Headquarters
United States Forces Korea
Unit #15237
APO AP 96205-5237

United States Forces Korea
Regulation 25-71

25 January 2008

Information Management

CROSS DOMAIN SOLUTION MANAGEMENT

***This regulation supersedes USFK Regulation 25-71, dated 11 Aug 03**

For the Commander:

DAVID P. VALCOURT
Lieutenant General, USA
Chief of Staff

Official:

ANDREA. A WILLIAMS
Captain, AG
Chief of Publications and
Records Management

Summary. This regulation prescribes procedures for Cross Domain Solution (CDS) Management within the United States Forces Korea (USFK)

Summary of Change. This regulation has been substantially changed. A full review of its contents is required.

Applicability. This regulation applies to all Commands/Services/Agencies (C/S/A) and will remain in effect until otherwise superseded or rescinded by regulation or other appropriate media.

Supplementation. Issue of further supplements to this regulation by subordinate commands is prohibited unless prior approval is obtained from HQ USFK, (FKJ6-CIA), Unit #15237, APO AP 96205-5237.

Records Management. Records created as a result of processes prescribed by this regulation must be identified, maintained, and disposed of according to AR 25-400-2 or applicable service regulations. Record titles are available on the Army Records Information System (ARIMS) website at https://www.arims.army.mil.

Forms. USFK forms are available at www.usfk.mil.

Suggested Improvements. The proponent of this regulation is HQ USFK (FKJ6-CIA). Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the HQ USFK (FKJ6-CIA), Unit #15236, APO AP 96205-5236.

Distribution. Electronic Media Only (EMO).

CONTENTS

Section I
GENERAL

1. PURPOSE. This regulation promulgates procedures for CDS Management within USFK for all Secret and below networks. This regulation is to provide guidance to Commanders, Information Assurance (IA) personnel, system administrators (SA), network managers (NM), Information Management Officers (IMO) and computer users in developing a solution-oriented framework for the CDS interoperability.

2. REFERENCES.

a. The following are required publications:

(1) Department of Defense Instruction 5200.40 (Defense Information Assurance Certification and Accreditation Process (DIACAP) Cited in paragraphs 6b and 7a.

(2) Chairman of the Joint Chiefs Staff Instruction (CJCSI) 6211.02B Defense Information System Network (DISN): Policy, Responsibilities, and Processes, 31 July 2003.

(3) Unified Cross Domain Management Office (UCDMO) Cross Domain Inventory ver. 2.1, 30 July 2007 (or current approved version).

b. The following are related publications:

(1) Chairman of the Joint Chiefs Staff Manual (CJCSM) 6510.01C Information Assurance Defense-In-Depth, 30 March 2001.

(2) National Institute of Standards and Technology (NIST) 800-53, Recommended Security Controls for Federal Information Systems, October 2006.

(3) Department of Defense Instruction (DODI) 8500.2, IA Implementation, 6 February 2003.

(4) USFK Command Policy Letter #13, IA, 26 June 2006 cited in paragraph 5.

(5) USFK Communications System Requirements Review Board Policy, 11 June 2007.

(6) 1st Signal Brigade applicable connection policy and requirements validation.

(7) 607th ACOMS applicable connection policy and requirements validation.

3. Abbreviations and Terms. Abbreviations and terms used in this regulation are explained in the glossary.

Section II
POLICY AND PROCEDURES

4. POLICY

a. CJCSI 6211.02B Defense Information System Network (DISN): Policy, Responsibilities, and Processes, 31 July 2003 appendix C-D-1, outlines the requirements for CDS management

within the command. The goal of CDS management is to ensure interoperability solutions for the Warfighter (within acceptable risks) to protect the integrity of and reduce the risk to the United States Defense Information Infrastructure. It is a network-centric process with procedures to review interconnections and leverage proven certified UCDMO baseline CDS solutions. It is founded on Information System Security Engineering (ISSE) principles whereby information systems security (INFOSEC) is integrated as a part of systems engineering and systems acquisition processes, strong customer participation in support of mission needs, and the optimal use of INFOSEC disciplines to provide security solutions.

b. The UCDMO provides a CDS product baseline consisting of Data Transfer Solutions, Access Solutions, and Multiple-Level Security Solutions. The UCDMO baseline approved CDS systems are the only CDS systems that are approved for acquisition or use on USFK networks without Flag Officer approval.

c. C/S/As are directed to follow the DITSCAP (until transition to DIACAP) which consists of four phases: Definition, Verification, Validation, and Post-accreditation. The CDS process places the local C/S/As customer with appropriate engineering, risk, vulnerability, training, and programmatic support necessary to develop the right solution for the customer's CDS requirement. See Appendix A “The USFK CD Connection Process” for step-by-step instructions on evaluating CDS requirements and obtaining a technical solution.

4. RESPONSIBILITIES.

a. HQ, USFK, J622, IA.

(1) Update this publication to ensure compliance with the references. Interim changes to this publication will be accomplished with the addition of a Change Record Memorandum, which will be placed at the front of the publication.

(2) Act as the POC to PACOM J6, the UCDMO (including Service CDMO staff), and JCS J6T for all USFK CDS initial requests.

(3) Validate and prioritize all CDS tickets with PACOM J6, the UCDMO (including assigned Service CDMO) and the JCS J6T.

(4) Coordinate all CDS ticket actions with the UCDMO (including Service CDMO), service agencies, NSA, and the DSAWG.

(5) Track all theater CDS ticket statuses and report as required.

(6) Coordinate with applicable USFK agencies and units to establish funding for training assigned CDS Staff. Coordinate with the applicable CDS Program Office (PO) for scheduled CDS training on CDS systems deployed in USFK in order to comply with annual Federal requirements.

(7) Coordinate with applicable USFK agencies and units to establish funding for CDS life-cycle management including development of modifications to CDS data transfer filters (CDS channels), system upgrades and system replacements.

(8) Participate in the applicable network connection policy and process for approval, validation and prioritization of resources for CD Connections.

(9) Follow the instructions of Appendix A "USFK CD Connection Process."

(10) Assist USFK agencies/units with the USFK CD Connection Process.

b. USFK agency/unit requiring a CDS.

(1) Follow the instructions of Appendix A "USFK CD Connection Process."

(2) Follow the instructions of applicable network connection policies and processes for approval, validation and prioritization of resources for CD Connections.

(3) Provide a knowledgeable representative for network connection approval meetings when the required CDS is on the agenda.

c. USFK agency/unit owning and managing the "high-side" network transport the CDS will connect to. This network may be of any classification, and may be connected to the Global Information Grid (GIG) SIPRNet or NIPRNet, or be a locally managed network not connected to the GIG.

(1) Follow the instructions of Appendix A "USFK CD Connection Process."

(2) Follow the instructions of applicable network connection policies and processes for approval, validation and prioritization of resources for CD Connections.

(3) Provide a knowledgeable representative for network connection approval meetings when the required CDS is on the agenda.

(4) The "high-side" network DAA will be designated as the CDS DAA.

(5) The CDS DAA will formally assign staff responsible for administrative O&M of the CDS. This will include a POC for the SGS database (CDS registration in SGS is accomplished in the CDS Process), and capable staff to register the CDS in VMS, respond to IAVM notifications, maintain the finding status of the CDS assets in VMS, and coordinate with the applicable CDS PO for resolution (fix, mitigate or POAM) of open findings against the CDS.

(6) The CDS DAA will formally assign staff responsible for technical O&M of the CDS. This will include separate individuals as required to meet the CDS specific role requirements. Technical O&M of the CDS is a daily requirement, and generally cannot be accomplished remotely. Assigned staff must be scheduled to meet the daily technical tasks specified for the CDS.

(7) The CDS DAA will assign staff to assist the DISA Field Service Office (FSO) Enhanced Compliance Visitation (ECV) Teams during scheduled inspections of the CDS. The connection of a CDS to a network mandates annual network enclave reviews and Joint Task Force-Global Network Operations (JTF-GNO) directed compliance inspections will be carried out annually. The JTF-GNO has designated the DISA FSO to complete these inspections under the ECV guidelines. The results of the ECV inspection are reported directly to the CDS DAA, and the JTF-GNO.

APPENDIX A: USFK CD CONNECTION PROCESS

1. PROCESS OVERVIEW.

a. The USFK CD Connection Process is tied to the DOD Global CDS process as directed in the References. Agencies or units (hereafter called "the customer") that may need a Cross Domain Connection need to understand that the higher approving agencies may take months (current guidance from the DSAWG is 12-18 months) to render a favorable decision on the installation of a new CDS.

b. The DSAWG requires the DAA of the "high-side" network of the CD Connection will be the CDS DAA (hereafter called the "CDS DAA"). The CDS DAA is responsible for the CDS, and responsible to complete all CDS DAA actions required to support the CDS through processing and life-cycle.

c. The decision to use a CDS that is not on the UCDMO Baseline will significantly lengthen the approval process, and require additional funding.

d. The installation of a new Cross Domain Connection via an additional CDS Channel on an existing USFK CDS will significantly shorten the approval process and reduce cost.

e. The USFK CD Connection Process is designed to call on CDS Subject Matter Experts within USFK to facilitate the Global process and expedite operational use of the CDS for USFK.

f. All networks have a connection policy and process. The customer will comply with the applicable network policies and procedures. The CDS DAA will be the ultimate authority in USFK for connection of the CDS.

g. The USFK Communications System Requirements Review Board (RRB) Policy governs requirements for USFK C2 networks. Contact the RCIO for requirements policy and process for connecting to US Army networks. Contact 607 ACOMS for policy and process for connecting to US Air Force networks. For the purpose of this publication, all network connection policies will be referred to as the RRB.

h. Special emphasis will be placed on the RRB (or equivalent policy). This is an integral part of the USFK CD Connection Process and is designed to ensure resources are available to meet all requirements/costs for the initial CD Connection engineering, CDS Processing, CDS data transfer filter (CDS channel) development, CDS purchasing and delivery, and CDS O&M operations for the lifetime of the CDS.

i. The steps described in the PHASES below may be accomplished concurrently, or in some cases may need to be accomplished sequentially. The J622, IA Branch, will assist in determining when it is appropriate to take the specified actions.

2. PHASE 0 - DETERMINATION OF REQUIREMENT.

a. The customer determines the need to move data with an automated process from one Security Classification Domain to a second (or multiple) Domain(s) with a different Security Classification.

b. The customer identifies the network DAA(s) for all Security Domains that will be connected. If the customer cannot make this determination, then contact the USFK J622, IA Branch, for assistance.

c. The customer drafts an informal description of the data. If the customer cannot determine the technical description of the data, then contact the USFK J622, IA Branch, for assistance. The J622, IA Branch, is not responsible for making this description, but will assist the customer with contacting the applicable Security Domain technical staff. This description will include:

(1) The data source system. This may be multiple systems, and they may reside on multiple Security or Administrative Domains.

(2) The data destination system. This may be multiple systems, and they may reside on multiple Security or Administrative Domains.

(3) The format of the data. Some examples are ASCII text, XML, Fixed Format (i.e.: USMTF, COP tracks, SNMP).

(4) Any and all Port, Protocol, Services (PPS) used by the source/destination systems to disseminate or receive the data.

(5) Average and Maximum data transfer volume. This may be expressed as Messages per interval, or bandwidth/throughput required, or message file size, or some combination of two or more of these metrics.

(6) Fund cites available for CDS Processing, development, delivery, and system O&M and life-cycle.

d. The customer will contact the J622, IA Branch, when they have the information required in paragraphs 2.c (1) - (6) of this Appendix and are ready to attend the RRB for approval to proceed with the CD Connection Process.

e. The J622, IA Branch, will review the provided information and assist the customer with obtaining additional information if required.

f. The J622, IA Branch, will schedule the Initial RRB briefing. The J622, IA Branch, will notify the customer and the network and CDS DAA representatives of the RRB briefing time and location. The attendance at the RRB of the customer and the CDS DAA representatives are required.

g. The J622, IA Branch, will prepare the RRB Initial CDS briefing.

h. The RRB will receive the initial briefing. The briefing will be presented by the J622, IA, and the customer will be available to substantiate the data transfer requirement and importance. The RRB will render a decision on whether to proceed with the CD Connection Process, and determine what resources will be assigned as a minimum for Phase 1 of the process.

i. The J622, IA Branch, will contact all applicable network architecture/engineering staff for high level network diagrams. The diagrams will be updated to include the proposed CDS. The diagrams will show all enclave connections, and IA controls at the enclave boundaries. The

network diagrams are mandatory and will be provided to the CDS DAA staff for use in completing the CDA Phase 1.

j. The CDS DAA technical staff MAY begin working on the CDA Phase 1 if directed by appropriate authority.

k. The CDS DAA technical staff MAY begin working on the Data Owner Guidance (DOG) if directed by appropriate authority. The informal data description provided by the customer in paragraphs 2.c. (1)-(6) of this appendix will form the basis for the DOG.

l. The J622, IA Branch, will draft the Cross Domain Validation Approval Request (CDVAR) and submit it to the CDS DAA staff for review and modification.

m. The CDS DAA staff will present the CDVAR to the DAA for signature. The CDS DAA signature will validate the DAA is willing to accept responsibility for the CDS.

n. The customer will draft an Operational Need Statement (ONS) and submit to the applicable staff for review and modification.

o. The staff will present the ONS to the approval authority for signature. The approval authority signature will validate the requirement for the data transfer. The signed ONS will be provided to the customer.

p. The customer will contact the J622, IA Branch, when the ONS is signed and the customer is ready to attend the RRB for the final briefing and approval. The customer will provide a copy of the signed ONS to the J622, IA Branch.

q. The J622, IA Branch, will schedule the final RRB briefing. The J622, IA Branch, will notify the customer and the network and CDS DAA representatives of the RRB briefing time and location. The attendance at the RRB of the customer and the CDS DAA representatives are required.

r. The RRB will receive the final briefing. The briefing will be presented by the J622, IA Branch. The signed CDVAR and the signed ONS will be available for review. Any changes to the CD Connection requirement will be briefed. The RRB will render a decision on whether to proceed with CD Connection Processing, and determine what resources will be assigned as a minimum for Phase 1 of the process.

3. PHASE 1 - DEFINITION.

a. The customer must define the requirement for their proposed Cross Domain connection by first submitting an ONS to the USFK, J622, IA office, collecting all required information to include the data owner, and receive local DAA approval with a signed Cross Domain Validation Approval Request (CDVAR), as outlined on page C-D-A-1 in reference a (2). The J622 Cross Domain Management Office (CDMO) can be contacted at 723-6669.

b. The J622, IA Branch, will open a CD Request by accessing the Global Information Grid Interconnection Approval Process (GIAP) website at http://giap.disa.smil.mil, using the automated database to manage the CDS process.

c. The CDS DAA staff will draft a CDA Phase 1. The CDA Phase 1 is required to be signed and uploaded to the SGS database within 45 calendar days of opening the CD request. Failure to provide a Phase 1 CDA within 45 days will result in termination of the CD request. A copy of the draft will be provided to the J622, IA Branch, for review and recommendations.

d. The CDS DAA staff will complete the DOG. The DOG 1 is required to be signed and uploaded to the SGS database within 45 calendar days of opening the CD request. Failure to provide a DOG within 45 days will result in termination of the CD request. A copy of the DOG will be provided to the J622, IA Branch, for review and recommendations.

e. The J622, IA Branch, will provide a copy of the CDA Phase 1 to the customer. The CDA Phase 1 requires the customer representative signature.

f. The J622, IA Branch, will provide a copy of the DOG to the customer. The DOG requires the customer representative signature.

g. The CDS DAA staff will present the CDA Phase 1 to the CDS DAA for signature. The CDA Phase 1 requires the CDS DAA signature.

h. The J622, IA Branch, will upload the signed CDA Phase 1 to the applicable CD request on the SGS website.

i. The J622, IA Branch, will upload the signed DOG to the applicable CD request on the SGS website.

j. The J622, IA Branch, will complete all SGS database entries required for the CD request. This information will be forwarded to the SIPRNET Connection Approval Office, (SCAO).

k. The SCAO will contact the SGS POC to verify administrative data is correct, assign a CDS ticket number, and provide a solution from the UCDMO CDS baseline list if a solution from the baseline list has not been formally requested for by the C/S/A. NOTE: C/S/As are encouraged to use a solution from the UCDMO baseline list due to cost and time constraints placed on certification and accreditation of un-certified CDS solutions.

l. The J622, IA Branch, will monitor the CDS process and will act as the liaison for C/S/As and the SCAO.

4. PHASE 2 - VERIFICATION.

a. The CDS DAA technical staff will prepare and staff the CDA Phase 2. The CDA Phase 2 is required to be signed and uploaded to the SGS database for review by the CDTAB, risk assessment by the NSA, and approval of the DSAWG for CDS installation and STE. A copy of the CDA Phase 2 will be provided to the J622, IA Branch, for review and recommendations.

b. The J622, IA Branch, will provide a copy of the CDA Phase 2 to the customer. The CDA Phase 2 requires the customer representative signature.

c. The J622, IA Branch, will upload the signed CDA Phase 2 to the applicable CDS ticket on the SGS website.

d. The J622, IA Branch, will complete all SGS database entries required for the CDS ticket. This information will be forwarded to the SCAO.

e. Ticket gets assigned to an ISSE team.

f. ISSE team will contact the CDS DAA POC and begin dialog on the CDA/SSAA.

g. ISSE team will conduct a Preliminary System Security Authorization Agreement Assessment Report (PSAR) to ensure CDA is complete and process can continue.

h. If corrections are needed the CDS DAA technical staff will update the CDA Phase 2 and resubmit to the ISSE team for review.

i. ISSE team will perform a full review, or System Security Authorization Agreement Assessment Report (SAR).

(1) Positive result from SAR will get support for an interim approval to connect (IATC), or interim approval to test (IATT).

(2) Negative result the C/S/A will recompile SSAA with guidance from ISSE team and re-submit.

j. Once SAR is complete, a System Security Engineer (SSE) will review the SAR for quality control.

k. SSE contacts Process Action Team (PAT) to schedule a meeting to review the technical and administrative aspects of the MSL connection.

(1) Positive result from PAT will get support for an interim approval to connect (IATC), or interim approval to test (IATT).

(2) Negative result the C/S/A will recompile SSAA with guidance/recommendations from PAT and resubmit.

l. Once approved, CDS Operations will forward the recommendation to the Defense Information Switching Network (DISN) Security Accreditation Working Group (DSAWG) for approval. NOTE: DSAWG is responsible for granting any connection to the SIPRNET, and advising the CDS DAA for connections that are not on the SIPRNET.

m. The SCAO will contact the CDS DAA POC with IATC/IATT and duration of testing.

5. PHASE 3 - VALIDATION.

a. The CDS PMO security team will conduct a Security Test and Evaluation (ST&E) on the system.

b. The CDS DAA technical staff will support the CDS Program Office installation and STE activities.

c. The independent STE agency submits the STE report to the NSA for review and risk assessment, and the certification authority for approval.

d. The CDS DAA technical staff will prepare and staff the CDA Phase 3. The CDA Phase 3 is required to be signed by the CDS DAA and uploaded to the SGS database for review by the CDTAB, risk assessment by the NSA and approval of the DSAWG. This will be the final approval for CDS operation. A copy of the CDA Phase 3 will be provided to the J622, IA Branch, for review and recommendations.

e. The J622, IA Branch, will provide a copy of the CDA Phase 3 to the customer. The CDA Phase 3 requires the customer representative signature.

f. The J622, IA Branch, will upload the signed CDA Phase 3 to the applicable CDS ticket on the SGS website.

g. The J622, IA Branch, will complete all SGS database entries required for the CDS ticket. This information will be forwarded to the SCAO.

h. ISSE team will conduct PSAR and SAR, (as explained in paragraph 7d), before making a compliance recommendation to the PAT.

i. PAT team reviews all the documentation and forwards a recommendation for Approval to Connect (ATC) to DSAWG.

j. DSAWG grants ATC. System is approved for operation.

k. The CDS DAA staff complete the network accreditation update to include the final version of the CDS design.

6. PHASE 4 - POST ACCREDITATION.

a. The CDS DAA is responsible for operating their approved cross domain solutions on their enclaves in compliance with approved conditions.

b. The CDS DAA or DAA approved representative must validate site information through GIAP on an annual basis.

c. 30 months after compliance approval C/S/As must resubmit their SSAA to the SCAO for revalidation.

d. J622, IA is responsible for contacting C/S/As 6 months prior to expiration of SSAA.

NOTE: Ticket will be closed and sites will have to start at Phase 1 if they fail to turn in the required documentation for revalidation.

GLOSSARY

ABBREVIATIONS

CDA	Cross Domain Appendix
CDS	Cross Domain Solution
C/S/A	Commands/Services/Agencies
DAA	Designated Approving Authority
DIACAP	Defense Information Assurance Certification and Accreditation Process
DISN	Defense Information Switching Network
DOG	Data Owner Guidance
DSAWG	DISN Security Accreditation Working Group
GIAP	Grid Interconnection Approved Process
GIG	Global Information Grid
IA	Information Assurance
IATC	Interim Approval to Connect
IATT	Interim Approval to Test
IMO	Information Management Officer
INFOSEC	Information Systems Security
ISSE	Information System Security Engineering
MSL	Multiple Security Level
NM	Network Manager
ONS	Operational Need Statement
PACOM	Pacific Command
PAT	Process Action Team
PO	Program Office
POC	Point of Contact
SA	System Administrator

SCAO SIPRNET Connection Approval Office

SIPRNET Secret Internet Protocol Router Network

SSAA System Security Authorization Agreement

SSE System Security Engineer

ST&E Security Test and Evaluation

UCDMO Unified Cross Domain Management Office

USFK United States Forces Korea