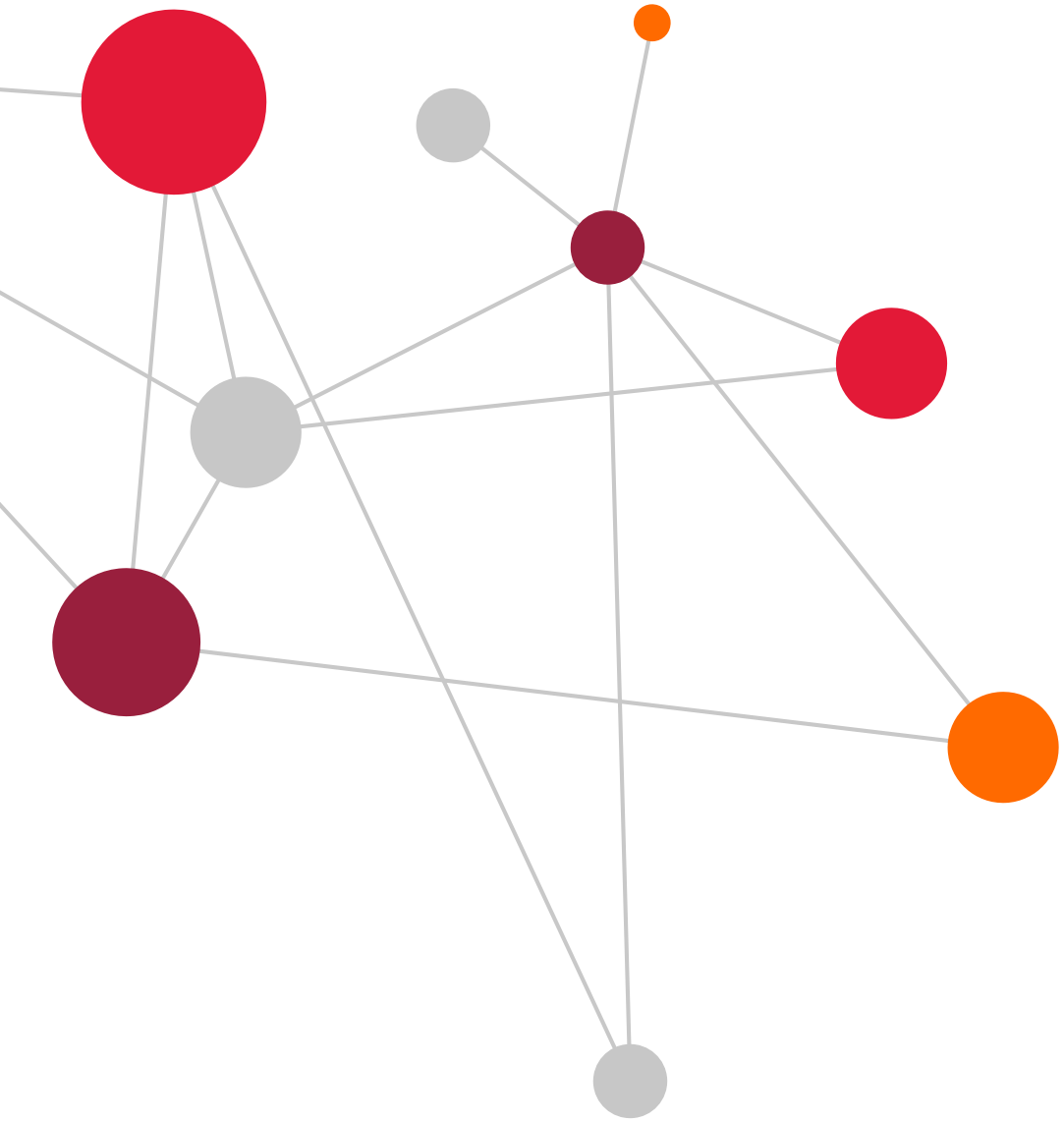


CGI

Experience the commitment®

Towards the desired state – One step at a time

Improving security posture and getting closer to the IAM desired state using SailPoint

December 2019

CDM Goals

Department of Homeland Cyber Security Mission:

- Improve the security posture of the entire civilian .gov network
- Identify and prioritize cybersecurity risk on a continuous basis while enabling agency cybersecurity professionals to manage and mitigate risks to government data and networks

Guiding Principles for CDM Practitioners

- **Inspect** the CDM object level data by observing the “actual state” of current data
- **Detect** differences between actual state and desired state data (aka Cybersecurity Posture Gap)
- **Protect** by providing the visibility and/or mechanism to implement an improvement, usually by remediating cybersecurity posture gaps

Asset Management | Identity and Access Management | Network Security Management | Data Protection Management

Desired State and Security Frameworks for IAM

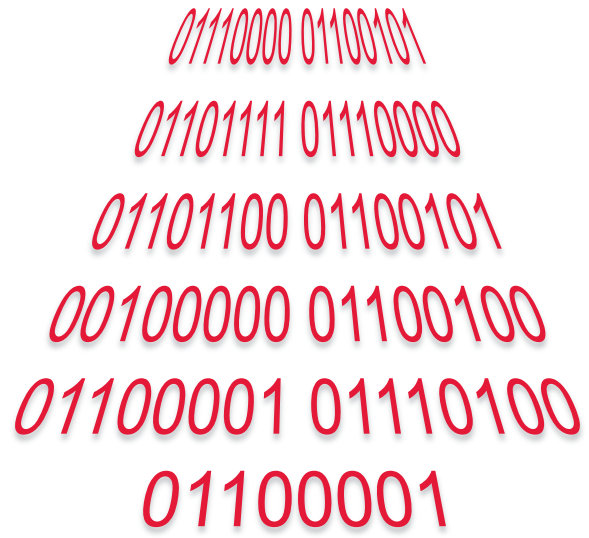
- Desired State is defined, **measured and assessed by Agency Specific processes and procedures**
- Multiple paths to **Risk Reduction and Security Posture improvement**
  - CDM design concepts and principles
    - CDM Actual State data compared with Desired State data
    - CDM Policy Decision Point (PDP) Machine-Readable Policies
  - NIST **Cybersecurity Framework**
  - **NIST SP 800-37** – *Risk Management Framework for Information Systems and Organizations: A **System Life Cycle Approach** for Security and Privacy*
  - **NIST SP 800-53** – *Security and Privacy **Controls for Information Systems** and Organizations*
  - **NIST SP 800-63** – *Digital **Identity Guidelines***
  - Federal Identity, Credential and Access Management (**Federal ICAM**)
  - **OMB M-19-17** – ***Enabling Mission Delivery** through Improved Identity, Credential, and Access Management*
  - Agency requirements
  - And more!

Federal standards and guidelines for IAM help to inform Agency Policies. CDM can help Agencies achieve their IAM Policy goals.

FISMA | FIPS | OMB | NIST SP | BOD | NISTIR | Laws | Mandates | Standards | Policy

CDM Data Interrogation

- Desired State is defined in “Machine Readable Policies” (MRP)
- Data **interrogation actions analyze the data** to determine desired state variants (cybersecurity posture gaps) and present the results in dashboards (SailPoint and Agency CDM Dashboard)
- The dashboard normalizes the gap data and provides metrics determined by the “Data Interrogation Actions and Interrogation Specifications” as defined
- The interrogation and the resulting metrics provides ***visibility*** into risk and ability to support:
  - CDM Program requirements
  - Common Federal report metrics (e.g., FISMA metrics)
  - Compliance with NIST guidance and standards (e.g., Special Publications and FIPS documents)
  - Object level data for Agency operationalization



So what about risk mitigation or cybersecurity posture gap closure?

SailPoint IdentityIQ Policy Administration

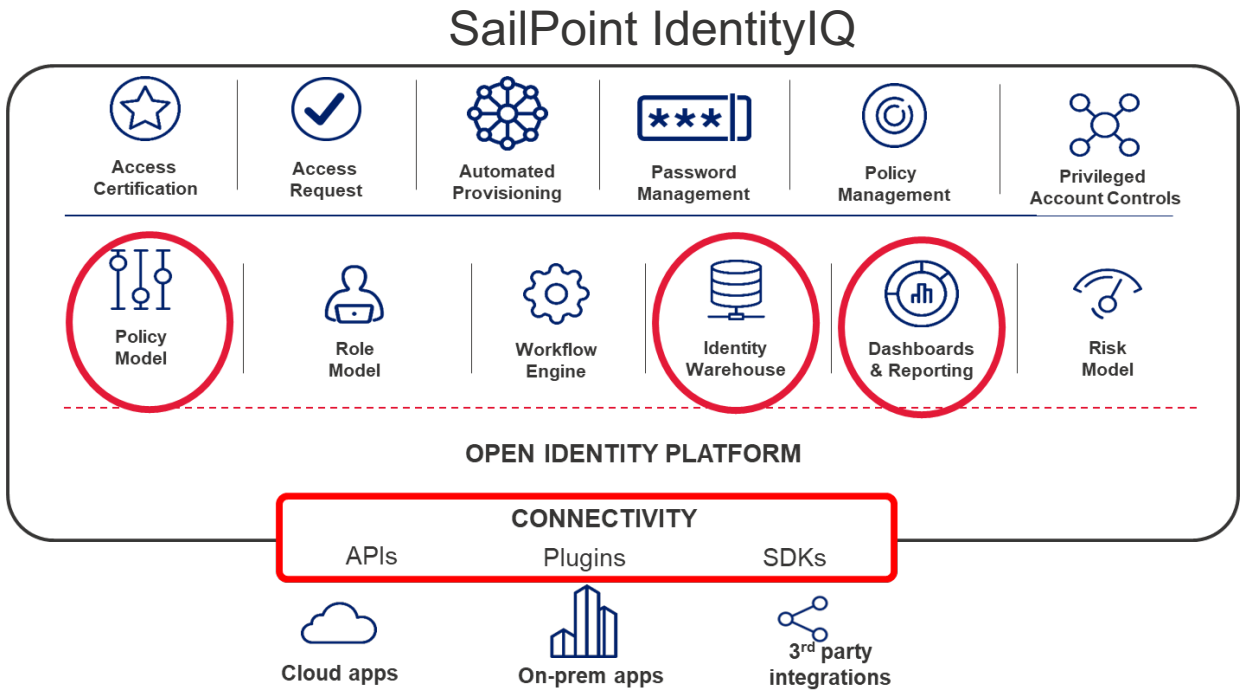
- IdentityIQ policies define the access **business policies of your Agency**
- Policies are defined specifically using MUR data and beyond
  - Identity Attributes
  - Privileged Access to systems and applications
  - Entitlements and Roles
- Detective and preventative
- Part of the Unified governance framework of **IdentityIQ Compliance Manager**
- Responsibility assigned to business owners, supervisors and CORs
- Visibility and granular control on variants

- **Entitlement SOD**
- **Role SOD**
- **Application**
- **Account-based**
- **Activity policies**
- **Risk-based policies**
- **Advanced policies**

Proactively detect and prevent inappropriate access and violations in real-time with point-and-click interfaces

Detect cybersecurity posture gaps

- **Detect** (Leverage Policies and Reports)
  - Define Policies and scan for policy violations
  - **Live reports** in SailPoint based on MUR attributes and violations detected
  - **Business-friendly reports** and analytics tools
  - Report on privileged and application access

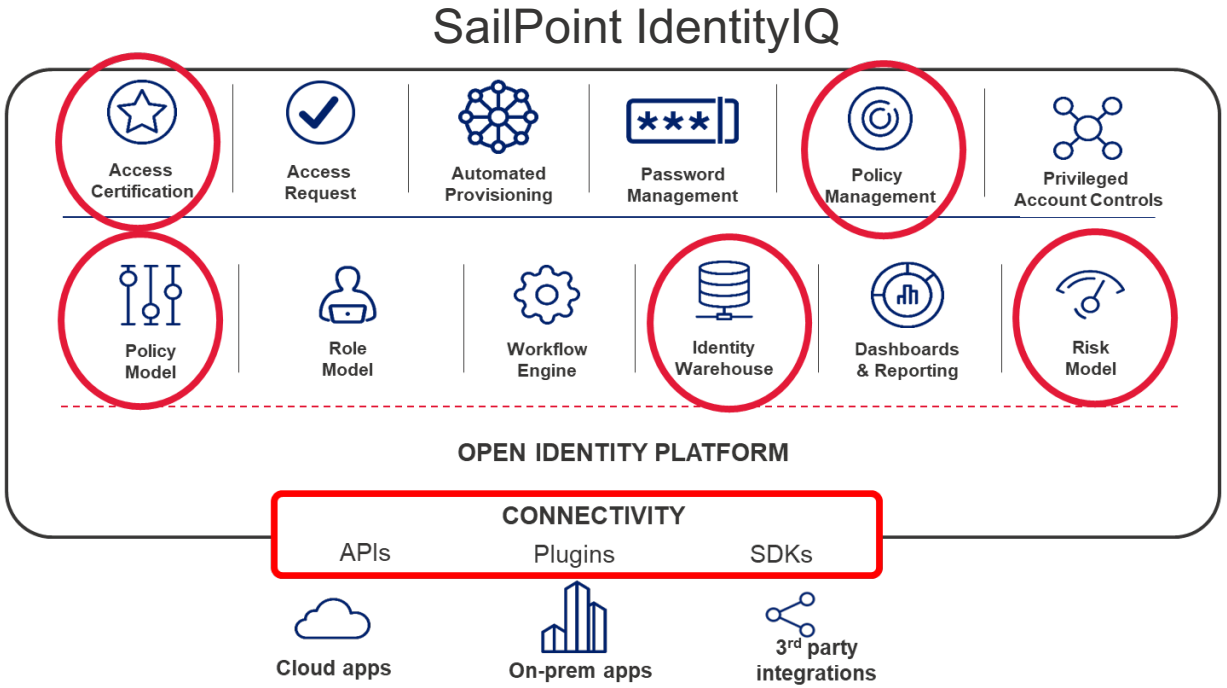


Added Benefit: Support FISMA and other compliance reporting needs and risk scoring

Remediate cybersecurity posture gaps

Remediate (Leverage Polices and Access Certification)

- Notify IT, supervisors or data stewards for **corrective action**
- Assign the policy violations to supervisors/CORs/data stewards
- Decision to revoke the access or to accept the risk based on **compensatory controls**
- Periodic access certifications to include Policy violations
  - On demand
  - Scheduled
  - Risk/event based

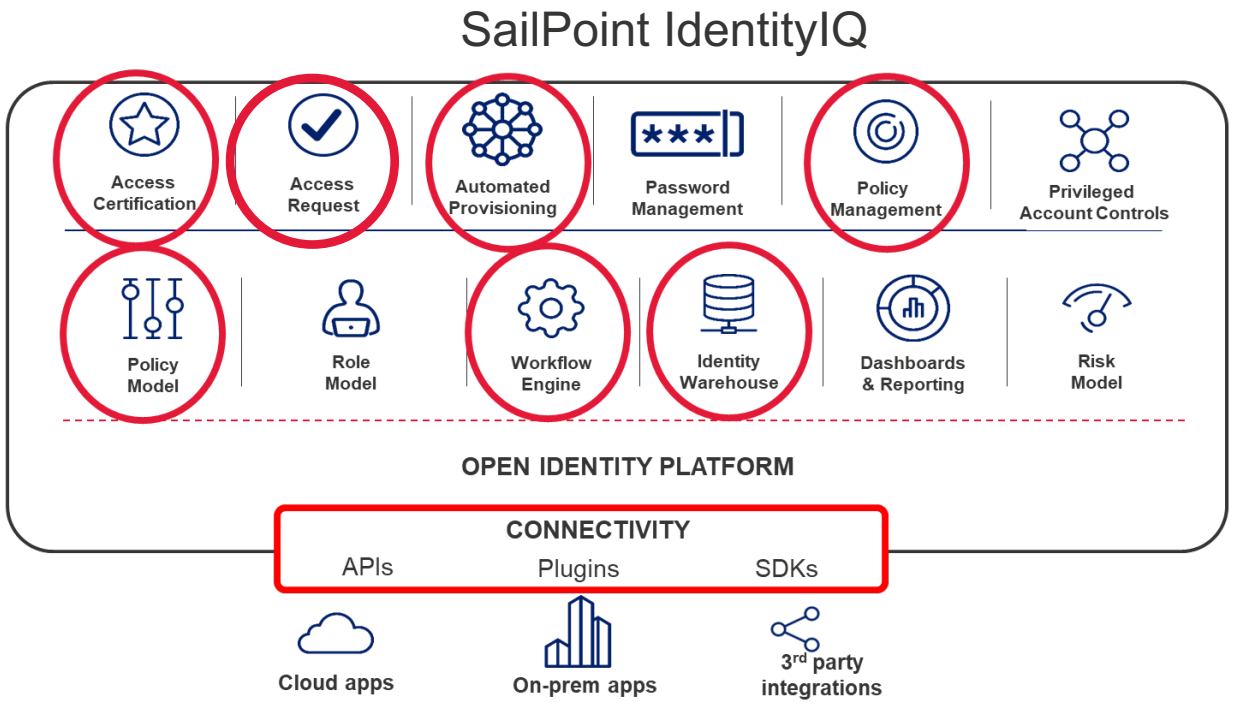


Added Benefit: Accurate, automated certifications, complete MUR data and exception management

Prevent cybersecurity posture gaps

Prevent (Leverage LCM)

- **Automatically disable user accounts** or revoke access when violations are detected or certified
- **Proactively prevent** inappropriate access and violations
- Lifecycle events and workflows to disable/revoke access
- Enforce a closed-loop provisioning process



Added Benefit: Accurate and automated remediation actions and access request management

CDM Identity and Access Management Desired State

- **TRUST**
  - All active users have an authorized trust level
  - Only users with appropriate security clearances have appropriate access

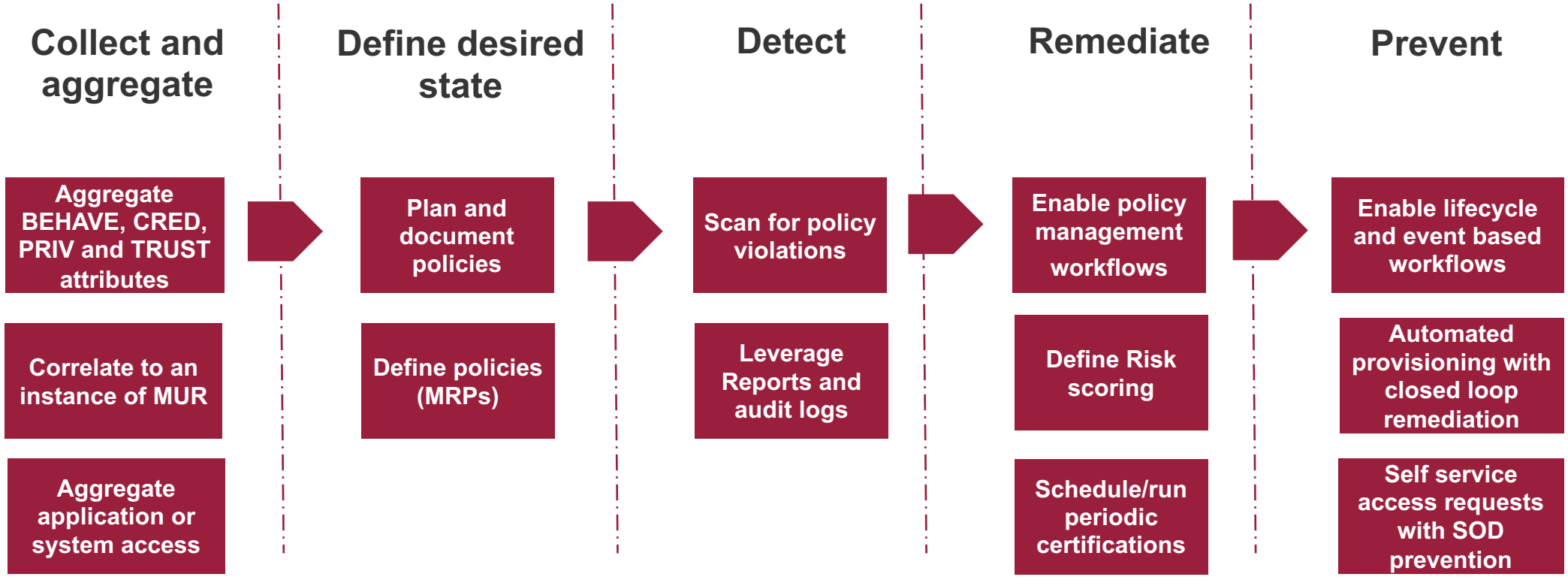
- **CRED**
  - Only authorized users are issued the authorized credentials of the correct type to access facilities, information, and networks.
  - All authorized users have their credentials reissued or reset on a periodic basis.
  - All credential types have appropriate expiration, reissuance, and revocation policies.

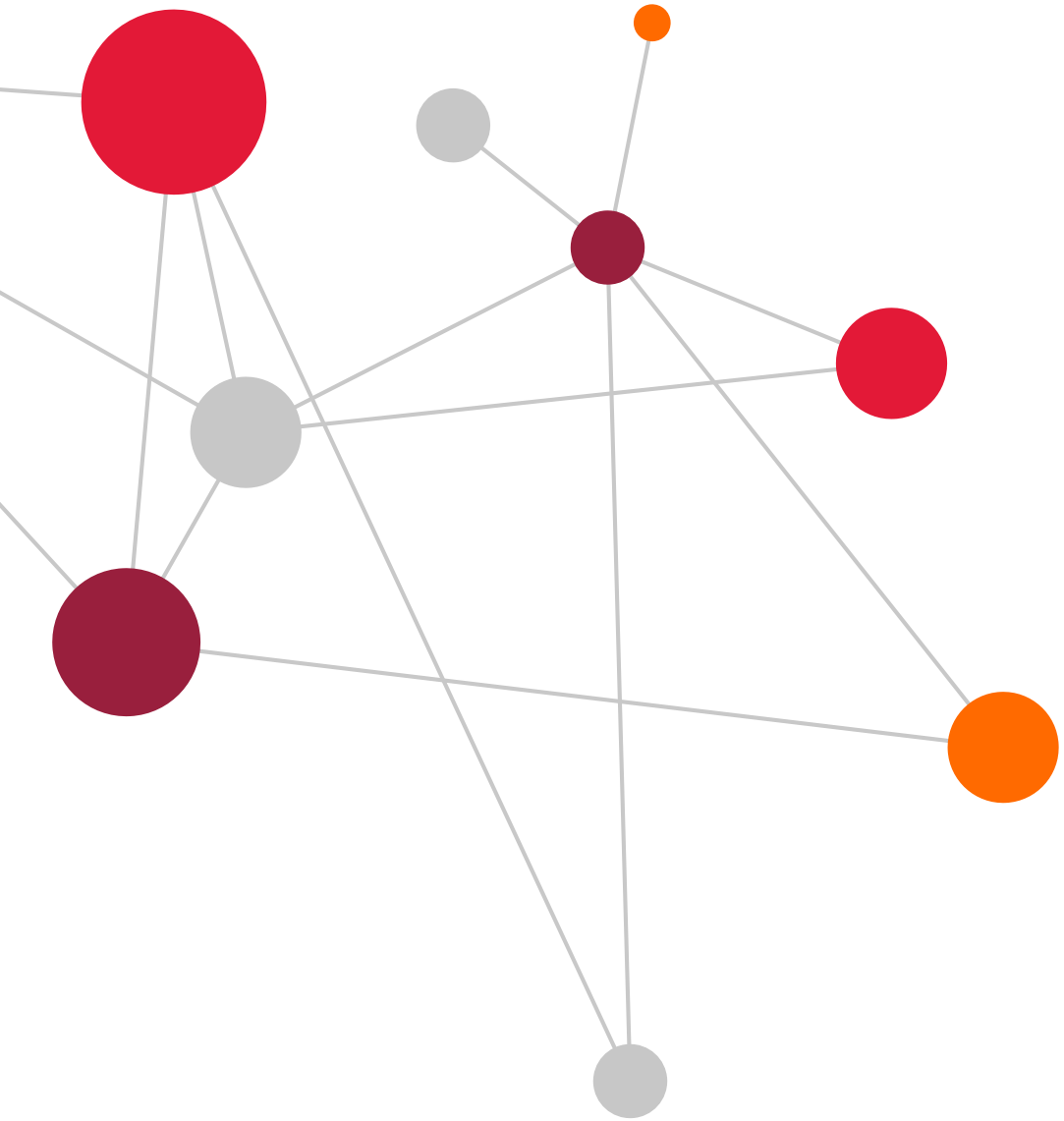
CDM Identity and Access Management Desired State

- **PRIV**
  - Only authorized users with authorized accounts of the correct type are accessing systems
  - All employees have only the privileges necessary to do their jobs
  - All accounts are in compliance with the agencies SOD policies
  - All authorized users have their accounts and accesses reauthorized on a periodic basis
  - All account types employ appropriate expiration and disable policies

- **BEHAVE**
  - All employees have completed Cyber Security Awareness Training.
  - All authorized users have completed Role-based Security Training.

One Step at a Time





CGI

Experience the commitment®

Questions?