



**DEPARTMENT OF DEFENSE  
HUMAN RESOURCES ACTIVITY  
DEFENSE MANPOWER DATA CENTER  
DoD CENTER MONTEREY BAY • 400 GIGLING ROAD  
SEASIDE, CALIFORNIA 93955-6771**

**MEMORANDUM OF UNDERSTANDING  
BETWEEN  
Defense Manpower Data Center (DMDC)  
AND  
The Federation for Identity and Cross Credentialing Systems (FiXs)**

- 1) **PURPOSE.** This Memorandum of Understanding (MOU) entered into, by and between DMDC and the Federation for Identity and Cross-Credentialing Systems, Inc. (FiXs) (a not-for-profit 501 (c) 6 trade association in the Commonwealth of Virginia), supersedes or amends the terms and conditions stated in the original MOU dated January 16, 2006 between the same organizations. The purpose of this document is to update/modify the earlier established terms and conditions under which DMDC and FiXs will use the below-listed DMDC and FiXs systems as part(s) of a secure federated identity suite of systems. This set of systems is designed to easily interoperate between the DoD and the federated commercial FiXs Network to provide interoperability for electronic verification, and authentication of the identity of personnel seeking physical or logical authorization to enter military installations or government-controlled areas, and networks and commercial facilities and networks supported by the FiXs Network. These systems use currently available commercially acceptable identity credential technology, in conjunction with biometric identification and meet existing government standards where applicable. The systems being offered by DMDC, and accepted by FiXs, and those being offered by FiXs, and being accepted by DMDC, are listed in addendums to this document, and will form the nexus of a federated, interoperable identity network between the parties.

Systems offered by DMDC to FiXs (Addendum A)

Systems offered by FiXs to DMDC (Addendum B)

2) **AUTHORITY**

- A. DoD Instruction 1000.25, 19 July 2004, DoD Personnel Identity Protection (PIP) Program
- B. DoD Instruction 1000.13, 5 December 1997, Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals
- C. DoD Instruction 4000.19, 9 August 1995, Interservice and Intergovernmental Support

- 3) **EFFECTIVE PERIOD and MODIFICATIONS.** The provisions of this MOU will commence on the date of mutual acceptance as indicated by the latest signature date contained in this MOU and will remain in effect indefinitely or until terminated upon 90 day advance notice in writing to the other party.
- 4) **CONCEPT OF OPERATIONS.** The provisions of this MOU are designed to support the operational framework for interoperability of DMDC and FiXs certified systems in establishing effective verification and authentication interoperability between such systems/applications as DCCIS, and other DMDC and FiXs system(s) as agreed.
- 5) **RESOURCES.** FiXs will maintain a secure test/lab facility which will interoperate with the DMDC contractor test environment. This interoperable environment will provide a test infrastructure where various elements/components (including both software and hardware) of the DCCIS/FiXs interoperable network can be tested and evaluated before being recommended to the Change Control Boards (CCB's) of each organization for pre-production testing and final production/operations. Each organization will exchange executable code and documentation to maintain the appropriate configuration control in each test and production site, as required, to maintain technical interoperability between the DCCIS and FiXs Trust Brokers. FiXs will also fund and maintain an acceptable Certification and Accreditation Program (CAP and C&A program) that meets Federal standards and specifications for the purposes of certifying and accrediting products and services being used on the FiXs Network by members of FiXs. DMDC will be offered a seat on the FiXs CCB and will provided the opportunity to review the FiXs C&A program on a periodic basis for the purposes of acceptance and modifications. FiXs will also fund and maintain a process to assign and manage commercial organization codes.
- 6) **OPERATIONAL RESPONSIBILITIES.** Operational responsibilities for the interoperable, federated, identity network that apply to both DMDC and FiXs are considered joint. In addition to joint responsibilities, each party has individual responsibilities. System-specific responsibilities are listed in the appropriate documentation for each system selected. Responsibilities for all DMDC and FiXs systems addressed by this Memorandum of Understanding are listed below.
  - A. Joint Operational Responsibilities. Both DMDC and FiXs will:
    - 1) Notify POC opposites, or their replacements, of any planned changes to data requirements or data formats at least 60 days in advance of any system/requirement changes. This notice allows the affected party to assess impact and to plan, resource and implement changes. All changes will be documented in the appropriate document for each project. *It is recognized that the 60 day notification requirement will change to, as soon as possible, when*

*modifications by the government are necessitated due to urgent information security or national security requirements.*

- 2) Notify POC opposites, or their replacements, no less than 60 days in advance of any deliverable on system upgrades or issues that could impact system availability, and provide updated status on implementation activities.
- 3) Be provided the opportunity to sit on respective CCBs, if required.
- 4) Transfer data securely, using an encrypted, authenticated transmission mechanism between the DCCIS and FiXs Trust Brokers and associated infrastructure components.
- 5) Give written notification to POC opposites of any material change in the POC roster for selected systems (POC roster(s) will be attached to any system documentation).
- 6) Abide by all applicable DoD and FiXs security rules, regulations, policies, data guidelines and standards, governing, Certification and Accreditation, and security management, relating to the exchange and use of data, including control data.
- 7) Assure compliance with the Privacy Act, as well as all applicable laws, regulations, policies and guidance governing records management and the release of personal information.
- 8) Abide by all applicable DoD security rules, regulations, policies, and guidance governing Personnel Identity Protection.
- 9) Develop a system interface and technical specification describing the technical interface and data description between DMDC and FiXs. The specification will be maintained by approved CCB processes for each organization.
- 10) In capacity of FiXs Government Advisor, DMDC will provide support to the ongoing collaboration, development and evolution of the technological interface between DMDC and FiXs.
- 11) Take newly released documents and standards, such as PIV & FIPS-201, as well as federated identity management standards, such as FiXs organization codes, SAML and Liberty Alliance, under consideration for inclusion in future releases. These future interfaces could include, but are not restricted to, such systems as: JPAS, DBIDS and CAC web based enrollment via DCCIS and FiXs, and web based visitor request systems.
- 12) DMDC and FiXs will develop and execute the appropriate public affairs materials, briefings, white papers, etc. required to provide the appropriate information to users, or potential users, of the federated, interoperable identity network.

**B. DMDC Operational Responsibilities:**

- 1) Provide a POC for governance activities (see Section 7) to provide liaison with FiXs regarding policies, procedures, business rules, FiXs commercial organization codes, CCB, hardware, software, security, C&A and other matters affecting the interoperability of the agreed to federated network.

- 2) Provide, and use, data in a consistent, and mutually agreed, format/means to ensure successful technical interoperability with the FiXs infrastructure and other DoD enterprise systems as required.
- 3) Support ongoing DCCIS operations with the FiXs infrastructure in conformance with applicable DoD policy.
- 4) Continue support throughout the operational process.
- 5) Provide training, or technical guidance, for modifications (if required).
- 6) Ensure DMDC's stated responsibilities for the Automated Data Processing Environment for each system selected is fulfilled.
- 7) Provide system software changes (if required) and interface updates as they become applicable to the FiXs infrastructure components.
- 8) Review the FiXs CAP and specific FiXs approved C&A reports on certified products and components used by FiXs member organizations. Authorize and accept the use of those certified products and components on the interoperable DCCIS/FiXs infrastructure. DMDC, however, reserves the right to conduct periodic audits of the FiXs CAP to ensure compliance with, and acceptance of, Federal standards and practices.

C. FiXs Operational Responsibilities:

- 1) Appoint a single POC to provide liaison with DMDC regarding policies, procedures, business rules, hardware requirements, and scheduling.
- 2) Notify DMDC immediately of changes/developments that could affect the current operational/deployment timeline. Share future changes in a timely manner, if they will affect joint operations or interoperability.
- 3) Support ongoing operations with DMDC and DCCIS, technical interoperability, and trusted exchange of identity credentials between trusted FiXs partners and DoD programs thru the FiXs Trust Broker and associated network components. Exchange and maintain data as required in support of this agreement, to include commercial organization codes to support interoperability.
- 4) Use data/hardware in a manner consistent with uses identified in each system description.
- 5) Prevent unauthorized personnel from obtaining physical access to system equipment.
- 6) Provide a safe and appropriate physical location for the installation, of all equipment required to support the interoperable network that is as free as possible from all environmental hazards including undue heat, cold, moisture, contamination, shock, or vibration. Maintain NIACAP certification where required.
- 7) Ensure FiXs member's stated responsibilities for all requirements of this MOU are carried out within their own organizations. This includes individual facilities that are identified as a FiXs node or end user site, of the interoperable federated identity network between DMDC and FiXs. To that end, each FiXs user member will sign a separate MOU/Terms of Use Agreement with FiXs reflecting the

specifics of this MOU between DMDC and FiXs. These individual FiXs member MOUs/Terms of Use Agreements will provide for assessments and certifications of adherence to all rules and policies of this agreement, as prescribed by either FiXs or DMDC.

- 8) Develop and maintain a Certification and Accreditation (C&A) program for member's products and services, that is acceptable to DMDC, and that aligns with NIST and other Federal standards and procedures as well as commercially reasonable practices from Industry. FiXs will offer DMDC all C&A documentation for review and acceptance, if requested. FiXs will also operate and maintain a test/lab environment interoperable with DMDC.
- 9) FiXs (The Federation) will conduct periodic random assessments and certifications that FiXs members are in compliance with the terms and conditions in this agreement and transferred to its membership that use the interoperable federated network and its products and services. Copies of these assessments will be made available to DMDC. If deemed appropriate DMDC may conduct its own independent assessments, with seven days prior notification to the FiXs Executive Committee.
- 10) FiXs will not store any personal identifying data received from DMDC.

**7. GOVERNANCE.** This MOU and its agreed to responsibilities, will be governed by existing forums within the DoD and FiXs. FiXs will provide appropriate liaison membership for DMDC assigned POC(s) to its Board of Directors, Executive Committee, CCB, Operations and Security Committees and all other committees and sub-committees established in accordance with the FiXs Bylaws and permitted by Federal statute. DMDC will provide for FiXs representation on/at management and oversight forums or meetings, for the purposes of: operating oversight; process changes; security requirements; CCB; C&A; developing, modifying and maintaining the interoperable federated network between FiXs and DMDC; or other policy, development or operational issues affecting the relationships established in this MOU.

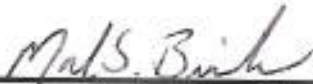
- 8. UNAUTHORIZED DISCLOSURE.** In the event DMDC determines that FiXs, or one of its members, has made an unauthorized disclosure of the data provided by DMDC, DMDC may:
- 1) Request a formal inquiry into an allegation of an unauthorized disclosure or, depending on severity, refer the issue to DoD and Federal law enforcement.
  - 2) Take appropriate action on 1 above, where an authorized release has been determined to have occurred, proceed with action required by law enforcement/general counsel. Require the submission of a corrective action plan formulated to implement steps to be taken to alleviate the possibility of any future unauthorized disclosure.
  - 3) Require the return of the data.
  - 4) Sanction against the further release of DMDC data to FiXs or its member users.

- 5) Additionally, FiXs acknowledges that criminal penalties under the Privacy Act (5 USC 552a (I) (3)) may apply if it is determined that FiXs, or any individual employed or affiliated therewith, knowingly and willfully obtained the file(s) under false pretenses.
- 6) In reciprocal terms, Items 1-4 above, apply to DMDC in the event of unauthorized disclosure of the data provided by FiXs to DMDC.

**9. ACCEPTANCE AND RATIFICATION.** The provisions of this MOU become effective upon signature and date as indicated below. *(It is recognized by both parties that changes to the operational infrastructure due to information assurance or national security requirements are outside the control of the parties to this agreement.)*

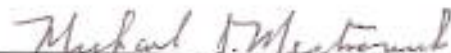
For: Defense Manpower Data Center  
400 Gigling Road  
Seaside, CA 93955

For: Federation for Identity and  
Cross-Credentialing Systems, Inc.  
10400 Eaton Place  
Suite 500A  
Fairfax, VA 22030-2208



---

Mark S. Breckenridge  
Deputy Director



---

Michael J. Mestrovich, PhD  
FiXs President and  
Chairman Board of Directors

---

Date: February 12, 2009

---

Date: February 12, 2009

Appendix:

1. References

Addendums:

A. Systems offered by DMDC to FiXs

B. Systems offered by FiXs to DMDC

## Appendix: REFERENCES

- a) DOD Instruction 5200.40, 30 December 1997, "DOD Information Technology Security Certification and Accreditation Process (DITSCAP)" and commercial equivalent NIACAP
- b) DoD Instruction 8510.1-M, 31 July 2000, Information Technology Security Certification and Accreditation Process (DITSCAP) Application Document.
- c) CJCSI 6212.01B, 8 May 2000, "Interoperability and Supportability of National Security Systems, and Information Technology Systems"
- d) ASD (C3I) Memorandum, 20 March 1997, "Secret and Below Interoperability (SABI)"
- e) FIPS 140-1, FIPS 140-2, 25 May 2001, "Security Requirements for Cryptographic Modules"
- f) DoD 5200.2, 9 April 1999 or latest release, "Personnel Security Program"
- g) Homeland Security Presidential Directive Number 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," August 26, 2004
- h) Federal Information Processing Standard (FIPS) 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors," March 2006
- i) Directive Type Memorandum 08-006, "DoD Implementation of Homeland Security Presidential Directive-12," November 26, 2008
- j) DMDC letter dated December 06, 2006 on acceptance of Commercial Organization Codes in the CHUID from FiXs.
- k) DMDC letter dated December 11, 2006 on coordination of the FiXs and DMDC testing environments
- l) FiXs letter dated February 05, 2007 on coordination of additional bar code and PIV CHUID specifications.
- m) FiXs Security Guidelines , v2.0 March 29, 2007
- n) FiXs Trust Model, v2.0 March 29, 2007
- o) FiXs Operating Rules, v3.2 November 13, 2008
- p) FiXs System Technical Description DRAFT, v2.0 March 29, 2007
- q) FiXs CAP Document, v1.1 September 15, 2008
- r) FiXs Configuration Control Board Procedures, v2.1 January 31, 2008
- s) FiXs Implementation Guidelines, v3.1 January 31, 2008
- t) FiXs Policy Document, v2.0 March 29, 2007

- u) DCCIS and FiXs Interface Specification (as referenced in the Addendum)
- v) Section 552a of title 5, United State Code, Privacy Act of 1974
- w) Office of Management and Budget, Circular No. A-130, "Management of Federal Information Resources" July 2, 1993 with revisions
- x) DoD 5400.7-R, September 1998, "Freedom of Information Act of National Security Systems, and Information Technology Systems"
- y) DoD 5400.11-R, 13 December 1999, "Department of Defense Privacy Program"
- z) DoD Directive 1000.25, July 19, 2004, "DoD Personnel Identity Protection Program"

## Addendum A: Systems offered by DMDC to FiXs

Defense Biometric Identification System (DBIDS)

Defense National Visitors Center (DNVC)

Defense Cross-Credentialing Identification System (DCCIS)

DoD Sensitive and Classified Visit Request System (under development by DMDC)

## Addendum B: Systems offered by FiXs to DMDC

FiXs Network, and its certified infrastructure components and certified credentials