BY ORDER OF THE COMMANDER
AIR FORCE SUSTAINMENT CENTER

TINKER AIR FORCE BASE
INSTRUCTION 17-1301

4 SEPTEMBER 2024
Certified Current, 23 December 2024
Cyberspace

AUTOMATED INFORMATION SYSTEM (AIS) ACCESS AND DATA RELEASE REQUIREMENTS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-Publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 72ABW/SCP

Certified by: 72ABW/SC
(Mr. Michael Wiles)

Supersedes: TINKERAFBI33-110, 13 November 2014

Pages: 13

This instruction implements Air Force Manual (AFMAN) 17-1301, Computer Security (COMPUSEC). 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. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the AirForce Records Disposition Schedule, which is located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the OPR listed above using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate chain of command to 72 ABW/SCP.

Chapter 1

GENERAL INFORMATION

1.1. Overview. 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.

Chapter 2

OBTAINING DATA SYSTEM ACCESS

2.1. All personnel requiring access to systems supported by 72 ABW/SC must. Complete the appropriate system authorization access request form, DD Form 2875 (DD2875).

2.1.1. A list of all AIS managed by 72 ABW/SC is available on the Web at: **https://usaf.dps.mil/sites/TMC719183/72ABWSCP/SitePages/SCP-Managed-Systems-Contacts-and-Information.aspx**. Each system has its own individual web page.

2.1.1.1. Additional system access requirements may also be found on the system web page bulletin or under the "Tools and Support Info," and/or "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 DD2875. 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 DD2875 form.

2.1.2.1.2. The immediate supervisor must supply an expiration date for the detail on the DD2875.

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 DD2875 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 DD2875.

2.2. Additional access requirements for contractors:

2.2.1. DD2875 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 DD2875 must be accompanied by a signed "Non-Disclosure Agreement (NDA) for Contractor Personnel," **https://usaf.dps.mil/sites/TMC719183/72ABWSCP/72ABWSCPL/NonDisclosure%20Agreement%20NDA/Forms/AllItems.aspx**. If access to multiple systems is being requested, a single Contractor NDA 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 DD2875 forms and NDA 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 Department of Defense Manual (DoDM) Air Force Manual 5200.02 (AFMAN) 16-1405, *Air Force Personnel Security Program* are complied with, including any required letters granting interim clearances (contact local OPR for special instructions), 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. 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.

Chapter 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/OPR for password resets. System help desk numbers can be found on the respective 72 ABW/SC system web pages at: **https://usaf.dps.mil/sites/TMC719183/72ABWSCP/SitePages/SCP-Managed-Systems-Contacts-and-Information.aspx**. 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. System access may be suspended for non-use after specified period of time, which may require password reset by the appropriate system help desk/OPR.

3.2. Safeguarding Passwords.

3.2.1. System users will protect passwords based on the sensitivity of the information or critical operations they protect.

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 Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B, *Cyber Incident Handling Program*.

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 17-1301)

3.3. Profile changes.

3.3.1. Changes of manager designator codes (MDC) and Equipment Specialist (ES) codes 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 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 DD2875 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, ES Code), the user to loan 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).

Chapter 4

MAINTENANCE OF DATA SYSTEM ACCESS

4.1. User ID reinstatements: A new DD2875 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 DD2875 form for deactivation 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 DD2875 forms are received from the user signed by the immediate supervisor of the **gaining** organization.

4.2.2. The user must submit new DD2875 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.

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, the user must submit a new DD2875 form for modification, annotating any role changes.

4.4. Name Changes: Users whose name changes must submit a new DD2875 forms for modification, annotating the name change.

4.5. Revalidation: 72ABW/SC will perform annual revalidation of user access to 72 ABW/SC managed systems as required. During revalidation, users will be required to submit new DD2875 if any of the user's contact information and/or job function has changed, or if necessary for Financial Improvement and Audit Readiness (FIAR) compliance.

Chapter 5

DEACTIVATION OF DATA SYSTEM ACCESS

5.1. Deactivation of Contractor's system access.

5.1.1. Contractor's access automatically expires on the contract expiration date unless the requirements outlined in this document 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 DD2875 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 a new DD2875 as a civil service employee to obtain system access 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 DD2875 to obtain new access to systems required to perform the person's contractual job duties. Access from the person's government employment will not be carried over.

Chapter 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 DD2875 and NDA on file) and would normally be able to query the system for the data being requested, then the contractor can request the data from the 72 ABW/SC System OPR as outlined in this publication.

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 Data Requests section of this document 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 NDA; attach copy of the NDA 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: 72ABW/SC AIS that is intended for use in the development/sustainment of another application, tool, or system must be submitted on a Coordination Package. The Coordination Package 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 (OC-ALC/OB; AFSC/LCMC/OM; 448SCMG/OMM) for coordination. Once both signatures are obtained, the form will be electronically forwarded to **72ABW.SC-CRM.Workflow@us.af.mil**.

ABIGAIL L.W. RUSCETTA, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFMAN 17-1301, *Computer Security (COMPUSEC)*, 10 February 2017

DoDMAN5200.02_AFMAN 16-1405, *Air Force Personnel Security Program*, 1 August 2018

5 USC § 552, *Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings*, 3 January 2012

5 USC § 552a, *Records Maintained on Individuals*, 7 January 2011

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

CJCSM 6510.01B, *Cyber Incident Handling Program*, 10 July 2012

Adopted Forms

AF 847, *Recommendation for Change of Publication*

DD Form 2875, *System Authorization Access Request*

Abbreviations and Acronyms

AFB—Air Force Base

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFRIMS—Air Force Records Information Management System

AIS—Automated Information System

COMPUSEC—Computer Security

COTR—Contracting Officer Technical Representative

DAU—Defense Acquisition University

FIAR—Financial Improvement and Audit Readiness

IAW—In Accordance With

ID—Identification

MDC—Manager Designator Codes

NDA—Non-Disclosure Agreement

OPR—Office of Primary Responsibility

POC—Point of Contact

RCO—Requirements Control Officer

RDS—Records Disposition Schedule

TCO—Technical Control Officer

USAF—United States Air Force

USC—United States Code

Terms

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.

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.

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.

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.

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

DATA REQUEST INFORMATION

Figure A2.1. Memorandum for Record Example.

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

MEMORANDUM FOR: 72 ABW/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 Agreement 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 Agreement(s)

Figure A2.2. Data Query Request Example.

System:

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

Selection Criteria:

Data Elements:

Needed By: