Defense Logistics Agency

Manual DD2875/SAAR process

DESK TOP GUIDE

February 27, 2017

DLA Access Management, J64A

Contents

1. Authorized application level access for DLA Employees 2
2. Privileged application level access for DLA Employees (No Token needed)................................ 3
3. Authorized access for external users (Users not in DLA Active Directory) 4
4. Privileged access for external users (Users not in DLA Active Directory).................................... 5
5. Application account deactivation (for all users) 6
6. NIPR Privileged System Admin access for DLA Employees (Requires Alternate Token) 7
7. SIPR Authorized access for DLA Employees 8
8. SIPR Privileged access for DLA Employees.. 9

* Identified enterprise process but not implemented in AMPS or the Manual process

1. Authorized application level access for DLA Employees
    a. User completes paper DD2875 or SAAR request
        i. DLA User
            1. Fills out all required blocks
                a. Initial or Modification
                b. User ID
                c. Date
                d. System Name
                e. Location of System
                f. Part I Blocks 1-12
                    i. Signature is optional if the supervisor is submitting on their behalf
                g. Block 13 (Justification)
                h. Block 14 (Authorized)
                i. Block 15 (Unclassified)
                j. Block 26
                k. Block 27 (Access being Requested)
                    i. All Access requested must be IT Level 3 (Generally Read Only)
                    ii. All Access listed must have the same Data Owner
    b. Supervisor/Sponsor validates and signs request
        i. Completes Part II
            1. Blocks 16 – 20b.
        ii. Verifies users need to know
        iii. Validates users training
    c. Data Owner validates and signs request
        i. Validates access being requested in block 27 is “authorized” and only requires an IT Level of 3.
        ii. Validates the user is a DLA Employee
        iii. Annually validate the users account
        iv. Completes blocks 21 – 21b
    d. Provisioner provisions the account
    e. Documentation uploaded into DACS
        i. Performed by J64 Identity and Access Management

2. Privileged application level access for DLA Employees (No Token needed)
    a. User completes paper DD2875 or SAAR request
        i. DLA User
            1. Fills out all required blocks
                a. Initial or Modification
                b. User ID
                c. Date
                d. System Name
                e. Location of System
                f. Part I Blocks 1-12
                    i. Signature is optional if the supervisor is submitting on their behalf
                g. Block 13 (Justification)
                h. Block 14 (Privileged)
                i. Block 15 (Unclassified)
                j. Block 26
                k. Block 27 (Access being Requested)
                    i. Access requested should require an IT Level 1 or 2 (Generally Update or Application Admin Level Access)
                    ii. Having more than 1 level of access requested will cause the SAAR to be returned to the supervisor if the user does not have the correct IT Level for Access
                    iii. All Access listed must have the same Data Owner
            2. *Completes privileged rules of behavior
    b. Supervisor/Sponsor validates and signs request
        i. Completes Part II
            1. Blocks 16 – 20b.
        ii. Verifies users need to know
        iii. Validates users training
    c. Security Officer signs request
        i. Completes Part III
            1. Blocks 28-32
    d. Data Owner validates and signs request
        i. Validates access being requested in block 27 is "privileged"
        ii. Validates the users IT Level is acceptable for the access requested in block 27
        iii. Annually validate the users account
        iv. Completes blocks 21 – 21b
    e. Provisioner provisions the account
    f. Documentation uploaded into DACS
        i. Performed by J64 Identity and Access Management

3. Authorized access for external users (Users not in DLA Active Directory)
    a. User completes paper DD2875 or SAAR request
        i. DLA User
            1. Fills out all required blocks
                a. Initial or Modification
                b. User ID (If Known)
                c. Date
                d. System Name
                e. Location of System
                f. Part I Blocks 1-12
                    i. Signature is optional if the supervisor is submitting on their behalf
                g. Block 13 (Justification)
                h. Block 14 (Authorized)
                i. Block 15 (Unclassified)
                j. Block 26
                k. Block 27 (Access being Requested)
                    i. All Access requested must be IT Level 3 (Generally Read Only)
                    ii. All Access listed must have the same Data Owner
                l. *Sign Consent to monitoring agreement
                m. *Signs Rules of Behavior
                n. *Attaches PII Training certificate
                o. *Attaches Cyber Awareness certificate
    b. Supervisor/Sponsor validates and signs request
        i. Completes Part II
            1. Blocks 16 – 20b.
        ii. Verifies users need to know
        iii. Validates users training
    c. Security Officer (External SO or DLA SO) signs request
        i. Completes Part III
            1. Blocks 28-32
    d. Data Owner validates and signs request
        i. Validates access being requested in block 27 is "authorized" and only requires an IT Level of 3.
        ii. Validates the users IT Level is acceptable for the access requested in block 27
        iii. Annually validate the users account
        iv. Completes blocks 21 – 21b
    e. Provisioner provisions the account
        i. User ID Generated
    f. Documentation uploaded into DACS
        i. Performed by J64 Identity and Access Management

4. Privileged access for external users (Users not in DLA Active Directory)
   - a. User completes paper DD2875 or SAAR request
     - i. External user
       - 1. Fills out all required blocks
         - a. Initial or Modification
         - b. User ID (If Known)
         - c. Date
         - d. System Name
         - e. Location of System
         - f. Part I Blocks 1-12
           - i. Signature is optional if the supervisor is submitting on their behalf
         - g. Block 13 (Justification)
         - h. Block 14 (Privileged)
         - i. Block 15 (Unclassified)
         - j. Block 26
         - k. Block 27 (Access being Requested)
           - i. System Name
           - ii. List of servers
           - iii. List of Databases
           - iv. All Access must have the same Data Owner
       - 2. *Completes privileged rules of behavior
   - b. Supervisor/Sponsor validates and signs request
     - i. Completes Part II
       - 1. Blocks 16 – 20b.
     - ii. Verifies users need to know
     - iii. Validates users training
   - c. Security Officer (External SO or DLA SO) signs request
     - i. Completes Part III
       - 1. Blocks 28-32
   - d. Data Owner validates and signs request
     - i. Validates access being requested in block 27 is “privileged”
     - ii. Validates the users IT Level is acceptable to the access requested in block 27
     - iii. Annually validate the users account
     - iv. Completes blocks 21 – 21b
   - e. Provisioner provisions the account
     - i. Creates User ID (If needed)
   - f. Documentation uploaded into DACS
     - i. Performed by J64 Identity and Access Management

5. Application account deactivation (for all users)
    a. Supervisor/Sponsor or Data Owner completes and signs request
        i. Check mark type of request as “Deactivate”
        ii. Enter the users id
        iii. Enter the date of request
        iv. Completes Part II
            1. Blocks 13 – 19
        v. If the requestor is the supervisor
            1. Complete blocks 17- 20b
        vi. If the requestor is the Data Owner
            1. Complete blocks 21 -21b
    b. Provisioner de-provisions the account
    c. Documentation uploaded into DACS
        i. Performed by J64 Identity and Access Management

6. NIPR Privileged System Admin access for DLA Employees (Requires Alternate Token)

a. User completes paper DD2875 or SAAR request

i. DLA User

1. Fills out all required blocks

a. Initial or Modification

b. User ID (Left Blank for initial request)

c. Date

d. System Name

e. Location of System

f. Part I Blocks 1-12

g. Block 13 (Justification)

h. Block 14 (Authorized)

i. Block 15 (Unclassified)

j. Block 26

k. Block 27 (Access being Requested)

i. System Name

ii. List of servers

iii. List of Databases

iv. All Access must have the same Data Owner

l. Completes privileged rules of behavior

2. Creates Remedy Work order and attaches DD2875 after it is signed by the Supervisor/Representative and Security Officer

b. Supervisor/Sponsor validates and signs request

i. Completes Part II

1. Blocks 16 – 20b.

ii. Verifies users need to know

iii. Validates users training

c. Data Owner validates and signs request

i. Validates access being requested in block 27 is “authorized” and only requires an IT Level of 3.

ii. Validates the user is a DLA Employee

iii. Annually validate the users account

iv. Completes blocks 21 – 21b

d. Provisioner provisions the account

e. Documentation uploaded into DACS

i. Performed by J64 Identity and Access Management

7. SIPR Authorized access for DLA Employees
   a. User completes paper DD2875 or SAAR request
      i. DLA User
         1. Fills out all required blocks
            a. Initial or Modification
            b. User ID (Left Blank for initial request)
            c. Date
            d. System Name
            e. Location of System
            f. Part I Blocks 1-12
            g. Block 13 (Justification)
            h. Block 14 (Authorized)
            i. Block 15 (Classified)
            j. Block 26
            k. Block 27 (Access being Requested)
         2. Creates Remedy Work order and attaches DD287 after it is signed by the Supervisor/Representative and Security Officer
   b. Supervisor/Sponsor validates and signs request
      i. Completes Part II
         1. Blocks 16 – 20b.
      ii. Verifies users need to know
      iii. Validates users training
   c. Data Owner validates and signs request
      i. Validates access being requested in block 27 is “authorized” and only requires an IT Level of 3.
      ii. Validates the user is a DLA Employee
      iii. Annually validate the users account
      iv. Completes blocks 21 – 21b
   d. Provisioner provisions the account
   e. Documentation uploaded into DACS
      i. Performed by J64 Identity and Access Management

8. SIPR Privileged access for DLA Employees
    a. User completes paper DD2875 or SAAR request
        i. DLA User
            1. Fills out all required blocks
                a. Initial or Modification
                b. User ID
                c. Date
                d. System Name
                e. Location of System
                f. Part I Blocks 1-12
                g. Block 13 (Justification)
                h. Block 14 (Privileged)
                i. Block 15 (Classified)
                j. Block 26
                k. Block 27 (Access being Requested)
                l. Completes privileged rules of behavior
            2. Creates Remedy Work order and attaches DD2875 after it is signed by the Supervisor/Representative and Security Officer
    b. Supervisor/Sponsor validates and signs request
        i. Completes Part II
            1. Blocks 16 – 20b.
        ii. Verifies users need to know
        iii. Validates users training
    c. Security Officer signs request
        i. Completes Part III
            1. Blocks 28-32
    d. Data Owner validates and signs request
        i. Validates access being requested in block 27 is “privileged”
        ii. Validates the users IT Level is acceptable for the access requested in block 27
        iii. Quarterly validate the users account
        iv. Completes blocks 21 – 21b
    e. Provisioner provisions the account
    f. Documentation uploaded into DACS
        i. Performed by J64 Identity and Access Management