DEPARTMENT OF THE NAVY
COMMANDER NAVY INSTALLATIONS COMMAND
716 SICARD STREET SE SUITE 1000
WASHINGTON NAVY YARD DC 20374-5140

CNICINST 2050.1
N6
19 Mar 2018

CNIC INSTRUCTION 2050.1

From: Commander, Navy Installations Command

Subj: CNIC IRIDIUM SATELLITE PHONE POLICIES AND PROCEDURES

Ref: (a) CNO WASHINGTON DC 131429Z Jun 14 (NAVADMIN 135/14)
(b) DoD/CIO Memo, Enhanced Mobile Satellite Services Gateway of 22 February 2016
(c) DODINST 8420.02
(d) EKMS Policy and Procedures for Navy Tiers 2 & 3, EKMS-1E of 7 Jun 2017

Encl: (1) Iridium User Agreement and Privacy Acknowledgment

1. Purpose. To issue policy and procedures governing the management and use of government owned Iridium Satellite phones by Commander, Navy Installations Command (CNIC) personnel in compliance with references (a) through (c), to efficiently control phone and device costs and to ensure cost-effective usage of these enterprise-wide devices.

2. Scope and Applicability. This instruction applies to CNIC Headquarters and all Regions.

3. Background. The Iridium Satellite phones are a component of the Defense Information Systems Agency (DISA) Enhanced Mobile Satellite Service (EMSS). These phones are used by CNIC for emergency communications in cases of natural disasters (per the CNIC Emergency Communication Plan), power outages and other events. The Iridium Satellite phones provide Region and installation Incident Commanders with reliable, effective communications to maintain local incident situational awareness and active coordination communication with headquarters.

a. CNIC Information Technology (N6) utilizes DISA Storefront, also referred to as DISA Direct Order Entry (DDOE), an ordering suite of tools for requesting telecommunication products and services. CNIC (N6) maintains access to DISA Direct to acquire Iridium products and services.

b. Enhanced Mobile Satellite Service is a Satellite-based Personal Communications System (PCS) using commercial satellite infrastructure to provide voice and low data rate data services from a mobile, lightweight terminal through a Department of Defense (DoD) dedicated gateway. This gateway accesses the Defense Information Systems Network (DISN). Each EMSS is capable of providing secure services, in addition to non-secure access to commercial telephone

services. EMSS supports DoD missions and operations, as well as other Federal, National Security and Emergency Preparedness communications. The EMSS system complements military terrestrial and satellite communications and improves warfighter beyond-line-of-sight connectivity by offering global access to all echelons of the DoD.

4. Policy

a. Official Use Only. Government issued satellite phones are for emergency events and for conducting official government business.

b. Standard Allowance. Region Commanders will ensure, all installation Commanding Officers, have the ability to communicate with the Region. Region Commanders will reflect and plan for loss of primary and secondary communications assets. Allowances per Region can fluctuate. Region Commanders will take into account missions to support government events, mission critical functions, emergency evacuations and disaster prone areas.

c. User Criteria. CNIC defines the following personnel categories authorized to conduct official business on a government owned satellite phone. Headquarters (HQ) staff and Region Commanders may apply standards that are more aggressive. Standards are defined for the following personnel categories:

(1) Command Staff Personnel. Management personnel involved with the exercise of command to include; essential and key emergency personnel will exercise C2 of military and government forces (including support contractors) this includes personnel responsible for execution critical to operational missions 24/7. This includes all emergency type personnel.

(2) Specific Requirement Personnel. Defined as personnel who perform unique duties that require use of a satellite phone. This will be validated and approved at the Region level by the Region (N6). CNIC (N6) will approve CNIC HQ requirements.

d. Usage Restrictions. Use of satellite phones requires strict adherence to the following:

(1) Only authorized Government personnel and support contractors with given authorization, for official Government use only.

(2) Dissemination of the satellite phone number should be restricted for official and authorized use.

(3) Stolen or missing satellite phones must be reported immediately to the Region (N6) or designated Information Technology representative so service can be cancelled to preclude illegal use. A financial liability investigation of property loss report, DD Form 200, will be initiated.

e. Iridium Satellite Equipment. The CNIC issued satellite phone kit consists of the following equipment and accessories:

(1) Iridium Satellite Handset.

(2) EMSS SIM Card.

(3) Rechargeable Lithium Ion Battery (2).

(4) AC Travel Charger with International Plug Kit.

(5) Auto Accessory Adapter.

(6) Antenna Adapter.

(7) Leather Holster.

(8) User Guide and Iridium Secure Module and DTD Cable (Issued separately to local EKMS Custodian/Account)

f. Iridium Satellite Phones Distributed

(1) Iridium 9505A Phone. The only CNO authorized Iridium phone for secure voice encryption. This phone will become obsolete and phased out by June 2019.

(2) Iridium 9575 Phone. Non-secure voice capability only, offers the fully integrated services of customizable GPS, online tracking and emergency SOS with notification.

(3) Iridium 9575A Phone. The next generation Iridium phone with secure voice encryption capability. This phone will replace the Iridium 9505A and 9575.

g. Subscriber Identity Module (SIM). A small smart card that contains service details, memory for storing phone book entries and messages.

h. Iridium Secure Module (ISM) and Data Transfer Device (DTD) key cable used for keymat loading.

(1) The ISM crypto keymat has reached end of life. A Key Extension Request (KER) approval is pending. The ISM2/Bearcat is the future replacement for the ISM. This device is currently unavailable for issue/purchase.

(2) Control Requirements: Per reference (d), EKMS1 and local EKMS Custodian.

(a) The ISM is a Controlled Cryptographic Item (CCI) and will be handled as such per reference (d) EKMS 1 Article 535. When the secure capability of the ISM has been activated the device must be protected to the classification level of the key it contains.

(b) Access to classified communications security (COMSEC) material requires a security clearance equal to or higher than the classification of the material.

(c) Appropriately keyed ISMs are approved to protect information of all classifications and categories.

(d) When talking at a classified/sensitive level or entering a personal identification number (PIN), be aware of environmental conditions, including the proximity of un-cleared individuals. Although the ISM can secure a telephone conversation, it cannot secure the surroundings.

(3) Accounting Requirements: The ISM is accountable by its serial number. The ISM is Accounting Legend Code 1, therefore is accountable within the COMSEC Material Control System.

(4) Access Requirements for Resident Aliens and Foreign Nationals:

(a) Resident aliens who are U.S. Government employees, U.S. Government contractor employees, or National Guard, active duty, or reserve members of the U.S. Armed Forces may be granted access to CCI provided their duties require access and approval has been granted by the phone custodian.

(b) Foreign Nationals Non-U.S. citizens who are employed by the U.S. Government at foreign locations where there is a significant U.S. military presence (two or more military bases) may handle CCI material in connection with warehouse functions, provided they are under the direct supervision of an individual who has been granted access to CCI material.

(5) Storage and Handling:

(a) So as not to overly inhibit its use, an ISM that has been loaded with key may be handled the same as an ISM without key, provided the PIN code remains separate from the device.

(b) The ISM user must maintain continuous physical control of the device per Electronic Key Management System (EKMS) 1B Annex AD.

(6) Transportation:

(a) ISM devices, with or without key (zeroized), will be shipped per the guidance contained EKMS 1 Article 535.

(b) A U.S. user may carry an ISM as an item of personal property to locations outside the United States, its territories and possessions, provided its use is restricted to official purposes only. To reduce the level of risk, ISM users should consider the following recommendations:

1. When talking at a classified/sensitive level or entering a PIN code, be aware of environmental conditions, including the proximity of uncleared individuals. Although the ISM can secure a telephone conversation, it cannot secure the surroundings.

2. Keep the ISM PIN code separate from the ISM. Under no circumstances will the ISM PIN code be printed and attached or included with the ISM.

5. Responsibilities

a. Installation Commanding Officer:

(1) Overall responsible for all satellite phones assigned by CNIC HQ.

(2) Ensure a minimum standard allowance of equipment is issued from CNIC HQ or resource the appropriate number of satellite phones necessary to sustain critical C2 in an emergency.

b. CNIC (N6) is responsible for:

(1) Developing and maintaining the CNIC policy, managing the enterprise Iridium Satellite phone and other communications contracts, coordinating within CNIC and with upper echelon commands, and overall management of the enterprise Iridium Satellite phone program within CNIC.

(2) Coordinating Iridium Satellite phone services with DISA.

(3) Managing and placing orders consistent with policy and budget.

(4) Communicating program guidance to installation and Region leadership, end users and the Region (N6), coordinating with Region (N6) in the management of their local satellite phone programs and supporting special requirements.

c. CNIC (N61) Iridium Program Lead (IPL) is responsible for:

(1) Overall administration and control of all the Iridium Satellite phones in the CNIC enterprise.

(2) Ensuring the Command Security Manager (CSM), Region Security Manager (RSM) or the Cognizant Security Authority (CSA) are aware of the Iridium Satellite phone under their purview; along with it capabilities, security requirements and requirement for protection and storage of the equipment.

d. Region (N6) CIO is responsible for:

(1) Appointing a Region (N6) Iridium Phone Manager (IPM) to manage the issuance of satellite phones within their respective Region.

(2) Management and accountability of all Region assigned satellite phones and accessories.

(3) Validate Iridium support requests or increase in standard allowance with the installation CO before submitting to CNIC (N6).

(4) Satellite phone troubleshooting and maintenance activities.

(5) Notifying CNIC (N61) when satellite phone(s) or equipment needs updating and/or replacement.

(6) Training users as necessary; overseeing and managing usage and satellite phone inventory.

e. CNIC Iridium Program Lead will:

(1) Possess a security clearance equal to or higher than the highest classification of the material this person has required access to.

(2) Support the CNIC (N61) Specialist and his/her representative with administration of the DISA/EMSS contract for CNIC users.

(3) Support the HQ EKMS Manager with CNIC HQ Iridium requirements.

(4) Review Iridium support requests received from installation CO's and forward to CNIC (N6).

(5) Ensure adherence to current and future satellite phone policy and directives issued by higher echelons. Communicate this policy throughout the CNIC enterprise.

(6) Monitor and log the usage and manage compliance with policy across the CNIC HQ and Region enterprise.

(7) Maintain a master Iridium Satellite phone inventory.

(8) Conduct periodic Iridium Inventory Data Call and report results to CNIC (N6/N61).

f. Region (N6) IPM will:

(1) Possess a security clearance equal to or higher than the highest classification of the material this person has required access to.

(2) Support the Region (N6) CIO and installation (N6) and EKMS Manager(s) with Iridium requirements.

(3) Validate and reconcile all Iridium Satellite phones on a quarterly basis to ensure up-to-date management data and inventory accuracy. Provide copy to CNIC IPL.

(4) Submit Region Iridium status summary as part of the CNIC (N61) bi-monthly ICP Maintenance DON Tracker report to the CNIC IPL.

(5) Ensure all satellite phone users sign and submit a Satellite Phone User Agreement and Privacy Acknowledgment (enclosure (1)) to the Region (N6) Iridium Manager. An electronic copy can be found on the Gateway 2.0 (G2) CNIC (N615) Emergency Communications team site: https://g2.cnic.navy.mil/teamsites/9063e09a-b6bb-4b73-9532-007d69cc68c5/Shared%20Documents/iridium.aspx.

(6) Account for Iridium Satellite phones as government minor property.

g. Installation (N6) Phone Manager will:

(1) Possess a security clearance equal to or higher than the highest classification of the material this person has required access to.

(2) Support the Region (N6) IPM and EKMS Manager(s) with Iridium requirements.

(3) Validate and reconcile all Iridium Satellite phones with the Region (N6) IPM to ensure up-to-date management data and inventory accuracy.

h. Iridium Satellite phone user will:

(1) Complete an Iridium User Agreement and Privacy Acknowledgment (enclosure (1)).

(2) Agree not to use the equipment for any unlawful purposes and regulations of all governmental authorities while using the equipment.

(3) Agree to use the equipment in a careful and proper manner.

(4) Agree not to use the equipment for any purpose that is contrary to the mission or purpose.

(5) Maintain the equipment in good repair and operating condition, allowing for reasonable wear and tear.

(6) Inspect the equipment and acknowledge that the equipment is in good and acceptable condition.

(7) If the device is lost or stolen, the user will notify the Region (N6) Iridium point of contact (POC) as soon as practical after the user notices the device is missing (temporary or permanent loss). A Financial Liability Investigation of property loss report (DD Form 200) must be initiated by the user up the chain of command for signature.

(8) Conduct periodic operation test as directed by CNIC IPL or Region (N6) Iridium POC.

(9) Physically protect the device when away from a secure location.

(10) Be responsible for the proper use and deployment of the Iridium.

(11) Be responsible for training anyone using the equipment on the proper use of the equipment.

i. Satellite Phone Testing. Satellite phones can be a critical lifeline in times of need. Regular testing ensures satellite-enabled devices are ready for use immediately when required. The ability to communicate is critical in an emergency. Iridium provides a dedicated test number to call and ensure your device is working properly at all times. To test complete the following steps:

(1) Dial 00 + 697 + 480-752-5105

(2) If the phone is working, a call completion confirmation message will be heard as well as some quick tips on proper phone usage.

(3) If the phone is not operational, contact your Region (N6) Iridium POC.

6. Records Management. Records created as a result of this instruction, regardless of media and format, must be managed per Secretary of the Navy Manual 5210.1 of January 2012.

7. Review and Effective Date. Per OPNAVINST 5215.17A, CNIC (N6) will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV and Navy policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will automatically expire 5 years after effective date unless reissued or canceled prior to the 5-year anniversary date or an extension has been granted.

8. Forms Management Control. Financial Liability Investigation of Property Loss, DD Form 200 (Rev. Oct 99), can be found on Gateway 2.0 (G2) CNIC (N615) Emergency

Communications team site: https://g2.cnic.navy.mil/teamsites/9063e09a-b6bb-4b73-9532-007d69cc68c5/Shared%20Documents/iridium.aspx. Completed DD Form 200 forms should be submitted to the Region (N6).

C. S. GRAY
Chief of Staff

Releasable distribution:
This instruction is cleared for public release and is available electronically only via CNIC Gateway 2.0, https://g2.cnic.navy.mil/CC/Documents/Forms/Directives%20Only.aspx

Iridium User Agreement and Privacy Acknowledgment

The command recognizes that Information Systems, which include military networks, Internet, cell phones, satellite phones, converged devices, pagers, etc., are necessary tools in the accomplishment of official duties. Command members are encouraged to utilize these resources. Staff personnel and others utilizing Government issued converged devices will observe the prohibitions, restrictions and limitations outlined in the CNIC policy governing Iridium/satellite device usage.

User hereby acknowledges that user has read and understands the CNIC policy governing Iridium device usage. User is reminded that systems under the control of the Government are subject to unlimited monitoring with no expectation of privacy from Government authorities, and any violation of established policy, prohibitions, restrictions or limitations imposed by the CNIC policy governing cellular, satellite and wireless device usage may result in loss of access privileges, adverse administrative, monetary or disciplinary action. User also understands and agrees to adhere to the policy and procedures outlined in CNICINST 5211.1, Privacy Program, for safeguarding Personally Identifiable Information (PII). Military, government civilian or contractor personnel may be subject to criminal penalties if they knowingly or willfully violate this policy.

Prior to permanently leaving this Command (e.g., transfer, retirement, separation, contract terminates), user agrees to return all assigned cellular, satellite, wireless or converged devices. User certifies that User has read and understands this policy and agrees to adhere to the direction contained herein.

Date Deployed / Issued:		Date Returned:	
Region/Command/ Installation/N-Code			
Iridium Type (Circle)	Satellite Phone #	Commercial Phone #	CNIC Asset #
9505A / 9575 / 9575A			
IMEI #		Hard Case with accessories	Yes or No
ICCID (SIM Card ID)		Iridium Secure Sleeve	Yes, No, NA
IA Training and Awareness Certification Completed		Date:	
Security Manager Validates Clearance Information and Clearance Level (If Yes, Include Security Manager Name)		Yes, No, NA /Name:	
User Printed Name:		User Digital Signature:	