A Synopsis

of

Federal Information Processing Standard (FIPS) 201

for

Personal Identity Verification (PIV)

of

Federal Employees and Contractors

Presentation by NIST March 2005

Topics

- HSPD-12 Requirements and Timeline
- FIPS 201 Development Process
- FIPS 201 Requirements
- Additional Guidance

HSPD-12 Presidential Policy Driver

Home Security Presidential Directive 12 (HSPD-12):

"*Policy for a Common Identification Standard for Federal Employees and Contractors*"

Dated: **August 27, 2004**

HSPD 12 Requirements

Secure and reliable forms of personal identification that is:

- Based on sound criteria to verify an individual employee's identity
- Strongly resistant to fraud, tampering, counterfeiting, and terrorist exploitation
- Rapidly verified *electronically*
- Issued only by providers whose reliability has been established by an official accreditation process

HSPD 12: Requirements (cont.)

- Applicable to *all* government organizations and contractors except identification associated with National Security Systems
- Used for access to Federally-controlled facilities and logical access to Federally-controlled information systems
- Flexible in selecting appropriate security level – includes graduated criteria from *least* secure to *most* secure
- Implemented in a manner that protects citizens' privacy

HSPD-12 Milestones

Timeline	Agency/Department Requirement/Milestone
August 27, 2004	**Directive signed and issued**
Not later than 6 months (February 25, 2005)	**Issue standard**
Not later than 4 months following issuance of standard (June 25, 2005)	**Program in place to ensure that identification issued by organizations meet the PIV Standard (part-1)**
Not later than 6 months following issuance of standard. (August 25, 2005)	**Identify additional applications that could benefit from conformance to the standard**
Not later than 8 months following issuance of standard (October 27, 2005)	**Compliance with standard (Part-1)**

FIPS 201 Development Process

- Preliminary thinking posted on PIV web site in late September 2004
- Held 4 workshops on draft standards (1 workshop for government only)
- Published preliminary draft and draft for public review
- Independent coordination with the Government Smart Card Interagency Advisory Board and Federal Identity Credentialing Committee
- Final consultations with Defense, State, Homeland Security, Justice, OSTP, and OMB
- Processed comments from over 90 organizations.

Nature of Comments on the Draft

- Differences from current systems and systems development programs in which substantial resources have been invested
- Resource and time required to implement changes to existing systems
- Privacy concerns held by unions and public
- Time required to conduct background checks
- Differences among agencies regarding best mechanisms for:
  - Physical and logical security
  - Technology
  - Performance
  - Business issues

Comment Evaluation - Considerations

Key balancing interests include:

- Increased security
- Enhanced interoperability
- Cost
- Time
- Privacy
- Employee/union interests
- Usability
- Industry concerns
- Training
- Agency flexibility vs. consistency
- Simplicity
- Installed base technology
- Emerging standards and technology
- Technology neutrality

All within the context of meeting the President's HSPD 12 mandate for change

Main Changes to FIPS 201
Based on Public Comments

- Identity Proofing, Registration and Issuance
  - Removed Position Sensitivity Levels
  - Require NACI for all employees and contractors, but allow issuance of the ID badge after NAC is completed
  - Reduced the number of face-to-face encounters required for PIV registration and issuance
  - Replaced Identity Proofing, Registration, and Issuance process description in Section 2 with functional and security requirements, and moved detailed process to Appendix A
  - Support the verification of identity source documents using mechanisms stronger than visual inspection.
- Privacy requirements - added
- Card Topology – modified to allow agencies more flexibility and provided clarifications.

Main Changes to FIPS 201
Based on Public Comments (Cont.)

- Biometrics
  - Removed the requirement for storing Facial Image on the card.
  - Moved Biometric data collection and formatting requirement to the *Biometric Data Specifications for PIV*, Special Publication 800-76. This will enable NIST to expedite future changes.
- Cryptography and Key Management
  - Moved references to algorithms and sizes to *Recommendation for Cryptographic Algorithms and Key Sizes*, Special Publication 800-78. This will enable NIST to expedite future changes.
- Graduated Criteria
  - Added Identity Authentication Assurance Levels and mapped them to OMB guidance and PACS
  - Provided Use Cases that illustrate the Identity Authentication Assurance Levels

FIPS 201 Requirements

Phased-Implementation In Two Parts

- Part 1 – Common Identification and Security Requirements
  - HSPD 12 Control Objectives
  - Identity Proofing, Registration and Issuance Requirements (revised from November Draft)
  - Effective October 2005
- Part 2 - Common Interoperability Requirements
  - Detailed Technical Specifications
  - Most Elements (revised) of October Preliminary Draft
  - No set deadline for implementation in PIV standard
- Migration Timeframe (i.e., Phase I to II)
  - Agency implementation plans to OMB before July 2005
  - OMB to develop schedule

PIV Identity Proofing and Registration Requirements

- Organization shall adopt and use an approved identity proofing and registration process.
- Process shall begin with initiation of a National Agency Check with Written Inquiries (NACI) or other Office of Personnel Management (OPM) or National Security community investigation required for Federal employment.
- National Agency Check (NAC) component of the NACI shall be completed before credential issuance.
- Applicant must appear in-person at least once before the issuance of a PIV credential.

PIV Identity Proofing and Registration Requirements (Cont.)

- Applicant shall be required to provide two forms of identity source documents in original form. Source documents must come from the list of acceptable documents included in *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification*. At least one document shall be a valid State or Federal government-issued picture identification (ID).

- PIV identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person.

PIV Issuance and Maintenance Requirements

- The organization shall use an approved PIV credential issuance and maintenance process.
- Ensure completion and successful adjudication of a National Agency Check (NAC), National Agency Check with Written Inquiries (NACI), or other OPM or National Security community investigation as required for Federal employment. The PIV credential shall be revoked if the results of the investigation so justify.
- At the time of issuance, verify that the individual to whom the credential is to be issued (and on whom the background investigation was completed) is the same as the intended applicant/recipient as approved by the appropriate authority.

PIV Issuance and Maintenance Requirements (Cont.)

- The organization shall issue PIV credentials only through systems and providers whose reliability has been established by the agency and so documented and approved in writing (i.e., accredited).

Privacy Requirements

- HSPD 12 requires that PIV systems are implemented with all privacy controls specified in this standard, as well as those specified in Federal privacy laws and policies including but not limited to the E-Government Act of 2002, the Privacy Act of 1974, and Office of Management and Budget (OMB) Memorandum M-03-22, as applicable.

- All agencies must:
  - have a privacy official role
  - conduct Privacy Impact Assessment (PIA) in accordance with standards
  - have procedures to handle Information in Identifiable Form (IIF)
  - have procedures to handle privacy violations
  - maintain appeals procedures for denials/revocation of credentials.

Identity Proofing and Card Issuance Requirements

- No single individual shall be capable of issuing a PIV card
- Role Based Model
  - Roles of PIV Applicant, Sponsor, Registrar, and Issuer are mutually exclusive (I.e. no individual shall hold more than one of these roles in the identity proofing and registration process.)
  - PIV Issuer and PIV Digital Signatory roles may be assumed by one individual or entity.
- System-Based Model
  - Requires highly developed personnel management system and remotely accessible database (e.g., DoD DEERS/RAPIDS)
  - No cards issued to individuals not in the database

Part 2
PIV
Requirements

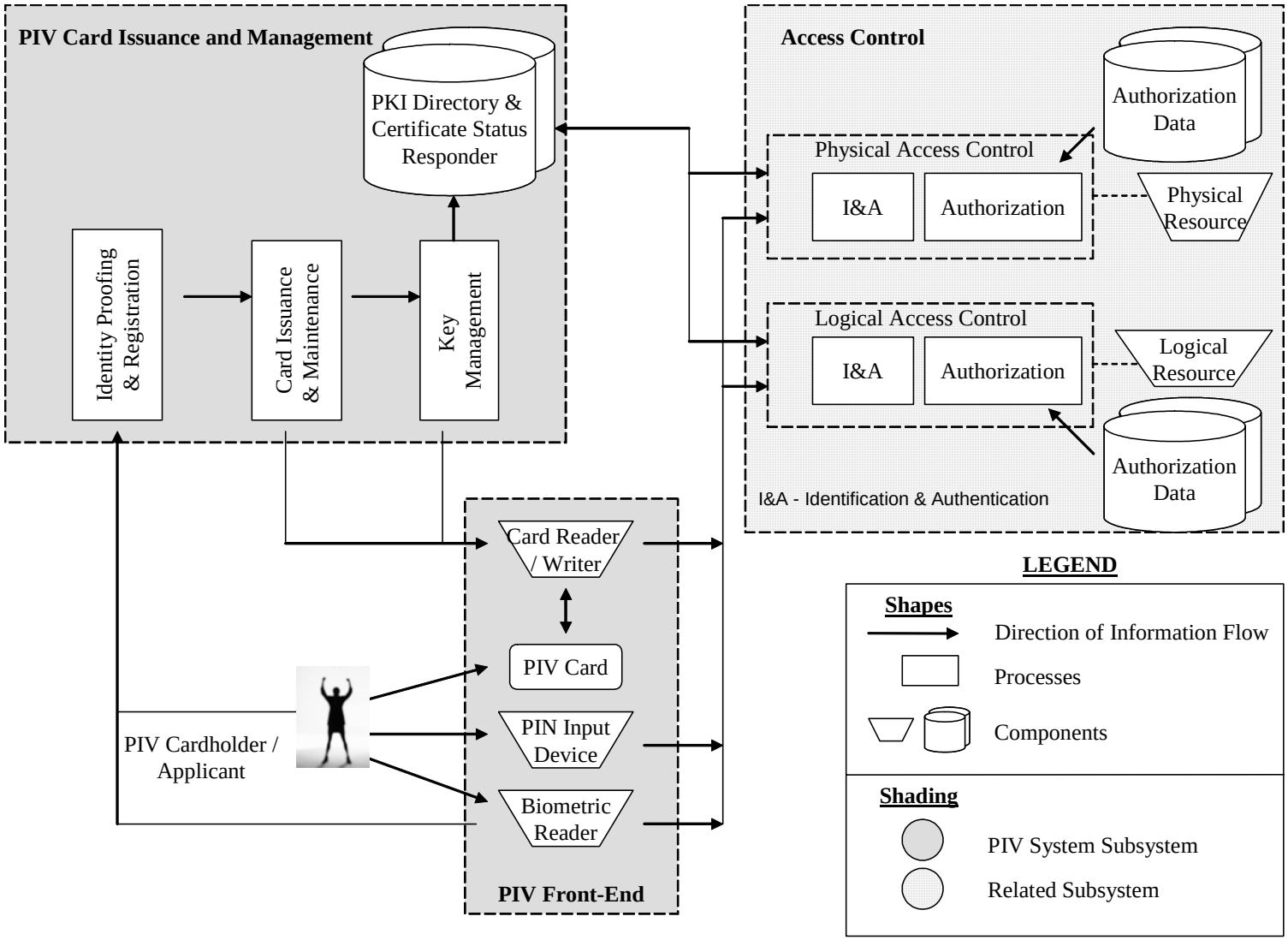
Functional Components

- PIV Front-End Subsystem — PIV Card, card and biometric readers, and personal identification number (PIN) input device. The PIV cardholder interacts with these components to gain physical or logical access to the desired Federal resource.

- PIV Card Issuance and Management Subsystem — the components responsible for identity proofing and registration, card and key issuance and management, and the various repositories and services (e.g., public key infrastructure [PKI] directory, certificate status servers) required as part of the verification infrastructure.

- Access Control Subsystem — the physical and logical access control systems, the protected resources, and the authorization data.

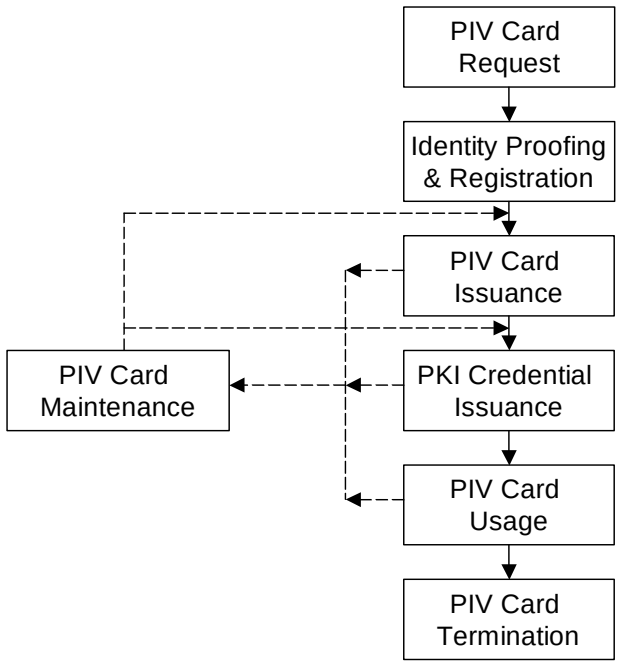
PIV Notional System



National Institute of Standards and Technology

FIPS 201 REQUIREMENTS

Life Cycle Activities



PIV Card Visual Data – Mandatory Items

Front

- Photograph
- Name
- Employee Affiliation
- Organizational Affiliation (Agency Name and/or Department)
- Expiration Date

Back

- Agency Card Serial Number
- Issuer Identification

PIV Card Visual Data – Optional Items

Front

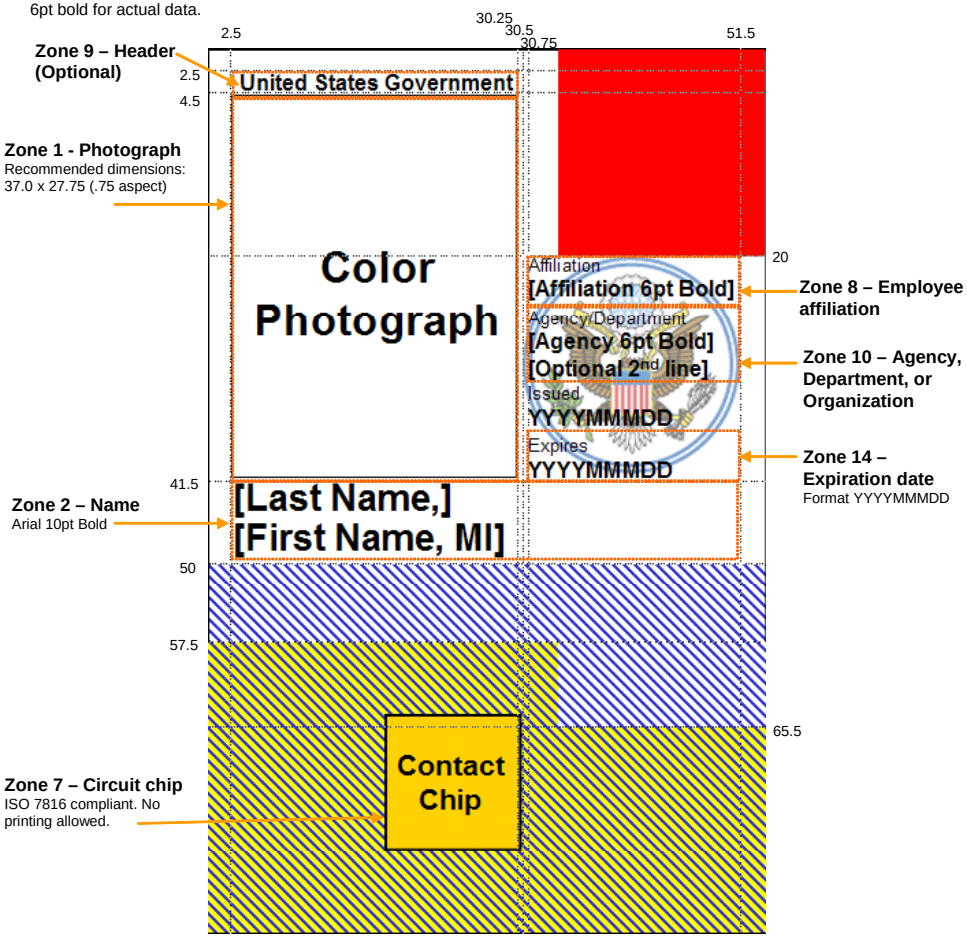
- Card Holder's Signature
- Agency Specific Text Area
- Rank
- Bar Code
- Agency Specific Header
- Agency Seal
- Agency Specific Footer
- Issue Date
- Color Codes for Employee Affiliation
- Photo Border for Employee Affiliation
- Agency Specific Data

Back

- Magnetic Stripe
- Return Information
- Physical Characteristics of Cardholder
- Additional Language for Emergency Responder Officials

PIV Card Front – Printable Areas

- All measurements around the figure are in millimeters and are from the top-left corner.
- All text is to be printed using the Arial font.
- Unless otherwise specified, the recommended font size is 5pt normal weight for data labels (also referred to as tags) and 6pt bold for actual data.



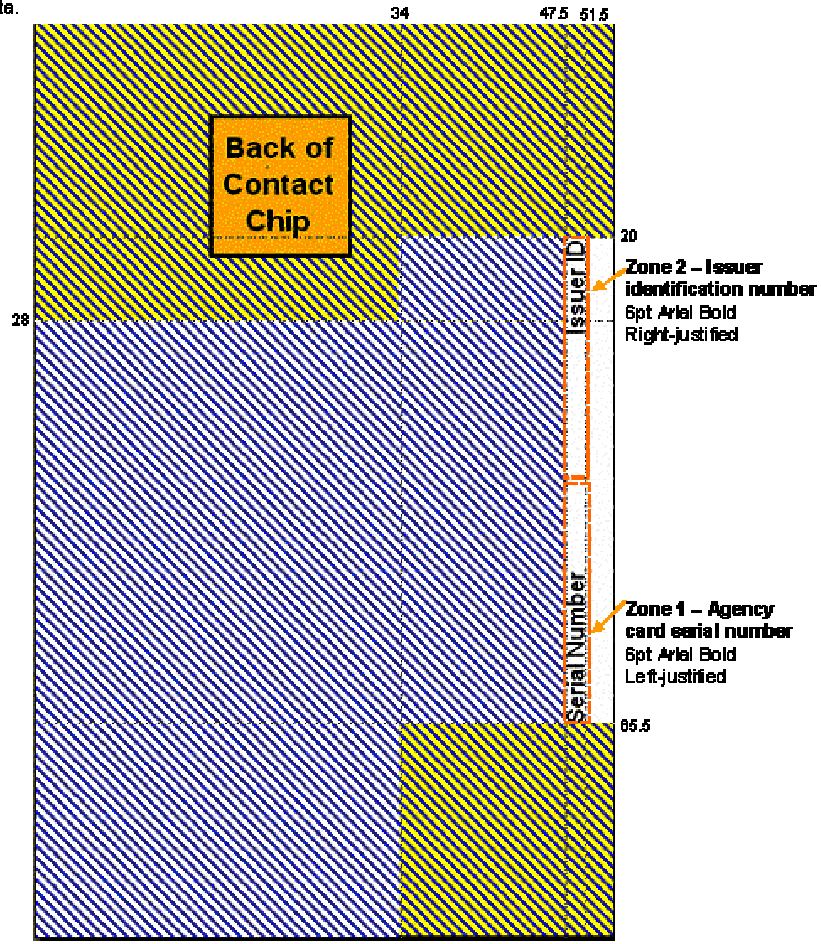
Area for additional optional data. Agency-specific data may be printed in this area. See other examples for required placement of additional optional data elements. Note: In this example, Zone 9,11, and 13 are optional but shall be placed as depicted and therefore are not in the blue shaded area.

Area likely to be needed by card manufacturer. Optional data may be printed in this area but may be subject to restrictions imposed by card and/or printer manufacturers.

Reserved area. No printing is permitted in this area unless verified as printable area by card and/or printer manufactuers.

PIV Card Back – Printable Areas

All measurements are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the recommended font size is 5pt normal weight for tags and 6pt bold for data.

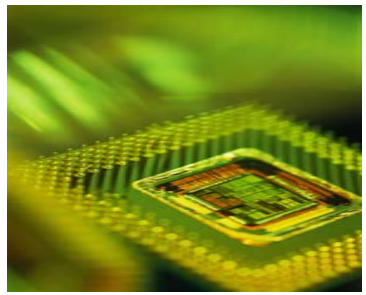


Optional data area. Agency-specific data may be printed in this area. See examples for required placement of optional data elements.

Optional data area likely to be needed by card manufacturer. Optional data may be printed in this area, but will likely be subject to restrictions imposed by card and/or printer manufacturers.

PIV Card Requirements

- Mandatory
  - Integrated Circuit to Store/Process Data
- Optional
  - Magnetic Stripe
  - Bar Code
  - Linear 3 of 9 Bar Code
- Interfaces:
  - Contact (ISO/IES 7816)
  - Contactless (ISO/IES 1443)



PIV Electronically Stored Data

Mandatory:

- PIN (used to prove the identity of the cardholder to the card)
- Cardholder Unique Identifier (CHUID)
- PIV Authentication Data (asymmetric key pair and corresponding PKI certificate)
- Two biometric fingerprints

Optional:

- An asymmetric key pair and corresponding certificate for digital signatures
- An asymmetric key pair and corresponding certificate for key management
- Asymmetric or symmetric card authentication keys for supporting additional physical access applications
- Symmetric key(s) associated with the card management system

Card Information Available for “Free Read”

- Federal Agency Smart Card Number (FASC-N)
  - Card-unique number
  - Agency-assigned number for card holder
  - Affiliation Category (Employee, contractor, etc.)
  - Employer identification code
- Card Expiration Date
- Digital Signature
- Optional Information (i.e. Information not required by FISP 201)
  - Data Universal Numbering System Number (DUNS)
  - Optional Global Unique Identifier (GUID)
  - Other Optional Information added at discretion of Issuing Agency

PIV Card Management

FIPS201 specifies:

- PIV Card Issuance
- PIV Card Maintenance
- PIV Card Renewal
- Card re-issuance
- Card PIN reset
- Card termination

Authentication Mechanisms

- Three Identity Authentication Assurance levels
- Authentication using PIV Visual Credentials
- Authentication using the PIV CHUID
- Authentication using PIV Biometric
- Authentication using PIV asymmetric Cryptography (PKI)

Graduated Assurance Levels for Identity Authentication

Authentication for Physical and Logical Access

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism **Physical Access**	Applicable PIV Authentication Mechanism **Logical Access** Local Workstation Environment	Applicable PIV Authentication Mechanism **Logical Access** Remote/Network System Environment
SOME confidence	VIS, CHUID	CHUID	PKI
HIGH confidence	BIO	BIO	PKI
VERY HIGH confidence	BIO-A, PKI	BIO-A, PKI	PKI

Further Guidance

- Supporting Publications
  - SP 800-73 – *Interfaces for Personal Identity Verification* (card interface commands and responses)
  - SP 800-76 – *Biometric Data Specification for Personal Identity Verification*
  - SP 800-78 – *Recommendation for Cryptographic Algorithms and Key Sizes*
- NIST PIV Website (http://csrc.nist.gov/piv-project/)
  - Draft Documents
  - Frequently Asked Questions (FAQs)
  - Comments Received in Original Format
- Forthcoming Planned Guidance
  - OMB Guidance (Policy)
  - FICC Guidance (Implementation)
  - NIST Guidance on Certification and Accreditation