

FOR OFFICIAL USE ONLY

Appendix 1 (Classified System User Account Request Procedure) to Annex H (Command, Control, Communications and Computer) to OPERATIONS ORDER 12-5, POF SUPPORT TO JCS/ USFK EXERCISES

References: See Base OPORD.

Time zone used throughout the order: Korean Standard Time (India).

1. **Classified Systems User Account:** The POF IMO will provide the account support for CENTRIX-K and SIPRNET to include administering the accounts.
 - 1) CENTRIXS-K (US and ROK Secret) User Account, administered by Joint Command Information Systems Activity (JCISA)
 - 2) Secure Internet Protocol Network (SIPRNET) also known as the Secure Wide Area Network – Korea (SWAN-K) (US Secret) User Account, administered by 1st Signal Brigade, Yongsan.

See the [POF's deployment website](#)

(<http://www.pof.usace.army.mil/About/OurOrganization/SecurityPlansandOperations/DeploymentInformation.aspx>) for correct forms and other information.

2. **Completing the DD2875 for CENTRIXS and SIPRNET:** Before the user digitally signs the DD2875 form, user should fill out all information (in the top portion), PART I 1-15 and 16a when establishing or modifying their USER ID. Instructions are on Page 3 of the form and below:
 - 1) Type of Request: Check Initial if you need a new account, Modification if you already have an account and need to make changes, or Deactivation if you want to delete your account. The new requests should be Initial.
 - 2) System Name: CENTRIXS-K if you need access to only US and ROK Secret; SWAN-K if you need access to only US Secret. If you need access to both, then it would be CENTRIXS-K/SWAN-K.
 - 3) Location: Yongsan, Korea
 - 4) Block#5: Type user AKO email address (@us.army.mil) or type user Enterprise Email (@mail.mil)
 - 5) Block#10: Make sure user select and type correct Information Awareness Exam of Training Date (annual training) (<https://ia.signal.army.mil/>)
 - 6) Block#13: Make sure user type their Common Access Card (CAC) DoD ID# or Electronic Data Interchange Personal Identifier (EDIPI) 10 digit number
 - 7) Block#16a: Make sure user type their CAC expiration date (ex, DEROS 14 Mar 2014)

(Once User signs, NO ONE can add/modify user's section)

-Before Supervisor digitally sign the DD2875 form PART II, Supervisor/Sponsor/Team Leader should complete

- 8) Block#14 and #15: Select "Authorized" and "Classified"
- 9) Block#16: select "I certify that this user requires access as requested."
- 10) Block 17-20b: Fill out Supervisor/Sponsor/Team Leader information before Supervisor/Sponsor/Team Leader digitally signs.

(Once Supervisor signs, NO ONE can add/modify the section)

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

Appendix 1 (Classified System User Account Request Procedure) to Annex H (Command, Control, Communications and Computer) to OPERATIONS ORDER 12-5, POF SUPPORT TO JCS/ USFK EXERCISES

11) Block#21-32 will be completed by POF IMO/S6 and SPO/S3.

3. Submitting the Documents for CENTRIXS: Send your documents (do not include social security numbers) no less than 30 days prior to STARTEX to the POF IMO/S6 Helpdesk helpdesk.pof@usace.army.mil . Before submitting your system access requests form to Helpdesk ensure you have all the necessary documents:

- 1) System Authorization Access Request (SAAR) DD2875 (Figure 1. SAAR DD2875). The DD2875form must be signed by the user, immediate supervisor, Information Owner, Information Assurance Support Officer, and the Security Manger by sequence.
- 2) United States Forces Korea (USFK) Joint Command Information Systems Activity (JCISA) CENTRIXS-K Acceptable Use Policy (Figure 2. JCISA AUP)
- 3) Information Assurance Awareness Exam Certificate (<https://ia.signal.army.mil/>).

4. Submitting the Documents for SIPRNet (SWAN-K): User will need to submit and complete following forms and mandatory training:

- 1) System Authorization Access Request (SAAR) DD2875 (For SIPRNet user account, you must submit .xpdf format form. .pdf format form is not acceptable by 1st Signal Brigade). The DD2875form must be signed by the user, immediate supervisor, Information Owner, Information Assurance Support Officer, and the Security Manger by sequence.
- 2) Korea LandWarNet (KWAN) AUP (Figure 3. KWAN AUP), see the [POF's deployment website](#).
- 3) Information Assurance Awareness Exam Certificate (<https://ia.signal.army.mil/>).
- 4) Mandatory Training: User MUST take from <https://iatraining.us.army.mil>.
**Need to register with an Army Knowledge Online, (AKO) <http://www.us.army.mil> account.
 - a) WNSF - Portable Electronic Devices and Removable Storage Media v2.0
 - b) WNSF - Phishing Awareness v1.0
 - c) WNSF - Safe Home Computing
 - d) WNSF - Personally Identifiable Information (PII) v1
- 5) Register and complete your profile setup: If you have an account in the Army Training and Certification Tracking System (ATCTS) site, [login](#) with your AKO UserID and password or CAC. The ATCTS site is <https://atc.us.army.mil/iastar/index.php>.
Once you login to the ATCTS site, you will see your profile information. Please verify/update /modify your Signal Command/FCIO and HQ/DRU information if needed.
If you don't have an account, please register with AKO account information or your CAC.
- 6) Make sure all the training records are shown on your ATCTS profile after taking training and tests. If all the training records are not verified by your ATCTS site manager, e-mail ATCTS Helpdesk at support@iastar.net (*please provide your AKO email address with your request for assistance*) with all training certificates. Ask ATCTS Helpdesk to verify all your training certificates.

-DoD IA Awareness Training, the site, <https://ia.signal.army.mil/DoDIAA>. There are two steps to complete. Once you complete "Step one: training" you should be able to print training certificate and after you complete "Step two: Annual DoD Information Assurance Awareness Exam " you should be able to print exam certificate. It takes time the status to be updated on your ATCTS site.

FOR OFFICIAL USE ONLY

Appendix 1 (Classified System User Account Request Procedure) to Annex H (Command, Control, Communications and Computer) to OPERATIONS ORDER 12-5, POF SUPPORT TO JCS/ USFK EXERCISES

- 7) Please make sure to send the signed KWAN Acceptable Use Policy (AUP) and DD 2875 to POF IMO/S6 Helpdesk (Helpdesk.pof@usace.army.mil).
- 8) Once DD2875 form is signed by the POF Information Owner, Information Assurance Support Officer, and the Security Manager, IMO/S6 will send you back a copy of the completed DD2875.
- 9) You must upload completed DD2875 and signed KWAN AUP into the ATCTS site.

Once everything completed, please send all forms and certifications to Helpdesk.pof@usace.army.mil. The POF Helpdesk must submit all forms and certifications to KWAN's Network Enterprise Center (NEC) for your KWAN/Enterprise Email User Account.

5. The POC for this action is the POF IMO/S6 Helpdesk (Helpdesk.pof@usace.army.mil). Please include your name, rank, grade and the words EXERCISE ACCOUNT REQUEST in the subject line.

FOR OFFICIAL USE ONLY

Appendix 1 (Classified System User Account Request Procedure) to Annex H (Command, Control, Communications and Computer) to OPERATIONS ORDER 12-5, POF SUPPORT TO JCS/ USFK EXERCISES

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)			
PRIVACY ACT STATEMENT			
AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act. PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form. ROUTINE USES: None. DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.			
TYPE OF REQUEST <input checked="" type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DEACTIVATE <input type="checkbox"/> USER ID			DATE (YYYYMMDD)
SYSTEM NAME (Platform or Applications) SIPRNET (Classified)		LOCATION (Physical Location of System) Yongsan, Korea	
PART I (To be completed by Requestor)			
1. NAME (Last, First, Middle Initial)		2. ORGANIZATION	
3. OFFICE SYMBOL/DEPARTMENT		4. PHONE (DSN or Commercial)	
5. OFFICIAL E-MAIL ADDRESS		6. JOB TITLE AND GRADE/RANK	
7. OFFICIAL MAILING ADDRESS		8. CITIZENSHIP <input type="checkbox"/> US <input type="checkbox"/> FN <input type="checkbox"/> OTHER	9. DESIGNATION OF PERSON <input type="checkbox"/> MILITARY <input type="checkbox"/> CIVILIAN <input type="checkbox"/> CONTRACTOR
10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS (Complete as required for user or functional level access.) <input type="checkbox"/> I have completed Annual Information Awareness Training. DATE (YYYYMMDD)			
11. USER SIGNATURE			12. DATE (YYYYMMDD)
PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 1 & .)			
13. JUSTIFICATION FOR ACCESS			
SIPRNET (Classified) access request Must type user's DOD ID# (10 digit number known as EDIPI number form CAC)			
14. TYPE OF ACCESS REQUIRED: <input checked="" type="checkbox"/> AUTHORIZED <input type="checkbox"/> PRIVILEGED			
15. USER REQUIRES ACCESS TO: <input type="checkbox"/> UNCLASSIFIED <input checked="" type="checkbox"/> CLASSIFIED (Specify category) <input type="checkbox"/> OTHER			
16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. <input checked="" type="checkbox"/>		16 a. ACCESS EXPIRATION DATE (Contractors must specify Company Name, Contract Number, Expiration Date. Use Block 27 if needed.)	
17. SUPERVISOR'S NAME (Print Name)	18. SUPERVISOR'S SIGNATURE	19. DATE (YYYYMMDD)	
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT	20 a. SUPERVISOR'S E-MAIL ADDRESS	20 b. PHONE NUMBER	
21. SIGNATURE OF INFORMATION OWNER/OPR	21a. PHONE NUMBER	21b. DATE (YYYYMMDD)	
22. SIGNATURE OF IAO OR APPOINTEE	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER	25. DATE (YYYYMMDD)

DD FORM 2875, AUG 2009

PREVIOUS EDITION IS OBSOLETE.

APD PE v1.00

<Figure 1. DD2875 form>

FOR OFFICIAL USE ONLY

Appendix 1 (Classified System User Account Request Procedure) to Annex H (Command, Control, Communications and Computer) to OPERATIONS ORDER 12-5, POF SUPPORT TO JCS/ USFK EXERCISES

USFK JCISA CENTRIXS-K Acceptable Use Policy 주한미군 통전부 정보체계처 지휘통제체계 사용인가 약관

1. **Understanding.** I understand that I have the primary responsibility to safeguard the information contained in USFK JCISA C2 Systems and Networks from unauthorized or inadvertent modification, disclosure, destruction, denial of service and use.

1. 동의. 본인은 인가 되지 않거나 부주의한 정보의 사용, 수정, 공개, 파괴, 소통 방해 등의 행위들로부터 주한미군 통전부 정보체계처 지휘통제체계 및 네트워크 내 정보를 보호할 일차적인 의무가 있음을 동의한다.

2. **Access.** Access to USFK JCISA C2 Systems and Networks is for official use and authorized purposes and as set forth in DOD 5500.7-R, "Joint Ethics Regulation", DODD 8500.1, "Information Assurance" or as further limited by this policy.

2. 접근. 국방성 규정 5500.7-R "합동 윤리 규정", 국방성 훈령 8500.1 "정보보증" 및 본 약관에 따라 주한미군 통전부 정보체계처 지휘통제체계 및 네트워크 접근은 업무 및 인가된 용도에 한한다.

3. **Revocability.** Access to USFK JCISA C2 Systems and Network resources is a revocable privilege and is subject to content monitoring and security testing.

3. 권한 해제. 주한미군 통전부 정보체계처 지휘통제 체계 및 네트워크는 내용물 감시 및 보안점검이 실시될 수 있으며, 이에 따라 사용자의 접근 권한이 해제될 수 있다.

4. **Applicability.** The USFK JCISA C2 Systems and Network resources provide information processing service for Classified releasable ROK/US. This Acceptable Use Policy applies to ALL ROK and US personnel who are required and are authorized access to the USFK JCISA C2 Systems and network resources.

4. 적용. 한미군 통전부 정보체계처 지휘통제 체계 및 네트워크는 한미간 기밀 정보처리 담당 체계를 제공한다. 사용인가약관은 주한미군 통전부 정보체계처 지휘통제 체계 및 네트워크에 대한 모든 한미 사용자의 접근 권한 및 승인부여에 적용된다.

5. **Classified information processing.** Your assigned government system(s) on USFK JCISA C2 Networks is a classified information system for your organization.

5. 기밀정보처리. 주한미군 통전부 정보체계처 지휘통제 체계는 소속 부서 공무를 위한 비밀정보 체계이다.

a. Your government system provides classified communication to your organization, the military services, external DOD elements, and other United States Government organizations. Primarily this is done via electronic mail. Your ROKUS classified system is approved to process up to ROKUS classified information only.

a. 이 체계는 소속부서, 각 군, 국방부 외부 부서 및 기타 미정부 기관에 비밀통신을 제공한다. 이통신은 일차적으로 이메일을 통해 이루어진다. 한미 비밀체계는 한미 비밀정보 처리용에 한하며, 미측 단독 비밀 체계는 미측 단독 비밀정보 처리에 한하여 사용토록 승인된다.

b. All government system users are responsible for preventing classified data "spillage." All removable media will be properly marked and these markings checked before use on a classified network. Media that is not marked or is improperly marked will not be used on the network. Data sent in e-mail attachments need to be properly marked, reviewed and verified before being sent over a classified network. Upon review, any question of being releasable will be reviewed and verified by the unit security manager or the foreign disclosure monitor. In the event of a classified data spillage, users will isolate the affected system and contact their security manager immediately.

b. 체계의 모든 사용자는 비밀 자료 "유출"을 방지할 책임이 있다. 모든 이동저장 매체는 정확히 등급 표기를 해야 하며, 비밀 네트워크에서 사용하기 전에 등급 표기를 확인해야 한다. 등급이 표기되지 않은

Version 2 dated July 7, 2011

Page 1 of 5

<Figure 2. USFK JCISA AUP>

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

Appendix 1 (Classified System User Account Request Procedure) to Annex H (Command, Control, Communications and Computer) to OPERATIONS ORDER 12-5, POF SUPPORT TO JCS/ USFK EXERCISES

USFK JCISA CENTRIXS-K Acceptable Use Policy 주한미군 통전부 정보체계처 지휘통제체계 사용인가 약관

매체의 네트워크 상 사용을 금한다. 이메일 및 첨부 파일로 전송할 데이터는 비밀 네트워크로 전송하기 앞서 정확히 등급을 표기, 검토, 검증해야 한다. 데이터 검토 시 해당 부대 보안 담당자 또는 대외 정보공개 담당관이 정보공개 문제를 검토 및 검증한다. 비밀 데이터가 유출 될 경우, 사용자는 문제된 체계를 차단시키고 즉시 해당 보안 담당자에게 연락을 취한다.

6. Personal Identifiable Information (PII) use. All PII designated by OMB Memorandum 07-16, the Health Insurance portability and Accountability Act of 1996 and the Privacy Act of 1974 will be protected in accordance with DOD 8400.11-R "DOD Privacy Program." PII will not be handled below a For Official Use Only (FOUO) designation.

6. 개인식별정보사용. OMB 양식 07-16, 1996년 제정된 건강 보험 양도 및 책임에 관한 법령, 1974년 제정된 개인정보 보호법에 따라 모든 개인식별정보는 국방성 규정 8400.11-R "국방성 규정 개인 정보 보호 강령"에 따라 보호를 받게 된다. 개인식별정보는 통제정보 아래 하에 취급되지 않는다.

7. Minimum security rules, requirements and unacceptable use. As a government system user, the following minimum security rules and requirements apply. I understand that monitoring of my assigned government system will be conducted for various purposes and information captured during monitoring may be used for administrative or disciplinary actions or for criminal prosecution.

7. 기본 보안 규칙. 지휘통제체계 사용자로서 다음의 기본 보안 규칙이 적용된다. 본인은 할당된 업무용 체계의 감시가 각종 목적을 위한 것이며, 감시 중 포착된 정보는 행정, 징계조치 또는 행사 기소 목적으로 사용될 수 있음에 동의한다.

I understand that the following activities include unacceptable uses of a government information system (IS):
본인은 다음의 행위가 정보체계의 사용 불가 사항에 해당됨을 숙지한다: (이니셜 기재)

_____ a. Personnel are not permitted access to any government systems unless authorized, trained and only after reading and completing this Acceptable Use Policy. I have completed initial user security awareness training and PII awareness training. I will participate in all training programs as required both before receiving system access and when refresher training is required.

_____ a. 사용자 인가, 교육 및 본 사용인가 약관을 숙지, 작성하기 전까지는 체계 접근을 불허 한다. 본인은 기초 사용자 보안의식 교육을 수료 하였으며, 체계 접근권한을 갖기 전이나 재교육이 필요할 때나 모든 교육 프로그램에 참석하겠다.

_____ b. I will immediately report the loss/suspected loss, compromised/suspected compromise, or discovery of PII and SI to the first O5 or GS14 in my chain of command and USFK JCISA.

_____ b. 본인은 주한미군통전부 정보체계처내 명령체계에 따라 분실 또는 분실이 의심되는 경우, 훼손 또는 훼손이 의심되는 경우, 개인식별정보와 민감한 정보사항의 습득을 O5(대령급) 또는 GS14에 즉시 보고한다.

_____ c. I will successfully complete the Personally Identifiable Information (PII) training prior to obtaining access to the USFK JCISA C2 Network(s).

_____ c. 본인은 주한미군통전부 정보체계처에 접근 권한을 부여받기에 앞서 개인식별정보 교육을 성공적으로 이수하기로 한다.

FOR OFFICIAL USE ONLY

Appendix 1 (Classified System User Account Request Procedure) to Annex H (Command, Control, Communications and Computer) to OPERATIONS ORDER 12-5, POF SUPPORT TO JCS/ USFK EXERCISES

USFK JCISA CENTRIXS-K Acceptable Use Policy 주한미군 통전부 정보체계처 지휘통제체계 사용인가 약관

_____ d. I will generate and protect passwords or pass-phrases. Passwords will consist of at least 14 characters with 3 each of uppercase, lowercase, numbers and special characters. I am the only authorized user of my account. I will not share personal accounts and passwords or permit the use of remote access capabilities by any individual.

_____ d.본인은 비밀번호를 작성하고 보호하겠다. 비밀번호는 최소 14 자리로 대문자, 소문자, 숫자, 특수문자 각각 3 자리를 포함하여 구성하도록 한다. 본인은 생성된 계정의 단독으로 인가된 사용자로서 본인의 계정 및 암호를 공유하지 않으며 타인의 사용을 불허한다.

_____ e. I will use only authorized government hardware and software. I will not install or use any personally owned hardware, software, shareware or public domain software. I will not disable or remove security or protective software or mechanisms and their associated logs. I will not alter, change, configure or use operating systems or programs, except as specifically authorized. I will not introduce executable code (such as, but not limited to .exe, .com, .vbs, or .bat files) without authorization, nor will I write malicious code. I will not add user-configurable or unauthorized software. I will not attempt to strain, test, circumvent, bypass security mechanisms or perform network traffic monitoring or keystroke monitoring.

_____ e.본인은 인가된 하드웨어 및 소프트웨어만을 사용할 것이며, 개인 소유 하드웨어, 소프트웨어, 공유웨어 또는 공개 소프트웨어를 절대 설치하거나 사용하지 않겠다. 본인은 보안 또는 보호용 소프트웨어, 매체 또는 관련 로그를 차단하거나 제거하지 않겠다. 특별히 인가되지 않는 이상 운영체제 또는 프로그램을 수정, 변경, 설정, 사용하지 않겠다. 허가 없이 실행가능 코드(.exe, .com, .vbs, .bat 파일과 같은 유형 및 기타 유형)를 삽입하지 않을 뿐만 아니라 악성코드도 기록하지 않겠다. 본인은 사용자 설정 또는 비인가 소프트웨어를 추가하지 않겠다. 보안장치를 오염, 시험, 회피, 바이패스 하지 않을 것이며, 네트워크 감시나 타건 감시를 금하겠다. (예: 웹브라우저 프록시 설정 변경)

_____ f. I will use USFK JCISA provided end point security and virus protection software and procedures before uploading or accessing information from any system, diskette, attachment, compact disk, thumb drive or any other removable and/or portable storage devices.

_____ f.본인은 모든 체계, 디스켓, 첨부파일, CD, USB 또는 기타 이동 저장장치의 정보를 저장하거나 접근하기 전 주한미군 통전부 정보체계가 제공하는 바이러스 검사 소프트웨어 및 최종 보안 절차를 활용하겠다.

_____ g. I will safeguard and mark with appropriate classification level, if required, all information created, copied, stored or disseminated from the information system and will not disseminate it to anyone without a specific need to know. I will not attempt to access or process data exceeding the authorized information system classification level. I will access information only for which I am authorized access to and have the specific need to know. I will not release, disclose or alter information without the consent of the data owner, the original classification authority (OCA) as defined by UNF-CFC Regulation 380-1, the individual's supervisory chain of command, Freedom of Information Act (FOIA) official, Public Affairs Office, or foreign disclosure officer's approval.

_____ g.본인은 생성, 복사, 저장되거나 정보체계에서 파생된 모든 정보를 보호할 것이며(필요 시 올바른 등급 표기) 특별한 사유 없이는 어느 누구에게도 전파하지 않겠다. 인가된 정보체계 등급을 초과하는 데이터를 접근하거나 처리하지 않을 것이며, 접근 인가가 있고 필요한 경우에만 정보에 접근하겠다. 본인은 유엔사 및 연합사 규정 380-1 에 의해 정보 자유법령 당국자, 공보실, 대외 공개

Version 2 dated July 7, 2011

Page 3 of 5

<Figure 2. USFK JCISA AUP>

FOR OFFICIAL USE ONLY

Appendix 1 (Classified System User Account Request Procedure) to Annex H (Command, Control, Communications and Computer) to OPERATIONS ORDER 12-5, POF SUPPORT TO JCS/ USFK EXERCISES

USFK JCISA CENTRIXS-K Acceptable Use Policy 주한미군 통전부 정보체계처 지휘통제체계 사용인가 약관

담당장교 등과 같은 지휘계통으로 규정된 원 등급 권한자(OCA) 즉, 데이터 소유권자의 허가 없이는 정보를 유포, 공개 또는 수정하지 않겠다

_____ h. I will not utilize DOD provided information systems for commercial use, financial gain or illegal activities. I will not use ISs in any manner that interferes with official duties, undermines readiness, reflects adversely on DOD or violates standards of ethical conduct. I will not intentionally send, store or propagate sexually explicit, threatening, harassing, political or unofficial public activity communications (LE/CI investigators, attorneys or other official activities operating in their official capacities only, may be exempted from this requirement). I will not participate in other activities inconsistent with public service.

_____ h. 본인은 국방성 제공 정보체계를 영리적인 이익 또는 불법행위의 목적으로 사용하지 않겠다. 공무를 방해하거나, 준비태세를 저하시키거나, 국방성에 대한 부정적 영향을 주거나, 윤리 강령 기준을 위배하는 범주의 정보체계 사용을 금하겠다. 본인은 노골적인 성표현, 위협적, 공격적, 정치적, 비공식적인 민간업무 (예를 들면 스팸 메일) 통신을 의도적으로 전송, 저장 또는 유포하지 않을 것이며, (공무 범위 내에서 체계를 운용하는 LE/CI 관련 조사관, 변호사 또는 공무 행위만이 본 조건 제의 대상 자임) 이 외에도 공무에 저해되는 기타 행위에 개입하지 않겠다.

_____ i. I will address any questions regarding policy, responsibilities and duties to my unit IASO. Maintenance of your system will be performed by USFK JCISA personnel and JCISA approved IMOs only. I will use screen locks and log off the system when departing the area.

_____ i. 본인은 정책, 책무, 의무에 관해서라면 소속 부대 정보보증 담당장교(IASO)에게 모든 것을 질의하겠다. 체계 경비는 주한미군 통전부 정보체계처 인원과 통전부 정보체계처에서 승인된 정보처리담당자(IMOs)에 한하며, 작업 장소를 떠날시 화면 잠금 기능을 사용하고 체계를 로그 오프 하겠다.

_____ j. I will immediately report any suspicious output, files, shortcuts or system problems to my unit IASO. I will report all known or suspected security incidents or violations of this Acceptable Use Policy and/or DODD 8500.1 or DODI 8500.2 to the IASO and USFK JCISA.

_____ j. 본인은 의심스런 출력, 파일, 비정상적 작업 또는 체계 이상 발생 시 즉각 소속 정보보증 담당장교에게 보고하겠다. 본인은 본 인가 사용 약관과 국방성훈령 8500.1 및 국방성지침 8500.2의 위반 행위 또는 알고 있거나 의심스러운 보안 사고 모두를 정보보증 담당장교 및 정보체계처에 보고하겠다.

_____ k. I understand that each information system is the property of the government and is provided to me for official and authorized uses. I further understand that each information system is subject to monitoring for security purposes and to ensure use is authorized. I understand that I do not have a recognized expectation of privacy in official data on the information systems and may have only a limited expectation of privacy in personal data on the information system and may only have a limited expectation of privacy in personal data on the information system. I realize that I should not store data on the information system that I do not want others to see.

_____ k. 본인은 각각의 정보체계가 정부 소유이며, 공무 및 인가된 용도로 사용토록 제공됨을 숙지한다. 또한 각각의 정보체계가 인가 사용을 보장하고 보안 목적을 위해 감시될 수 있음을 숙지한다. 또한 각각의 정보체계가 인가 사용을 보장하고 보안 목적을 위해 감시될 수 있음을 숙지한다. 본인은

Version 2 dated July 7, 2011

Page 4 of 5

<Figure 2. USFK JCISA AUP>

FOR OFFICIAL USE ONLY

Appendix 1 (Classified System User Account Request Procedure) to Annex H (Command, Control, Communications and Computer) to OPERATIONS ORDER 12-5, POF SUPPORT TO JCS/ USFK EXERCISES

USFK JCISA CENTRIXS-K Acceptable Use Policy
주한미군 통전부 정보체계처 지휘통제체계 사용인가 약관

정보체계 내 공무 데이터에 관해서는 프라이버시가 인정될 수 없으며 정보체계 내 개인 데이터 범주에서는 제한적으로만 프라이버시를 기대할 수 있음을 숙지한다. 본인은 타인에게 노출하기 싫은 데이터를 정보체계에 저장할 수 없음을 숙지한다.

8. Penalties. I understand that violations of this agreement may be punitive in nature and punishable under Article 92 of the UCMJ or ROK Only UNC/CFC Security Supplement Regulation (as amended 2004.12.01).

7. 처벌. 본인은 본 협약 위반 시 미군복무규율 92 조 또는 2004.12.01 개정 한국군용 유엔사/연합사 보안업무시행규칙에 의거하여 실제적인 형벌이나 처벌이 가해질 수 있음을 숙지한다.

9. Acknowledgement. I have read the above requirements regarding use of my assigned government system(s) on the USFK JCISA C2 Network(s). I understand my responsibility regarding my government system(s) and the information contained therein.

9. 인정. 본인은 본인에게 할당된 주한미군 통전부 정보체계처 지휘통제 체계 사용과 관련된 상기 필수조건을 숙지하였으며, 주한미군 통전부 정보체계처 지휘통제 네트워크 내 본인의 업무체계 및 정보와 관련된 책무를 숙지한다.

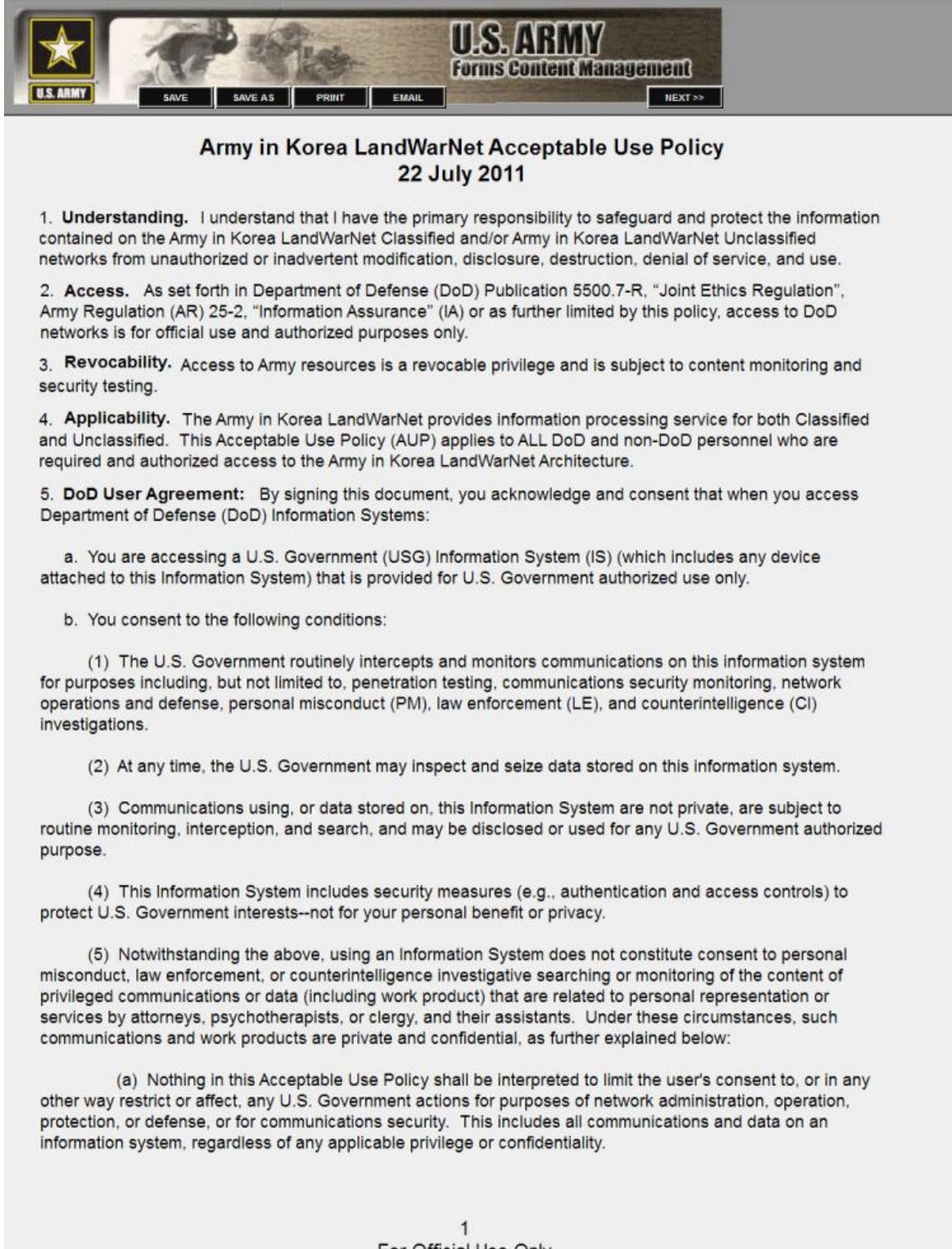
_____	_____
Unit/Division/Branch 부대/부처/과	Date 일자
_____	_____
Last Name, First, MI 성,이름	Rank/Grade 계급
_____	_____
Signature 서명	Phone Number 연락처

<Figure 2. USFK JCISA AUP>

FOR OFFICIAL USE ONLY

Appendix 1 (Classified System User Account Request Procedure) to Annex H (Command, Control, Communications and Computer) to OPERATIONS ORDER 12-5, POF SUPPORT TO JCS/ USFK EXERCISES

<Sample of KWAN AUP>

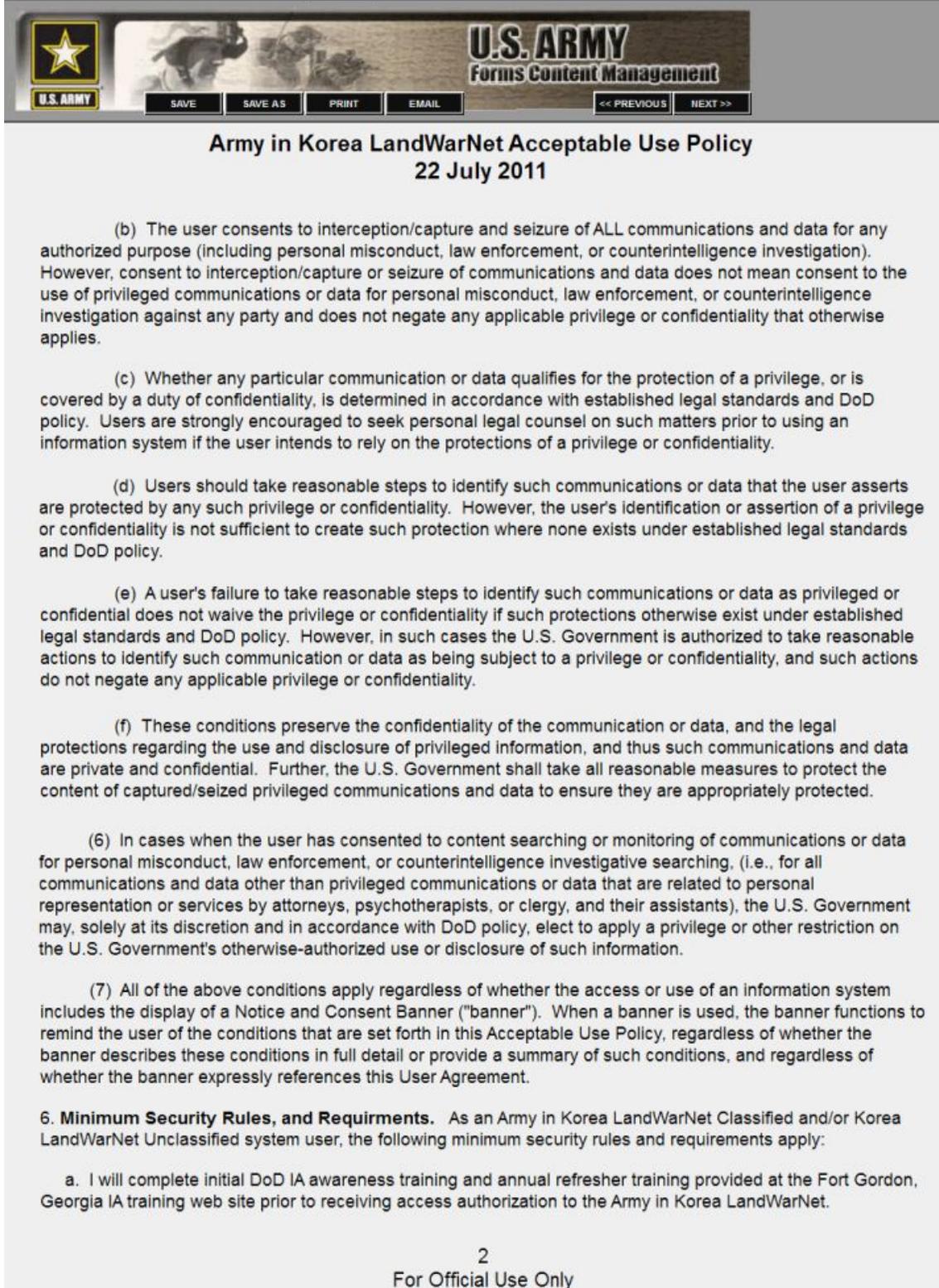


The screenshot shows a web interface for U.S. Army Forms Content Management. At the top, there is a header with the U.S. Army logo, a star, and the text 'U.S. ARMY Forms Content Management'. Below the header are buttons for 'SAVE', 'SAVE AS', 'PRINT', 'EMAIL', and 'NEXT >>'. The main content area displays the title 'Army in Korea LandWarNet Acceptable Use Policy' and the date '22 July 2011'. The document text includes five numbered sections: 1. Understanding, 2. Access, 3. Revocability, 4. Applicability, and 5. DoD User Agreement. Section 5 includes sub-sections a and b, with b containing five numbered conditions (1) through (5). At the bottom of the page, there is a page number '1' and the text 'For Official Use Only'.

<Figure 3. KWAN AUP>

FOR OFFICIAL USE ONLY

Appendix 1 (Classified System User Account Request Procedure) to Annex H (Command, Control, Communications and Computer) to OPERATIONS ORDER 12-5, POF SUPPORT TO JCS/ USFK EXERCISES



The screenshot shows a web interface for U.S. Army Forms Content Management. At the top, there is a navigation bar with a U.S. Army logo, a star icon, and a background image of soldiers. Below the logo are buttons for 'SAVE', 'SAVE AS', 'PRINT', 'EMAIL', '<< PREVIOUS', and 'NEXT >>'. The main content area displays the title 'Army in Korea LandWarNet Acceptable Use Policy' and the date '22 July 2011'. The text of the policy is presented in a list of paragraphs, each starting with a letter in parentheses. The text is as follows:

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

(c) 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.

(d) 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.

(e) 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.

(f) 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.

(6) In cases when the user has consented to content searching or monitoring of communications or data for personal 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.

(7) 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 Acceptable Use Policy, regardless of whether the banner describes these conditions in full detail or provide a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

6. Minimum Security Rules, and Requirements. As an Army in Korea LandWarNet Classified and/or Korea LandWarNet Unclassified system user, the following minimum security rules and requirements apply:

a. I will complete initial DoD IA awareness training and annual refresher training provided at the Fort Gordon, Georgia IA training web site prior to receiving access authorization to the Army in Korea LandWarNet.

FOR OFFICIAL USE ONLY

Appendix 1 (Classified System User Account Request Procedure) to Annex H (Command, Control, Communications and Computer) to OPERATIONS ORDER 12-5, POF SUPPORT TO JCS/ USFK EXERCISES



U.S. ARMY
Forms Content Management

SAVE SAVE AS PRINT EMAIL << PREVIOUS NEXT >>

Army in Korea LandWarNet Acceptable Use Policy 22 July 2011

b. I will use my common access card (CAC) for authentication on my government system and will not circumvent any installed security. I will remove my CAC when leaving my system for short periods of time and log off the system when departing the area for extended periods. I will perform a restart on my government system each work day to ensure that updates are applied. If required, I will generate, store, and protect passwords or pass-phrases. Passwords will be at least 15 characters, consisting of 2 each uppercase and lowercase letters, numbers and special characters. I will not share personal accounts and passwords or permit the use of remote access capabilities by any individual.

c. As a system user, I will not install or remove programs or hardware (government or personally owned), disable security configurations or audit logs, or alter operating system configurations. I will not attempt to strain, test, circumvent, bypass security mechanisms, or perform network line monitoring or keystroke monitoring. I will not introduce any executable code nor will I write any malicious code.

d. I will use virus-checking procedures before uploading or accessing information from any system or device. I will use government provided virus-checking software and procedures before uploading or accessing information from any system, diskette, attachment, compact disk, thumb drive, or any other removable and/or portable storage devices.

e. I will immediately report any suspicious output, files, shortcuts, or system problems to my unit Information Management Officer (IMO) and/or Information Assurance Support Officer (IASO) and cease all activities on the system. I will report all known or suspected security incidents, or violations of this acceptable use policy and/or AR 25-2 to the IASO, IMO, and Network Enterprise Center (NEC).

f. I will safeguard, and mark with the appropriate classification level, all information created, copied, stored, or disseminated from the information system and will not disseminate it to anyone unless they have a specific need to know. I will also include authorized official travel markings if I have been authorized to remove a government owned mobile computing device or data storage device from a government facility. I will not attempt to access or process data exceeding the authorized information system classification level. I will access information only for which I am authorized access to and have the specific need-to-know.

g. I will not utilize Army or DoD provided IS for commercial financial gain or illegal activities. I will not use IS in any manner that interferes with official duties, undermines readiness, reflects adversely on the Army, or violates standards of ethical conduct.

h. I will not intentionally send, store, or propagate sexually explicit, threatening, harassing, political, or unofficial public activity (spam) communications (LE/CI investigators, attorneys, or other official activities, operating in their official capacities only, may be exempted from this requirement.).

i. I will not misuse government resources involving: pornography or obscene material (adult or child); copyright infringement (such as the sharing of copyright material by means of peer-to-peer software); gambling; the transmission of chain letters; unofficial advertising, soliciting, or selling except on authorized bulletin boards established for such use; or the violation of any statute or regulation.

7. Protection of Personally Identifiable Information (PII), Sensitive Information (SI), and Data-at-Rest Requirements.

a. I will identify PII and SI data on any USG owned system, mobile computing device, data storage device, or removable media in my possession or under my control. I will safeguard all USG owned devices and data in my possession from loss, suspected loss, theft, unauthorized access, unauthorized disclosure, by any person or multiple persons that do not have an official need to know the information.

<Figure 3. KWAN AUP>

Appendix 1 (Classified System User Account Request Procedure) to Annex H (Command, Control, Communications and Computer) to OPERATIONS ORDER 12-5, POF SUPPORT TO JCS/ USFK EXERCISES

U.S. ARMY
Forms Content Management

SAVE SAVE AS PRINT EMAIL << PREVIOUS

Army in Korea LandWarNet Acceptable Use Policy 22 July 2011

b. I will not remove any USG owned computing device, data storage device, or removable media with PII or SI data from a government facility without approval of the Commander or Director in the grade of O6/GS15 and above in the chain of command.

c. I will encrypt all PII and SI sensitive data when removed from a USG facility, or when contained within an electronic mail. To encrypt electronic mail, I will use the encrypt email solution built into Microsoft Outlook. To encrypt data on removable media, I will use the solution outlined in the 8th Army Data-At-Rest (DAR) OPORD or the current capabilities of the operating system.

d. I will safeguard and protect PII and prohibit any uploading of PII on ALL USFK, 8th Army, or any other SharePoint portals operating on the Army in Korea LandWarNet architecture.

e. I will not download any PII or SI to a non-government owned computing system or device.

f. I will immediately report the loss/suspected loss, compromised/suspected compromise, or discovery of PII and SI to the first O5 or GS14 in my chain of command and the local servicing NEC.

g. I will successfully complete the Personally Identifiable Information (PII) training prior to obtaining access to the Army in Korea LandWarNet (Unclassified and Classified) networks.

h. As an Authorized Official Traveler, I will complete the official traveler's checklist and obtain approval prior to removing a device from a government facility IAW DAR 8th Army OPORD. Upon returning, I will take the device to the IMO, Information Assurance Manager (IAM), Information Assurance Support Officer (IASO), or System Administrator (SA), to be scanned using an Army approved compliance scanning tool prior to the device being reconnected to the network.

8. **Penalties.** I understand that violations of this agreement may be punitive in nature and punishable under Article 92 of the UCMJ or other administrative and criminal statutes. These violations are covered under AR 25-2, paragraph 1-1j.

9. **Acknowledgement.** I have read the above requirements regarding use of DoD and 8th Army IS. I understand my responsibilities for safeguarding and protecting these systems and the information contained

Unit/Directorate/Division/Branch _____ Date _____

Last Name, First, MI _____ Rank/Grade/Contractor _____

Signature _____ Phone Number _____

SIGNATURE _____

<Figure 3. KWAN AUP>