Prescription **M**onitoring **I**nformation e**X**change

Advancing PDMP Data Sharing Through Standardization and Innovation

Proposed Security Standard Review
November 27, 2017

History & Overview

- Original PMIX Architecture
  - SOAP vs Rest
- Security Standards Subcommittee
- Assistance from the Office of Justice Programs
- Overview of the Standard
  - National Institute of Standards and Technology
  - Federal Information Processing Standard
  - Process for using NIST 800-171 r1

Explaining NIST 800-171

- Hazem Eldakdoky, Director of Information Security and Chief Information Security Officer, Department of Justice, Office of Justice Programs
- Jaime Noble, Deputy Director for IT Security & Deputy Chief Information Security Officer, Department of Justice, Office of Justice Programs

NIST 800-171

- The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components.
- The specific requirements for safeguarding CUI in nonfederal information systems and organizations are derived from the above authoritative federal standards and guidelines to maintain a consistent level of protection.
- Some of the FISMA-related requirements expressed in the NIST standards and guidelines are uniquely federal, the requirements in this publication have been *tailored* for nonfederal entities.

NIST 800-171

- *Controlled Unclassified Information* is any information that law, regulation, or government wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, *Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

Security Requirements

SECURITY REQUIREMENT FAMILIES	
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

Security Requirements

- Security controls drawn from NIST Special Publication 800-53 associated with the basic and derived requirements.
- Organizations can use Special Publication 800-53 to obtain additional, non-prescriptive information related to security requirements (e.g., supplemental guidance related to each of the referenced security controls, mapping tables to ISO/IEC security controls, and a catalog of optional controls that can be used to help specify additional requirements if needed).
- This information can help clarify or interpret the requirements in the context of mission and business requirements, operational environments, or assessments of risk.

How will it work?

- Compliance
  - Certifying compliance by a state
  - Compliance for hubs/intermediaries
  - Plans of Action
  - Waivers
  - Does not supersede or amend any requirements imposed by the laws, rules, or policies of an individual state or federal government

Benefits of the Security Standard

- Based on Nationally Recognized Standards
- Provides a baseline for security across multiple organizations
- Demonstrates due diligence
- Flexibility – can be applied to many mechanisms
- Certified Trusted Partners
  - Other States
  - Hub Partners