

# FIPS 140-2 Validation Requirements

**Duration:**

2 days

**Audience:**

This course is aimed at development team members who will be involved in a FIPS 140-2 evaluation.

**Prerequisites:**

Basic knowledge of FIPS 140-2 standard, a working knowledge of cryptography and supporting functions such as key management is helpful.

**Course Goals:**

After completing this course, the trainee will have the knowledge and skills to:

- Understand FIPS 140-2 security requirements for each level
- Understand testing requirements
- Understand the required Security Policy content

**Course Outline:**

- Motivation for FIPS 140-2
  - FISMA
  - DoD
  - Industry
- Related Documents
  - FIPS 140-2
  - FIPS 140-2 Derived Test Requirements
  - FIPS 140-2 Implementation Guidance
  - FIPS 140-2 Annexes
  - Approved Function Standards and Special Publications)

- Validation Requirements:
  - Security Policy
  - Crypto Module Specifications
  - Crypto Module Ports and Interfaces
  - Roles, Services and Authentications
  - Finite State Model
    - Example of Finite State Diagram
    - Example of State Transition Table
  - Physical Security
  - Operational Environment
  - Key Management
  - EMI/EMC
  - Self Tests
  - Design Assurance
  - Mitigation of Other Attacks
- The Validation Process
  - Document Review
  - Design Review
    - Software
    - Firmware
    - Hardware
  - Testing (laboratory)