

PERnet
Request
Form
and
Procedures

Information Paper-Draft v1

Subject: Steps for Requesting HRC Systems Access for Units undergoing PSDR Conversion

1. General:

a. The procedures outlined in this document are meant to supplement the HRC established procedures for requesting access to HRC Systems. The procedures are to be utilized by units preparing for **PSDR Conversion ONLY**.

2. Concept:

a. HRC has identified the need to supplement the current procedures in order to prioritize system access requests for units preparing for PSDR Conversion. The priority window for these units starts with the New Organizational Training Team (NOTT) Coordination Visit and ends the last day of NOTT Conversion Training. This is approximately a 120 day window.

b. The Concepts Development & Integration Division (CDID PSDR Team) will become the "Front Door" for all HRC Systems Requests that meet the criteria established in this document. This change allows CDID to prioritize each request and annotate a new PSC Code on each form. The PSC Code is required for TOPMIS Update Capability Access.

3. Rules of Engagement:

a. Each BDE will be authorized 8 TOPMIS Accounts, 4 of which can have update capability. Each BN will be authorized 3 TOPMIS Accounts, all of which can have update capability. This must be annotated on the 49-R.

b. TOPMIS is based on a PSC Code Hierarchy. Upon issuance of the new PSC Code "UA" each legacy TOPMIS account that is associated to the old PSC Code must be transferred to the new PSC Code. Accounts currently issued to a BDE or BN, under the old PSC Code, will only require a PSC Code update. IASOs can complete the attached spreadsheet (TOPMIS PSC Code Update) and submit to CDID at PSDR@hoffman.army.mil. A 49-R is not required. Accounts currently issued to PSB users, or units outside the converted BDE or BN, will be required to submit a "transfer" request with the new IASO. IASOs must submit the transfer request to CDID at PSDR@hoffman.army.mil.

c. TOPMIS accounts issued during the priority window will have an effective date coinciding with the start of NOTT Conversion Training, which will also coincide with the issuance of the new PSC Code. This will allow current users to operate using their existing account up until the issuance of the new PSC Code. New users will receive view capability, while update capability will be restricted until the issuance of the new PSC Code. The logic behind this decision is that new users are requesting access specifically

due to PSDR; therefore, these accounts should not be activated until implementation of PSDR.

4. Process:

a. Before a PERNET System Access Registration Form (49-R) can be submitted, the command MUST appoint an Information Assurance Security Officer (IASO) on orders using the IASO Appointment Order Form (50-R). The approving authority for this form must be a DoD Government Employee. Contractor Personnel are not authorized to appoint IASOs using this form. Upon approval, forward the 50-R to the PERSINSD User Registrar at userregistrar@hoffman.army.mil or debra.trimble@hoffman.army.mil.

b. The PERNET System Access Registration Form (49-R) will be completed for users requesting access to the following HRC Systems:

- (1.) TOPMIS
- (2.) EDAS
- (3.) Data Query
- (4.) ITAPDB
- (5.) TAPMR
- (6.) OSSS/DAPMIS
- (7.) Printing and Pubs
- (8.) OERS
- (9.) DCIPS

c. A Security Investigation Status must be completed for all "New User Accounts" and "Transfer Accounts." A favorable National Agency Check (NAC) or a favorably adjudicated NAC investigation must have been completed on the user.

5. Procedures:

a. Unit Commander appoint IASO using Form 50-R.

b. IASO forward completed 50-R to User Registrar at userregistrar@hoffman.army.mil.

c. IASO complete a 49-R on all new users. The following are required blocks:

- (1.) Part A. Blocks 1-11.
- (2.) Part A. Blocks 16-20.
- (3.) Part B. New and Transfer accounts only.
- (4.) Part C. Can be completed before or after submission to HRC.

d. IASO ensure accurate and complete information is annotated in Part A. Ensure the user AKO meets the established guidelines (see attached).

e. IASO signs the 49-R and forwards to the Security Manager.

- f. Security Managers verifies favorable NAC and completes Part B.
 - g. Security Manager signs Part B, Block 24 and forwards to IASO.
 - h. IASO completes Part C and forwards to CDID at PSDR@hoffman.army.mil.
 - i. CDID will perform quality assurance measures and annotate a PSC Code on the 49-R. Notify the IASO of any discrepancies.
 - j. CDID forwards the 49-R to the User Registrar.
 - k. User Registrar performs quality assurance measures, validate 50-R, then forwards to respective HRC agencies.
- 6. Common Errors on the 49-R:**
- a. Handwritten copies are not legible
 - b. Office Symbol is missing
 - c. User AKO is missing or incorrect in Part A, Block f.
 - d. IASO is not appointed on a 50-R.
 - e. IASO does not sign the 49-R.
 - f. Part B is not completed for "New" and "Transfer" accounts.
 - g. Security Manager does not sign the 49-R.

ARMY HUMAN RESOURCES COMMAND

INFORMATION ASSURANCE SECURITY OFFICER

APPOINTMENT

The individuals listed below have been appointed Information Assurance Security Officer (IASO)/ Alternate Information Assurance Security Officer (AIASO), for account number (if known), Organization HHC 1BDE, MACOM/ARQODA See Attached, IAW AR 25-2, Information Assurance, 14 November 2003, Chapter 3-2f. The IASO/AIASO understand that all data retrievals/queries are to be treated as "FOR OFFICIAL USE ONLY" and are to be utilized in the performance of their official duties as a Department of Defense employee (military, civilian or contractor). Failure to comply with the above guidance will result in removal as IASO/AIASO.

NOTE: IASO/AIASO cannot appoint themselves.

<u>IASO APPOINTMENT</u>	<u>AIASO APPOINTMENT</u>
<u><i>Pammy Lass</i></u> Signature	<u><i>Alternate Lass</i></u> Signature
<u>Primary IASO</u> Name (Typed/Printed)	<u>Alternate IASO</u> Name (Typed/Printed)
<u>ABCD-1BDE (example)</u> Office Symbol - Telephone No.	<u>ABCD-1BDE</u> Office Symbol - Telephone No.
<input type="checkbox"/> Replaces _____ Name of Current IASO	<input type="checkbox"/> Additional AIASO <input type="checkbox"/> Replaces _____ Name of Current AIASO

APPROVING AUTHORITY

Must Be DoD Gov Employee
Name, Title (Typed/Printed)

Doc Goo
Signature

3 Oct 06
Date

ARMY HUMAN RESOURCES COMMAND

INFORMATION ASSURANCE SECURITY OFFICER

APPOINTMENT

The individuals listed below have been appointed Information Assurance Security Officer (IASO)/ Alternate Information Assurance Security Officer (AIASO), for account number _____, Organization _____, MACOM/ARQODA _____, IAW AR 25-2, Information Assurance, 14 November 2003, Chapter 3-2f. The IASO/AIASO understand that all data retrievals/queries are to be treated as "FOR OFFICIAL USE ONLY" and are to be utilized in the performance of their official duties as a Department of Defense employee (military, civilian or contractor). Failure to comply with the above guidance will result in removal as IASO/AIASO.

NOTE: IASO/AIASO cannot appoint themselves.

<u>IASO APPOINTMENT</u>	<u>AIASO APPOINTMENT</u>
_____ Signature	_____ Signature
_____ Name (Typed/Printed)	_____ Name (Typed/Printed)
_____ Office Symbol - Telephone No.	_____ Office Symbol - Telephone No.
<input type="checkbox"/> Replaces _____ Name of Current IASO	<input type="checkbox"/> Additional AIASO <input type="checkbox"/> Replaces _____ Name of Current AIASO

APPROVING AUTHORITY

Name, Title (Typed/Printed) Signature Date

PERnet SYSTEM ACCESS REGISTRATION

A. USER/IASO INFORMATION

Date: 3 Oct 2006

1. USER NAME (Last, First, Middle Initial) USER, JOHN K.		2. Grade GS7	3. Employee Type: <input checked="" type="checkbox"/> Govt <input type="checkbox"/> Contractor		4. Room# / Mail Stop:
5. Organization/Contractor Company: HHC, (BDE) - ECHOLON			6. Office Symbol: ***ABCD-1BDE***		
7. Address a. Street: ***1 User Way***		b. City/State: ***/**		c. ZIP Code: 12345-0000	
8. User Phone Number:		DSN: 111-1111		COMM: (111)111-11111	
9. Duty/Position Title:			10. MACOM/ARQODA: ***SEE ATTACHED***		
11. Type of Request: New <input checked="" type="checkbox"/> Update		Transfer <input checked="" type="checkbox"/>		Delete	
12. Pre-Registration: (ORB/2A, Attached) Yes		No		Arrival Date:	
13. Transfer From Acct #:			14. PERnet Userid:		
15. Access Requested: TOPMIS II <input checked="" type="checkbox"/>		EDAS <input checked="" type="checkbox"/>		MS51 <input checked="" type="checkbox"/>	
COPS <input checked="" type="checkbox"/>		DCIPS <input checked="" type="checkbox"/> <i>NA</i>		DATA QUERY <input checked="" type="checkbox"/>	
OTHER a: Check all that apply		b: Add Specifics		c: i.e. Promotions	
d: i.e. Strength		e: i.e. TOPMIS Update			
f: AKO User ID: john.user @us.army.mil					
16. IASO Name: IASO KING			17. Signature: <i>John King</i>		
18. IASO Phone Number:		DSN: 222-2222		COMM: (222)222-2222	
19. Account Number (if known):		20. IASO AKO: iaso.king@us.army.mil			

DCIPS CM IS ONLY USED AT CMAOC + CAC LEVEL

PART B. SECURITY INVESTIGATION STATUS (TO BE COMPLETED BY SECURITY MANAGER)

21. "I verify that a favorable National Agency Check (NAC) or a favorably adjudicated NAC investigation has been completed on the user. I will notify the IASO who in turn will notify ISD Security immediately to terminate this access approval if the investigation status of the user changes"

I Verify

"HRC Users Only - If the access requested is for a classified system, I verify the user has a valid SECRET clearance. If the person holds an ADP I position as specified in AR 380-67, I verify that a successful Single Scope Background Investigation has been completed"

I Verify

22. Security Manager's Name: Security Manager

23. Phone Number: DSN : 333-3333 COMM: (333)333-3333

24. Signature: *Security Manager* Date: 3 Oct 2006

PART C. IASO CERTIFICATION

I, _____ have briefed/will brief _____ on the AHRC Form 49-1-R (AHRC Information System Use/Security Awareness Agreement). I will maintain the signed copy on file along with access information.

PART D. FOR PERSINSD USE ONLY

25. PERnet Userid:	26. CICS Opr ID:	27. Company Code:	28. Org. Code:
29. SIC Code:		30. Account Number:	
31. ISD Security/Phone/Date:		32. Remarks:	
33. Domain User ID:		34. Legacy User ID	

PERnet SYSTEM ACCESS REGISTRATION

A. USER/IASO INFORMATION

Date: 3 Oct 2006

1. USER NAME (Last, First, Middle Initial)		2. Grade	3. Employee Type: <input type="checkbox"/> Govt <input type="checkbox"/> Contractor		4. Room# / Mail Stop:			
5. Organization/Contractor Company: UNIT NAME + ECHELON				6. Office Symbol:				
7. Address	a. Street:		b. City/State:		c. ZIP Code:			
8. User Phone Number:	DSN:		COMM:					
9. Duty/Position Title: SEE ATTACHED MATRIX			10. MACOM/ARQODA:					
11. Type of Request:	New	Update	Transfer	Delete				
12. Pre-Registration: (ORB/2A, Attached)		Yes	No	Arrival Date: SECTION				
13. Transfer From Acct #:			14. PERnet Userid:					
15. Access Requested:		TOPMIS II	EDAS	MS51	COPS	DCIPS	NA	DATA QUERY
OTHER	a:	b:	c:	d:	e:			
f: AKO User ID: _____@us.army.mil				PSC CODE: _____				
16. IASO Name:			17. Signature:					
18. IASO Phone Number:		DSN:	COMM:		FAX:			
19. Account Number (if known) :			20. IASO AKO:					

PART B. SECURITY INVESTIGATION STATUS (TO BE COMPLETED BY SECURITY MANAGER)

21. "I verify that a favorable National Agency Check (NAC) or a favorably adjudicated NAC investigation has been completed on the user. I will notify the IASO who in turn will notify ISD Security immediately to terminate this access approval if the investigation status of the user changes"

I Verify

"HRC Users Only - If the access requested is for a classified system, I verify the user has a valid SECRET clearance. If the person holds an ADP I position as specified in AR 380-67, I verify that a successful Single Scope Background Investigation has been completed"

I Verify

22. Security Manager's Name: _____

23. Phone Number: _____ DSN : _____ COMM: _____

24. Signature: _____ Date: _____

PART C. IASO CERTIFICATION

I, _____ have briefed/will brief _____ on the AHRC Form 49-1-R (AHRC Information System Use/Security Awareness Agreement). I will maintain the signed copy on file along with access information.

PART D. FOR PERSINSD USE ONLY

25. PERnet Userid:	26. CICS Opr ID:	27. Company Code:	28. Org. Code:
29. SIC Code:		30. Account Number:	
31. ISD Security/Phone/Date:		32. Remarks:	
33. Domain User ID:		34. Legacy User ID	

PERnet SYSTEM ACCESS REGISTRATION

A. USER/IASO INFORMATION

Date: _____

1. USER NAME (Last, First, Middle Initial)		2. Grade	3. Employee Type: <input type="checkbox"/> Govt <input type="checkbox"/> Contractor		4. Room# / Mail Stop:
5. Organization/Contractor Company:				6. Office Symbol:	
7. Address	a. Street:		b. City/State:		c. ZIP Code:
8. User Phone Number:	DSN:		COMM:		
9. Duty/Position Title:			10. MACOM/ARQODA:		
11. Type of Request:	New		Update		Transfer Delete
12. Pre-Registration: (ORB/2A, Attached)		Yes	No	Arrival Date:	
13. Transfer From Acct #:			14. PERnet Userid:		
15. Access Requested:	TOPMIS II	EDAS	MS51	COPS	DCIPS DATA QUERY
OTHER	a:	b:	c:	d:	e:
f: AKO User ID: _____@us.army.mil					
16. IASO Name:			17. Signature:		
18. IASO Phone Number:	DSN:		COMM:		FAX:
19. Account Number (if known) :			20. IASO AKO:		

PART B. SECURITY INVESTIGATION STATUS (TO BE COMPLETED BY SECURITY MANAGER)

21. "I verify that a favorable National Agency Check (NAC) or a favorably adjudicated NAC investigation has been completed on the user. I will notify the IASO who in turn will notify ISD Security immediately to terminate this access approval if the investigation status of the user changes"

I Verify

"HRC Users Only - If the access requested is for a classified system, I verify the user has a valid SECRET clearance. If the person holds an ADP I position as specified in AR 380-67, I verify that a successful Single Scope Background Investigation has been completed"

I Verify

22. Security Manager's Name:					
23. Phone Number:	DSN :		COMM:		
24. Signature:				Date:	

PART C. IASO CERTIFICATION

I, _____ have briefed/will brief _____ on the AHRC Form 49-1-R (AHRC Information System Use/Security Awareness Agreement). I will maintain the signed copy on file along with access information.

PART D. FOR PERSINSD USE ONLY

25. PERnet Userid:	26. CICS Opr ID:	27. Company Code:	28. Org. Code:
29. SIC Code:		30. Account Number:	
31. ISD Security/Phone/Date:		32. Remarks:	
33. Domain User ID:		34. Legacy User ID	

HRC System's Functions/Roles for HURS Implementation

CATEGORIES				SYSTEM										
PSC Code	Echelon	Duty Position	Section	ORD Update	TOPMIS			EDAS			COPS			MS91
					Requisitions	Strength	View	Promotions	Requisitions	DataQuery	Deletion/Deferment	View	View	View
UA/UB	BDE and Div/Corps STB	Sr. HR Manager	NA	X	X	X		X	X	X	X		X	X
		HR Manager	NA	X				X						X
		HR Clerk	NA	X										X
BN	Sr. HR Manager	NA		X		X								X
	HR Manager	NA		X										X
	HR Clerk	NA		X										X
All Other	MPD	Sr. HR Manager	Pers Services	X				X						X
		HR Manager	Pers Services	X				X						X
		HR Clerk	Pers Services	X										X
	Sr. HR Manager	Strength Mgt		X	X				X	X	X			X
	HR Manager	Strength Mgt		X	X				X	X	X			X
	HR Clerk	Strength Mgt		X	X				X	X	X			X
Any	G1/U1	Sr. HR Manager	Other				X						X	X
		HR Manager	Other				X						X	X
		HR Clerk	Other				X							X
	Sr. HR Manager	Strength Mgt		X	X				X	X	X			X
	HR Manager	Strength Mgt		X	X				X	X	X			X
	HR Clerk	Strength Mgt		X	X				X	X	X			X
Non-UA/UB	HRC	Sr. HR Manager	Other				X						X	X
		HR Manager	Other				X						X	X
		HR Clerk	Other				X							X
Any	Other	NA	NA				X						X	X
		Other	Other											X

HRC users will be profiled based on their Office Symbol. No change to current procedures

MACOM (ARQODA) CODES:

AS	US ARMY INTEL AND SECURITY CMD	USAISC
CB	U.S. ARMY CRIMINAL INVESTIGATION COMMAND	CIC CMD
CE	U.S. ARMY CORPS OF ENGINEERS	COE
DF	DEPARTMENT OF DEFENSE AGENCIES	DOD AGENCIES
E1	US ARMY EUROPE	USAREUR
FA	US ARMY FIELD OPERATING AGENCIES	US ARMY FOA
FC	U.S. ARMY FORCES COMMAND	FORSCOM
HQ	HEADQUARTERS, DEPARTMENT OF THE ARMY	HQDA
J1	US ARMY ELEMENT SHAPE (JOINT)	US ARMY ELEMENT SHAPE
JC	US ARMY CENTRAL COMMAND (JOINT)	CENTCOM
JE	US EUROPEAN COMMAND (JOINT)	US EUROPEAN CMD
JJ	US JOINT FORCES COMMAND (JOINT)	US JOINT FORCES CMD
JN	US NORTHERN COMMAND (JOINT)	US NORTHERN CMD
JP	US PACIFIC COMMAND (JOINT)	US PACIFIC CMD
JR	US STRATEGIC COMMAND (JOINT)	US STRATEGIC CMD
JS	US SOUTHERN COMMAND (JOINT)	US SOUTHERN CMD
JT	US TRANSPORTATION COMMAND (JOINT)	US TRANSPORTATION CMD
JX	US SPECIAL OPERATIONS COMMAND (JOINT)	US SPEC OPS CMD
MC	U.S. ARMY MEDICAL COMMAND	U.S. ARMY MED CMD
MT	SURFACE DEPLOYMENT AND DISTRIBUTION COMMAND	SURFACE DPLY DIST CMD
MW	U.S. ARMY MILITARY DISTRICT OF WASHINGTON	MDW
PI	U.S. ARMY PACIFIC	USARPAC
P8	EIGHTH US ARMY	EIGHTH US ARMY
SC	U.S. ARMY SPACE AND MISSILE DEFENSE COMMAND	SMDC
SP	US ARMY SPECIAL OPERATIONS COMMAND	USASOC
TC	US ARMY TRAINING AND DOCTRINE COMMAND	TRADOC
TH	TRAINEES, HOLDEES, AND STUDENTS	THS
XI	US ARMY MATERIEL COMMAND	AMC

AHRC Systems POC Roster

System	Function	Name	Comm	DSN	Email
TOPMIS	Training	Arnold Quick	(703) 325-2077	221	arnold.quick@conus.army.mil
TOPMIS	ORD (Records Update)	Santi Boriboon	(703) 325-5132	221	santi.boriboon@conus.army.mil
TOPMIS	Requisition	Tom Dukeman	(703) 325-5125	221	thomas.dukeman@conus.army.mil
TOPMIS	Data Standard	Vicki Kidd	(703) 325-0767	221	kiddv@conus.army.mil
TOPMIS	Strength/Data Query	Frank Greenlee	(703) 325-4553	221	frank.greenlee@conus.army.mil
TOPMIS	ORB/Data Accuracy	Phyllis Hampton	(703) 325-5131	221	phyllis.hampton@conus.army.mil
TOPMIS	EAC/Data Integrity	Joey Consuegra	(703) 325-9299	221	hermogenes.consuegra@conus.army.mil
Citrix		Roy William	(703) 325-6112	221	william.roy@conus.army.mil
Citrix		Robert Coley	(703) 325-4000	221	robert.coley@conus.army.mil
Citrix		Travis Cavanaugh	(703) 325-2519	221	travis.cavanaugh@conus.army.mil
ISD	Supervisor	Jane Payne	(703) 325-5424	221	jane.payne@conus.army.mil
ISD	PERNET	Michael Montgomery	(703) 325-9079	221	michael.k.montgomery@conus.army.mil
ISD	PERNET	Delores Coates	(703) 325-3423	221	delores.coates@conus.army.mil
ISD	Registrar	Debra Trimble	(703) 325-2546	221	userregistrar@conus.army.mil
GOPS		Luther Monroe	(703) 325-9644	221	luther.monroe@conus.army.mil
DCIPS CM	CACs Only	Scot Angus	(703) 325-0005	221	scot.angus@conus.army.mil
EDAS	Account Management	Valerie Anderson	(703) 325-8943	221	valerie.m.anderson@us.army.mil
EDAS	UIC Manager	Wanda Violette	(703) 325-3977	221	wanda.violette@us.army.mil
EDAS	UIC Manager	Jose Rivera	(703) 325-3979	221	jose.van.rivera@us.army.mil

INSTRUCTIONS FOR COMPLETING TAPC FORM 49-R

All blocks must be filled out legibly and completely in accordance with these instructions. Failure to comply will delay or prevent the processing of your request.

TASO / IASO must submit completed forms to the PERNET Registrar: at userregistrar@hoffman.army.mil or debra.trimble@hoffman.army.mil . Scanned copies are preferred over faxed copies as they provide a better quality of resolution.

Block #	INSTRUCTIONS
1	Self-explanatory
2	Military or Civilian GS rating
3	Select appropriate block
4	Enter your room number
5	List same organization as the TASO's organization on the TAPC Form 50-R
6	List same Office Symbol as the TASO's office symbol on the TAPC Form 50-R
7	a-c: List duty address as requested
8	a-b: List duty phone number as requested
9	Be specific with duty title (i.e. Records clerk/MPD, Promotions clerk, etc)
10	List units Major Command (i.e. FORSCOM, IMA, USAREUR)
11	If user has a PERNET account check "Update": If no current account check "New"
12	Check "NO" and list requester's arrival date to organization
13	If user already has a PERNET Account list the account # here (user's account number is on their previous TAPC-R form in block 30)
14	List PERNET ID for those with current accounts (must have checked "Update" in block # 11.
15	Leave blank
16	List all access being requested: If user is requesting a TOPMIS II Account, have them put "CITRIX" under block 14a (Other). Request for DATAQUERY Accounts must be accompanied by a separate memorandum of justification. Generally, only those working in the PAS should have DQ access due to its complicated nature. MUST INCLUDE AKO USER ID.
17-20	List information of TASO / IASO (name must match that on file with PERNET Security). Must include all pertinent information or accounts will not be established
21	Have unit Security manager check this block. A favorable NAC Background check is required for access --- this is not the same as a SECRET Clearance. Requestor does not need to have a SECRET clearance for access to PERNET
22-24	Have Security manager complete all blocks and sign / date in the appropriate blocks
PART C	Brief the user on the HRC Information Systems Use / Security Agreement and maintain on file with the Requestor's application.

Submit completed application to: PERNET REGISTRAR at above email

US Army Human Resource Command Information Systems Use/Security Awareness Agreement

This agreement provides an overview of policies that apply to the use of HRC Information Systems:

1. General:

- a. HRC Information Systems are available to facilitate the operational and administrative work of authorized users. These systems will be used for official government business only except for specifically authorized limited personal use IAW the Joint Ethics Regulation and will not be used for any illegitimate or fraudulent purpose. System access is not anonymous and your use constitutes consent to monitoring.
- b. Users will use HRC resources responsibly and abide by normal standards of professional and personal courtesy and conduct at all times. In accessing these systems, all users agree to comply with all policies and procedures governing the use of HRC owned or supported systems. They agree to take full responsibility for all actions performed via the account assigned. Inappropriate use of these systems may be a basis for consideration of criminal or administrative disciplinary action against users. Any user who fails to comply with HRC rules and procedures will be denied system access.
- c. Your Information Assurance Security Officer (IASO) is required to have you read and sign this statement and maintain it on file.
- d. All users will be part of a security training and awareness program IAW Chapter 3-2, Army Regulation (AR) 25-2. The program will ensure that all users are aware of proper operational and security-related procedures and risks.

2. Environment:

- a. HRC systems operate in a shared/limited resource environment processing sensitive data. As an authorized user, you have access to computer resources to do your job. Take advantage of the vast knowledge and information available through these systems to accomplish your mission, but use these resources judiciously in order to conserve our limited capabilities. Do not abuse your access.
- b. HRC computer systems process defense information at the Sensitive but Unclassified (SBU) level. Information labeled SBU must be protected to ensure confidentiality, availability and integrity and may or may not require protection from foreign intelligence services or other unauthorized personnel. Examples may include information dealing with logistics, medical care, personnel management, Privacy Act data, contractual data, Freedom of Information Act information, For Official Use Only (FOUO) information and certain categories of financial data.

3. Individual guidelines:

- a. Your job assignment requires your receipt of a logon ID and password that permits access to HRC information systems. Do not disclose this to anyone unless required by systems administrator, in which case you will change it afterwards. You are personally responsible for any use of your account accessed with this password.
- b. Avoid any communication that could result in the disclosure of sensitive information received from HRC systems to unauthorized personnel. Information accessed will be used for official business only and disseminated only to personnel with a need to know.
- c. Do not use HRC systems in a way that will interfere with your official duties, undermine readiness or reflected adversely on DOD or the Army. Your use not involve: pornography, offensive material, chain letters, unofficial advertising, personal commercial purpose or gain, soliciting, selling, game playing, illegal activities, unauthorized system access, subterfuge (using someone else's account and/or create deception as if they're responsible), inappropriately handled classified materials or other uses incompatible with public service
- d. Resources will not be used in a manner that overburdens our communications systems or interferes with their performance. Do not send E-mail or make file transfers that could reasonably be expected to either cause, directly or indirectly, excessive strain on any communication facilities or unwarranted or unsolicited interference with others' use of systems.
- e. Make yourself aware of and abide by the limitation and/or proper use rules for any interconnected network which you access through your account. Do not use directories other than your own, including system directories, to store files without the permission of the owner.
- f. Any software on HRC systems will be legally installed and documented IAS copyright laws. Do not run any unauthorized software under your account.
- g. Report any suspicious activity or erratic behavior of your system to you IASO.

4. Conscientious use of HRC systems will help avoid overburdening our scarce resources and eliminate service disruptions that could be easily avoided.

I have read the US Army Human Resource Command Information Systems Use/Security Awareness Agreement. I understand my responsibilities and I understand that my use of the system is subject to monitoring. I am accountable and responsible for my actions or actions performed by others using my account and/or privileges. If I fail to comply with the rules and procedures of this agreement, my access will be revoked and I could face criminal or administrative disciplinary action for any inappropriate use.

USER'S NAME (PRINT)

SIGNATURE

DATE

USER'S PHONE #

USER'S UNIT/SECTION/OFFICE SYMBOL

PERnet SECURITY AWARENESS BRIEFING

1. You have been assigned duties involving the use of the PERnet computer system which processes sensitive defense information at the unclassified sensitive two (US2) level. IAW Army Regulation 25-2, 14 November 2003 and is defined as follows:

US2 is unclassified information which primarily must be protected to ensure its availability, integrity and confidentiality. Such information may include logistics, medical care, personnel management, privacy act data, contractual data, and 'For Official Use Only' (FOUO) information.

2. All persons accessing an Automated Information System (AIS) will be part of a security training and awareness program IAW AR 25-2. The program will ensure that all persons responsible for managing AIS resources or who access and AIS are aware of proper operational and security-related procedures and risks. Your Information Assurance Security Officer (IASO) is required to have you read and sign this statement, and maintain it on file along with your access request.

3. Your job assignment requires receipt of logon and password that permits access to a computer system processing sensitive information. You must bear in mind that AR 25-2 requires all such password to be controlled at the highest level if sensitive information is on the system.

4. I (supervisor) am required to impress upon you the extreme need for caution and discretion in any contracts, either personal or professional. As in any interesting activity, the temptation is great to refer to your professional accomplishments. You are cautioned to avoid any conversation that could result in a disclosure of sensitive information received from PERnet systems to unauthorized personnel.

5. Personnel failing to comply with the rules and procedures of this activity will have their access revoked.

I have read the PERnet System Usage Agreement and the PERnet Security Awareness Briefing and understand my responsibilities.

USER'S SIGNATURE

DATE

SUPERVISOR'S SIGNATURE

DATE