

**BY ORDER OF THE
INSTALLATION COMMANDER JOINT
BASE ANDREWS**

JOINT BASE ANDREWS INSTRUCTION 10-201

2 JULY 2014



Operations

**INSTALLATION WARNING SYSTEM
OPERATING PROCEDURES**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publication 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: 11 WG/CP

Certified by: 11WG/CP
(Lt Col Ryan P. Brandt)

Pages: 7

This instruction implements AFPD 10-2, *Readiness*, and AFPD 10-25, *Emergency Management*. It outlines the purpose, procedures, and responsibilities associated with the operation of the Joint Base Andrews (JBA) Installation Warning System (IWS). It applies to all active-duty and Department of Defense civilian personnel assigned to the 11th Wing and 79th Medical Wing, and is informational for personnel assigned to Headquarters, Air Force District of Washington, 89th Airlift Wing, 844th Communications Group, 457th Airlift Squadron, and other mission partner units located on Joint Base Andrews. This publication may not be supplemented or further implemented / extended. Air Force Reserve Command, Air National Guard, and Civil Air Patrol personnel will follow guidance from their appropriate major command (MAJCOM) or Guard Bureau. Refer recommended changes and questions about this instruction to the OPR using the AF Form 847, Recommendation for Change of Publication. Waiver authority for this instruction is the 11 WG/CC. This publication requires the collection and / or maintenance of information protected by the Privacy Act (PA) of 1974. The authorities to collect or maintain the records prescribed in this publication are contained in 10 USC 8012. The information will be used by management to alert personnel in the event of an emergency. Routine uses listed in AFDIR 37-144, *Air Force Privacy Act Systems of Records Notices*, apply. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 33-363, Management of Records, and disposed of IAW the Air Force Records Disposition Schedule located at <http://www.my.af.mil/afirms/afirms/afirms.rims.cfm>.

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.

1. Description.

1.1. The JBA IWS fulfills the installation's need for a reliable, rapid, and broad-based method to deliver time-sensitive emergent notifications to JBA-assigned personnel. The system is designed to transmit computer-generated alert notifications in an expeditious manner via desk-top computer pop-up windows, home/work emails, and home/work/mobile telephones. It is not designed, nor does it have the capability, to fully replace manual notification procedures.

1.2. The most valuable feature of the IWS system is its capability to rapidly transmit desktop computer, email, and Short Message Service (SMS) text message alerts advising JBA personnel of emergency situations or advisories in time to take the appropriate protective measures.

1.3. IWS alerts consist of the desktop pop-up, work e-mail, personal e-mail, text messaging, text-to-speech to duty phones, and text-to-speech to personal phones.

1.3.1. Desktop Pop-up. The Desktop pop-up is the system default for all alerts, and is most effective during duty hours. When actuated, a "pop-up window" appears in each workstation connected to the AFNCR network. The pop-up may be accompanied by an audio message or tone. Desktop alerts may include response options for the end user to select, or hyperlinks for end users to click. Clicking the "Acknowledge and close" button on the bottom of the alert window closes the alert.

1.3.2. Work E-mail. Work e-mail notifications provide a non-invasive means to notify users during duty hours. In general, notifications to user work E-mail address will be used for all notifications.

1.3.3. Personal E-mail. Alerts sent to personal E-mail are sent to the commercial E-mail accounts provided by end users in the IWS personal information section. End users have the option to respond by calling a number provided or responding via email. Note: Messages may be automatically filed in the end user's "junk E-mail" or "spam" box if they have not selected the sending address as a trusted source.

1.3.4. SMS Text. The IWS system will send a message to the mobile device provided by end users in the IWS personal information sections. Messages may include response options, which may be tracked by the publishing author.

1.3.5. Telephone (text-to-speech). The system sends a text-to-voice message to the end user's work, home, and/or mobile phone. Messages may include response options (i.e., "Press 1 to acknowledge"), which may be tracked by the publishing author. Note: IWS will only attempt one "call back" if there is no response. **Note:** Phone alerting is not normally employed in an emergency since sending alerts to phone devices may overload the telephone network with phone calls, and may take several hours to reach all recipients in the IWS database.

2. Policy

2.1. All military and civilian personnel assigned to JBA and Air Force personnel assigned to Joint Base Anacostia-Bolling (JBAB) not already required to enroll in IWS per paragraph 2.2 below, are highly encouraged to enroll their contact information in the JBA IWS system.

2.2. The JBA IWS shall not be used to directly contact individual personnel for accountability or other unit-wide recalls. The pyramid notification / recall process has been established IAW JBAI 10-218 for this purpose. This injunction does not preclude the use of IWS to rapidly mobilize leadership and key staff personnel to facilitate the expeditious execution of unit-wide recalls.

2.3. To avoid saturation of end users, IWS notifications shall be mission-essential only. In addition, alerts directed to personal mobile devices shall be kept to an absolute minimum, consistent with mission execution.

2.4. Mandatory enrollment:

2.4.1. All 11 WG- and 79 MDW-assigned military and Department of Defense civilian personnel shall enter all applicable organizational information into the system.

2.4.2. 11 WG- and 79 MDW-assigned active-duty personnel shall enter into IWS their work email, work phone, home phone, home email, cellular phone, and text messaging device (may be different than their cellular phone). Mobile devices may be used for “home phones” if the member does not possess a land-line at his / her residence.

2.4.3. 11 WG- and 79 MDW-assigned Department of Defense civilian personnel:

2.4.3.1. Emergency essential. DoD civilian personnel designated as “emergency essential” by their core document shall register their devices per paragraph 2.1.2.

2.4.3.2. Not emergency-essential. DoD civilian personnel not designated as “emergency essential” by their core document are required to provide organizational information per paragraph 2.1.1, and enroll their work email and work phone in IWS. Registration of other devices is highly encouraged to ensure the timely receipt of critical life, health, and safety information.

2.4.4. Members appointed to the JBA Emergency Operations Center and / or the Crisis Action Team shall enter their information as per paragraphs 2.4.1, 2.4.2, and 2.4.3 above, as applicable.

2.5. Optional enrollment:

2.5.1. Contractors with a Common Access Card and a user account on the AFNCR network may elect to enter their contact information into the IWS system.

2.5.2. All users may, at their discretion, elect to provide a spouse’s mobile device number as an “alternate” number in IWS, enabling spouses or personnel other than the member to receive emergency IWS alerts.

2.6. Publishing authority.

2.6.1. 11 WG and JBA-wide alert:

2.6.1.1. Only Andrews Regional Command Post (ARCP) duty controllers may initiate 11 Wing- and/or JBA-wide IWS alerts.

2.6.1.2. The events and specific devices used for alerting will be listed and approved in the IWS Notification Matrix (see paragraph 3.5.2).

2.6.1.3. Within ARCP, only properly certified controllers may publish alerts. Certification training will consist of the following:

2.6.1.3.1. Understanding of the “two person concept”

2.6.1.3.2. Task signed off on AF Form 623

2.6.1.3.3. Understanding of Controller Basic Checklist #10

2.6.1.4. Alerts issued by ARCP shall have the highest priority on the IWS system and take precedence over all other notifications.

2.6.2. Unit-wide alerts. O-6 level commanders of units directly supported by ARCP may designate personnel to publish IWS notifications to personnel within their scope of authority (see paragraph 3.2).

2.7. Users shall disenroll from IWS prior to PCS from JBA or separation from military / Federal service (see paragraph 3.7.2).

2.8. User registration in IWS should be periodically exercised to ensure the robustness of the user device database and ability of users to receive alerts.

2.9. IWS administrators and publishers at all levels will strictly limit access to Privacy Act information contained within the IWS system to authorized personnel only with a bona fide “need to know”. Reports generated from the IWS system that contain personally identifiable information (PII) will be encrypted during transmission and shall only be reviewed by law enforcement, Inspector General (IG), ARCP personnel, unit-level administrators, and applicable unit-level leadership. Reports containing PII shall be shredded / destroyed upon completion of need.

3. Roles and Responsibilities.

3.1. 11 WG/CC or designated representative:

3.1.1. The declaration authority for all 11 WG or installation-level IWS alerts.

3.1.2. Approve the IWS Notification Matrix for the installation (see paragraph 3.6.2).

3.2. Commanders of units directly supported by ARCP, or his/her designated representative:

3.2.1. The declaration authority for IWS alerts to personnel with in their scope of command.

3.2.2. May appoint personnel (“unit publishers”) to publish IWS alerts to their units.

3.2.3. If a unit publisher(s) is appointed, commanders must also appoint IWS administrator(s) to assist ARCP with unit user account administration.

3.2.4. Appoint IWS administrators and publishers in writing, and a copy of the appointment letter must be provided to ARCP.

- 3.2.5. Ensure unit-level administrators and publishers will be fully trained by ARCP personnel prior to being granted access to the IWS system.
- 3.2.6. Ensure unit-level IWS administrators shall not also function as IWS publishers; the two duties shall be distinct and separate.
- 3.2.7. Ensure unit-level publishers transmit only the alerts listed on the IWS Notification Matrix (see paragraph 3.6.2).
- 3.2.8. Coordinate through ARCP to add alerts to the Matrix, as desired.
- 3.2.9. Strictly limit access to Privacy Act information stored on the IWS system to authorized personnel with a valid “need to know”.
- 3.3. Wing agency directors, and group and squadron commanders:
 - 3.3.1. Ensure IWS enrollment is included in unit / agency in-processing checklists.
 - 3.3.2. Ensure personnel assigned to specialized teams (i.e., Crisis Action Team (CAT), Emergency Operations Center (EOC), etc) enroll their information in IWS upon appointment.
 - 3.3.3. Ensure compliance with paragraph 2.4
- 3.4. 11 FSS:
 - 3.4.1. Ensure IWS disenrollment is a required item on the JBA virtual out processing checklist.
 - 3.4.2. Verify at “final out” that disenrollment has occurred.
- 3.5. 11 WG/XP: Exercise IWS to periodically verify system operation and personnel registration of required devices in IWS.
- 3.6. ARCP (11 WG/CP):
 - 3.6.1. Train ARCP controllers, unit-level administrators, and unit-level publishers on the use of the IWS system.
 - 3.6.2. Maintain the IWS Notification Matrix, detailing each event that requires an IWS notification and which devices shall be used to disseminate the alert. Coordinate proposed changes to the Matrix through 11 WG/CC.
 - 3.6.3. Maintain IWS scripts corresponding to each event in the IWS Notification Matrix.
 - 3.6.4. Conduct weekly tests of the IWS system to verify system connectivity to AFNCR workstations.
 - 3.6.5. Configure the system to remove user accounts after prolonged inactivity. “Prolonged inactivity” is defined as the user not logging into the AFNCR domain for 220 days or longer.
 - 3.6.6. Configure the system to present a desktop pop-up at each login to users who have not provided information as required by paragraph 2.4.
 - 3.6.7. Color-code desktop pop ups according to the following scheme:
 - 3.6.7.1. Emergencies / FPCON changes: Black and red.

3.6.7.2. INFOCONs: Yellow

3.6.7.3. Informational: Blue

3.6.7.4. Weather: Gray

3.6.7.5. Warning: (Tornado / HURCON1 / active shooter “all clear”): Red

3.6.7.6. Other “All Clear”: White

3.6.7.7. Heat stress conditions: Same as the condition’s color

3.6.8. Upon request, transmit IWS Notification Matrix-listed alerts on behalf of supported unit commanders in an expeditious manner.

3.7. Unit Client Support Administrators. Assist individual users with IWS client issues on unit workstations.

3.8. Individuals:

3.8.1. Enroll in IWS by entering the required information (see paragraphs 2.4 and 4) within 30 days of arrival on JBA.

3.8.1.1. If personnel only possess a cell phone and do not have a land line at their residence, that number should only be entered as the “mobile phone”. Users should not enter the same number for both “home” and “mobile” phone numbers.

3.8.1.2. Individuals are highly encouraged to register their spouse’s mobile device (if applicable) in the “Alternate” contact information field.

3.8.2. Disenroll from IWS by deleting their information not earlier than the last duty day prior to their final out appointment (see paragraph 5).

3.8.3. Self-identify in IWS if they are a member of the JBA CAT, EOC, 320 AEW Operations Center, or other specialized distribution group.

4. Enrolling in IWS:

4.1. Detailed instructions for enrollment in IWS may be found at the ARCP Sharepoint site at https://afdw.afncr.af.mil/org/11_WG/CP/Offical%20Documents/Forms/AllItems.aspx

5. Disenrollment from IWS.

5.1. Detailed instructions for disenrollment from IWS may be found at the ARCP Sharepoint site at

https://afdw.afncr.af.mil/org/11_WG/CP/Offical%20Documents/Forms/AllItems.aspx.

WILLIAM M. KNIGHT, Colonel, USAF
Commander, 11th Wing/Joint Base Andrews

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFMAN 33-363, *Management of Records*, 1 Mar 2008
AFPD 33-5, *Warfighting Integration*, 11 Jan 2013

Prescribed Forms

None

Adopted Forms

None

Abbreviations and Acronyms

AFNCR—Air Force National Capitol Region

ARCP—Andrews Regional Command Post

CAT—Crisis Action Team

EOC—Emergency Operations Center

INFOCON—INFORMATION CONDITION

IWS—Installation Warning System

JBA—Joint Base Andrews

PCS—Permanent change of station

Terms

AFNCR Network—The computer network supporting Air Force personnel assigned to JBA, Joint Base Anacostia-Bolling, and the Pentagon.

ARCP Sharepoint Site—A website maintained by ARCP personnel containing guides to aid IWS enrollment and disenrollment.

https://afdw.afncr.af.mil/org/11_WG/CP/Offical%20Documents/Forms/AllItems.aspx.

IWS Notification Matrix—A memorandum signed by the 11th Wing commander or vice commander detailing all events for which that authorized JBA IWS system publishers may initiate notification, and the means by which that notification may be disseminated (i.e., work E-mail, work phone, home E-mail, home phone, mobile phone, SMS text, alternate phone).

Publishers—Those personnel who have been trained and authorized to initiate notification scripts in IWS that broadcast to some or all personnel connected to the JBA IWS.

Pyramid Notification/Recall Procedures—Pyramid notification / recall procedures are the requirements implemented to notify or recall base personnel during crisis situations. These procedures utilize a top-down method of notification and bottom-up acknowledgement.