

**BY ORDER OF THE COMMANDER
NATIONAL AIR & SPACE
INTELLIGENCE CENTER**

NASIC INSTRUCTION 33-103

2 MARCH 2012



Communications & Information

**NATIONAL AIR & SPACE INTELLIGENCE
CENTER BUSINESS COMMUNICATIONS**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-publishing website at www.e-publishing.af.mil for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: NASIC/SCXS

Certified by: NASIC/SCX
(Gregory J. O'Brien)

Pages: 11

This NASIC instruction implements AFD 33-2, *Information Assurance (IA) Program*, AFI 33-200, *Information Assurance (IA) Management* and AFI 33-119, *Air Force Messaging*. This instruction adds organizational guidance and procedures for using and managing organizational mailboxes, a highly structured environment for using electronic communications e-mail in mass, as well as guidance and procedures for using cellular communications, a mobile messaging tool. This instruction applies to all NASIC civilian and military personnel as well as all Air Force Reserve Command (AFRC) Units and Air National Guard (ANG) Units assigned to NASIC. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Form 847s from the field to NASIC Publications Office (NASIC/SCOK), 4180 Watson Way, Wright-Patterson AFB, OH 45433-5648 (ATTN: Publications/Forms Managers). Maintain records created as a result of the prescribed processes identified in this directory in accordance with (IAW) AFMAN 33-363, *Management of Records*, and dispose of them in IAW the AF Records Disposition Schedule (RDS) found on the Air Force Portal link at <https://www.my.af.mil/afrims/afrims/afrims/rims.cfm>. Contact supporting records managers as required. 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.

SUMMARY OF CHANGES

The title of this instruction changed from NASIC Electronic Organization Mailbox Policy to NASIC Business Communications. This publication updates the Office of Primary Responsibility (OPR) from NASIC/SCOK to NASIC/SCXS. This revised instruction also

updates the use and management of NASIC corporate e-mail distribution lists and establishes responsibilities and procedures for requesting, purchasing, configuring and using government-purchased mobile messaging devices (e.g. Blackberry devices).

1. OVERVIEW.

1.1. When used properly, the distribution of e-mail through official organizational mailboxes will improve NASIC communications effectiveness and efficiency by enabling organizational leaders and their trained delegates and sponsors to control the flow of information and related work. Personnel sending communications through official boxes have greater assurance that e-mails will be read and acted upon promptly and appropriately by the receiving organization. Use of organizational e-mail boxes will reduce the numbers and length of e-mails. Shared access to organizational e-mail accounts will enable efficient filing, retrieving, and appropriate retention of record copies according to established records management practices.

1.2. Mobile messaging devices (e.g. Blackberry) provide great versatility for keeping in touch with the organization but the capability comes with a price. By their very design, as is the case with most wireless electronic devices, their use poses a greater security risk—specifically, greater opportunity for intercept and exploitation—than wired devices. Great care must be exercised when using and maintaining these devices.

1.3. For this instruction, digital certificates, also known as public & private key certificates, are software-based items that use Public Key Infrastructure (PKI) technologies to electronically sign and encrypt e-mail. These software-based certificates (heretofore, referred to as “Soft Certificates”), unlike hardware-based smart cards or tokens (e.g. Common Access Cards (CAC)), are stored on the computer. Because the use of them is to add “trust and security”, it is very important to adhere to all provisions for their use and control. Improper use or control would warrant reporting the event, incident or mismanagement as a security incident.

2. ORGANIZATIONAL MAILBOXES (ORG BOXES).

2.1. Organizational e-mail accounts mailboxes (or Org Boxes) will be used for official taskings, requests for information, organizational appointments, notices regarding recurring staff meetings, organizational invitations, announcements, bulletins and notices.

2.2. IAW AFI 33-119, all Org Boxes on the NIPRNet system that receive For Official Use Only (FOUO), Privacy Act information (PA), Personally Identifiable Information (PII), contract data, export controlled technical data, Operations Security (OPSEC), information specified for encryption by data owners pertaining to individual areas of responsibility or individually identifiable health, payroll, finance, logistics, and foreign government information must have the ability to encrypt/decrypt e-mail.

2.2.1. Sending e-mail that contains the type of information described in Sec 2.2 to organizational mailboxes that do not have Soft Certificates and the ability to encrypt/decrypt the e-mail is strictly prohibited.

2.2.2. “For Official Use Only (FOUO)” is information that has not been given a security classification pursuant to the criteria of an Executive Order, but could cause foreseeable harm if disclosed to unauthorized personnel. It must be protected at the need-to-know.

Additional information concerning protection of For Official Use Only information can be found in DoD Regulation 5400.7/AF Sup1, *Freedom of Information Act Program*.

2.2.3. The NASIC Critical Information Lists provide generalized lists of organizational information that should be considered FOUO and therefore encrypted when sent via e-mail.

2.3. To support encryption requirements, all two and three letter Org Boxes will be issued Soft Certificate.

2.4. Waivers and exceptions must be approved by the NASIC Director of Staff (DS).

2.5. Special Interest Org Boxes will not require encryption capability unless they will receive/send FOUO information. A Special Interest Org Box box is maintained by groups or persons that are not mission-related (e.g. Angel Tree and Summerfest). Establishment of Special Interest Org Boxes must be approved by the NASIC DS.

2.6. Calendar invites (created within organizational mailboxes) do not have the capability to be encrypted. Therefore, invites cannot be sent via e-mail if they contain FOUO information. This includes subject line, body of the message, and attachments.

3. ORGANIZATIONAL MAILBOX (ORG BOX) RESPONSIBILITIES.

3.1. Group Commanders and Directors will appoint a sponsor for all Group/Directorate organizational mailboxes that require encryption/decryption capability. The sponsor's appointment letter will be forwarded to the NASIC Information Assurance (IA) Branch (SCXS). (See sample appointment letter in Attachment 2)

3.2. Group Commanders, Directors and Squadron/Division Chiefs are the owners of their specific Org Box. As such, they direct and oversee all aspects of their assigned Org Boxes, to include:

3.2.1. Monitor and maintain practices and procedures for daily use and shared access of assigned Org Boxes. Org Boxes will be regularly monitored from beginning to end of each shift of duty.

3.2.2. Designate records custodians to maintain the contents of Org Boxes according to established records management procedures.

3.2.3. Determine who is authorized to read, edit, or delete e-mails sent to the Org Box.

3.2.4. Request removal of an Org Box when no longer needed.

3.2.4.1. Org Box removal process will consist of:

3.2.4.1.1. Removal request letter submitted to the NASIC IA Branch (SCXS) with concurrence from the Functional Area Records Manager (FARM). (See sample Org Box removal request letter in Attachment 3)

3.3. Information Assurance Branch (SCXS) will:

3.3.1. Maintain a current list of sponsors and their organizational mailbox.

3.3.2. Provide training, education and oversight.

3.3.3. Annually, conduct an inspection of the use of organizational boxes to ensure sponsors are adhering to the secure operations/control requirements.

3.4. Organizational Mailbox Sponsors will:

- 3.4.1. Be the focal point for Org Boxes,
- 3.4.2. Maintain the list of authorized users that have access to the organizational mailbox (i.e can receive/review/forward encrypted e-mail).
- 3.4.3. Attend program management and operational security training

3.5. Records Managers will:

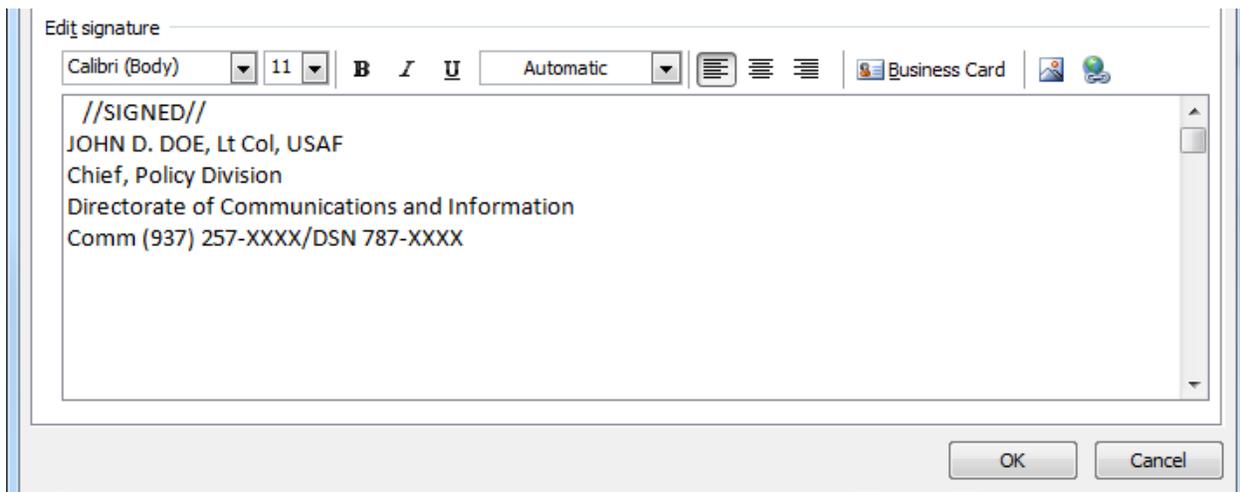
- 3.5.1. Move official e-mail records to the official records repository (e.g. NASIC//O:drive) for proper retention IAW the office file plan and AFMAN 33-363, *Management of Records*.
- 3.5.2. Move e-mails to the Records Center Libraries for further action and collaboration.
- 3.5.3. Certify disposition of all e-mails prior to closure of an Org Box.
- 3.5.4. Monitor Org Box for proper use and protection of FOUO information.

3.6. The Client Services Branch (SCOS), known as Communications Focal Point (CFP) will:

- 3.6.1. Create and delete organizational mailboxes.
- 3.6.2. Add and remove individual access and permissions to organizational mailboxes.

3.7. Signature Elements: All e-mails sent from an organizational mailbox will contain a signature element. The following format will be used for e-mail signature elements:

Figure 3.7. E-mail Signature Element.



4. SHARED DISTRIBUTION LISTS.

4.1. Organizational mailbox owners will review all e-mail destined for multiple organizational boxes. The CFP will own and manage NASIC e-mail distribution lists, including accomplishing full coordination to ensure currency and accuracy. Lists are as follows:

Table 4.1. NASIC Distribution Lists.

NASIC All =	All NASIC personnel
NASIC A =	All 2-Ltr Organization boxes
NASIC B =	All 3-Ltr Organization boxes
NASIC C =	All 4 Ltr Organization boxes

4.2. All NASIC distribution lists may be used by 2-Ltr Organizational account holders and designees. In addition, subordinate distribution lists may be used by parallel level organizations (e.g., any org on Distro List B can use “B” plus “C” but not A). Action officers who wish to use lists above their authority (for example: NASIC All) must forward proposed e-mails through their chain of command to an authorized office. No external personnel may be listed in the distribution lists.

4.3. As the mission dictates, some personnel may be granted authority to use distribution lists above their current level (e.g. a 3-Ltr with NASIC All capability). Use of distribution lists under these circumstances is restricted to For Official Use only. Official Use is directly related to mission accomplishment and includes emergency communications (for example: network system downtimes, building construction status, fire alarm tests, etc.).

5. MOBILE MESSAGING.

5.1. All corporate-sponsored mobile messaging devices (e.g. Blackberry) must be approved by the NASIC Commander.

5.2. All devices are considered IT equipment and must be procured using the SC requirements process using the SC Computer Systems Requirements Document (CSRD) process.

5.2.1. Groups/Directorates must coordinate with their approving authority and Resource Advisor (RA) to obtain additional devices. Sustainment costs will be the responsibility of the Group/Directorate.

5.3. SC will fund/manage the costs (for services rendered) and is the POC between the vendor and NASIC. SC will also manage and fund basic core devices and services. All non-core devices and services will be funded by the Groups/Directorates.

5.3.1. Core services consist of Continental US (CONUS) email, web service, mobile to mobile, and 300 anytime minutes.

5.3.2. Non-core services consist of (but are not limited to) international services which allows email and web service. International service is an additional cost plus any additional minute charged for phone calls.

5.3.3. SC RA will coordinate funding of mission phones and additional services with mission RAs during budget planning.

5.4. SC will establish the standard configuration and is the only authorized POC to change the configuration. Users will not have access to the device configuration settings.

5.4.1. All devices will be configured for unclassified phone and data use in CONUS.

5.4.1.1. Maintenance of all devices will be managed by and carried out by SC.

5.4.2. Configuration changes, such as adding international capabilities, will be submitted to SC using the CSRD system. The CSRD process will allow NASIC to document configuration changes. Customer's organization will be required to fund the additional service for at least one full month of use.

5.4.3. SC will contact and coordinate any maintenance actions with the vendor as needed.

5.5. Devices are authorized to process unclassified information only. Any security incidents must be immediately reported to NASIC Security Officer (SOO).

5.6. If viruses or malware are discovered on the device, the owner/user must immediately report this event to the CFP in accordance with NASICVA 33-104, *Reporting Computer Viruses*. Treat all information concerning the infection at a minimum of CONFIDENTIAL and use secure means to contact the CFP (e.g. make a personal visit, send an e-mail on SIPRNET, and call on a STE phone).

5.7. Customers are responsible for keeping the device secured (meaning within your control or possession at all times). Signing the hand receipt for the equipment is acceptance and acknowledgement that the customer is familiar with the information contained in this document, and the corresponding AFIs; AFI 33-111, *Voice Systems Management*, AFI 10-712, *Telecommunications Monitoring and Assessment Program (TMAP)* and AFI 33-119, *Air Force Messaging*.

5.8. All personnel are highly discouraged from bringing their government-owned cellular device into the SCIF. However, if brought into the SCIF, individuals are responsible for following security procedures outlined in NASICI 31-106, *Portable Electronic Devices (PEDS)*, which governs the operational and security requirements when bringing a cellular device inside the SCIF.

KATHLEEN C. SAKURA, Colonel, USAF
Commander

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

AFI 10-712, *Telecommunications Monitoring and Assessment Program (TMAP)*, 8 June 2011

AFI 33-111, *Voice Systems Management*, 22 November 2011

AFI 33-119, *Air Force Messaging*, 2 September 2008

AFI 33-200, *Information Assurance (IA) Management*, 15 October 2010

AFMAN 33-363, *Management of Records*, 13 October 2011

AFPD 33-2, *Information Assurance (IA) Program*, 3 August 2011

DoD Regulation 5400.7/AF Sup1, *DOD Freedom of Information Act Program*, 24 June 2002

NASICI 31-106, *Portable Electronic Devices (PEDS)*, 11 August 2010

Visual Aids

NASICVA 33-104, *Reporting Computer Viruses*, 30 November 2011

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*, 22 September 2009

Terms and Abbreviations

AFPD—Air Force Policy Directive

AFI—Air Force Instruction

AFMAN—Air Force Manual

ANG—Air National Guard

AFRC—Air Force Reserve Command

AFRIMS—Air Force Records Information Management System

CAC—Common Access Cards

CFP—Communications Focal Point

CONUS—Continental United States

CSRD—Computer Systems Requirements Document

DS—Director of Staff

FARM—Functional Area Records Manager

FOUO—For Official Use Only

IA—Information Assurance

IAW—In Accordance With

NASIC—National Air & Space Intelligence Center

NIPRNet—Non-Classified Internet Protocol Router Network

OPR—Office of Primary Responsibility

OPSEC—Operations Security

PA—Privacy Act

PEDS—Portable Electronic Devices

PII—Personally Identifiable Information

PKI—Public Key Infrastructure

POC—Point of Contact

RA—Resource Advisor

RDS—Records Disposition Schedule

SCIF—Secret Compartmented Information Facility

Attachment 2
SPONSOR MEMORANDUM

Figure A2.1. Designation of Soft Certificate PKI Sponsor.

	<p>DEPARTMENT OF THE AIR FORCE NATIONAL AIR & SPACE INTELLIGENCE CENTER (AF ISR AGENCY) WRIGHT-PATTERSON AFB OHIO</p>
<p>MEMORANDUM FOR NASIC/SCXS</p>	
<p>FROM: NASIC/XXXX</p>	
<p>SUBJECT: Designation of Soft Certificate PKI Sponsor for (Organizational Mailbox Name)</p>	
<p>References:</p> <ol style="list-style-type: none"> 1. Air Force LRA Certification Practices Statement, dated 6 Dec 02. 2. DoD PKI Medium Assurance Group/Role-Based Certificate Request Procedures, dated July 2008 	
<p>The subject account is an authorized account used for organizational support and requires software PKI certificates for receiving encrypted e-mail.</p>	
<p>Specific account information is:</p> <ul style="list-style-type: none"> • Account Display Name: (Display Name as it appears in the GAL) • E-mail Address: (Primary SMTP E-mail address) 	
<p>The following individual is designated as the PKI sponsor for the software certificates:</p> <ul style="list-style-type: none"> • Name and Grade: • CN: (LASTNAME.FIRSTNAME.MIDDLE NAME.EDIPI) <i>(i.e., Common Name (CN) portion of the subject name from individual's CAC)</i> • NIPRNET e-mail address : • DSN Phone : • Commercial Phone : 	
<p>In accordance with referenced documents, the PKI sponsor will sign the 2842-NPE acknowledging receipt of the certificates/token and exercise custody control of the certificates.</p>	
<p>My Point-of-Contact for additional information or assistance regarding this appointment is: (Name, position, phone, e-mail address).</p>	
<p>(Signature Block & Date)</p>	
<p>Note: Signature to be GS-15/O6 or above. Note: <i>If the mailbox involved is ~SCXX and the Chief of SCX is not GS-15/O6 their signature as Chief of the function is acceptable as the official having oversight for the function.</i></p>	
<p>cc: (Each Appointee)</p>	
<p><i>"Freedom Through Vigilance"</i></p>	

1st Ind. (Sponsor Name)

TO: NASIC/SCXS

Date: _____

I, (Sponsor Name), acknowledge receipt of this appointment. I have read and understand the responsibilities assigned in this appointment.

(Sponsor's Signature Block & Date)

Attachment 3

ORGANIZATIONAL MAIL BOX REMOVAL

Figure A3.1. Organizational Mail Box Removal Request.



DEPARTMENT OF THE AIR FORCE
NATIONAL AIR & SPACE INTELLIGENCE CENTER (AF ISR AGENCY)
WRIGHT-PATTERSON AFB OHIO

MEMORANDUM FOR NASIC/SCXS
 FROM: NASIC/XXX
 SUBJECT: Organization Mail Box Removal Request

- Request removal of the (org box name) organization mail box.
- Please contact XXXXX if you have additional questions.

Org Box Owner Signature Block

1st Ind. Your FARM Office Symbol Date, _____

TO: NASIC/SCOK

- I reviewed the content of the (org box name) organizational mail box and all official records have been moved to the FARM drive. I concur with the removal of the org box.

FARM Signature Block

2nd Ind. SCOK

TO: NASIC/SCXS

- I approve removal of the organizational mail box.

Base Records Manager Signature Block

"Freedom Through Vigilance"