

PRIVACY

1. Is a Privacy Impact Assessment (PIA) required for all agency data systems used to collect and store information related to the personal identity verification process?

Yes, a PIA is necessary.

2. How does FIPS 201 protect privacy?

During card issuance and life cycle management, all agencies are required to comply with FIPS 201, Section 2.4, "PIV Privacy Requirements," which outlines strict control measures to ensure the privacy of PIV card applicants and cardholders is protected. In addition, Personally Identifiable Information (PII) stored on the card is minimal, as is PII acquired and retained by the issuance system. PII such as electronic fingerprints will be encoded as minutiae templates while stored on a PIV card. The PIV card, once activated, is in the control of the individual it identifies, who can then determine where and under what circumstances to present it. (Refer to OMB Memorandum 06-19 for additional information)

3. FIPS 201 2.4 requires that all systems provide continuous auditing of privacy compliance covering collection, use, and distribution of information during program operation. Exactly what information needs to be recorded, how should it be recorded, and how should it be made available to the appropriate people?

Privacy Compliance is the responsibility of the Senior Agency Official for Privacy and should follow OMB guidance for privacy documentation. Part one of FIPS 201 outlines these requirements and NIST Special Publication 800-79 provides accreditation guidelines.

4. Are there any specific requirements for when and/or how identity data should be protected, and who should or should not be able to access it? How does this requirement specifically affect communications with the IDMS and the FBI IAFIS for PIV-related fingerprint checks?

It is the responsibility of the Senior Agency Official for Privacy to ensure the identity data is properly protected from unauthorized disclosure. Agencies may use alternative methods for protecting information in transit and at rest. Interface specifications are under development and information on these may be accessed at <http://www.idmanagement.gov>. (Ref: FIPS 201, Section 2.4)

5. Do PIV systems require any specific support for limiting access to Information in Identifiable Form (IIF) beyond the standard login process? If so, what are the requirements?

No. Specific uses for the PIV security features are outside the scope of FIPS 201. Please refer to NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, and to FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, for recommendations on protection and access control for IIF.