically on the Air Force Portal at:
<https://www.my.af.mil/gcss-af/afp40/USAF/ep/globalTab.do?command=base&channelPageId=1073755344&pageId=681742>; contact the Base Publishing Office for an electronic copy if you lack access.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 55 CS/SCSF

Certified by: 55 CG/CC
(Colonel Boykin B. Jordan Jr.)

Supersedes AFI 33-332_OAFB SUP 1,
26 August 2005

Pages: 14

AFI 33-332 dated 29 Jan 2004, is supplemented as follows: This supplement establishes policies and procedures for compliance and management of the Air Force Privacy Act program. This instruction applies to contractors by contract or other legally binding action, whenever an Air Force contract provides for the operation of a system of records or portion of a system of records to accomplish an Air Force function. Ensure that all records created as a result of processes prescribed in this publication is maintained in accordance with AFMAN 37-123 (will convert to AFMAN 33-363), *Management of Records*, and are disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at <https://afrims.amc.af.mil/>. Contact supporting records managers as required. This publication requires collection and maintenance of information subject to the Privacy Act of 1974. The authority to collect and maintain this information is 5 U.S.C. 552a, *Privacy Act of 1974* and, AFI 33-332, *Privacy Act Program*, 10 U.S.C. 8013 and E.O. 9397 (SSN). System of records notice F033 AF B applies. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. Refer recommended changes and questions about this publication to the Offutt AFB Freedom of Information Act Office (55 CS/SCSF), 201 Lincoln Highway, Suite 206, Offutt AFB NE 68113-2040.

SUMMARY OF CHANGES

This document is substantially revised and must be completely reviewed. This revision updates policy and procedures for reporting of Personally Identifying information, Privacy Act training, use of last four digits for social security numbers, and personal responsibilities at all levels. This revision also updates web site sources for digital training products and information.

1.6.9.1. The 55th Communications Squadron Freedom of Information Act (FOIA) and Privacy Act Office is designated as the base Privacy Act program single point of service for host organizations and units supported by an approved Host-Tenant Support Agreement (HTSA).

1.6.10.3. All Offutt AFB publications, forms, web pages, and unclassified contingency and operations plans will be reviewed and coordinated on by the Privacy Act Officer. The Privacy Act Officer will also conduct random reviews of web pages to ensure information posted meets the requirements of the Privacy Act. The Base Privacy Act Officer will review all new and renewed HTS agreements to determine specific Privacy Act support and services to be provided.

1.6.10.5. Individuals submitting a Privacy Act complaint or request for investigation must do so in writing and provide any evidential documents that support the complaint or request for investigation. The Privacy Act Officer will review and investigate the circumstances for which the complaint/investigation is based and will prepare a written report of validated violations or summary of policy adherence. Complaints or investigations warranting further action will be referred to the Wing Staff Judge Advocate, Civilian Personnel or other applicable office for action. Reporting loss, theft or compromise of personally identifying information (PII) will be accomplished within 48 hours of receiving notification of the occurrence to the Headquarters Air Combat Command (HQ ACC) Privacy Act Office.

1.6.10.6. Privacy Act program compliance reviews will be accomplished on a 24-month cycle and documented by the organization Privacy Act monitor using HQ ACC-developed (and base Privacy Act Officer supplemented) review criteria, to include local Privacy Act compliance criterion. Privacy Act compliance as it relates to official and vital records is also incorporated into the Records Management (RM) staff assistance visit program checklist. The Privacy Act Officer will conduct random program reviews to ensure organizations are adhering to Privacy Act program requirements and following proper procedures when accessing, modifying or extracting PII from approved systems of records as listed at <http://www.dod.mil/privacy/notices>. The checklist can be accessed at <https://afkm.wpafb.af.mil/ASPs/docman/DOCMain.asp?Tab=0&FolderID=OO-SC-AC-40-12&Filter=OO-SC-AC-40>. Follow Privacy Act program review report format found at Attachment 6 (Added).

1.6.11.2. System Managers (SM), Client System Administrators (CSA) or designated Privacy Act monitors are responsible for providing training to assigned organization personnel. The Privacy Act Officer offers a variety of Privacy Act training presentation tools via the 55th Wing FOIA/PA Community of Practice Page at <https://afkm.wpafb.af.mil/ASPs/docman/DOCMain.asp?Tab=0&FolderID=OO-SC-AC-40-12&Filter=OO-SC-AC-40>. The RM Office also incorporates applicable Privacy Act elements into its RM training courses.

1.6.11.3. Each SM and CSA should implement measures of protection for Privacy Act information. Some of these measures are, but are not limited to:

1.6.11.3.1. (Added) Control access to privacy act information based on an "official need to know."

1.6.11.3.2. (Added) Provide storage media that prevents unauthorized access to information.

1.6.11.3.3. (Added) Label external storage media (CD-ROM, diskettes, binders) to clearly identify information contents are subject to the Privacy Act.

1.6.11.3.4. (Added) Provide internal written procedures consistent with Privacy Act policy and approved systems of records notices when processes require use of PII.

1.6.11.3.5. (Added) Conduct periodic risk analysis to identify strengths and weaknesses of system and human resources to which the Privacy Act applies.

1.6.11.3.6. (Added) Ensure locally developed databases that collect Privacy Act information are necessary and are approved through Federal Register channels before being implemented. Develop applicable warning screens to alert users prior to accessing Privacy Act data. See **Attachment 7 (Added)** for instructions on how to develop a Privacy Act splash screen.

1.6.13. (Added) **Group Commander Responsibilities.** Designate a Group level organization primary and alternate Privacy Act Monitor in writing and forward a copy of the designation letter to the Privacy Act office. Groups may elect to appoint squadron level Privacy Act monitors at their option.

1.6.14. (Added) **Squadron Commander Responsibilities.**

1.6.14.1. (Added) Display OAFBVA 33-5, *Privacy Act Monitor*, and OAFBVA 33-6, *Personally Identifying Information Essentials*, in a visible location such as a bulletin board or customer service area.

1.6.14.2. (Added) Ensure that personnel are aware of procedures for reporting loss, theft or compromise of PII and promptly report occurrences within 24 hours of discovery. Prepare and submit notification of PII loss, theft or compromise to affected individuals within 10 working days of the occurrence. Use the sample template as shown in **Attachment 8 (Added)**.

1.6.14.3. (Added) Continuously review information collection practices to ensure social security number (SSN), including last four digits, is only collected when required by written law or policy.

1.6.15. (Added) **Privacy Act Monitor Responsibilities.**

1.6.15.1. (Added) Ensure organization recall rosters, personnel locator lists and similar documents have the required Privacy Act warning statement, and when applicable, the "For Official Use Only" designation incorporated into the document prior to release. Documents which display a Privacy Act warning and/or "For Official Use Only" designation will not be posted on bulletin boards, unrestricted access electronic folders or other method of display that subject the information to unauthorized disclosure.

1.6.15.2. (Added) Ensure electronic storage media displays the applicable Privacy Act warning statement.

1.6.15.3. (Added) Conduct a Privacy Act program review every 24 months, to include access and use of approved systems of records whereby information is entered, accessed or extracted. Examples of approved systems may include but are not limited to the Air-to-Air Weapons System Evaluation Program, Security Forces Management Information System, Air Force Freedom of Information Act Tracking System, or My Biz/Workplace. Use checklist and report format criterion provided by the Base Privacy Act Officer.

1.6.16. (Added) **Individual Responsibilities.**

1.6.16.1. (Added) Protect Privacy Act material when sending documents through official mail channels. Documents should be mailed using the guidelines shown in **Attachment 9 (Added)**. DO NOT place documents containing Privacy Act information in the mail system without taking the proper protective measures for the document.

1.6.16.2. (Added) Ensure hand delivery of Privacy Act documents includes attaching an AF Form 3227, *Privacy Act Cover Sheet*, to the document or placing the document in a mailing container and labeling the container as shown in **Attachment 9 (Added)**. Privacy Act cover sheets or placement of documents in a sealed envelope should be practiced when using in-baskets or distribution boxes as the method of delivery.

1.6.16.3. (Added) Review Privacy Act information stored on internal and external electronic storage devices and delete information that is no longer required. Follow Air Force records disposition standards for documents that are defined as official and/or vital records under provisions of AFI 33-322, *Records Management Program*; and AFI 33-364, *Records Disposition-Procedures and Responsibilities*. Ensure that information stored on internal or external media cannot be altered.

1.6.16.4. (Added) Ensure folders have required access and security permissions established to prevent unauthorized disclosure when filing electronic information subject to the Privacy Act under the standard Air Force electronics records management architecture. Additionally, documents should have alteration protection features enabled.

1.6.16.5. (Added) Restore form templates and other devices used to collect, assemble and create documents to their original blank state. Ensure a "clear" feature is used for information collected on web pages.

1.6.16.6. (Added) Place applicable privacy act warning statement on all memorandums that display and transmit Privacy Act information as shown in **Attachment 9 (Added)**.

1.6.16.7. (Added) Ensure organization developed information collection devices such as worksheets, database input formats or similar devices which require collection of Privacy Act information from an individual, have the applicable Privacy Act statement displayed on the device.

2.1. Obtaining Law Enforcement Records. The 55th Security Forces Squadron provides direct response to Privacy Act requests for incident reports, accidents, traffic tickets, and blotter entries using the provisions of AFI 33-332, and AFI 31-204_OAFB Supplement 1, *Installation Traffic Supervision Code*.

2.3. (Added) Processing Insurance Company Requests for Law Enforcement, Vehicle Accident and Related Traffic Documents and Records.

2.3.1. (Added) Individuals making requests for vehicle accident records can have all pertinent information recorded on the documents as it relates to the claims process. Individual social security numbers and other personally identifying information are not authorized for release. Treat photographs and blotter entries in the same manner as other vehicle accident records.

2.3.2. (Added) Insurance companies representing an individual for the claims process must include a written release consent document from the individual they represent.

2.3.3. (Added) Insurance companies employing the use of insurance clearing house activities to obtain copies of accident reports will only receive the synopsis of the accident, patrolmen worksheet and AF Forms 1168, *Statement of Suspect/Witness/Complainant*, excluding all personally identifying information pertaining to individuals and their vehicles. The blotter entry provides the necessary information when available in the majority of cases.

3.3.4. (Added) Validate the need to have the entire SSN with the policy outlining the requirement to collect, maintain and transmit PII. Follow guidelines shown in **Attachment 9 (Added)** and **Attachment 10 (Added)** when applying "For Official Use Only" designation. The last four digits of an individual's SSN will be protected in the same manner as the entire SSN. Communications will contain the required FOUO designation markings when the last four digits are displayed in the communication.

4.2.3. Offices having specific systems of records responsibility, who provide direct Privacy Act request service to persons making requests for their records, will provide individuals with a written explanation

when their request cannot be processed within the required 10 working days and no later than 20 working days from the original request date. Offices may implement necessary information collection device(s) in order to properly assess and process requests. Information collection devices must have the proper Privacy Act warning or Privacy Act statement if personal identifier information is collected.

4.4.2.4. (Added) Other Medical Requests. Individuals requesting medical records for the purpose of third party liability claims or other litigation will follow the procedures outlined in Title 28 of the *Code Federal Regulations*, AFI 51-502, *Personnel and Government Recovery Claims*, and local policy set forth by the servicing medical facility.

7.3. **Sending Personal Information Over Electronic Mail.** Use the warning statements identified in Attachment 9 (Added) and Attachment 10 (Added) of this supplement when transmitting sensitive information, of which the content is designated as acquisition, legal, medical, Privacy Act, or For Official Use Only. Microsoft Outlook has an "E-mail statement" feature which enables users to select the information type and insert the required warning statement at the beginning of the e-mail. **DO NOT INDISCRIMINATELY USE THESE STATEMENTS.**

8.1. **Evaluating Information Systems for Privacy Act Compliance.** All organizations performing systems development of databases and other computer applications that collect and maintain Privacy Act information, will forward the following information to the Privacy Act Office upon acceptance of the project or initiative to ensure the requirement exist to collect Privacy Act information and that proper information protection measures are in place: Name of project, purpose of collecting and maintaining the data, specific data to be collected, persons or agencies requiring access to the data, method of update (if any), and projected future modifications to application. The Privacy Act Office will determine the need to collect Privacy Act data and whether a Privacy Act assessment is required. Privacy Act assessments will be submitted according to the provisions of AFI 33-332, paragraph A4C.

10.3. **Disposing of Records.** Offutt AFB organizations and supported tenant units may dispose of Privacy Act information in several ways. Material can be hand torn beyond reconstruction and recognition, shredded using an approved office shredder or entering into a fee for service agreement with an authorized commercial vender who is bonded to destroy privacy act and/or For Official Use Only material. Organizations are responsible to ensure that commercial vendors meet the requirements to receive and destroy Privacy Act material. Organizations may only present material residue (already shredded material) for recycling pickup and disposal.

12.1. **Disclosure Considerations.** Organizations will use OAFB Form 1974, *Privacy Act Release*, to record individual consent to release Privacy Act information such as social rosters and similar documents which require individual consent. The form will be retained by the office of record having ownership for the creation of the document or record requiring written consent until individual rescinds it, departs the organization (permanent change of station, retirement, separation, etc.), replaces existing form with an updated form or the information collected for which the consent form was created is discontinued.

13.1.1. (Added) **Documenting Privacy Act Training.** Supervisors will document training in an approved training source document such as the AF Form 623, *OJT Record*; Automated AF Form 971, *Civilian Employee Brief*; or an approved automated training tracking system. Air Force-sponsored training methods such as the Advanced Distributed Learning Service may also serve as a recorded training repository.

13.1.2. (Added) **Frequency of Privacy Act Training.** Privacy Act training is required for all personnel on a yearly basis as part of the continuing effort to prevent loss, theft or compromise of personally identi-

ying information. It is recommended that all airmen and junior officers who are defined as first duty station personnel and first time hire civilians, to include contractors, take the initial Privacy Act training and refresher training thereafter. All other military and civilian personnel should take the refresher training. If an Air Force level standard training module exists, the base level presentations will be available as supplemental training.

13.4.1. Adopted Forms or IMTs. AF Form 623, *OJT Record*; AF Form 971, *Civilian Employee Brief*; and AF Form 1168, *Statement of Suspect/Witness/Complainant*.

13.4.2. Prescribed Forms or IMTs. Offutt AFB Form 1974, *Privacy Act Release*.

13.4.3. (Added) Prescribed Visual Aids. Offutt AFB Visual Aid 33-5, *Privacy Act Monitor*; and Offutt AFB Visual Aid 33-6, *Personally Identifying Information Essentials*.

AFI 31-204_ Offutt AFB Sup 1, *Installation Traffic Supervision Code*

AFI 33-322, *Records Management Program*

AFI 33-332, *Privacy Act Program*

AFI 33-364, *Records Disposition Procedures and Responsibilities*

AFI 51-502, *Personnel and Government Recovery Claims*

Attachment 6 (Added)

PRIVACY ACT PROGRAM REVIEW REPORT FORMAT

REPLY TO ATTN OF: *PRIVACY ACT MONITOR*TO: *ORGANIZATION COMMANDER RECEIVING VISIT*

SUBJECT: Privacy Act Program Review

1. On _____ (*Show date*) a privacy program review was conducted on your organization under the provisions of AFI 33-332, *Privacy Act Program*, and paragraph 1.6.10.6.
2. The purpose of the program review was to assess four basic principles of the Privacy Act Program.
 - a. Specific Approved Systems of Records Employed _____ (*Show specific system(s) name and associated number; i.e. ARMS F011 AF XO A*). Information resource management practices are reviewed as it relates to access, maintenance, disclosure, and transmission of personally identifying information. Review actions should identify any potential for loss, theft, or compromise of information. A review of system disclosure actions determines compliance with procedures for processing requests for information under the Privacy Act and recording required disclosures on the AF Form 771, *Accounting of Disclosures*, or equivalent format.
 - b. Promotion of the Program. Privacy Act program promotion requires that organizations display OAFB Visual Aid 33-5, *Privacy Act Monitor*, and other 33-series Privacy Act visual aids in visible locations such as organization bulletin boards or Orderly Rooms. This provides personnel with a central point of contact to receive assistance on Privacy Act matters.
 - c. Program Preventative Measures. This aspect of the Privacy Act focuses on providing personnel with the necessary training tools to enforce policy and procedures when accessing, maintaining, transmitting, or disposing of Privacy Act information. The prevention element also looks the organization's efforts in collecting only privacy act information that is necessary to conduct official DoD duties.
 - d. Privacy Act Protection Requirements. This aspect of the privacy act focuses on whether privacy act information resources are being protected from unauthorized disclosure to include the proper use of warning statements (includes e-mail, official memorandums, recall rosters internal collection devices), use of AF Form 3227, *Privacy Act Coversheet*, implementation of warning screens for databases containing privacy act information, protection of documents placed in central mail bins, access restrictions to databases and paper based information resources containing Privacy Act information, and proper destruction of Privacy Act information no longer needed for official DoD duties. The protection element also focuses on accountability of privacy act information resources when records and documents are removed by personnel.
3. Each of the three elements is given a risk assessment rating of low, moderate or high.
 - a. Low Risk -- the identified program deficiency does not pose a significant risk for unauthorized disclosure.
 - b. Moderate Risk -- the identified program deficiency, if not corrected, poses a probable risk for unauthorized disclosure of privacy act information. Some requirements are in place to reduce the probability, but other measures are necessary to afford the information maximum protection.

c. High Risk -- the identified program deficiency, if not corrected, would result in the unauthorized use of disclosure of privacy act information if proper methods are not utilized. There are no requirements currently in place to afford information protection when subject to the Privacy Act of 1974.

4. Summarize all deficiencies from checklist items and show the level of risk each deficiency represents.

PRIVACY ACT MONITOR SIGNATURE

Attachment 7 (Added)**DEVELOPING PRIVACY ACT WARNING SPLASH SCREENS FOR THE ACCESS DATA-BASE APPLICATION****Set up for Startup Form:**

- Open the Access Database
- In the small window Under Objects Click > Forms (Ref #1)
- Click > Create Forms in Design view (Ref #2)
- Right-click in the grey area
- Select Toolbox from the list
- Ensure it is displayed
- Click Label on the toolbox to display a text box
- Click in the grey form box to start the text box
- Type in what you want then press enter
- Move the box or resize it at this time.
- Click > File-> Save As
- Type in the name "Startup Form" or whatever

Button Creation:

- Click Command Button on the toolbox
- Click on the form where you want the Close button to be
- A Wizard should pop up asking some questions
- Under Category select Form Operations
- Under Action select Close Form
- When clicked, this button will close the Startup Form
- Click > Next
- Click on TEXT, type in OK, Click Next
- Type a name for the button if you want (not required) Finish
- Save form, close out and reopen
- Test the button
- Close the form

Making the form your startup form:

- In the main database window
- Click > Tools > Startup

- In the Display Form/Page click the Arrow
- Select Startup Form from the menu
- Click OK
- You are now done. There are a few things that you could do to make the startup form more visually appealing.

Form Options:

- Open the form
- Right click on it and select Form Design
- Right click and select Properties
- In the Properties window at the top select the dropdown menu and select Form
- Click On the All tab
- If you would like you can change all or none of the following
 - Scroll bars - Neither
 - Record Selectors - No
 - Navigation Buttons - No
 - Min Max Buttons - None

Attachment 8 (Added)

SAMPLE PRIVACY ACT NOTICE TO INDIVIDUAL OF LOST, COMPROMISED, OR STOLEN PERSONALLY IDENTIFYING INFORMATION (PII)

Organization Commander Mailing Address

Affected Individual Mailing Address

Dear Mr./Ms.

As you know, the Department of the Air Force (HQ USAF) is making concerted efforts to ensure the protection of your privacy.

Unfortunately, we were apprised of a *(possible/ actual loss, theft or compromise)* of your Personally Identifying Information (PII). Specifically, *(identify the personally identifying information that was lost, stolen, or compromised)* was *(lost, stolen, or compromised)* as a result of *(provide circumstance that resulted in the lost, stolen, or compromised personally identifying information)*.

While there is no evidence to suggest that personal data was accessed or misused, it is HQ USAF policy to apprise individuals who may have had personal data *(lost, stolen, or compromised)* so they may steps they feel appropriate to minimize any risk would result from identity theft.

To assist you, we recommend you consider visiting the Federal Trade Commission's (FTC) web site at <http://www.consumer.gov/idtheft> for guidance on possible protective measures and for information on contacting the three major credit bureaus. The FTC urges you to consider immediately placing an initial fraud alert on your credit file. The fraud alert is good for a period of 90 days during which creditors are required to contact you before a new credit card is issued or an existing card changed. The site also provides other valuable information regarding identity theft.

Because HQ USAF takes your protection of your privacy very seriously, it is reviewing its current policies and practices with a view of determining what steps must be taken to preclude similar actions from happening in the future. At a minimum, we will provide additional training regarding personal protection of Personally Identifying Information and *(identify specific measures being taken for the circumstance in this case)*.

Should you have any questions regarding this matter, contact the Base Privacy Act Officer at 402-294-9994 or e-mail offutt.foia@offutt.af.mil. You may also contact the Air Combat Command Privacy Office at 764-757-2265 or e-mail acc.foia@langely.af.mil.

We deeply regret this unfortunate development and apologize for any inconvenience or undue concerns this may cause you.

Sincerely,

Unit Commander Signature

Attachment 9 (Added)**PRIVACY ACT WARNING STATEMENTS FOR OFFICIAL MEMORANDUMS, MAIL CONTAINERS, AND RECALL ROSTERS****A9.1. (Added) Official memorandums:**

A9.1.1. (Added) Place "For Official Use Only" warning at top and bottom of the memorandum if all the information is For Official Use Only.

A9.1.2. (Added) Place (FOUO) next to the applicable paragraphs or label attachments that are designated "FOUO" if only a selected portion of the memorandum is designated as "For Official Use Only."

A9.1.3. (Added) Place the below warning statement as the last paragraph of the memorandum:

"Information contained in this communication is subject to the Privacy Act of 1974 and must be protected from unauthorized disclosure. Any further distribution of this information within DoD must be to those individuals with an official need to know. If this communication is received in error, please notify the originator immediately."

A9.2. (Added) Marking envelopes to mail Privacy Act material.

A9.2.1. (Added) Place this statement on the bottom portion of the mailing envelope:

"To be opened by addressee only." Identify the person to receive the information by name (i.e., ATN: Ms. Jane Doe).

A9.2.2. (Added) Place document in a sealed envelope with the above marking and place inside properly addressed SF 65, when using an SF 65.

A9.3. Recall rosters: Place this privacy act warning at the bottom of the recall roster:

"Privacy Act Statement--Data contained on this communication is for use by authorized personnel and will not be disclosed to any person not otherwise authorized to receive this information IAW AFI 33-332, *Privacy Act Program*; DoD 5400.7R, *DoD Freedom of Information Act*, and DOD 5400.11R, *Privacy Program*. This communication is designated For Official Use Only (FOUO)."

A9.4. Database splash screens: Place this privacy act warning statement within the splash screen:

"This database contains FOR OFFICIAL USE ONLY (FOUO) information that must be protected under the Privacy Act of 1974 (see AFI 33-332). Do not release outside of DoD channels without the consent of the originator's office."

Attachment 10 (Added)

REQUIRED PRIVACY ACT WARNING STATEMENTS FOR E-MAIL

Table A10.1. Privacy Act Warning Statements for E-Mail.

Statement Title	Statement	Circumstance for use	Examples
Acquisitions	“FOR OFFICIAL USE ONLY. This electronic transmission contains trade secrets, or commercial or financial data not intended for disclosure outside government channels and exempt from mandatory disclosure under Freedom of Information Act, 5 U.S.C. 552. Exemption 4 may apply. Do not further distribute this message without the consent of the originator’s office. If you received this message in error, please notify the sender by reply e-mail and delete all copies of this message.”	Use the “Acquisitions” statement if and only if proprietary, privileged, or sensitive information from a private non-government source is included in the electronic mail. <i>NOTE:</i> For more information see Exemption 4 of the Freedom of Information Act.	“The estimated fixed fee from the 8A contractor was \$11.2 million.” “Intel’s proposal features a new chip under an exclusive patent that outperforms the nearest competitor.”
Medical	“FOR OFFICIAL USE ONLY. This electronic transmission contains personal medical information protected by the Privacy Act of 1974 (see AFI 33-332) and the Health Insurance Portability and Accountability Act (HIPAA) (see DoD 6025.18-R) not intended for disclosure outside government channels and exempt from mandatory disclosure under the Freedom of Information Act, 5 U.S.C., 552. Exemption 6 may apply. Do not release outside of DoD channels without the consent of the originator’s office. If you received this message in error, please notify the sender by reply e-mail and delete all copies of message.”	Use the “Medical” statement if and only if information obtained from personal medical records is included in the electronic mail. <i>NOTE:</i> For more information see Exemption 6 of the Freedom of Information Act.	“Airman Jones went to life skills today after stating he’s battling depression.” “Airman Smith was diagnosed with diabetes in 2004 and is being treated at the base hospital.”
For Official Use Only (FOUO)	“FOR OFFICIAL USE ONLY. This electronic transmission contains internal matters that are deliberative in nature and/or are part of the agency decision-making process, both of which are protected from disclosure under the Freedom of Information Act, 5 USC 552. Do not release outside of the DoD channels without advance approval from the sender. If you received this message in error, please notify the sender by reply e-mail and delete all delete all copies of this message.”	Use the “FOUO” statement if and only if information or material is included in the electronic mail that may not be appropriate for public release. <i>NOTE:</i> For more information see Exemption 5 of the Freedom of Information Act.	“The base plans to buy the land immediately east of the airfield to prevent further encroachment.” “The Wing Command Post just released a BSD directing us to go to FPCON B.”

Statement Title	Statement	Circumstance for use	Examples
Privacy Act	<p>"This electronic transmission contains FOR OFFICIAL USE ONLY (FOUO) information that must be protected under the Privacy Act of 1974 (see AFI 33-332). Do not release outside of DoD channels without the consent of the originator's office. If you received this message in error, please notify the sender by reply e-mail and delete all copies of message. (Note: Use FOUO in subject line if partial/full SSN or other personally identifying information is included)</p>	<p>Use the "Privacy Act" statement if and only if information, which if released, would result in a clearly unwarranted invasion of personal privacy. If your e-mail contains a partial/ full SSN or other personally identifying information, the e-mail MUST have FOUO at the beginning of the subject line.</p> <p><i>NOTE:</i> For more information see Exemption 6 of the Freedom of Information Act.</p>	<p>"Per your request, her home number is 000-000-0000 and SSN is 000-00-0000."</p> <p>"Capt Smith has 4 children at home and is going through a divorce."</p>

JAMES J. JONES, Brigadier General, USAF
Commander