BY ORDER OF THE COMMANDER
KADENA AIR BASE

KADENA AIR BASE INSTRUCTION
17-202

20 MARCH 2025

Cyberspace

CELLULAR TELEPHONE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: 18CS/SCXA

Certified by: 18CS/CC
(Lt Col Rachel L. Reynolds)

Supersedes: KADENAABI17-202, 20 September 2018

Pages: 9

This instruction implements Department of the Air Force Policy Directive (DAFPD) 17-2, *Cyber Warfare Operations*. It provides guidance and implements instructions for individuals and organizations requesting cellular phones for which usage is limited to official duties, from the 18th Communications Squadron (18 CS). All personnel controlling these devices will ensure strict accountability regarding usage and possession to avoid abuse and wasted resources. It applies to all 18th Wing (18 WG) and partner units, and members supported by the 18 WG. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with (IAW) the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the office of primary responsibility (OPR) using the DAF Form 847, *Recommendation for Change of Publication*; route DAF Forms 847 from the field through the appropriate functional chain of command.

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed. Major changes include the addition of the roles and responsibilities for the Resource Advisor (RA) and the Property Custodian (PC). It also explains the new process for requesting cellular telephone service.

1. Roles and Responsibilities.

1.1. **Base Equipment Control Officer (BECO).**

1.1.1. Will track appointment of Property Custodians (PC).

1.1.2. Will process the receipt, transfer and disposal of all accountable information technology (IT) assets and complete necessary documentation to establish custodial responsibility.

1.1.3. Will assist PC in determining the ownership, reassignment, or disposition of all found-on-base accountable IT assets.

1.1.4. Will direct PCs to conduct inventories in accordance with (IAW) Department of the Air Force Manual (DAFMAN)17-1203, *Information Technology Asset Management (ITAM) and Accountability.*

1.1.5. Will provide PCs with training on requirements and standardized procedures.

1.1.6. Will provide inventory assistance IAW DAFMAN17-1203.

1.2. **Cellular Phone Liaison (CPL).**

1.2.1. Will act as the liaison between the requestor and the cellular phone vendor.

1.2.2. Will issue cellular telephones (CT) to requesting customer.

1.2.3. Will process payments made by the requesting customer's squadron Resource Advisor (RA).

1.2.4. Will notify RAs when a payment is late or has issues.

1.3. **Unit Accountable Property Officer (UAPO).**

1.3.1. Organization commanders (or equivalent) shall serve as UAPO and are responsible for providing guidance and procedures to ensure adequate protection and oversight is afforded to safeguard IT assets under their control.

1.3.2. Will appoint at least one primary and one alternate PC per account IAW Department of Defense Instruction (DoDI) 5000.64, *Accountability and Management of DoD Equipment and Other Accountable Property*, section 3.2, paragraph f. The UAPO will ensure appointed PCs acknowledge their duties with handwritten or digital signatures, and the UAPO will provide a copy of the documentation to the Equipment Control Officer (ECO).

1.3.3. Must be responsible for the accountability of all accountable IT hardware assets assigned to their unit.

1.3.4. Must approve purchase requests for systems to support mission needs IAW DAFMAN 17-1203, paragraph 2.5.

1.3.5. Will ensure assets are inventoried according to DAFMAN 17-1203, Attachment 4.

1.3.6. Will ensure PCs perform out-of-cycle inventories as directed.

1.3.7. Must direct the primary PC to complete a gain-loss inventory no later than 30 calendar days prior to out processing for primary custodian changeover.

1.3.8. Will monitor the acquisition, storage, utilization, and disposition of property within his or her assigned accountable area. Identify underutilized, impaired, or obsolete property and take appropriate actions to increase utilization or ensure disposition.

1.3.9. Will develop physical inventory plans and procedures, schedule physical inventories, and assist in their completion IAW DAFMAN 17-1203 Attachment 4.

1.3.10. Will ensure PCs complete required training.

1.4. **Property Custodian (PC).**

1.4.1. UAPO must appoint primary and alternate PC in writing. There is no minimum rank requirement for PCs.

1.4.2. Contractors may serve as PCs, if allowable under the contract terms and conditions and approved by the organization commander.

1.4.3. PCs shall be accountable for all assigned accountable IT hardware assets within their respective custodian accounts.

1.4.4. PCs will ensure individuals receiving accountable assets validate acceptance with signed documentation i.e., AF Form 1297, *Temporary Issue Receipt*, or locally developed receipt. PC will retain a copy of the signed document.

1.4.5. Will perform, at a minimum, an annual inventory of all accountable IT hardware assets under their purview, as prescribed in DODI 5000.64.

1.4.6. Must be approved to out-process by the UAPO and ECO.

2. Cellular Telephone (CT) Use Policy.

2.1. Acquisition of new CT devices. The use of CTs is restricted to personnel who require communications of an immediate nature that cannot be satisfied through the use of other communication means. CTs will not be used for command and control. They may be used for administrative purposes only. The 18th Communications Squadron (18 CS) coordinates all new CT services with Yokota Air Base (AB) contracting office (374 CONS).

2.2. An occasional personal call on a CT is justified under some circumstances (e.g., call home to inform family when delayed by official business or in emergency situations). Personal calls on government CTs must be the exception, not the rule. Morale, welfare and recreational calls are not authorized on CTs. Use a regular telephone (landlines) as a first priority when and where available. Cellular services are generally more expensive; limit their use.

2.3. Special Telephone Features and Services.

2.3.1. To manage and control the configuration of CTs, any new requirements (to include additions and/or upgrades) to service plans must be processed and approved using 18 CS request procedures.

2.3.2. Global Access. This feature should only be considered if the CT will be used outside of Japan and the user fully understands the rates incurred by this service. Global Access service incurs higher rate charges for all data transfers, emails, and incoming/outgoing calls.

2.4. Telephone Monitoring and Recording.

2.4.1. The Air Force uses unsecured telecommunications systems such as telephones, CTs, radios, facsimile, computer networks and other wired and wireless electronic devices to conduct day-to-day official business. Adversaries can easily monitor these unsecured systems that could provide information on military capabilities, limitations, intentions and activities.

2.4.2. When the CT is issued, the CT user is required to sign the form found in **Attachment 2** that includes the following notice and consent statement: **"Do not transmit classified information over unsecured telecommunications systems. Official DoD telecommunications systems are subject to monitoring. Using this telecommunications system or device constitutes consent to monitoring."** Users are also required to sign an DAF Form 4394, *Department of the Air Force User Agreement – Notice and Consent Provision* (**Attachment 3**). The signed forms will be retained by a squadron Property Custodian.

3. Requesting Cellular Telephone (CT) Services.

3.1. All CT requests must be submitted with appropriate documentation in advance of purchase.

3.2. CTs are funded by the requesting unit. Initial requests for CTs will be made by completing a DD Form 428, *Communication Service Authorization,* which must be filled out with the requested information to include the unit's Project Task Expenditure Organization (PTEO), along with the Resource Advisor's (RA) signature. After being signed the RA will send the DD Form 428 to the 18 CS cellular phone liaison (CPL) at **18cs.itam.cellphones@us.af.mil** for processing.

3.3. Prior to a CT being ordered, a Base Equipment Control Officer (BECO) will verify that the requesting unit's PC account is compliant. If the account is compliant the 18 CS will forward the request to Yokota AB contracting office (374 CONS) who will process the request and forward the order to the appropriate CT vendor. The unit RA will fulfill the order and the CPL will retrieve the product from the vendor. The CPL will contact the unit Property Custodian (PC) for pick up.

3.4. CT orders take approximately 14 duty days to process once the CPL forwards the request to Yokota AB contracting office (374 CONS).

4. Billing for Unofficial Calls.

4.1. Unit CTs with global access service are charged for all outgoing/incoming calls and data packet transfers when used outside of Japan.

4.2. Unit Property Custodians (PC) are responsible for maintaining proper accountability of all CT devices assigned to their account.

4.3. The requesting unit is responsible for all bills and charges associated with their CT service. The 18 CS will not review and does not require the review of any telephone data associated with the requesting unit and the CT service. All incidents pertaining to *Fraud, Waste and Abuse* are to be rectified by the requesting unit.

5. Annual Requirements.

5.1. An annual DD Form 428, *Communication Service Authorization*, for revalidation will be accomplished for each unit each September by the unit RA to ensure CT service is still required by the unit.

5.2. An annual payment revalidation will be accomplished at the beginning of every fiscal year using a DD Form 428. This form, provided by the CPL, must be filled out and signed by the unit RA. 18 CS will forward all DD Forms 428 to Yokota AB contracting office (374 CONS) to ensure proper payment of CT bills. Since 18 CS/SCX manages billing for CT service, it is important that the Unit RA accomplishes this annual revalidation to avoid service termination for **all** of their squadron's CTs. RAs must provide Project Task Expenditure Organization (PTEO) information with the amount of their approved annual budget to cover their CT bills for the fiscal year. For tenant units a Military Interdepartmental Purchase Request (MIPR) or Miscellaneous Obligation Reimbursement Document (MORD) must be provided by the unit RA and sent to **18cs.ITAM.cellphones@us.af.mil**.

NICHOLAS B. EVANS
Brigadier General, USAF
Commander, 18th Wing

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoDI 5000.64, *Accountability and Management of DoD Equipment and Other Accountable Property*, 27 April 2017

DAFPD 17-2, *Cyber Warfare Operations*, 27 October 2020

DAFMAN 17-1203, *Information Technology Asset Management (ITAM) and Accountability*, 13 September 2022

AFI 33-322, *Records Management and Information Governance Program*, 10 March 2020

Prescribed Forms

None

Adopted Forms

DD Form 428, *Communication Service Authorization*

DAF Form 847, *Recommendation for Change of Publication*

DAF Form 4394, *Department of the Air Force User Agreement Statement - Notice and Consent Provision*

AF Form 1297, *Temporary Issue Receipt*

Abbreviations and Acronyms

AB—Air Base

BECO—Base Equipment Control Officer

DAFI—Department of the Air Force Instruction

DAFPD—Department of the Air Force Policy Directive

CPL—Cellular Phone Liaison

CT—Cellular Telephone

ECO—Equipment Control Officer

IAW—In accordance with

IT—Information Technology

ITAM—Information Technology Asset Management

MIPR—Military Interdepartmental Purchase Request

MORD—Miscellaneous Obligation/Reimbursement Document

OPR—Office of Primary Responsibility

PC—Property Custodian

PTEO—Project Task Expenditure Organization

RA—Resource Advisor

UAPO—Unit Accountable Property Officer

Terms

Cellular Telephone (CT)—Radio devices that offer telephone-like services through a wireless commercial infrastructure.

Cell Phone Liaison (CPL)—Point of Contact between 18th Communications Squadron and local CT provider (AU).

Resource Advisor (RA)—Unit person responsible for all financial purchases and transactions.

Property Custodian (PC)—Unit person responsible for ensuring all telephone activities are monitored for abuse, as well as overseeing inventory for all CTs.

Attachment 2

CUSTOMER BRIEFING AND ACCOUNTABILITY RECEIPT

A2.1. This briefing is intended to inform those using any government cellular telephone (CT) of the user responsibilities regarding its use.

A2.2. Cellular Telephone (CT) Costs. The using squadron is billed for each individual cellular phone number. Locally billable charges include all calls placed from a CT but do not include all incoming calls to a CT. Calls placed from and received by cellular phones under the control and accountability by the 18 CS must be government official in nature. Our service provider, AU will bill Kadena AB at a commercial rate; therefore, personal calls are not authorized to be placed using these phones. Regular telephone (land lines) must be used as a first priority when and where available. Emergency use situations must be authorized on a case-by-case basis at the user's unit level. Each unit is responsible for paying for all bills and charges associated with their CT(s). Be aware that some CTs have Global Passport access, which allows the phones to be used internationally. This service is highly expensive, as all calls coming in and going out are double charged. The Global Passport service should be used very sparingly or preferably not at all.

A2.3. Fraud, Waste and Abuse. Using a government CT for other than official government business without prior unit approval is fraud. Using a CT in lieu of other available government landlines, where available, is abuse. Using a CT when other communication means will accomplish the mission is waste.

A2.4. Statements of Understanding. By signing below, I certify that I will not discuss classified or sensitive information on either device. I acknowledge and understand the following statement. **"Do not transmit classified information over unsecured telecommunications systems. Official DoD telecommunications systems are subject to monitoring. Using this telecommunications system or device constitutes consent to monitoring."** I acknowledge receipt of and responsibility for the items described herein. I certify that all charges incurred on this cellular phone while it is signed out to me will be for government official calls, unless otherwise noted.

User Name: _____

User Signature: _____ Date: _____

Attachment 3

AIR FORCE USER AGREEMENT STATEMENT – NOTICE AND CONSENT PROVISION

Figure A3.1. Department of the Air Force User Agreement Statement – Notice and Consent Provision.

DEPARTMENT OF THE AIR FORCE USER AGREEMENT STATEMENT - NOTICE AND CONSENT PROVISION

The policy described in this memorandum is in accordance with Air Force Instruction AFI 10-701, Operations Security (OPSEC); AFMAN 17-1301, Computer Security (COMPUSEC); AFMAN 17-1203, Information Technology (IT) Asset Management (ITAM); DoDI 5000.64_DAFI 23-111, Accountability and Management of DoD Equipment and Other Accountable Property; AFI 17-130, Cybersecurity Program Management; DoDI 8500.01, Cybersecurity; Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs); and DISA Security Requirements Guides (SRGs).
AUTHORITY: DoDI 8500.01, AFI 10-701, AFMAN 17-1301, AFMAN 17-1203, DoDI 5000.64_DAFI 23-111, and AFI 17-130.
PRINCIPAL PURPOSE: To ensure users are made aware of, and consent to, DoD and DAF monitoring policies and procedures.
ROUTINE USES: May be disclosed for the purpose of verifying individuals were made aware of monitoring policies and procedures.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.
Prescribed by AFMAN 17-1301

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:

You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.

You consent to the following conditions:

The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the U.S. Government may inspect and seize data stored on this information system.

Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.

This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests -- not for your personal benefit or privacy.

Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:

Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.

The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.

Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.

Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.

A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.

These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.

In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

1. NAME (Last, First, Middle)	2. STATUS
Doe, John, M.	☐ Civilian ☐ Contractor ☑ Military
3. USER SIGNATURE	**4. DATE (YYYYMMDD)**
Click to sign	2024-03-01

DAF FORM 4394, 20230912

AUTHORITY: 10 U.S.C. Section 9013, Secretary of the Air Force; AFI 33-332; and E.O. 9397 (SSN)
PREVIOUS EDITIONS ARE OBSOLETE