DEPARTMENT OF THE AIR FORCE
HQ Air Force Intelligence Service (AFIS)
Fort Belvoir VA 22060-5788

AFISR 205-1

4 April 1986

Security

DEFENSE INTELLIGENCE AGENCY

ON-LINE SYSTEMS (DIAOLAS) ACCESS

This regulation establishes policies, responsibilities, and procedures governing access to the DIAOLS system. It applies to AF/IN activities as concurred in by the Assistant Chief of Staff, Intelligence, and to AFIS activities located in the Washington metropolitan area.

1. References:

a. DIA Manual 50-2, Security of Classified Information in the Defense Intelligence Agency On-Line System (DIAOLS), 22 Feb 79.

b. DIA Automated Data Processing (ADP) Files Reference Catalogue (published as required).

2. Policy. DIAOLS access will be processed as prescribed in the above references, and as implemented by this regulation.

3. Responsibilities:

a. Directors, commanders, and chiefs of comparable level offices will establish responsibilities and procedures in their activities to comply with this regulation.

b. The Reference Library, Directorate of Estimates (AF/INEGD) is responsible for necessary planning and coordinating with external agencies involved in DIAOLS access security.

c. The Special Security Office, HQ USAF, Assistant for Security and Communications Management (AF/INSD), ACS/Intelligence, is responsible for verifying and certifying SCI accesses upon request.

4. Procedures. DIAOLS access is dependent on a unique User Access Code that consists of a User Identification (ID) and Password for each individual needing access. The following access procedures apply:

a. Initial Access:

(1) One copy of DIA Form 836, DIAOLS Access Authorization (see Attachment 1) and one copy of the briefing certificate (see Attachment 3), will

Supersedes AFISR 205-1, 4 April 1980
No. of Printed Pages 9
OPR: AF/INEGD (Mrs. O.R. Spotwood)
Writer-Editor: SSgt L. J. Covington
Approved by: Col F. J. Capillupo
Distribution: F

be completed for each single file requested. For the purpose of this regulation, each of the following will be considered a single file:

(a) All installation files.

(b) All order of battle files.

(c) Imagery requirements objective files.

(d) All Air Force and DIA document index files.

(2) The requester's supervisor will:

(a) Request AF/INSD verify and certify the requester's SI/TK access to DIA OS-4A listing RSI-3A as the DIA point of contact.

(b) Complete DIA Form 836, Section IV.A. Requester Supervisor.

(c) Forward one copy of the completed form and one copy of certificate to AF/INEGD.

(d) Retain one copy each of the request and certificate for office reference.

(e) DIAM 50-2, Chapter 3, paragraph 2a requires all non-DIA users in the Washington DC area to recertify their clearances annually prior to the expiration date of existing certification. Failure to do this will result in cancellation of system access. A clearance recertification message must be sent to the SSO DIA with an information copy to RSI-3A, and must include:

a. Full name

b. Social Security Number

c. Clearance

d. New expiration date

e. DIA Point-of-Contact: RSI-3A, 373-2229

f. Purpose: Access to DIAOLS

(3) When access has been approved by DIA, the requester will be issued a User Access Code in a sealed envelope marked **"CONFIDENTIAL EYES ONLY."** Also contained in the envelope, will be passwords that are keys to accessing DIAOLS. These passwords are normally changed on a quarterly basis. The exclusive knowledge of the User Access Code and Passwords will not be divulged to any person. The requester must sign and return the receipt provided by DIA in order to obtain access to the DIAOLS system.

(4) AF/INEGD will:

(a) Review DIA Form 836 to ensure that it is completed properly, then forward one copy of the form and briefing certificate to DIA (RSO) for processing.

(b) If AF/INEGD is the file action officer, complete DIA Form 836, Section IV.B, Office of Primary Interest (OPI) Indorsement. In the event AF/INEGD is not the OPI, the request will be forwarded to the responsible OPI for processing.

b. Subsequent Access. Subsequent to initial access, an additional file access will be requested and processed in the same manner as for initial access, except the briefing certificate will not have to be reaccomplished.

c. Termination of Access. DIAOLS access will be terminated for personnel who no longer require access, for example, PCS, or loss of compartmented access, by completing two copies of DIA Form 836, Sections I, II.D., and signature the block in Section III. The requester's supervisor will complete Section IV.A., forward one copy to AF/INEGD, and retain one copy for office reference. (The termination request will be reviewed by AF/INEGD for completeness and one copy will be towarded to DIA (RSI) for processing.)

5. Supply of form. DIA Form 836 is available on request from AF/INEGD Bolling AFB, Washington, DC 20332-5000, 767-1526.

OFFICIAL

SCHUYLER BISSELL, Maj Gen, USAF
Commander

CAROL M. YARC, Major, USAF
Chief, Administrative Division

3 Atch
1. Sample of DIA Form 836, DIAOLS Access Authorization
2. An Excerpt from DIAM 50-2, DIAOLS Security Briefing
3. Briefing Certificate

SAMPLE FORM

SECTION I: GENERAL INFORMATION

NAME: (LAST, FIRST, M.I.)	GRADE	BUILDING
SMITH, JAMES	GS-12	Pentagon

ROOM	OFFICE SYMBOL	OFFICE PHONE	USER I.D.
4B-137	AFIS/INDOC	697-4844	

SECTION II: ACCESS REQUEST

A. ACCESS REQUESTED FOR DIAOLS

☐ AIRES ☐ COINS ☒ SYSTEM 1 ☐ SYSTEM 2

B. REQUEST ISS FILE ACCESS (USE SEPARATE FORM FOR EACH FILE, FAMILY OF FILES, OR AIRES OVERLAYS)

NAME _____ _____ AIRES

TYPE OF ACCESS: READ ☒ WRITE ☐ _____ OVERLAYS

C. CHANGE ACCESS FOR ISS FILE _____ FROM: READ ☐ WRITE ☐

TO: READ ☐ WRITE ☐

D. TERMINATE ACCESS TO THE FOLLOWING FILE(S) OR SYSTEM(S): _____

SECTION III: JUSTIFICATION

Duties as Chief of Intelligence Reference Branch requires routing access to installations files.

James Smith — REQUESTER'S SIGNATURE:

24 March 1980 — DATE:

SECTION IV: COORDINATION

A. REQUESTER'S SUPERVISOR: ☒ APPROVE ☐ DISAPPROVE

AFIS/IND — OFFICE SYMBOL

John L. Green — SIGNATURE

(date approved/disapproved) — DATE

Lt Col Green — PRINTED NAME

B. FILE OPI ENDORSEMENT: ☐ APPROVE ☐ DISAPPROVE

OFFICE SYMBOL SIGNATURE DATE

SECTION V: (FOR ACCESS MANAGEMENT USE ONLY)

CLEARANCE VERIFICATION: INIT. _____ DATE _____

USER I.D. _____

DIA FORM 836 (7-77) ON LINE AUTHORIZATION

Previous editions obsolete.

SAMPLE FORM

GPO 916-244

INSTRUCTIONS FOR PREPARING DIA FORM 836

SECTION	ENTRY

I. Enter name, grade, building and room number, office symbol, and phone number of the requester. User I.D. block will be completed by DIA for initial access. If you have been previously issued a user I.D., complete this book.

II.A. Check appropriate box to indicate type access requested as follows:

System 1 - Bibliographic, Order of Battle, and Installation Files.

System 2 - Computational and Programming Files.

COINS - Intelligence Community Files.

AIRES - Imagery Files.

II.B. Enter name of file for which access is needed on line labled "NAME." Check block labled "READ" when a read only capability is needed. Check block labled "READ - WRITE" when a write capability is needed.

II.C. Complete this section only when a change in access capability is requested.

II.D. Complete this section only when terminating access. List the file or system being returned or no longer needed.

III. Give a brief statement on need to access file.

IV.A. Self-explanatory.

IV.B. Completed by the office responsible for the requested file.

V. Will be completed by DIA.

DIAOLS
SECURITY BRIEFING

1. **Purpose.** To emphasize individual responsibilities as they pertain to the DIAOLS and to DIAOLS users.

2. **General.** The fundamental approach to the security of the DIAOLS is based on the principles of individual responsibility, accountability, and need-to-know. Features incorporated into DIAOLS that are required to provide adequate protection for the system and for the data contained within the system include both technical and procedural provisions.

3. **Individual Responsibilities:** The burden of responsibility for the security of classifed information stored and manipulated within the DIAOLS must ultimately rest with each person who uses or who has access to the system. No matter how elaborate the built-in precautions and safeguards, they provide little security if each person using the system is not aware of, or does not discharge, personal responsibilities.

a. Use of the DIAOLS for other than official Government business is strictly prohibited and any violation of this prohibition will result in removal from access to the system, and may result in administrative or punitive sanctions. Among the specific prohibitions are use of the DIAOLS for personal gain, entertainment, or other private pursuits, gambling, betting, lottery, or in any other similar activity.

b. The IG has been tasked to conduct an in-depth inspection of each directorate to ascertain the existence of any activities that may be in violation of the President's Executive Order No. 11905 which prohibits any illegal or inappropriate activites or improprieties. All files on DIAOLS are subject to unannounced inspection by the IG in accordance with the provisions of Executive Order 11905, DIAR 40-3, and DIAR 60-4, and are to be in compliance with the Executive Order, the Privacy Act, the Freedom of Information Act, and the policies of the Defense Investigative Review Council. If you now have files, data, or programs stored on DIAOLS System Two, it is suggested that you review each and delete all which may be construed as inappropriate for inclusion on a government-owned system. You are also reminded that System Two is for collateral use only and is not to be used to store or manipulate any compartmented data.

c. The following are key responsibilities of each individual associated with the DIAOLS:

(1) Your DIAOLS Password is **FOR YOUR EYES ONLY** and will not be disclosed or used by anyone else regardless of the situation or circumstances. Such discloure to, or use by, another is considered a security violation and will result in your suspension from access to the DIAOLS.

(2) It is your responsibility to control access and utilization of any "private" files or programs which you have stored on the DIAOLS under your Access Code. You are accountable for any use made of such files, programs, or data and for the correct classification, caveats, and any modifications made to them.

(3) Recommend to the cognizant OPR any changes which you feel should be made to the classification and/or handling caveats of any file or program which you use.

(4) Immediately report to the RTSO any indications of a possible system malfunction. This particularly applies to any malfunction which results in your I.D. being locked out of the DIAOLS. Since all lockouts are monitored and recorded, system malfunctions which are not reported are recorded as individual violations.

d. There are several specific precautions which you must always take when using the DIAOLS in order to protect both yourself and the DIAOLS from possible compromise.

(1) Insure that no other person is in position to see the terminal keyboard while your password is being typed in.

(2) Insure that the teletype does not print your password. Should it do so, notify the RTSO immediately.

(3) Insure that whenever you receive an invalid, inconsistent, or unexpected system response, including invalid responses to the commands HELLO or CONTROL C, you immediately cease operations, sign-off if necessary, and notify the RTSO of the events.

(4) Insure that whenever you modify a program or file, regardless of its originator, that the classification and/or special handling caveats correctly apply to all material imbedded within the program or file.

(5) Insure that any data which you input into a file or program does not exceed the overall classification and special handling caveats of the file.

(6) Insure that information retrieved from the files on DIAOLS is carefully reviewed to determine that the classification and/or special handling caveats as marked are consistent with those known to be applicable to the file or program from which the data are obtained.

(7) Insure that all output is handled in accordance with regulations and procedures applicable to the handling of classified material.

(8) Insure that the command BYE is entered in the system when you have finished using the terminal, and that the DIAOLS DISCONNECTS message is showing and is the only writing visible on the terminal.

(9) Insure that before leaving the terminal, all output has been detached and that all waste paper has been put in a burn bag.

(10) Insure that you notify the appropriate RTSO if you receive a lockout notice from the system.

e. Additionally, in order to avoid unnecessary delay, embarrassment, and a possible security violation, do not:

(1) Interrupt the sign-on sequence once you have entered your User I.D.

(2) Attempt to access a file or subsystem for which you have not requested access or for which your access has not been approved.

(3) Attempt to perform a function not permitted to your level of access (i.e., READ-WRITE, Privileged).

(4) Leave an active terminal unattended and without the system-generated DIAOLS DISCONNECT, or equivalent message showing.

f. You are directed not to attempt to use or to discover an authenticator assigned to another individual or to use any other means for attempting to circumvent the system safeguards. Any such attempt to circumvent the system safeguards is a security violation. If you think you have found a weakness in the DIAOLS security features, please discuss the matter with the ISSO, at 373-2237.

4. Security. As can be seen from the above list, the individual provides much of the protection for the information contained in the DIAOLS. If your security alertness is relaxed at anytime, a security violation or compromise may result which could cause grave damage to the National Security. In the final analysis, DIAOLS security, like all security, depends upon the individual.

DIAOLS BRIEFING CERTIFICATE

I certify that I have read the DIAOLS Security Briefing and understand my security responsibilities as a user of the System. I further understand that my DIAOLS Access Code is for my eyes only, that use of the DIAOLS for other than official government business is strictly prohibited, and that any violation of these prohibitions on my part will result in my removal from access to the system and possible suspension or criminal prosecution.

PRINTED NAME _____

DATE _____

ELEMENT _____

OFFICE LOCATION _____

TELEPHONE NUMBER _____

_____
(Signature)

User Number _____