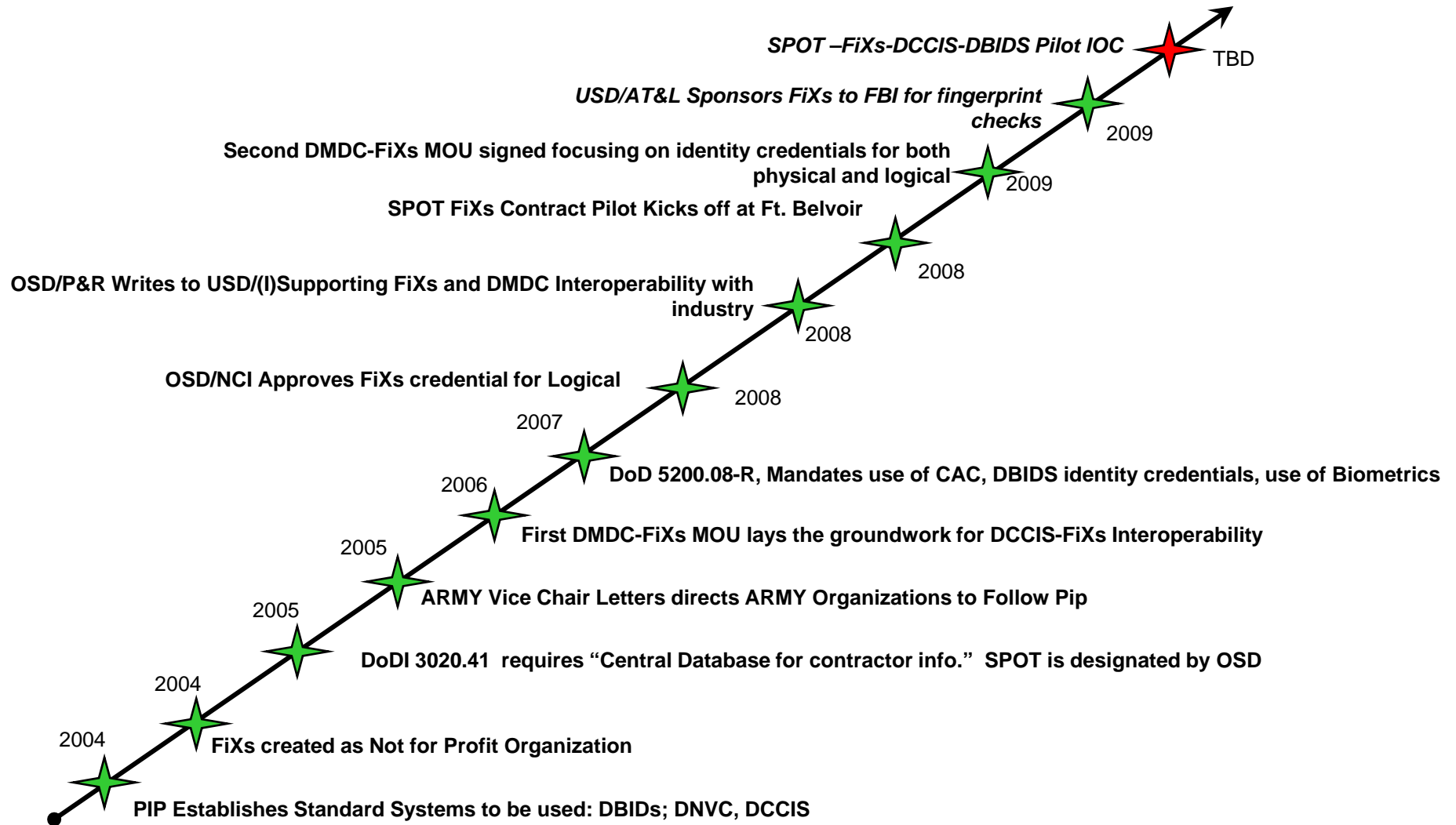


Overview of DoD Policy Leading to SPOT-FiXs-DCCIS-DNVC-DBIDS Federated Infrastructure and Operations



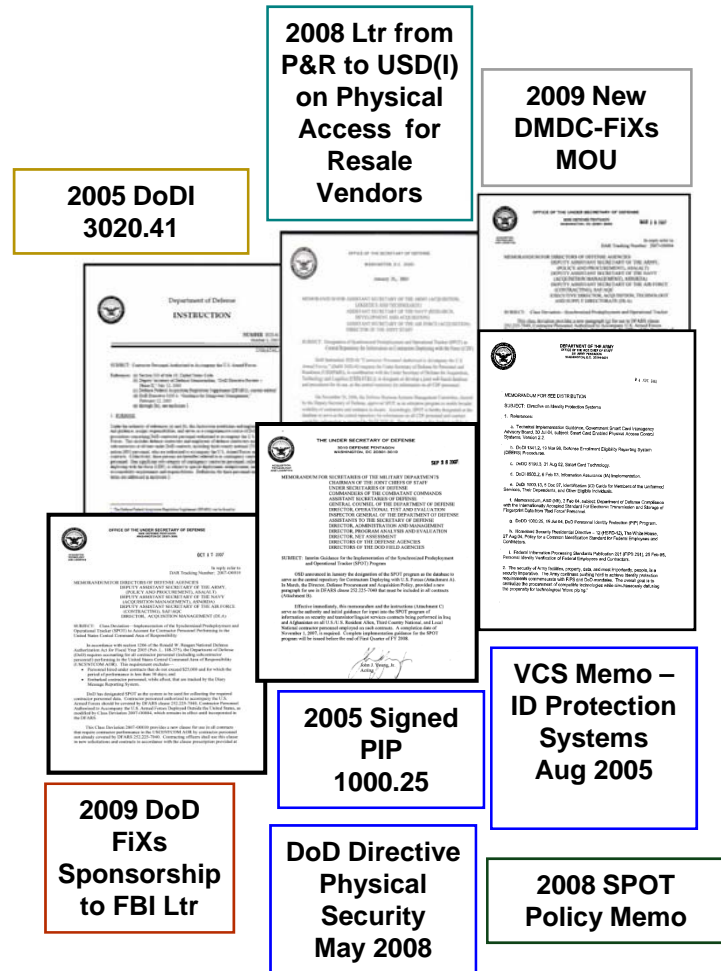
SPOT-FiXs-DCCIS-DBIDS Policy Timeline



SPOT-FiXs-DCCIS-DBIDS Policy Timeline

- 2004 – PIP Establishes Standard Systems to be used: DBIDs; DNVC, DCCIS

“4.3. The PIP Program shall use emerging technologies to support the protection of individual identity and to safeguard DoD physical assets and logical systems from unauthorized access based on fraudulent or fraudulently obtained credentials. Further, identification credentials shall be authenticated to ensure that they are currently valid and issued to the individuals presenting them, whenever possible. “



SPOT-FiXs-DCCIS-DBIDS Policy Timeline

“4.3.1. Oversight for the PIP program shall be from the IPMSCG. The IPMSCG shall be a cohesive DoD-wide policy recommendation, requirements, strategy, and oversight group for managing the physical and virtual identities of all our personnel, support contractors, business partners, and other entities consistent with the Global Information Grid Architecture. It shall focus on Federal Sector and Department-wide interoperability standards, performance matrices; ways to exploit identity management tools as means for enhancing readiness, business processes, and security; and being cognizant of protecting entities' identifiable information. The following are examples of systems that meet PIP criteria: 4.3.1.1.

DBIDS is a fully configurable force protection system and shall serve as a physical access control and critical property registration system. DBIDS implements the policies outlined in DoD Directive 5200.8 and DoD Directive 8190.3 (references (p) and (q)) and is an approved system under the PIP. DBIDS is authorized to issue DoD identity credentials to those individuals needing physical access and not otherwise credentialed under reference (d). 4.3.1.2.

The **DNVC** is the system for DoD facilities to authenticate DoD credential-carrying visitors using a web-based connection. DNVC is available to DoD law enforcement and force protection elements and is recognized as an approved system under the PIP. 4.3.1.3.

The **DCCIS** shall provide mutual authentication of issued identity credentials between participating Federal Agencies and private sector business partners. Use of a federated identity system for recognition of credentials shall strengthen the security of the Department of Defense. DCCIS is an approved system under the PIP.”



SPOT-FiXs-DCCIS-DBIDS Policy Timeline

2004– FiXs created as Not for Profit. FiXs Bylaws established

The purposes and objectives of the Federation are generally set forth in the Articles of Incorporation and include but are not limited to the following specific purposes and objectives:

- a. Establish, maintain and oversee the Federation for Identity and Cross-Credentialing Systems (“FiXs®”) Network (“FiXs Network”) and standards for the purpose of interconnecting and cooperating for the specific efforts of identity protection, management and authentication for physical and logical access requirements, including compliance with certain common trust models, business rules, policies, and technical specifications standards adopted by the Federation. (The first instantiation of the Network was with the Department of Defense (“DoD”), which established an interface between its Defense Cross-Credentialing Identification System (“DCCIS”) and FiXs. Subsequent instantiations will provide solutions that satisfy Homeland Security Presidential Directive 12 (HSPD-12) and potentially other commercial and government requirements both domestically and internationally.
- b. Establish a foundation for the interoperability of identity authentication and verification standards within the FiXs Network to include biometrics.
- c. Maintain and enforce the provisions of the various governance documents that provide the foundation for the Federation, including the Trust Statement, the FiXs Policy, the Operating Rules (“Rules”), the Technical Interface and Specifications, Implementation Guidelines, Security Guidelines, and any governance documents, Memoranda of Understanding, or agreements between government and industry.



SPOT-FiXs-DCCIS-DBIDS Policy Timeline

2005– DoDI 3020.41 requires “Central Database for contractor info.” SPOT is designated by OSD

“4.5. Maintain by-name accountability of all CDF personnel and contract capability information in a joint database. This database shall provide a central source of CDF personnel information and a summary of services or capabilities provided by all external support and systems support contracts. This information shall be used to assist planning for the provision of force protection, medical support, personnel recovery, and other support. It should also provide planners an awareness of the nature, extent, and potential risks and capabilities associated with contracted support in the area of responsibility (AOR). This requirement may be waived by the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)).”

“4.6. Designate in all external support and system support contracts the specific deployment center or process CDF must use to prepare for deployment and redeployment.”

“4.7. Designate the requirement for all CDF to process through the joint reception center (JRC) designated by the geographic Combatant Commander in all external support and system support contracts. This requirement may be waived by USD(AT&L).”



SPOT-FiXs-DCCIS-DBIDS Policy Timeline

2005– ARMY Vice Chair Letters directs ARMY Organizations to Follow Pip

b. New procurements of Physical Access Systems used in the Army will conform to the technical and policy specifications of the above references. Existing legacy Physical Access Systems will continue to operate until replacement or upgrade. At that point, those systems will meet the Physical Access requirements of reference 1.a. to operate in accordance with the standards of the Federal Agency Smart Credential.

c. The granting of access privileges remains a local policy and business operation function of the local facility, but must function in concert with Personnel Identity Protection policy and procedures.



SPOT-FiXs-DCCIS-DBIDS Policy Timeline

2007 – Force Protection Directive mandates use of CAC, DBIDS Identify Credential, use of Biometrics Interoperability between the systems (HSPD-12 Adherence)

DL1.9. Personnel Identity Management and Protection. **A business process that validates, authenticates and secures an individual's identity. The process includes: identity vetting; a binding of the identity to an identity protection and management system** through the issuance of a DoD credential; the linkage of the Personal Identity Verification (PIV) credential to the individual through the use of uniquely identifying characteristics and a personal identification number; and digital authentication of the identification credential linkage to the individual.

C2.1.3. Physical security planning includes: C2.1.3.1. **Using biometric, electronic and/or mechanical technological security systems to mitigate both vulnerability to the threat and reduce reliance on fixed security forces.**

C2.1.4.8. Credential technologies, access control devices, biometrics, materiel or asset tagging systems, and contraband detection equipment.

C2.5.2. **Federal Information Processing Standards (FIPS) 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors," March 01, 2006, (Reference (r)) provides guidance** for the acquisition of Federal PIV credentials and supporting equipment, when fulfilling the requirements for Federal standards of identity and access control.



SPOT-FiXs-DCCIS-DBIDS Policy Timeline

2008 – OSD/NCI Approves FiXs credential for Logical Use

“...The Federation for Identity and Cross-Credentialing Systems (FiXs) that there is no additional approval required from my office or the 000 CIO for use of approved PKI certificates for authentication to DoD web servers. **FiXs credentials that include PKI certificates issued from any DoD ECA vendors are acceptable for use by 000 web based systems.** Access control, however, remains the prerogative of the application owner'. Our members will be pleased to learn that "FiXs Certified Credentials that include PKI certificates issued from ECA vendors are acceptable for use...”

2008 – OSD/P&R Writes to USD/(I) Supporting FiXs and DMDC Interoperability with industry

“...During a recent meeting of the Executive Resale Board, the Military Departments expressed great concern about delays and costs of identification credentials for physical access to bases by vendors who supply the commissary, exchange, and morale, welfare, and recreation (MWR) systems. The House Committee on Armed Services raised similar concerns during testimony before the Subcommittee on Military Personnel the past three years and requests a report on the feasibility of using the CommonAccess Card (CAC) for physical access by vendors...”

“...**Credentialing Systems (FiXs) effort as a solution for vendor access. In the absence of standards, this is an industry attempt to comply as best they understand the requirements for identity proofing and vetting leading to identity credential issuance in the form of a card that might be acceptable to the Department.** This is complicated by the absence of...”



SPOT-FiXs-DCCIS-DBIDS Policy Timeline

2009 – Second DMDC-FiXs MOU signed focusing on identity credentials for both physical and logical

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.**



SPOT-FiXs-DCCIS-DBIDS Policy Timeline

2009 – USD/AT&L Sponsors FiXs to FBI for fingerprint checks

“...The Department of Defense (DoD) would like to sponsor the Federation for Identity and Cross-Credentialing Systems (FiXs) organization for Federal Bureau of Investigation (FBI) fingerprint checks. This sponsorship is in support of the Synchronized Pre-deployment and Operational Tracker (SPOT) system and limited in scope and duration to facilitate an interoperability pilot program between FiXs and SPOT, which, for the period from April 1, 2009 to March 31, 2010, **will test the use of the FiXs card as a commercial equivalent of the Common Access Card (CAC)**. Under this sponsorship, DoD would like the FBI to agree to provide the results of fingerprint checks to FiXs, upon its request when, pursuant to the SPOT pilot program, FiXs is verifying the identity of contractor personnel seeking to enter U.S military installations and other U.S. government-controlled areas...”

