

USFK REGULATION 25-71

INFORMATION MANAGEMENT (25)

SECRET and Below Interoperability

11 August 2003

UNCLASSIFIED

HEADQUARTERS
UNITED STATES FORCES, KOREA
UNIT #15237
APO AP 96205-5237

USFK Regulation
No. 25-71

11 August 2003

(Effective: 11 August 2003)
Information Management

SECRET AND BELOW INTEROPERABILITY

SUPPLEMENTATION. Supplementation of this regulation and issuance of command and local forms by subordinate commands is prohibited unless prior approval is obtained from the Commander, USFK (FKJ6-CIA), Unit #15237, APO AP 96205-5237.

INTERNAL CONTROLS. This regulation does not contain management control checklists.

1. PURPOSE. This regulation prescribes procedures for Secret and Below Interoperability (SABI) within the United States Forces Korea (USFK).

2. APPLICABILITY. This instruction applies to all Commands/Services/Agencies (C/S/A).

3. REFERENCES.

a. The following are required publications:

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

(2) United States Forces Korea (USFK) Information Assurance Policy Letter #29, 22 March 2001. Cited in paragraph 5.

b. The following are related publications:

(1) Department of Defense Manual 8510.1-M, Defense Information Technology Security Certification and Accreditation Manual (DITSCAP).

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

4. INTENT. The intent of 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 interoperability. This regulation is the result of a conscious decision to concentrate on key elements of the SABI program.

USFK Reg 25-71

5. INTRODUCTION.

a. USFK Information Assurance Policy Memorandum, 22 March 2001, para 6.6.2 and 6.6.3 prescribe the requirements for SABI within the command. The goal of SABI is to ensure interoperability solutions for the Warfighter (within acceptable risks) to protect the integrity of and reduce the risk to the United States (U.S.) Defense Information Infrastructure. It is a network-centric process with procedures to review interconnections and leverage proven solution reuse. 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. C/S/As are directed to follow the DITSCAP. The SABI process teams the local C/S/As site customer with appropriate engineering, risk, vulnerability, training, and programmatic support necessary to develop the right solution for the customer's SABI requirement. National Security Agency (NSA) and Defense Intelligence Service Agency (DISA) provide assistance in solution identification, system security engineering, INFOSEC training, risk analysis, and help coordinate a community effort to develop and execute joint vulnerability assessments.

c. The SABI framework follows the DITSCAP, which consists of four phases: Definition, Verification, Validation, and Post-accreditation. (Appendix A, Separate pullout document).

6. PHASE 1 - DEFINITION.

a. C/S/As must define the requirement for a multiple security level connection, collect all information, and receive local DAA approval.

b. Provide Phase 1 System Security Authorization Agreement (SSAA), IAW DoDI 5200.40 (DITSCAP), to the Sensitive Internet Protocol Router Network (SIPRNET) Connection Approval Office (SCAO).

c. Open a SABI ticket by accessing the Global Information Grid Interconnection Approval Process (GIAP) Website at <http://giap.disa.smil.mil>, using the automated tool to manage the SABI process.

d. Answer critical questions needed to determine a multiple security level connection (MSL), or single level connection.

e. Enter administrative information about the connection, such as site and DAA POC information. This information will be forwarded to the SCAO.

f. The SCAO will contact DAA POC to verify administrative data is correct, assign a SABI ticket number, and provide a solution from the SABI Referenced Implementation (SRI) list. If C/S/A requests unproven solution, SCAO advises C/S/As of the cost and schedule risks and continues process. **NOTE: C/S/As are encouraged to use a solution from the SRI list.**

g. Contact USFK J6 IA Division, Strategic Plans Branch, with ticket number and administrative information. J6-IA will monitor the SABI process and will act as the liaison for C/S/As and the SCAO.

7. PHASE 2 - VERIFICATION.

a. Provide Phase 2 SSAA, IAW DODI 5200.40 (DITSCAP), to SCAO.

b. Ticket gets assigned to an ISSE team.

c. ISSE team will contact the DAA POC and begin dialog on the SSAA.

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

e. If corrections are needed C/S/A will update SSAA and resubmit to the ISSE team for review.

f. 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 resubmit.

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

h. 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.

i. Once approved, SABI 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.**

j. SCAO will contact DAA POC with IATC/IATT and duration of testing.

k. Notify J6-IA with status of ticket.

USFK Reg 25-71

8. PHASE 3 - VALIDATION.

- a. C/S/A will conduct a Security Test and Evaluation (ST&E) on the system.
- b. C/S/A submits Phase 3 SSAA to ISSE team.
- c. ISSE team will conduct PSAR and SAR, (as explained in paragraph's 7d and 7e), before making a compliance recommendation to the PAT.
- d. PAT team reviews all the documentation and forwards a recommendation for Approval to Connect (ATC) to DSAWG.
- e. DSAWG grants ATC. System is approved for operation.
- f. Present J6-IA with copy of SSAA and approval letters.

9. PHASE 4 - POST ACCREDITATION.

- a. Local DAA is responsible for operating their approved enclaves in compliance with approved conditions.
- b. 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. J6-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 SSAA for revalidation.

Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander, USFK (FKJ6-CIA), Unit #15237, APO AP 96205-5237. This publication is available on the Eighth Army homepage at: <https://www-eusa.korea.army.mil>

FOR THE COMMANDER:



F. W. MORRIS
Assistant Adjutant General

OFFICIAL:
CHARLES C. CAMPBELL
Lieutenant General, USA
Chief of Staff

- 1 Appendix
- A. SABI Flow Pullout (Separate Powerpoint File)

Glossary

DISTRIBUTION:
Electronic Media Only

GLOSSARY

Abbreviations

ATC	Approval to Connect
C/S/A	Commander in Chief/Service/Agencies
DISA	Defense Intelligence Service Agency
DISN	Defense Information Switching Network
DITSCAP	Defense Information Technology Security Certification and Accreditation Process
DSAWG	DISN Security Accreditation Working Group
GIAP	Grid Interconnection Approved Process
IA	Information Assurance
IATC	Interim Approval to Connect
IATT	Interim Approval to Test
IAW	in accordance with
IMO	Information Management Officers
INFOSEC	Information Systems Security
ISSE	Information System Security Engineering
MSL	Multiple Security Level
NM	Network Managers
NSA	National Security Agency
PAT	Process Action Team
POC	Point of Contact

USFK Reg 25-71

PSAR	Preliminary System Security Authorization Agreement Assessment Report
SA	Systems Administrator
SABI	Secret and Below Interoperability
SAR	System Security Authority Agreement Assessment Report
SCAO	SIPRNET Connection Approval Office
SIPRNET	Sensitive Internet Protocol Router Network
SRI	SABI Referenced Implementation
SSAA	System Security Authorization Agreement
SSE	System Security Engineer
U.S.	United States (of America)
USFK	United States Forces Korea

SEE

USFK REG 25-71

PULLOUT

IN A

POWERPOINT

SEPARATE

DOCUMENT ON THIS

WEBSITE