Summary of the FiXs Certification and Accreditation (C&A) Process

All FiXs C&A assessments will be conducted in accordance with guidance outlined in NIST Special Publication 800-37, the National Information Assurance Certification and Accreditation Process (NIACAP), and FiXs Security Policy and Operating Procedures. The basis of the C&A effort is further defined by identifying the specific sources of security policy, security controls and operating requirements which will be reviewed during the assessment. The following source documents are the basis for that review:

- Federation for Identity and Cross-Credentialing Systems (FiXs) By-Law, Version 2.2
- FiXs Policy Document, Version 2.0
- FiXs Security Guidelines, Version 2.0
- FiXs Implementation Guidelines, Version 3.0
- FiXs Policy Document, Version 2.0
- FIXS Operating Rules, Version 2.0
- FIXS Logical Operating Rules, Addendum Version 0.4
- National Institute of Standards and Technology (NIST) Special Publication 800-37
- Federal Information Processing Standard (FIPS) Publication 201-1
- NIST Special Publication 800-79
- NIST Special Publication 800-53
- NIST Special Publication 800-53A
- National Information Assurance Certification and Accreditation Process (NIACAP) { NSTISSI No. 1000}

The specific applicability of the above listed publications will be delineated in an assessment checklist supplied by the FiXs approved C&A contractor prior to the start of the C&A assessment. The C&A contractor, working with the applicant organization, and based on the scope of the requested assessment will develop a custom checklist for that organization. Any previous non-FiXs C&A efforts, which may be applicable and acceptable, will be considered as part of the pre-assessment leading up to the FiXs C&A.

The Application for a C& A is supplied below.