DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND
5001 EISENHOWER AVENUE, ALEXANDRIA, VA 22333-0001

AMC Supplement 1   20 February 1996
to AR 530-1

Operations and Signal Security

OPERATIONS SECURITY (OPSEC)

This supplement may be further supplemented by major subordinate
commands (MSC) and separate reporting activities (SRA) of the Army
Materiel Command (AMC). One copy each of supplement will be provided to
the Deputy Chief of Staff for Intelligence (DCSINT), ATTN: AMXMI-SCM and
the Chief, AMC Security Support Division, ATTN: AMXMI-SD.

AR 530-1, 3 March 1995, is supplemented as follows:

Page i, Applicability. Add the following:

This supplement applies to Headquarters, AMC; AMC MSCs and SRAs,
including subordinate installations and activities; and AMC program,
product and project managers.

Page ii, Appendixes. Add Appendix M, Requests for Technical
Surveillance Countermeasures (TSCM) Services, and Appendix N,
Preparation of OPSEC Plan.

Page 1, paragraph 1-1, Purpose. Add the following:

This supplement implements AR 530-1, Operations Security (OPSEC). It
prescribes policies and procedures for the establishment and management
of the AMC OPSEC Program.

Page 1, paragraph 1-6, Application. Add to subparagraph f:

    (3) AMC activities involved in treaty inspections will ensure an
OPSEC annex and/or plan is included in each treaty implementation and
compliance plan.

_____

Page 1, paragraph 1-6, Application. Add subparagraph g:

   g. AMC commanders will apply the OPSEC planning sequence as outlined in paragraph 3-3 of the basic regulation to the programs as listed and in the priority shown below:

      (1) Special access programs (SAP) under the proponency of AMC.

      (2) Programs involving classified information.

      (3) Treaty Inspections.

      (4) Programs involving militarily critical technologies.

      (5) Programs involving the physical security of arms, ammunition and explosives, and any assets valued in excess of $10,000 as described in AR 190-11 and AR 190-51.

      (6) Programs involving privileged information provided to AMC in the procurement or personnel arena (Privacy Act).

      (7) Programs involving information, other than classified information, exempt from public disclosure under the Freedom of Information Act (FOIA). This includes the proprietary information of prospective and current contractors if the content falls within those areas identified by the OPSEC planning guidance of the commander of the AMC contracting activity.

      (8) Programs involving the exchange of information, coproduction, and codevelopment between AMC and foreign governments and contractors.

      (9) Other programs as directed.

Page 1, paragraph 1-7, Proponent. Add the following to first paragraph:

"or OPSEC is assigned to the staff element the commander deems can best implement an OPSEC program. The Deputy Chief of Staff for Intelligence (DCSINT) is the HQ AMC staff proponent for the AMC OPSEC Program."

Page 1, paragraph 1-7, Proponent. Add the following to subparagraph b.

"or OPSEC is assigned to the staff element the commander deems can best implement an OPSEC program. The Deputy Chief of Staff for Intelligence (DCSINT) is the HQ AMC staff proponent for the AMC OPSEC Program."

Page 2. Add paragraph 1-8:

1-8. Definition of OPSEC.

OPSEC is a process of analyzing friendly actions attendant to military operations and other activities to--

a.   Identify those actions that can be observed by adversary intelligence systems.

b.   Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

c.   Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

Page 2, paragraph 2-1, All commanders at battalion and higher echelons. Add subparagraphs c through g:

c.   All materiel developers must furnish proper OPSEC guidance to test agencies when classified or sensitive materiel is subjected to testing. If there are no OPSEC considerations applicable to the materiel or act of testing, the test agency is to be so advised in writing.

d.   AMC commanders with missions in research and development will also--

(1) Establish a command security/OPSEC program to identify and protect classified and sensitive information. The program will encompass related activities at test centers, ranges, laboratories, contractor facilities, and deployment locations, as required.

(2) Identify all categories of information regarding the program or project that, for the present and foreseeable future, fall into one of the following four categories:

(a) Unclassified information concerning the program or project identifiable as being in the public domain or releasable to the public (see AR 360-5, Public Information). NOTE: Coordinate with Public Affairs elements for guidance on public release.

(b) Sensitive Information requiring essential secrecy.

(c) Classified but present security measures are sufficient (see AR 380-5, Department of the Army Information Security Program).

(d) Classified and requires special access security measures (see AR 380-381, Special Access Programs).

(3) Reassess the security/OPSEC posture of the activity at each major milestone of the research and development cycle through the conduct of OPSEC surveys and implement necessary changes.

(4) Prepare an OPSEC plan per appendix N of this supplement to be included with the Test Program Requirement (TPR) when test and evaluation (T&E) is initiated. Materiel developers will use the local threat assessment provided by the T&E sponsor when developing OPSEC plans. This guidance will be provided to the T&E sponsor at least 90 days prior to test.

e. AMC commanders with a test and evaluation or quality assurance mission will--

(1) Prepare local threat assessments of the test facilities under their control to be made available to AMC materiel developers requiring test and evaluation or quality assurance support.

(2) Conduct OPSEC assessments of the test facilities under their control to evaluate the degree of compliance of subordinate organizations with the published OPSEC plan or OPSEC program.

f. AMC commanders with a logistics or readiness mission will--

(1) Incorporate OPSEC protective measures in all functions performed in support of the operations plans of other Army MACOMs and the Unified and Specified commands.

(2) Perform OPSEC surveys and assessments of all exercise participation by elements of their command and incorporate the findings into future exercise, logistics, and operations planning.

g. AMC commanders will ensure OPSEC measures are included in AMC industrial activities and contracts when it is essential to protect classified or sensitive information.

Page 2, paragraph 2-5, Commander, U.S. Army Materiel Command (AMC). Add the following to subparagraph a:

The DCSINT will ensure OPSEC principles and procedures are effectively implemented. Additionally, the AMC DCSINT will--

(1) Support the MSC/SRA commander with OPSEC guidance and assistance through staff assistance visits, correspondence, and conferences.

(2) Respond to inquiries from MSCs and SRAs regarding OPSEC and U.S. Army Intelligence and Security (INSCOM) OPSEC support.

(3) Support the AMC proponent for the Acquisition Systems Protection Program (ASPP) with OPSEC guidance and assistance through membership on working groups and OPSEC survey teams.

(4) Provide or obtain OPSEC support to Headquarters, AMC.

Page 2, paragraph 2-5, Commander, U.S. Army Materiel Command (AMC). Add the following to subparagraph b:

The AMC DCSINT is responsible for coordination of such efforts within AMC.

Page 2, paragraph 2-5, Commander, U.S. Army Materiel Command (AMC). Add the following to subparagraph c:

    (1) The AMC Deputy Chief of Staff for Research, Development, and Engineering (AMCRD) is responsible for identifying OPSEC requirements for Research and Development (R&D) beyond Technology Base programs (i.e., 6.3b and beyond) within AMC including the assigning of tasks to subordinate commands, as required.

    (2) The Director, Army Research Laboratory (ARL) is responsible for identifying OPSEC requirements for Technology Base R&D within AMC including the assigning of tasks to subordinate commands, as required.

    (3) Each AMC staff element with life cycle management responsibilities will coordinate with U.S. Army Training and Doctrine Command (TRADOC) to provide consistency to OPSEC throughout Army life cycle development and logistical support.

Page 2, paragraph 2-5, Commander, U.S. Army Materiel Command (AMC). Add the following to subparagraph d:

The Commander, U.S. Army Aviation and Troop Command (ATCOM), is responsible for coordinating with the U.S. Army Chief of Engineers.

Page 2, paragraph 2-5, Commander, U.S. Army Materiel Command (AMC). Add subparagraphs f, g, and h:

    f. The Deputy Chief of Staff for Personnel (AMCPE) will ensure that the AMC Security Support Division (AMXMI-SD) examines AMC activities for compliance with this supplement and the basic regulation during their command inspections. AMXMI-SD will provide copies of their inspection reports that include OPSEC to the ODCSINT (AMXMI-SCM).

    g. Incorporate OPSEC into appropriate treaty implementation and compliance plans.

    h. Incorporate OPSEC into appropriate exercise and field test directives and contingency planning documents.

Page 3, paragraph 2-9, Program Executive Officers (PEO) and Program Managers Project Managers/Product Managers (PM). Add subparagraph e:

    e. AMC subordinate intelligence organizations and OPSEC POCs will provide functional support to the PEOs/PMs as requested. Support

includes assistance in the preparation of OPSEC plans and conduct of OPSEC assessments and surveys.

Page 4, paragraph 3-2, OPSEC programs. Add the following to first sentence of subparagraph a:

Within AMC, the OPSEC officer for each MSC/SRA will be appointed in writing with a copy furnished to AMXMI-SCM. Commanders will determine the administrative method for the appointment of OPSEC POCs in their own OPSEC planning guidance.

Page 4, paragraph 3-2, OPSEC Programs. Add the following to second sentence of subparagraph a:

"or OPSEC is assigned to the staff element the commander deems can best implement an OPSEC program."

Page 4, paragraph 3-2, OPSEC programs. Add the following to subparagraph e:

All MSCs and SRAs will submit an annual OPSEC Activities Report. MSCs will submit one consolidated report covering their subordinate elements. The forwarding of the reports of subordinate elements will not satisfy this requirement. Reports will be addressed to Commander, AMC, ATTN: AMXMI-SCM to arrive no later then 1 November each year. A copy of the AMC consolidated report will be disseminated to all reporting activities for information.

Page 5, paragraph 3-8, Application of appropriate countermeasures (OPSEC measures). Add subparagraph g:

    g. The benefits from OPSEC protective measures will be evaluated to determine whether they clearly outweigh the costs prior to incorporation into the OPSEC plan or annex. The MSC/SRA Commander is responsible for the implementation of OPSEC protective measures and the conduct of OPSEC surveys.

Page 6, paragraph 3-11, Intelligence threat analysis support to OPSEC. Add the following:

The local threat assessment required for OPSEC planning purposes will be prepared by the local commander with the assistance of the local military intelligence (MI) and security support organizations. Requests for Foreign Intelligence Services (FIS) threat analysis support will be submitted directly to the local resident office of the supporting MI organization. Those activities without local MI support will submit their requests to AMXMI-SCM for assistance. Requests for Counter-intelligence (CI)/OPSEC service in the absence of local MI support will be forwarded to AMXMI-SCM for submission to INSCOM. All requests for TSCM inspections and surveys will be forwarded to AMXMI-SCM for further

processing on INSCOM Form 40 (Request for TSCM Services). See appendix M of this supplement for assistance in processing INSCOM Form 40.

Page 6, paragraph 4-1, General. Add the following:

This review is not to be confused with a "security review," which identifies classified information within publications and is conducted per ARs 360-5 and 380-5. The security review may be conducted concurrently with the OPSEC review.

Page 6, paragraph, 4-2, Procedures. Add the following to subparagraph a:

Other documents such as abstracts, papers, technical reports, articles, point papers, news releases, short items to be included in other publications, academic papers on work-related subject matter, speeches, briefings, media presentations, training materials, munitions cases, environmental impact statements, and other forms of information, including film, audio tapes and videocassettes, which could divulge critical information, will be subjected to OPSEC review. Also included is information released through Internet and creation/establishment of Home Pages on World-Wide Web.

Page 6, paragraph 4-2, Procedures. Add subparagraphs d and e.

    d. The individual conducting the OPSEC review will--

      (1) Be technically qualified relative to the subject matter.

      (2) Be generally aware of the current foreign intelligence interest and methods of collection.

      (3) Certify the benefit of the release of the information outweighs the potential damage to the essential secrecy of projects, programs, weapons systems, and items of materiel that have been determined to require OPSEC protective measures. The specific net benefit need not be identified for the record but the reviewer must be prepared to defend his or her position if challenged.

    e. The OPSEC officer will establish and implement an effective OPSEC review process within the organization, to include maintenance of records of OPSEC reviews, as appropriate.

        (1) These records are subject to the review of the organizational OPSEC officer and Public Affairs/Information officer or representative. Additionally, these records will be made available to inspectors of the AMC Security Support Division and Inspector General.

        (2) These records will reflect the following items of information concerning each OPSEC review conducted within the activity: name, grade, and position/title of the reviewer; date of review;

identification of the information reviewed; abstract, summary, or copy of the information reviewed; recommendation of the reviewer; and certification that subparagraphs d(1) through (3) above have been accomplished.

(3) The certification will read substantially as follows:

"I, the undersigned, am aware of the foreign intelligence interest in open source publications and in the subject matter of the information I have reviewed for OPSEC purposes. I certify that I have sufficient technical expertise in the subject matter of this paper and that, to the best of my knowledge, the net benefit of this public release outweighs the potential damage to the essential secrecy of all related (command/activity), AMC, Army, or other DOD programs of which I am aware. //signature, date//."

(4) The reviewer must determine whether sensitive information is involved. Should the reviewer determine that the sensitive information in the item would cause damage to the national security if released, the local security manager should be consulted immediately for further classification guidance.

(5) The organization OPSEC/FOIA adviser, designated per AR 25-55, will be familiar with exemptions of the FOIA and their applicability to the sensitive information identified in the OPSEC planning guidance of their organizations.

Page 6, Section II, OPSEC Assessment, paragraph 4-4. Add the following to subparagraph a:

Commanders will provide funding and manpower as appropriate for the conduct of OPSEC surveys and assessments in support of their OPSEC program (not including TSCM). Advice and guidance is available from the supporting MI unit for the management and conduct of surveys and assessments.

Page 6, Section II, OPSEC Assessment, paragraph 4-4. Add subparagraph c:

c. OPSEC assessment should be conducted prior to impending treaty inspection/visit.

Page 9, paragraph 6-1, Overview. Add the following:

Instructions to contractors will cover the total problem by addressing vulnerabilities and countermeasures. They will be oriented to those instances in which evaluations indicate program weaknesses which could lead to disclosure of sensitive information. OPSEC plans should be included in these contracts.

Page 9, paragraph 6-2, Policy and procedures. Add subparagraphs h through o:

   h. Contracts that do not involve classified information will not contain OPSEC requirements beyond those protective measures present at the contractor facilities where the work is to be performed, unless needed to provide protection for unclassified militarily critical technology or as required in the basic regulation and this supplement.

   i. Unclassified contracts imposing OPSEC requirements are not under the jurisdiction of the Defense Investigative Service for compliance inspection. The contracting agency is responsible for ensuring the contractor is adhering to OPSEC contract provisions when included in unclassified contracts.

   j. Existing AMC programs and projects that have not undergone OPSEC review shall be examined biennially, within the contract life cycle, to determine if OPSEC protective measures are required.

   k. AMC contracting officers will ensure that AMC contractors submit all information under the proponency of AMC for OPSEC review prior to public release. This includes technical papers based on findings of RDTE done under AMC contract. Contracting officers will also ensure established information release review procedures are adhered to when coordinating contractor-generated requests for public release.

   l. Reference to Army and AMC OPSEC directives is not sufficient as the total requirement for OPSEC in an AMC contract. OPSEC protective measures will be detailed as specific provisions in AMC contracts. Where the contractor is required to prepare OPSEC planning guidance for a program or project, the correct provision will be to make an OPSEC plan or annex a deliverable product to be prepared per Army or AMC directives.

   m. When OPSEC is incorporated into a procurement package, the applicable requirements will be stated on the DD Form 1423 (Contract Data Requirements List), the Statement of Work (SOW), the DD Form 1664 (Data Item Description), and, when applicable, on the DD Form 254 (Contract Security Classifications Specifications).

   n. DD Forms 254 will only be annotated to incorporate OPSEC when the required OPSEC protective measures are above and beyond those outlined in DOD Regulation 5220.22M, DOD National Industrial Security Program Operating Manual (NISPOM).

   o. Release of intelligence information under AMC contracts is prohibited without approval by the originator (see AR 381-1, Security Controls on the dissemination of Intelligence Information) and must be accomplished prior to issuing threat portions of OPSEC planning requirements in contracts.

(1) Requests for release of data marked not releasable to foreign nations (NOFORN) will be submitted to AMXMI-SCM for forwarding to the intelligence community originator.

(2) The threat provisions of appendix E, basic regulation, though general in nature, may be sufficient for contract purposes and should be considered in lieu of the classified product provided through MI channels.

Page 10, Appendix A, References, Section ll, Related Publications. Add the following:

DODD 5530.3
International Programs

Page 12, Appendix C, Sample Questions for Essential Elements of Friendly Information (EEFI). Add the following sample list of AMC Essential Elements of Friendly Information (EEFI).

This list is not exclusive or restrictive. AMC commanders are encouraged to create new categories and to be more specific when defining command EEFI in their OPSEC planning guidance.

C-6. Supplies.

d. What are the system parameters/capabilities/ vulnerabilities and can they be easily identified?

e. What is the readiness rate of our equipment?

C-21. Research, Development, Test and Evaluation (RDT&E) Programs).

e. What is the status and priorities of the specific RDTE project or program?

f. Do we have foreign cooperation; and, if so, to what extent?

g. What is the identified threat?

h. What militarily critical technology do we want to control?

i. What are the capabilities of the technology?

j. How much lead time does the U.S. enjoy over other countries in these technologies?

C-28. <u>Foreign Military Sales</u>.

    a. Who are our current and potential foreign customers?

    b. What is the materiel, technology, and/or information they are considering?

C-29. <u>Security</u>.

How effective is the command security program in protecting sensitive information/materiel?

C-30. <u>Readiness and contingency planning</u>.

How will we handle contingency operations and crises?

<u>Page 15, paragraph E-7, Non-traditional threats</u>. Add the following:

Individuals involved in international and security assistance programs are more apt to come in contact with non-traditional threats. At a minimum these individuals should review delegation disclosure authority letters (DDL) on periodic basis to ensure the terms and limitations.

<u>Page 18, Appendix I, Annual OPSEC Report Format</u>. Add the following to paragraph 1-3.

Summarize difficulties encountered implementing the regulation and this supplement. Make recommendations for correction of policy to solve the problem. Identify systemic problems in other AMC-wide or local practices, policies, and procedures that have OPSEC implications.

<u>Page 23</u>. Add appendixes M and N.

> The proponent of this supplement is the United States Army Materiel Command. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander, HQ AMC, ATTN: AMXMI-SCM, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001.

FOR THE COMMANDER:

OFFICIAL: BILLY K. SOLOMON
                                       Major General, USA
                                       Chief of Staff

LEROY TILLERY
Chief, Printing and Publications
Branch

DISTRIBUTION:
Initial Distr H (47) 1 ea HQ Acty/Staff Ofc
LEAD (SIOLE-DO-I) (2)
AMCIO-I-SP stockroom (150)

SPECIAL:
HQ IOC/AMSIO-IML (4)
ARL/AMSRL-CI-TG (4)
ATCOM/AMSAT-B-D-CARP (4)
CBDCOM/AMSCB-CIR (4)
CECOM/AMSEL-IM-BM-I (4)
LOGSA/AMXLS-IM (4)
MICOM/AMSMI-RA-SO (4)
SSCOM/AMSSC-S-IMS (4)
STRICOM/AMSTI-CS (4)
TACOM/AMSTA-DRM (4)
TECOM/AMSTE-CT-N (4)
USASAC/AMSAC-IM-O (4)

APPENDIX M

REQUESTS FOR TECHNICAL SURVEILLANCE
COUNTERMEASURES (TSCM) SERVICES

1. <u>Purpose</u>. This appendix prescribes the procedures for requesting TSCM services within AMC.

2. <u>Reference</u>. AR 381-14, (S) Technical Surveillance Countermeasures (U), 3 November 1986.

3. <u>Applicability</u>. This appendix applies to all activities as stated in the introduction to this supplement.

4. <u>Definitions</u>. Definitions of TSCM Services are listed below:

    a. <u>TSCM Survey (540)</u>. A service performed by Certified TSCM Special Agents (CTSA) to ascertain that offices, conference rooms, rooms, emergency operations centers, etc., where sensitive classified defense information is discussed on a frequent basis, are free of clandestine technical surveillance systems, hazards, and weaknesses, and to furnish recommendations for the elimination of these situations in order to obtain a technical security posture commensurate with pertinent regulations.

    b. <u>TSCM Inspection (550)</u>. A service performed by CTSAs as a follow-up action to a CI Technical Survey to determine the effectiveness of established technical security policies, compliance with applicable regulations, and to ensure elimination of technical security surveillance systems, hazards, and weaknesses. This service also includes limited TSCM inspections such as in-conference monitors and inspections of equipment. Separate codes have been added to clearly define which type of technical inspection is desired.

        (1) 551 - Technical inspection with in-conference monitor.

        (2) 552 - Radio Frequency Search.

        (3) 554 - Equipment inspection.

    c. <u>Preconstruction Technical Assistance (AAO)</u>. This service consists of rendering security advice during the planning phase for the construction of or modification to secure areas. It is designed to ensure that all technical and physical security aspects are considered in planning and are included in initial construction to obviate costly modifications of security features after an area is constructed.

    d. <u>Technical Security Advice and Assistance (AAI)</u>. This service is simply informal advice and assistance and may be requested directly from the servicing unit. No formal report is rendered nor is this type support considered in the programming cycle.

5. <u>Policy</u>. Requesters will review the provisions of reference and submit requests to AMXMI-SCM or the supporting MI unit per the procedures prescribed.

6. <u>Procedures</u>. AMC requesters will use INSCOM Form 40 (Request for TSCM Services). The form will be completed by following the instructions in this supplement (M-3 through M-12). Requests will be submitted to AMXMI-SCM for forwarding to INSCOM by letter justifying the request and providing sufficient background for the ODCSINT to assist in the filling of the requirement. Copies of INSCOM Form 40 may be obtained from AMXMI-SCM for local reproduction.

Items 1 - 7, 20 - 25, and 27 for INSCOM and servicing unit use only.

ITEM NO	ITEM NAME	ENTRY REQUIREMENT	INFORMATION TO BE SUPPLIED
1.	REQUESTER NUMBER	FOR INSCOM USE ONLY	Enter the five-digit requester number of the major requester submitting this form.
	SEQUENCE NUMBER	FOR INSCOM USE ONLY	Enter the five-digit sequence number of this request. The first digit of this number represents the fiscal year in which the service is to be performed.
2.	SERVICING UNIT	FOR INSCOM USE ONLY	Enter the name of the MI unit or other servicing organization that will perform the service. The following codes will be used:

CODE	UNIT
902	MI Bn (CI)(Technical) 902d MI Group, Ft Meade, MD.
66	66th MI Group, Munich GE
470	470th MI Group, Panama
501	501st MI Group, Seoul, KS
650	650th MI Group, SHAPE BE
NIS	Naval Security & Investigative Service Command, WASH DC
OSI	Air Force Office of Special Investigations, Bolling AFB, WASH DC

ITEM NO	ITEM NAME	ENTRY REQUIREMENT	INFORMATION TO BE SUPPLIED
3.	NUMBER OF SERVICES	FOR INSCOM USE ONLY	This block is used when the same service is accomplished more than once in a given timeframe. For example: Advice and Assistance support is rendered on 5 separate locations within the same facility and for the same requester. The entry in this block would

Items 1 - 7, 20 - 25, and 27 for INSCOM and servicing unit use only.

ITEM NO	ITEM NAME	ENTRY REQUIREMENT	INFORMATION TO BE SUPPLIED
			then be "05" and the total number of man-hours for all 5 services will be included in the man-hours block (Item 7). This block will be filled in only if more than one service is conducted. The entry "01" is not required.
4.	STATUS	FOR INSCOM USE ONLY	Enter one of the following codes for the status of the service:

CODE   STATUS

P   PENDING - Service is waiting to be performed.

R   RESCHEDULED - A previously scheduled service will be accomplished on a different date than the originally scheduled one.

C   CANCELLED - The service will not be performed. When a service is cancelled by a servicing unit, the reason for the cancellation must be entered in the remarks block (Item #34).

F   FINISHED - The service has been performed and the report written and dispatched.

N   NONVALIDATED - The area on which support was requested does not meet validation criteria.

M   MISSION SHORTFALL - INSCOM resources were not available to provide the support.

ITEM NO	ITEM NAME	ENTRY REQUIREMENT	INFORMATION TO BE SUPPLIED
5.	SCHEDULED DATE	FOR USE BY SERVICING MI UNIT ONLY	Enter the date on which the service will be performed. Dates will be entered by year, month, and day. EXAMPLE: 851012 schedules the service for 12 October 1985. If a specific day has not been determined, simply enter the year and month with zeros for the day, i.e., 851000.

M-4

Items 1 - 7, 20 - 25, and 27 for INSCOM and servicing unit use only.

ITEM NO	ITEM NAME	ENTRY REQUIREMENT	INFORMATION TO BE SUPPLIED
6.	COMPLETION DATE	FOR USE BY SERVICING MI UNIT ONLY	Enter the date the service was completed using the same format as defined in item 5, Scheduled Date. Completion date is the last day of the on-site visit.
7.	MAN-HOURS	FOR USE BY SERVICING MI UNIT ONLY	Enter the total number of man-hours expended to complete the service. Enter the number at the right side of the box and fill the left side with zeros, as appropriate. For example, 20 man-hours should be entered as 00020. On-site time, travel time to and from the site, time expended for preparation for the service and report writing, should all be included in the total man-hours.
8.	UNIT OR ACTIVITY	TO BE COMPLETED BY REQUESTER OF SERVICE	Enter the name of the unit, activity, installation or project requiring the service. Do not use periods in any abbreviations. Examples of entries are as follows: HQ FORSCOM; HQ INSCOM; USAISC Det Huachuca, etc.
9.	POST OR STREET ADDRESS	TO BE COMPLETED BY REQUESTER OF SERVICE	Enter the post name (military installation) or the street address of the unit which is to be serviced, i.e., FT MEADE or 1710 W. Maine Ave.
10.	CITY	TO BE COMPLETED BY REQUESTER OF SERVICE	Enter the city in which the unit to be serviced is located. If a unit is located on a military installation, no entry in this block is required.

M-5

Items 1 - 7, 20 - 25, and 27 for INSCOM and servicing unit use only.

ITEM NO	ITEM NAME	ENTRY REQUIREMENT	INFORMATION TO BE SUPPLIED
11.	STATE	TO BE COMPLETED BY REQUESTER OF SERVICE	Enter one of the following state codes if the unit is located in the United States. If the unit to be serviced is located in a country other than the United States, see item 12.

CODE	STATE	CODE	STATE
AL	Alabama	MO	Missouri
AK	Alaska	MT	Montana
AZ	Arizona	NE	Nebraska
AR	Arkansas	NH	New Hampshire
CA	California	NM	New Mexico
CO	Colorado	NC	North Carolina
CT	Connecticut	NV	Nevada
DE	Delaware	NJ	New Jersey
DC	District of Columbia	NY	New York
		ND	North Dakota
FL	Florida	OH	Ohio
GA	Georgia	OK	Oklahoma
HI	Hawaii	OR	Oregon
ID	Idaho	PA	Pennsylvania
IL	Illinois	RI	Rhode Island
IN	Indiana	SC	South Carolina
IA	Iowa	SD	South Dakota
KA	Kansas	TN	Tennessee
KY	Kentucky	TX	Texas
LA	Louisiana	UT	Utah
ME	Maine	VT	Vermont
MD	Maryland	VA	Virginia
MS	Mississippi	WA.	Washington
MN	Minnesota	WV	West Virginia
MI	Michigan	WI	Wisconsin
MA	Massachusetts	WY	Wyoming

Items 1 - 7, 20 - 25, and 27 for INSCOM and servicing unit use only.

ITEM NO	ITEM NAME	ENTRY REQUIREMENT	INFORMATION TO BE SUPPLIED
12.	COUNTRY	TO BE COMPLETED BY REQUESTER OF SERVICE	Enter one of the following country codes to indicate the country in which the unit to be serviced is located.
13.	ZIP CODE OR APO/FPO	TO BE COMPLETED BY REQUESTER OF SERVICE	Enter the ZIP CODE or APO/FPO of the unit to be serviced.
14.	BUILDING	TO BE COMPLETED BY REQUESTER OF SERVICE	Enter the name or the numerical designation of the building in which the unit to be serviced is located.

CODE	COUNTRY	CODE	COUNTRY
AU	Austria	NL	Netherlands
BE	Belgium	PN	Panama, Republic of
DK	Denmark	PR	Puerto Rico
CH	China, Republic of	RP	Philippines
EG	Egypt	SA	Saudi Arabia
FR	France	SW	Switzerland
GE	Germany, Republic of	TQ	Trust Territory of the Pacific Isl
GU	Guam		
GR	Greece	TU	Turkey
IC	Iceland	UK	United Kingdom
IY	Iraq (Neutral Zone)	US	United States
IU	Israel	BQ	US Misc Caribbean Isl
IT	Italy	IO	US Misc Pacific Isl
JA	Japan	VQ	Virgin Islands
KS	Korea, Republic of	WO	Wake Islands
MQ	Midway Islands	WB	West Berlin
NO	Norway		

M-7

Items 1 - 7, 20 - 25, and 27 for INSCOM and servicing unit use only.

ITEM NO	ITEM NAME	ENTRY REQUIREMENT	INFORMATION TO BE SUPPLIED
15.	ROOM NO.	TO BE COMPLETED BY REQUESTER OF SERVICE	Enter the room or room numbers in which the service is to be performed. If several rooms are involved, enter See Rmks in this block and then enter all additional data in Item 34.
16.	POINT OF CONTACT	TO BE COMPLETED BY REQUESTER OF SERVICE	Enter either the name or position of the individual to be contacted for purposes of coordination between the servicing unit and the facility to be supported.
17.	RANK	TO BE COMPLETED BY REQUESTER OF SERVICE	Enter the rank, grade, or title of the point of contact identified in Item 16.
18.	TELEPHONE NUMBERS	TO BE COMPLETED BY REQUESTER OF SERVICE	Enter the DSN or commercial telephone number of the point of contact. (If commercial, do not forget the area code.) Either the DSN or the commercial telephone number, (to include OCONUS) must be entered in this block.
19.	TYPE OF SERVICE	TO BE COMPLETED BY REQUESTER OF SERVICE	Enter one of the following codes based upon the type of service desired. (See para 4 of this app for definition of services.)

CODE	TYPE OF SERVICE
540	Technical Survey
550	Technical Inspection
551	Technical Inspection with In-conference Monitor
552	Radio Frequency Search
554	Technical Equipment Inspection
AA0	Preconstruction Technical Assistance
AA1	Technical Advice and Assistance

Items 1 - 7, 20 - 25, and 27 for INSCOM and servicing unit use only.

ITEM NO	ITEM NAME	ENTRY REQUIREMENT	INFORMATION TO BE SUPPLIED
26.	PRIMARY USE OF AREA	TO BE COMPLETED BY REQUESTER OF SERVICE	Enter the primary use of the area to be serviced based upon the following codes:
27.	SCIF ID NUMBER	FOR INSCOM USE ONLY	Unique ID number assigned to a specific sensitive compartmented information facility (SCIF).
28.	ACCESS CLEARANCE	TO BE COMPLETED BY REQUESTER OF SERVICE	Enter one of the following codes based upon the type of security clearance personnel performing the service must have in order to gain access to the area to be serviced.

Item 26:

CODE	PRIMARY USE	CODE	PRIMARY USE
ADP	ADP FACILITY	R&D	RESEARCH AND DEVELOPMENT
CFR	CONFERENCE ROOM	RES	RESIDENCE
CLS	CLASSROOM	SAP	SPECIAL ACCESS PROGRAM
EAF	EMERGENCY AC- TION FACILITY	SIG	SIGINT
EOC	EMERGENCY OPERATIONS CENTER	SPJ	SPECIAL PROJECT
		SIS	SI/SAO AREA
		SPW	SPECIAL WEAPONS AREA
IOA	INTEL OPS AREA	TCC	TELECOMMUNICATIONS CTR
OFC	OFFICES	VEH	VEHICLES
		O	OTHER (Indicate in Item 34)

Item 28:

CODE	CLEARANCE	CODE	CLEARANCE
S	SECRET	M4	TS/CRYPTO
TS	TOP SECRET	M5	TS/SI/TK/CRYPTO
M1	TS/SI/TK	M6	TS/SI/TK/CNWDI/NATO
M2	TS/SI	O	OTHER - (Indicate other access requirements in Item 34)
M3	TS/CNWDI		

Items 1 - 7, 20 - 25, and 27 for INSCOM and servicing unit use only.

ITEM NO	ITEM NAME	ENTRY REQUIREMENT	INFORMATION TO BE SUPPLIED
29.	SECURITY CONTROLS	TO BE COMPLETED BY REQUESTER OF SERVICE	Indicate the types of security controls applied to the area to be serviced by placing an X in the boxes corresponding to the following codes. Leave the box blank if that type of control is not used.

	TYPE OF			TYPE OF	
CODE	CONTROL		CODE	CONTROL	
GF	Guard Force		CA	Controlled Access	
ID	Intrusion De- tection Sys		PS	Pass and Badge System	
			24	24-Hour Operation	
PB	Physical Barrier		LR	Locked Room	
			RA	Restricted Area	

| 30. | NUMBER OF TELEPHONES | TO BE COMPLETED BY REQUESTER OF SERVICE | Enter the number of telephones within the area to be serviced. SGL indicates the number of single line telephones; MUL, the number of multiple line telephones; and DIR indicates the number of call director telephones. If the number of each type of telephone is less than 10, place a zero in the left space and the number in the right space, i.e., 01, 04, etc. If there are no telephones in the area to be serviced, fill all spaces with zeros. |

| 31. | SIZE OF AREA | TO BE COMPLETED BY REQUESTER OF SERVICE | Enter only the size of the area to be serviced expressed in square feet. (NOTE: This item is extremely important and should be as accurate as possible, since the size of an area is used as a guide by INSCOM to determine the approximate amount of time that will be required to perform the service.) Do not give dimensions of entire buildings when only a given area within will be subjected to a service. Decimal |

M-11

Items 1 - 7, 20 - 25, and 27 for INSCOM and servicing unit use only.

ITEM NO	ITEM NAME	ENTRY REQUIREMENT	INFORMATION TO BE SUPPLIED
32.	CLASSIFI-CATION OF DISCUSSION	TO BE COMPLETED BY REQUESTER OF SERVICE	points should not be used in this item. If the square footage is 125.6, round this figure up to the next higher figure--126; if the square footage equals 125.4, round the figure down--125. Enter the code for the highest classification if discussions held in the area to be serviced. <u>CODE</u>　　<u>CLASSIFICATION OF DISCUSSIONS</u> I　　SI M　　SI/SAO T　　TOP SECRET S　　SECRET O　　OTHER (Specify in item 34)
33.	FREQUENCY DISCUSSED	TO BE COMPLETED BY REQUESTER OF	Enter one of the following codes to indicate the frequency of classified discussions held in the area to be serviced. <u>CODE</u>　　<u>FREQUENCY OF DISCUSSIONS</u> D　　Daily W　　Weekly M　　Monthly Q　　Quarterly Y　　Yearly
34.	REMARKS	OPTIONAL ENTRY	Enter any other information that would be helpful in the scheduling of a service.

APPENDIX N

PREPARATION OF OPSEC PLAN

1. Purpose. This appendix prescribes the format and procedures for
preparing Operations Security plans.

2. Applicability. The guidance in this appendix applies to all
programs and projects for items of materiel and weapons systems which are
the responsibility of the Army Materiel Command.

3. Policy. OPSEC plans will be prepared--

    a. At the inception of RDTE (Concept Phase) programs or projects.
The plan will be updated at each milestone of the acquisition cycle.

    b. For programs or projects within the acquisition phase at each
principle milestone of the acquisition cycle.

    c. At the inception of programs, projects or other activities which
support the acquisition cycle and/or the Army Technology base, other than
6.1 research.

4. Procedures.

    a. An OPSEC plan will be prepared prior to the finalization of any
security classification guide.

    b. Plans will conform to the format in paragraph 5 below. They will
be reviewed and, if necessary, updated at every significant project
milestone. OPSEC follow-up is essential to the success of the plan.
Plans must be continually updated to reflect the changing nature of the
threat and to reflect adjustments to OPSEC measures.

    c. Applicable security classification guides will be referred to
when developing OPSEC plans.

5. Format. AMC OPSEC plans will contain, at a minimum, the elements
below:

    a. General.

    (1) Identity of the system(s) or activity(ies) item(s) covered by
the plan and of the categories of critical information that must be
protected.

    (2) Essential Elements of Friendly Information.

    (3) Reference to the applicable security classification guide.

(4) Identity of points of contact for clarification of guidance, including secure voice, commercial, and DSN telephone numbers.

b. Applicable collection threat.

(1) Human Intelligence (HUMINT), including media.

(2) Signals Intelligence (SIGINT) and other electronic threats, including TEMPEST.

(3) Imagery Intelligence (IMINT), including overhead, handheld, and infrared collection threats.

(4) Other technical collection methods that would be effective against the item.

c. Vulnerabilities and countermeasures. Characteristics of the item or program susceptible to the identified collection threats. This is the time to finalize the EEFI. Once vulnerabilities have been identified, appropriate suggested or required OPSEC protective measures should be implemented to overcome or minimize these vulnerabilities based on the assessed risk. NOTE: Funding for sophisticated protective measures must be considered and resolved prior to inclusion in the plan.

d. Remarks. Include any amplification of the above guidance such as clarification of apparent conflicts with other security directives. The elements above should be presented in such a way that each element builds on the information in the previous one.

6. <u>AMC plans</u>. AMC plans will be authenticated by the signature of the proponent commander or the signatures of the organizational OPSEC officer and the proponent project manager.