**Outline**

* Architecture Review Diagram
  + Display/Describe the Use Cases:
    - Use Case 001 - PACS
      * Agency personnel uses mobile phone/tablet to authenticate and gain access through a PACS using PIV credential
    - Use Case 002A - APPS&SYS
      * Agency personnel uses mobile phone/tablet to access workstation and for federated single sign-on (SSO) for web applications using PIV credential
    - Use Case 002B - APPS&SYS
      * Agency personnel uses mobile phone/tablet to access workstation and for federated single sign-on (SSO) for web applications using FIDO2 credential
    - Use Case 003 - TEMP
      * Agency personnel use mobile phone/tablet to access a workstation and for federated single sign-on (SSO) for web applications using PIV-I credential
    - Use Case 004 - PACSTEMP
      * Agency personnel use mobile phone/tablet to authenticate and gain access through a PACS using PIV-I credential
    - Use Case 005 - PROV
      * Issuer provisions PIV and FIDO2 credentials to the PIV wallet on the mobile phone/tablet
* What specific tools or suite of tools are being used in the POC?
  + NOTE: Vendors must be specific in identification. Many have an umbrella suite of tools or tools with various modules. Vendors need to be explicit in what tools in the suite or modules are being used as applicable.
* Solution Prerequisites:
  + PACS hardware, devices, and configuration align to the APL on idmanagement.gov and can read required credentials on the mobile phone/tablet
  + Workstation that is PKI and/or FIDO2 enabled
  + Application suite that is PKI and/or FIDO2 enabled
  + Phones / Tablets that can install the mobile wallet and maintain PIV and FIDO2 credentials.
* NIST 800-63-3 Alignment
  + Describe how solutions align to NIST 800-63-3
* Differencing Feature(s) (i.e., What distinguishes you from other, anticipated solutions?)
* Licensing
  + Licensing or Cost Model (i.e., user, subscription, device, transaction, hybrid, etc.)
* Current Customers
  + Government
* **Demo**
* *Scenario 1 - PACS*
  + User walks up to the PACS turnstile and holds the mobile phone/tablet up to the PACS reader. The reader validates the PIV PKI certificate on the phone and validates the credential is authorized for access. Access is granted.
* *Scenario 2 - PACSTEMP*
  + User walks up to the PACS turnstile and holds the mobile phone/tablet up to the PACS reader. The reader validates the PIV-I PKI certificate on the phone and validates the credential is authorized for access. Access is granted.
* *Scenario 3 - APP*
  + User attempts to access a workstation or web application. Workstation or web application allows for multi credentials for authentication and presents the user with a choice of credentials inside the user's digital wallet on their mobile phone/tablet. The workstation or web application validates the user's PIV PKI certificate on the phone/tablet. The workstation and/or web application successfully validates the certificate, user is granted access.
* *Scenario 4 - APPTEMP*
  + User attempts to access a workstation or web application. Workstation or web application allows for multi credentials for authentication and presents the user with a choice of credentials inside the user's digital wallet on their mobile phone/tablet. The workstation or web application validates the user's PIV-I PKI certificate on the phone/tablet. The workstation and/or web application successfully validates the certificate, user is granted access.
* *Scenario 5 - APPFIDO*
  + User attempts to access a workstation or web application. Workstation or web application allows for multi credentials for authentication and presents the user with a choice of credentials inside the user's digital wallet on their mobile phone/tablet. The workstation or web application validates the FIDO2 credentials on the phone/tablet. Once the workstation or web application successfully validates the credential, user is granted access.
* *Scenario 6 - PROV*
  + Issuer receives notification that a user with a PIV account was issued a mobile phone and/or tablet. Issuer also receives notification of what credentials to provision to the mobile phone and/or tablet. Issuer provisions the requested derived/alternate credentials to the PIV wallet on the mobile phone and/or tablet. User's PIV account is updated with information regarding derived/alternate credentials. Depending upon the offered solution, a credential “wallet” may be required first. PIV, PIV-I, and FIDO2 credentials are then loaded onto the phone/tablet, in various configurations. These configurations include single credentials, or a combination of PIV/PIV-I and FIDO2.