

Administrative Changes to TINKERAFBI 33-110, *Automated Information System (AIS) Access and Data Release Requirements*

OPR: 72 ABW/SCP: Special Mission Division

References throughout to “<https://wwwmil.tinker.af.mil/ites/opr.asp>” change to “<https://org.eis.afmc.af.mil/sites/ocalcit/72ABWSCP/systems/default.aspx>” .

Reference throughout to “76MXW/OB” change to “OC-ALC/OB”.

Reference throughout to “327ASW/OM” change to “AFSC/LCMC”.

Reference throughout to “948SCMG/DD” change to “448SCMG/OMM”.

Reference throughout to “ocalc.it.crm.workflow@tinker.af.mil” change to [72ABW.SC-CRM.Workflow@us.af.mil](mailto:72ABW.SC-CRM.Workflow@us.af.mil).

Reference throughout to “Oklahoma Air Logistics Center” change to “Oklahoma City Air Logistics Complex”.

21 February 2014

**BY ORDER OF THE COMMANDER  
TINKER AIR FORCE BASE**

**TINKER AIR FORCE BASE INSTRUCTION  
33-110**



**3 SEPTEMBER 2009**  
*Certified Current, 13 November 2014*  
**Communications and Information**

**AUTOMATED INFORMATION SYSTEM (AIS)  
ACCESS AND DATA RELEASE  
REQUIREMENTS**

---

**ACCESSIBILITY:** Publication and forms are available on the e-publishing website at [www.e-Publishing.af.mil](http://www.e-Publishing.af.mil) for downloading or ordering.

**RELEASABILITY:** There are no releasability restrictions on this publication.

---

Supersedes: TINKERAFBI33-110,  
28 December 2006

Certified by: 72ABW/SC,  
(Col. Mary M. Gillam)  
Pages: 11

---

This instruction outlines requirements for access to 72 ABW/SC managed, unclassified automated information systems (AIS) and requesting data from those AIS. It also outlines requirements for maintaining AIS access accounts. This publication requires the collection and or maintenance of information protected by the Privacy Act (PA) of 1974. The authorities to collect and or maintain the records prescribed in this publication are Executive Order 10450, 9397. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF form 874s from the field through publications/forms managers. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at <https://www.my.af.mil/gcss-af61a/afirms/afirms/>.

**SUMMARY OF CHANGES**

The requirement for an AIS Interim access memo to accompany the DD2875 has been removed. Also office symbols have been updated where necessary.

**1. General Information:** This instruction establishes procedures and requirements for obtaining and maintaining access to 72 ABW/SC supported, unclassified automated information systems (AIS) and requesting data from 72 ABW/SC managed AIS. This instruction applies to

all Air Force military, civilian, and contractor personnel at Tinker Air Force Base that request AIS access and/or data queries from 72 ABW/SC managed AIS.

## 2. Obtaining Data System Access

2.1. All personnel requiring access to systems supported by 72 ABW/SC must complete the appropriate system access request forms.

2.1.1. A list of all AIS managed by 72 ABW/SC is available on the Web at: <https://wwwmil.tinker.af.mil/ites/opr.asp>. Each system has its own individual web page.

2.1.1.1. Each system has specific access forms available on its system web page under "Access Requirements.

2.1.1.2. Additional system access requirements may also be found on the system web page bulletin or under the "Briefings," "Tools and Support Info," and/or "Helpful Links" sections of the individual system web pages.

2.1.2. The organization, office symbol/department, job title, and email address must be supplied for the position of record on the system access request form. Additional information is required for employees in situations as follows:

2.1.2.1. Employees detailed to another organization:

2.1.2.1.1. The organization, office symbol/department, job function, and email address for the detail position must be included as part of the justification for access on the system access request form.

2.1.2.1.2. The immediate supervisor must supply an expiration date for the detail on the system access request form.

2.1.2.2. Employees assigned to work a special project, on a team, or as an intern on rotation:

2.1.2.2.1. The project, team, or internship information must be stated on the system access request form as part of the justification for access, along with the job function being performed on the assignment requiring system access.

2.1.2.2.2. The immediate supervisor must supply an expiration date for the detail on the system access request form.

2.2. Additional access requirements for contractors:

2.2.1. System access request forms for contractors must include the company name, contract number, and contract expiration date. The forms must be signed off by the sponsor, (i.e. USAF program manager, project officer, contracting officer, Contracting Office Technical Representative [COTR], etc.)

2.2.2. Contractor system access requests must be accompanied by a signed "Contractor Non-Disclosure Statement," Attachment 3. If access to multiple systems is being requested, a single Contractor Non-Disclosure Statement listing all systems may be submitted.

2.2.3. A contractor's system access will be terminated on the contract expiration date, unless or until new system access request forms and non-disclosure statements are received showing the contractor still requires access, and provides a new contract number, if applicable, and new contract expiration date.

2.3. Interim Access requirements for personnel without a security clearance and a pending investigation.

2.3.1. If the requestor does not have a security clearance it is the responsibility of the requestor's security manager to ensure that the requirements in AFI 31-501 are complied with, including any required letters granting interim clearances, in order to give the requestor interim access. By signing the DD2875, the security manager is validating that all security clearance/investigation requirements are met in order to grant the requestor AIS access.

2.3.2. Upon notification of an unfavorable investigation/denied clearance, the security manager will notify 72 ABW/SC. The user's AIS accounts will be terminated.

### 3. Modification of Data System Access

3.1. Password Reset requirements will vary by system.

3.1.1. Users should call the appropriate help desk for password resets. System help desk numbers can be found on the respective 72 ABW/SC system web pages at: <https://wwwmil.tinker.af.mil/ites/opr.asp>. Each system has its own individual web page.

3.1.2. Other password requirements exist, but vary by system. In general, the user can expect the following with respect to passwords:

3.1.2.1. Users may be prompted to change a system password after a certain number of days.

3.1.2.2. System access may be suspended for non-use after specified period of time, which may require password reset by the appropriate system help desk.

3.2. Safeguarding Passwords.

3.2.1. System users will protect passwords based on the sensitivity of the information or critical operations they protect. At a minimum, passwords must be safeguarded as "For Official Use Only" (FOUO). (Reference AFMAN 33-223)

3.2.2. Users are encouraged not to keep a copy of their written password, but if this is impossible, the password should be protected IAW CJCSM 6510.01, Appendix A, Enclosure C, for instance.

3.2.2.1. Do not store the password where it is easily accessible to computer.

3.2.2.2. Do not keep the password and user ID together.

3.2.2.3. Store the password in a locked drawer, cabinet, or container.

3.2.3. System users must not disclose their passwords to other employees. Disclosure of passwords is considered a security violation. Anyone in violation will have their system access terminated. A notification will be sent to the employee's immediate supervisor,

commander, and Information Assurance Officer with a copy to 72 ABW/SC. (Reference AFMAN 33-223\_AFMCSUP1)

### 3.3. Profile changes.

3.3.1. Changes of manager designator codes (MDC) on a user ID profile must be submitted to the System OPR via e-mail by the immediate supervisor of the user. The e-mail must include a signature block that identifies the sender as the immediate supervisor. The e-mail should include the user's name, user ID, and old codes to be removed and new codes to be added.

3.3.2. Changes to a user's type of access, i.e. currently has read-only access, but now requires input capability, must be submitted to the System OPR on a new system access request form, indicating the request is a modification to the user's current system access.

3.3.3. Requests to loan a user's workbaskets/privileges must be submitted to the System OPR via e-mail by the immediate supervisor of the user. The e-mail must include the user's workbasket/privilege information (i.e. MDC), the user to load the workbasket/privileges to, a start date, and an end date. The e-mail must also include a signature block that identifies the sender as the user's immediate supervisor, team lead or coordinator, Requirements Control Officer (RCO), or Technical Control Officer (TCO).

## 4. Maintenance of Data System Access

4.1. User ID reinstatements: A new system access request form is required for all user ID reinstatements.

4.2. Reassignments/Permanent Promotions: User information and profiles must remain accurate and appropriate for the job function of the user. When a user changes jobs, the user's organization/contact information and system user profiles must be updated.

4.2.1. The user and the immediate supervisor of the **losing** organization must submit a system access request form indicating all the systems the user has access to and an expiration date for the access. The user's access will expire on that date unless new system access request forms are received from the user signed by the immediate supervisor of the **gaining** organization.

4.2.2. The user must submit new access request forms for all systems required to perform the user's new job, signed by the immediate supervisor of the **gaining** organization, and indicate the start date for the user on the new position. If the user no longer requires access to a particular system, then a system access request form should be submitted indicating that the access should be deactivated.

4.3. Details/Temporary Promotions: User information and profiles must remain accurate and appropriate for the job function of the user. When a user is detailed to a different position or is promoted temporarily, the user's organization/contact information and system user profiles must be updated.

4.3.1. If the user is detailed or promoted for a **period of 120 days or less**, the supervisor for the detail position or the temporary promotion position must notify the System OPR for each system via e-mail. The e-mail should include the user's name, system(s)/User ID(s), type of access required, codes to add/remove, etc, along with the **expiration date**

of the detail/temporary position. Additionally, the e-mail must include a signature block that identifies the sender as the immediate supervisor of the user.

4.3.2. If the user is detailed or promoted for a **period of more than 120 days**, the user and losing and gaining immediate supervisors must follow the guidance in 4.2. for maintenance of system access.

4.4. Name Changes: Users whose name changes must submit a new system access request form for modification, annotating the name change. The form can include all systems the user has access to rather than doing a separate form for each system.

4.5. Revalidation: 72 ABW/SC will perform annual revalidation of user access to 72 ABW/SC managed systems. During revalidation, users will be required to submit new system access request forms if any of the user's contact information and/or job function has changed.

## **5. Deactivation of Data System Access**

5.1. Deactivation of Contractor's system access.

5.1.1. Contractors' access automatically expires on the contract expiration date unless the requirements in 2.2. have been fulfilled prior to the contract expiration date.

5.1.2. The sponsors of contractors that terminate employment prior to the contract expiration date must submit a system access request form listing the systems the employee had access to indicating that the access should be terminated.

5.1.3. Contractors that become civil service employees must submit new system access request forms as a civil service employee to obtain system access (Para 2.) for their civil service job duties. System access from contractor employment will not be carried over.

5.2. Separation from service and reassignments of personnel to external agencies to Tinker AFB.

5.2.1. 72 ABW/SC obtains personnel losses listings from the personnel office regularly. All system access to 72 ABW/SC managed systems for all personnel appearing on the listing will be terminated immediately.

5.2.2. Personnel that separate from service and return to work as a contractor must submit system access request forms to obtain new access to systems (Para 4.) required to perform the person's contractual job duties. Access from the person's government employment will not be carried over.

5.3. Interim Access/Unfavorable Investigation/Denied Clearance: Upon notification of denied clearance and/or unfavorable investigation, for a system user, the user's system access will be terminated immediately.

## **6. Data Requests**

6.1. **Ad Hoc Data Query Requests from 72 ABW/SC Supported AIS.**

6.1.1. Requests for data queries that are not intended for use in the development/sustainment of another application, tool, or system, can be requested from the 72 ABW/SC System OPR via e-mail. The requester will supply the system name,

cycle date if applicable, selection criteria, and the need date in the request. Attachment 2 contains a sample format for data query requests.

6.1.2. Ad Hoc Data Query requests **from contractors.**

6.1.2.1. If the contractor requesting data already **has access** to the system(s) the data comes from (with the appropriate system access request form and non-disclosure statement on file) and would normally be able to interrogate the system for the data being requested, then the contractor can request the data from the 72 ABW/SC System OPR as outlined in 6.1.1.

6.1.2.2. If the contractor requesting data **does not currently have access** to the system(s) the data resides in, then the data requests are to be submitted in writing by e-mail or memorandum, Attachment 2, from the sponsor to the 72 ABW/SC System OPR. The e-mail or memorandum will incorporate the following information and attachments:

6.1.2.2.1. Certify that the contractor requires the data requested to perform contractual job duties. This statement will incorporate the following information:

6.1.2.2.1.1. Contractor's name.

6.1.2.2.1.2. Contractor's company name.

6.1.2.2.1.3. Government organization the contractor is supporting.

6.1.2.2.1.4. Data required will be listed as an attachment (sample format - Attachment 2). Refer to 6.1.1. for information to be included in the data query request.

6.1.2.2.1.5. Explanation of what the data will be used for, i.e., research, analysis, etc.

6.1.2.2.2. Certify that the contractor has signed a Contractor Non-Disclosure Statement; attach copy of the Contractor Non-Disclosure Statement to the e-mail or memorandum.

6.1.2.2.3. Authorize the release of the data to the contractor, or other specified Point of Contact (POC).

6.1.2.2.4. The signature element, whether e-mail or memorandum, must indicate that the person signing the memorandum or sending the e-mail is the sponsor of the contract employee requesting the data.

6.1.2.2.5. POC information for the memo/e-mail.

6.2. Data requested from 72 ABW/SC AIS that is **intended for use in the development/sustainment of another application, tool, or system** must be submitted on an AF IMT 3215. The AF IMT 3215 will be signed by the requesting organization's Group Commander (or Division level for Staff organization structures) and then submitted to the organizational business/budget office (76MXW/OB; 327ASW/OM; 948SCMG/DD) for coordination. Once both signatures are obtained, the form will be electronically forwarded to [ocalc.it.crm.workflow@tinker.af.mil](mailto:ocalc.it.crm.workflow@tinker.af.mil).

**7. Records:**

- 7.1. System Access Request forms.
- 7.2. Contractor Non-Disclosure Statements.
- 7.3. E-mail Notifications (5.3. and 6.3.).
- 7.4. Contractor Data Release Memorandums/E-mails.
- 7.5. Data Query Requests.

**8. Adopted Form:** AF 847, *Recommendation for Change of Publication.*

Allen J. Jamerson, Col, USAF  
Commander, 72ABW/CC

**Attachment 1****GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

DoD 5200.2-R. *Personnel Security Program*, 16 January 1987

DoD 8500.2. *Information Assurance (IA) Implementation*, 06 February 2003

CJCSM 6510.01. *Defense-In-Depth: Information Assurance (IA) and Computer Network Defense CND*, 25 March 2003

DoD 5200.28. *Security Requirements for Automated Information Systems (AIS)*, 02 September 1986

DoD 8500.1. *Information Assurance (IA)*, 24 October 2002

AFI 31-601. *Industrial Security Program Management*, 29 June 2005

AFI 33-112. *Computer Systems Management*, 07 April 2006

AFMAN 33-223. *Identification and Authentication*, 29 July 2005

AFMAN 33-223\_AFMCSUP1. *Identification and Authentication*, **(HOLDOVER)**

Defense Acquisition University (DAU) Glossary of Defense Acquisition Acronyms and Terms, 12<sup>th</sup> Edition

***Terms***

1. **Automated Information System (AIS)**: A combination of computer hardware, computer software, and/or data that performs functions such as collecting, processing, storing, transmitting and displaying information. (DAU Glossary) The term “system” will be used interchangeably with AIS in this instruction.
2. **Contractor**: An employee of an entity in private industry which enters into contracts with the government to provide goods or services. (DAU Glossary) **NOTE**: May also be referred to as a contractor employee or as contractor personnel.
3. **Interim Access**: Access to an AIS granted to an employee on an interim basis pending completion of a background investigation and/or receipt of a security clearance.
4. **Sponsor**: For the purposes of this instruction, a sponsor is an Air Force military or civil service employee, i.e. USAF program manager, project officer, contracting officer, or Contracting Officer Technical Representative (COTR), who may sign as a sponsor authorizing a contractor to obtain AIS access.
5. **System Access Request Form**: A form that is completed by a civil service, military, or contract employee to obtain access to a particular AIS. The actual form used may vary depending on the system.

**Attachment 2**  
**SAMPLE LETTER**



DEPARTMENT OF THE AIR FORCE  
HEADQUARTERS OKLAHOMA CITY AIR LOGISTICS CENTER  
(AFMC)  
TINKER AIR FORCE BASE OKLAHOMA

MEMORANDUM FOR :72ABW/SC

FROM:

SUBJECT: Data Query Request

1. I certify that the following contractor, (Contractor's Name), (Contractor's Co. Name), requires the data requested in the attached Data Query Request to fulfill duties supporting (ORGN) personnel in (DUTIES)
2. I also certify that a Contractor Non-Disclosure Statement has been completed by each Contractor employee working the project; a copy is attached.
3. I hereby authorize 72 ABW/SC to release data in this request directly to (CONTRACTOR)  
OR
3. I hereby authorize 72 ABW/SC to release data in this request to (ORGN), (POC)
4. (POC info)

(Sponsor Signature)  
(Signature Element)

Attachments

1. Data Query Request
2. Contractor Non-Disclosure Statement(s)

**Attachment 2 (Cont')**

**DATA QUERY REQUEST**

System:

“Cycle” or “As of Date” (if applicable):

Selection Criteria:

Data Elements:

Needed By:

**Attachment 3**

**SAMPLE FORMAT**

FOR OFFICIAL USE ONLY

Personal Data – Privacy Act of 1974 Applies

Non-Disclosure Statement for Contractor Personnel

I, [Click **here** and type name], citizen of [Click **here** and type country], will under no circumstances use data extracted via [Click **here** and type system(s), ie D043] for other than government purposes, nor will I make this information available to any contractor(s)/vendor(s) or third parties.

SSN: [Click **here** and type SSN]

Signature: \_\_\_\_\_  
Typed/Printed Name: [Click **here** and type name]

Date: \_\_\_\_\_

This information is governed by the Privacy Act of 1974; therefore, it must be controlled and disposed of accordingly.

Personal Data – Privacy Act of 1974 Applies

**FOR OFFICIAL USE ONLY**