

# *Continuous Diagnostics and Mitigation* **Webinar Series**

**Getting Ready for  
Phase 2 CDM Security  
Capabilities: TRUST,  
BEHAVE, CRED, and  
PRIV**



**Homeland  
Security**

# Introduction

- Overview of CDM and Key Concepts
- How the Security Capabilities Work Together
- Role of FICAM
- Phase 2 Security Capabilities
  - TRUST
  - BEHAVE
  - CRED
  - PRIV



# CDM PMO Program Managers

*No discussion or questions regarding CDM acquisition or procurement activities – this is strictly a CDM learning community activity. For agency-specific queries, contact:*

- **Group A – DHS**
  - Betsy Proch ([betsy.proch@hq.dhs.gov](mailto:betsy.proch@hq.dhs.gov))
- **Group B – DOE, DOI, DOT, USDA, VA, OPM**
  - Derrick Williams ([derrick.Williams@hq.dhs.gov](mailto:derrick.Williams@hq.dhs.gov))
- **Group C – DOC, DOJ, DOL, State, USAID**
  - Paul Loeffler ([paul.loeffler@hq.dhs.gov](mailto:paul.loeffler@hq.dhs.gov))
- **Group D – GSA, HHS, NASA, SSA, Treasury, USPS**
  - Odell Blocker ([odell.blocker@hq.dhs.gov](mailto:odell.blocker@hq.dhs.gov))
- **Group E – Educ, EPA, HUD, NRC, NSF, SBA**
  - Matt Hartman ([matthew.Hartman@hq.dhs.gov](mailto:matthew.Hartman@hq.dhs.gov))
- **Group F – Non-Chief Financial Officer (CFO) Act Agencies**
  - Geri Clawson ([geraldine.clawson@hq.dhs.gov](mailto:geraldine.clawson@hq.dhs.gov))
- **Unsure?**
  - [CDM.FNR@hq.dhs.gov](mailto:CDM.FNR@hq.dhs.gov)



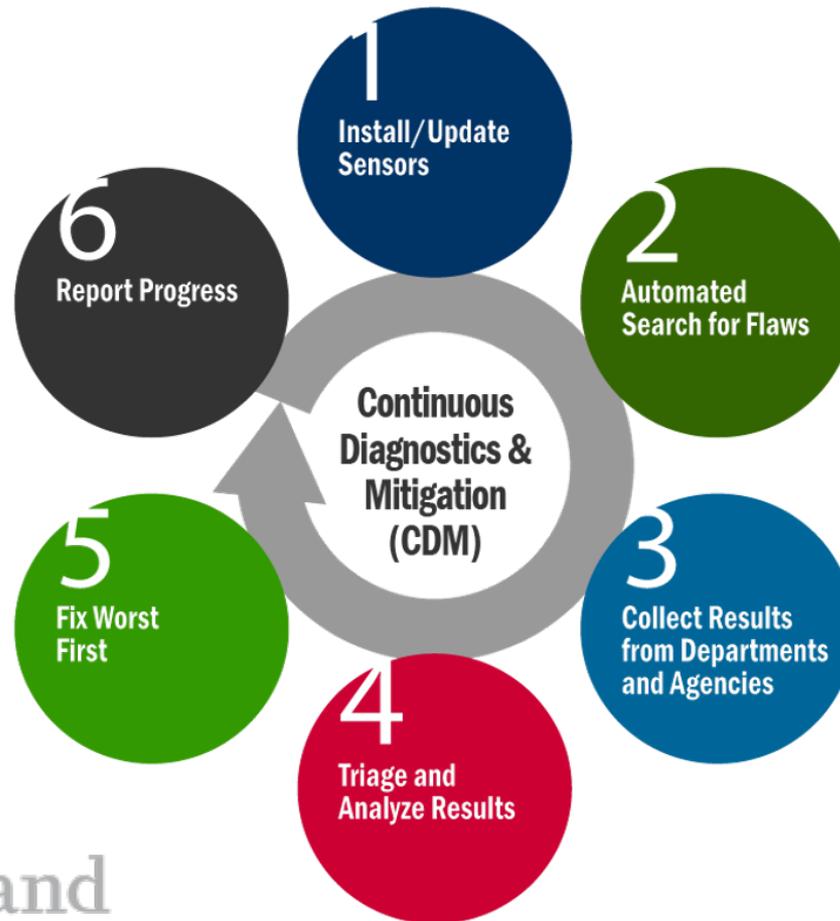
Homeland  
Security

# What is the CDM Program?

- Establish consistent, government-wide set of information security continuous monitoring tools to help protect .gov networks.
- Leverage the buying power of government organizations to achieve savings for cybersecurity tools and services.
- Provide dashboards to improve situational awareness, enhance agencies' ability to identify, and respond to risk of emerging cyber threats on the agency and government-wide level.
- Support risk-based decision making for resource allocation (best bang for the buck).



# How does it Work?

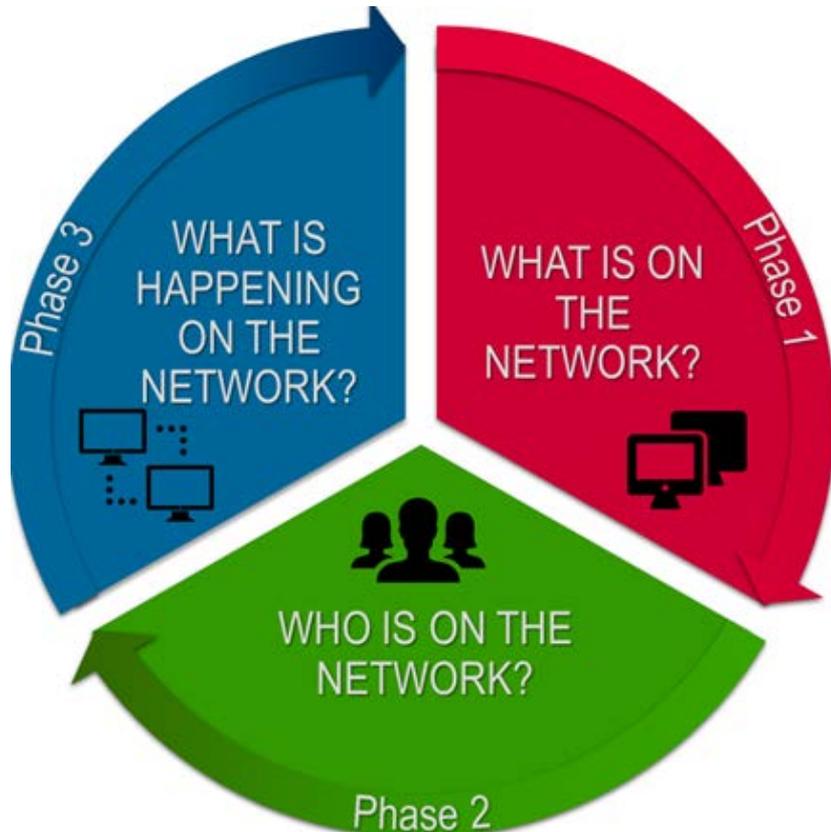


Homeland  
Security

# Who is Involved?

- **Departments and Agencies**
- **Department of Homeland Security**
- **Office of Management and Budget**
- **General Services Administration**
- **Federal CIO Council and ISIMC**
- **CMaaS Providers/ Commercial System Integrators**
- **Federal Level Working Groups**
  - PACS

# Implementation Phases of CDM



What is on the Network?

Who is on the Network?

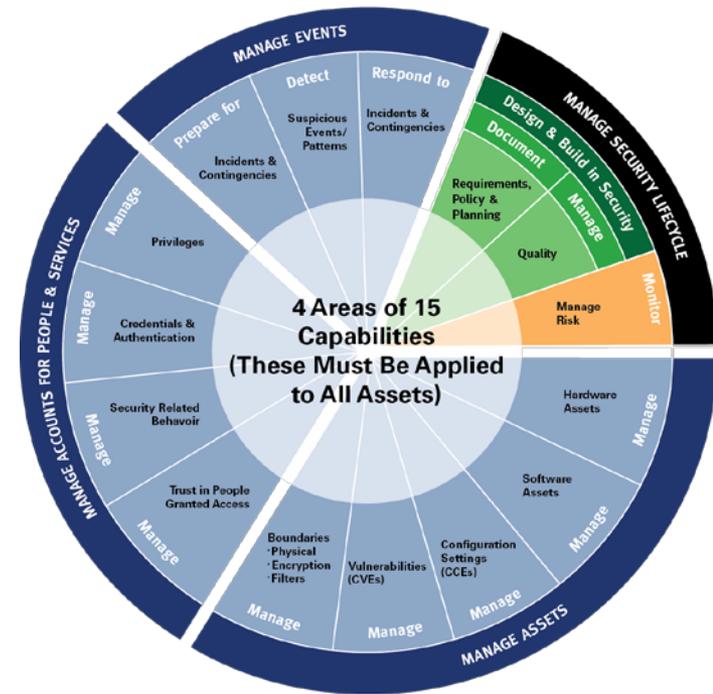
What is Happening on the Network?



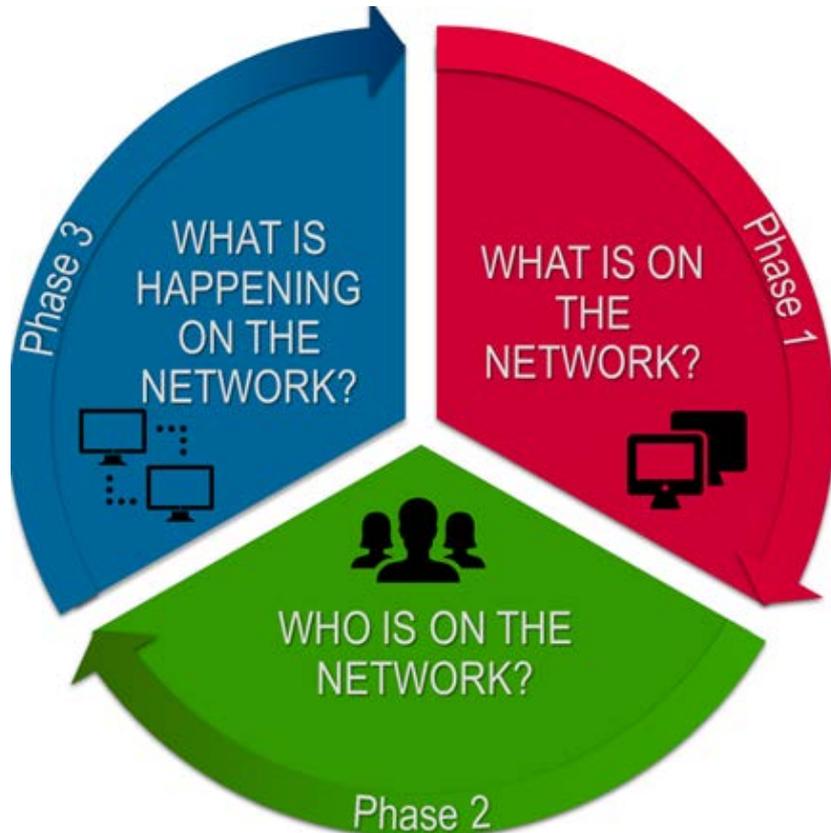
Homeland Security

# Key CDM Concepts

- Security Capabilities
- Actual State
- Desired State
- Defect and Defect Check
- Objects and Attributes
- Data Format
- Dashboard
- Master User Record
- Master Device Record



# Focus on Phase 2 Security Capabilities



Who is on the Network?

TRUST  
BEHAVE  
CRED  
PRIV

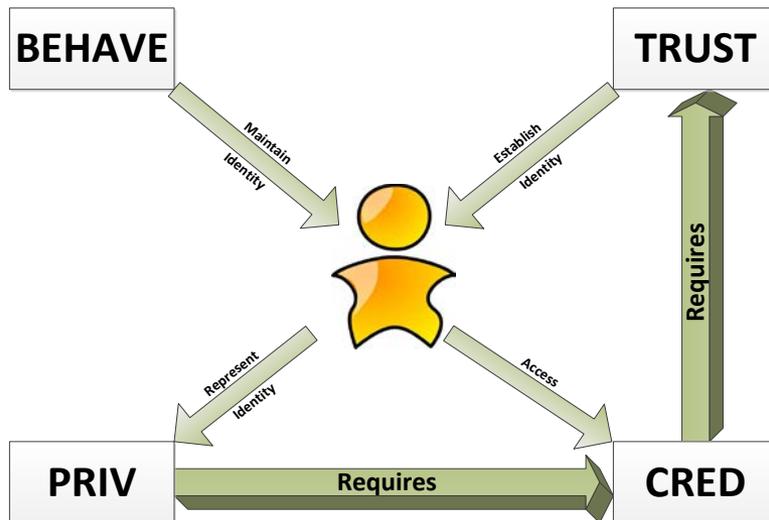


Homeland  
Security

# Focus on Phase 2

## Security Capabilities

Trust, Behave, Cred and Priv  
Linkage to the User



USER is a generic term that applies to any entity (including non-person entities) that access any resource, physical or logical, in an organization.

TRUST is used to validate a person's identity and the degree to which they have been vetted.

CRED binds a type of credential or authentication mechanism to an identity established in TRUST with a level of assurance and is used to grant access (physical and logical).

PRIV establishes the privileges associated with the credential and in turn the individual or service.

BEHAVE identifies that the individual has the proper knowledge and training for the roles they are assigned and that they remain up to date.



Homeland  
Security

# TRUST Security Capability



WHO IS ON THE  
NETWORK?

Phase 2

**Trust**

*Behave*

*Credentials*

*Privileges*



Homeland  
Security

# TRUST Security Capability

## TRUST



The TRUST CDM security capability provides the D/A visibility into the risk associated with the vetting of users.



Homeland  
Security

# What is the Risk?

- The agency employed mechanisms for user screening/indoctrination before granting access to sensitive data are not monitored on a regular basis nor with efficiency.
- “Key trust level attributes” are not validated and available to systems and processes that monitor/enforce access.



# How the TRUST Security Capability Helps

Verifies the existence of TRUST artifacts.

TRUST Artifacts	TRUST Security Capability
Security Clearance Determination	Validates existence and currency per policy
Suitability Determination	
Fitness Determination	



# TRUST Planning Actions

1. Identify the stakeholders for personnel security systems.
2. Determine availability of data and policy in machine readable format (able to store in database).
3. Establish or update policies regarding how long a given trust level is valid before it expires and formal re-vetting of the user is required.
4. Define what the re-vetting and re-indoctrination policies/processes are for each trust level.



# BEHAVE Security Capability



*Trust*  
***Behave***  
*Credentials*  
*Privileges*



Homeland  
Security

# BEHAVE Security Capability

## BEHAVE



The BEHAVE CDM security capability provides the D/A insight into risks associated with non-compliance of IT related training and role requirements.



# What is the Risk?

- Users are granted access to facilities, systems, resources, information (sensitive data) without:
  - Current policy
  - Appropriate security training
  - Demonstrated skill specialty
  - Knowledge
  - Certification
  - Completing proper security-related documentation or training
  - Signed agreements



# What is the Risk?

Poorly trained users can engage in behaviors that compromise systems, expose sensitive data, or subvert security policies meant to mitigate risk.

- Examples
  - Ineffective training
  - Users have not been assigned the proper training for the access



# How the BEHAVE Security Capability Helps

Verifies the existence of BEHAVE artifacts.

User Behavior	BEHAVE Security Capability
Complete awareness training at least annually	Validates Existence and Currency per Policy
Complete role-based training as required	
Read and accept rules of behavior or other types of system agreements	
If testing is utilized, set a passing score, such as meeting an 80% level for passing	



# BEHAVE Planning Actions

1. Identify stakeholders for BEHAVE artifacts.
2. Determine whether BEHAVE artifacts are in “data format” – if not, how to get in data format.
3. Review or establish policies about mandatory training attributes, such as:
  - How long the training is valid
  - Grace period for not completing training
  - Refresher training requirements
  - Testing requirements



# CRED Security Capability



WHO IS ON THE  
NETWORK?

Phase 2

*Trust*

*Behave*

**Credentials**

*Privileges*



Homeland  
Security

# CRED Security Capability

## CRED



The CRED CDM security capability provides the D/A insight into risks associated with weaknesses in its management of credentials and the mechanisms used to authenticate users to facilities and systems.



# What is the Risk?

- Authentication, reissuance, and revocation activities are not in compliance with policy and introduce risks.
- Users are not authenticated appropriately for access to facilities, systems, and information.
- Authentication, reissuance, and revocation policies are incurring more risk than deemed acceptable by the agency.



# How the CRED Security Capability Helps

Verifies the existence of CRED artifacts.

CRED Artifacts	Cred Security Capability
USER attributes identifying a credential being Issued to each user	Validates Existence and Currency per Policy
USER attributes identifying date and state of issuance, revocation, reissuance, or suspension	
Credential (account) attributes identifying the associated user(s) and authentication mechanisms	
Credential attributes for usage, complexity, duration, and grace period	
Credential attributes for revocation	



# How the CRED Security Capability Helps

Verifies the existence of CRED artifacts.

CRED Artifacts	Cred Security Capability
Authentication mechanism for every account	Validates Existence and Currency per Policy
Default accounts/passwords enabled	



# CRED Planning Actions

1. Review or establish policies for the following:
  - How long a given credential type is valid before it expires
  - Reissuance, revocation, or suspension for each credential type
  - Credential requirement policies for systems, facilities, and services
  - Credential quality
  - Non Person Entity credentials and policy compliance



# CRED Planning Actions

2. Determine if the following user account attributes are in data format on the system:
  - Account identifier
  - System or applications that account is allowed to access
  - Authorized user and authorization status
  - Date first authorized, date last authorized
  - Date revoked, suspended



# PRIV Security Capability



WHO IS ON THE  
NETWORK?

Phase 2

*Trust*  
*Behave*  
*Credentials*  
**Privileges**



Homeland  
Security

# PRIV Security Capability

## PRIV



The PRIV CDM security capability provides the D/A insight into risks associated with the privilege(s) granted to a credential(s) issued to user(s) of facilities systems and services.



# What is the Risk?

- Credentials that are no longer needed to perform a function are NOT disabled or deleted.
- Privileges accumulated over time or through role changes are not removed.
- Credentials have excess access.
- Credentials have excess privileges.



# How the PRIV Security Capability Helps

Verifies the existence of PRIV artifacts.

PRIV Artifacts	PRIV Security Capability
Physical access authorizations issued to each credential	Validates Existence and Currency per Policy
Credential restrictions implemented	
Privileges enabled for each credential	



# PRIV Planning Actions

1. Review or establish policies for the following:
  - Separation of duties
  - How long a given authorization and credential type are valid before they expire
  - Applicable reauthorization
  - Credential restrictions, such as time of day, duration, etc.
  - Locking credentials
  - Disabling credentials
  - Physical access

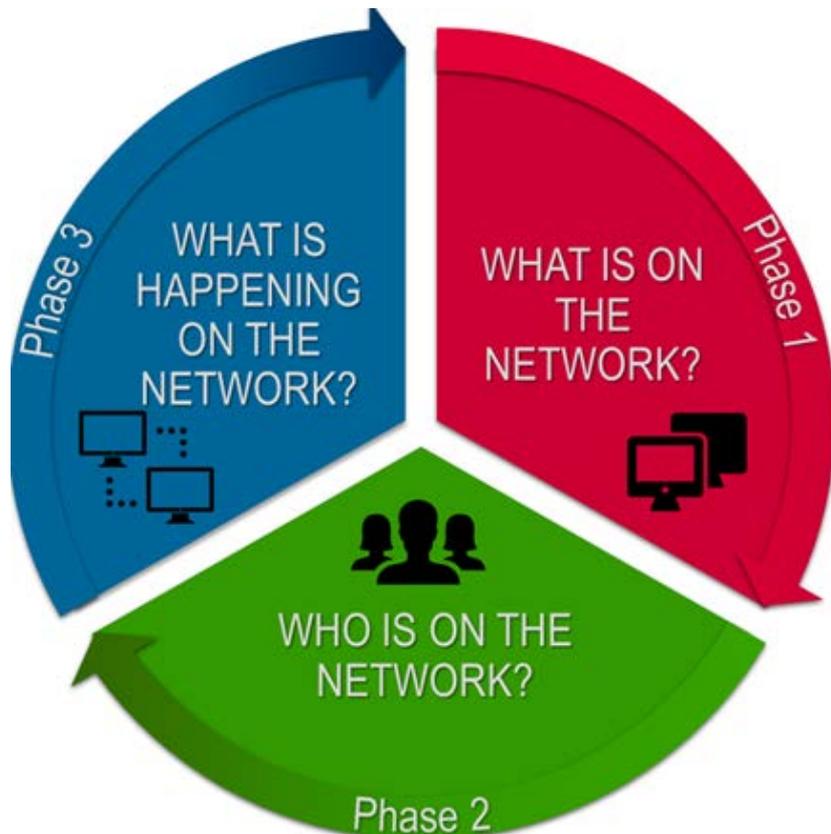


# PRIV Planning Actions

2. Identify where existing attributes are in data format for the following:
  - Separation of duties
  - Account authorization and type validation
  - Account restrictions, such as time of day, duration, etc.
  - Locking accounts
  - Disabling accounts
  - Physical access



# How the Phase 2 Security Capabilities Work Together



Who is on the Network?

Trust

Behave

Credentials

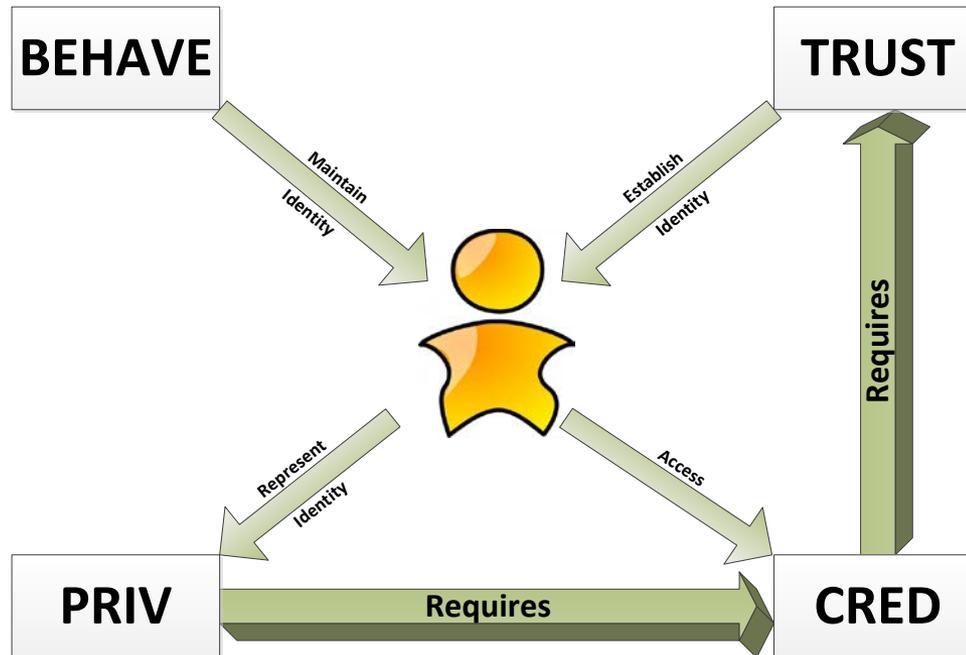
Privileges



Homeland  
Security

# How the Phase 2 Security Capabilities Work Together

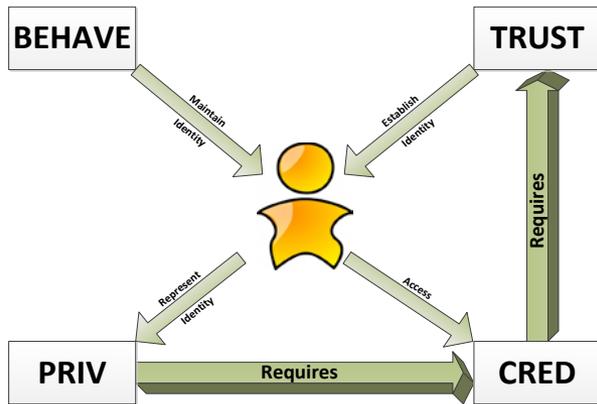
Trust, Behave, Cred and Priv  
Linkage to the User



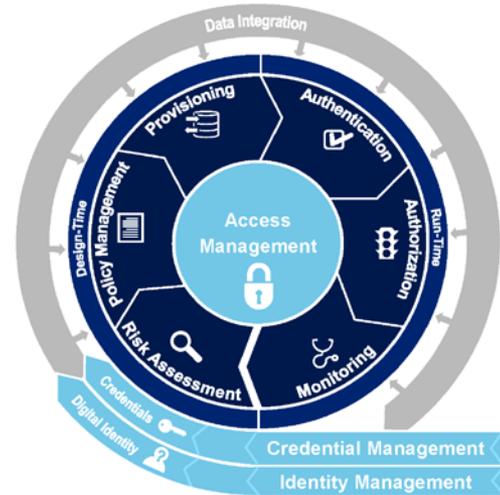
Homeland  
Security

# Role of FICAM

Trust, Behave, Cred and Priv  
Linkage to the User



Identity, Credential, and Access Management



- Identity Management**  
The processes for establishing and maintaining the identity data of an individual.
- Credential Management**  
The processes for managing objects that authoritatively bind an identity to a token.
- Access Management**  
The processes and technologies used to govern and automate access.
- Risk Assessment**  
Evaluate potential threats to establish security mechanisms and policy for a resource.
- Authorization**  
Run-time decision if a thing is granted access.
- Policy Management**  
The processes for determining and maintaining access rules to digitally protect resources.
- Monitoring**  
Dynamically checking and evaluating the efficacy of access controls and conducting remediation activities.
- Provisioning**  
Management of accounts and privileges for access to applications and facilities.
- Digital Identity**  
The bits that make a person or thing unique.
- Authentication**  
Run-time validation of a credential and digital identity.
- Credentials**  
An object that digitally or physically represents a person or thing.



Homeland Security

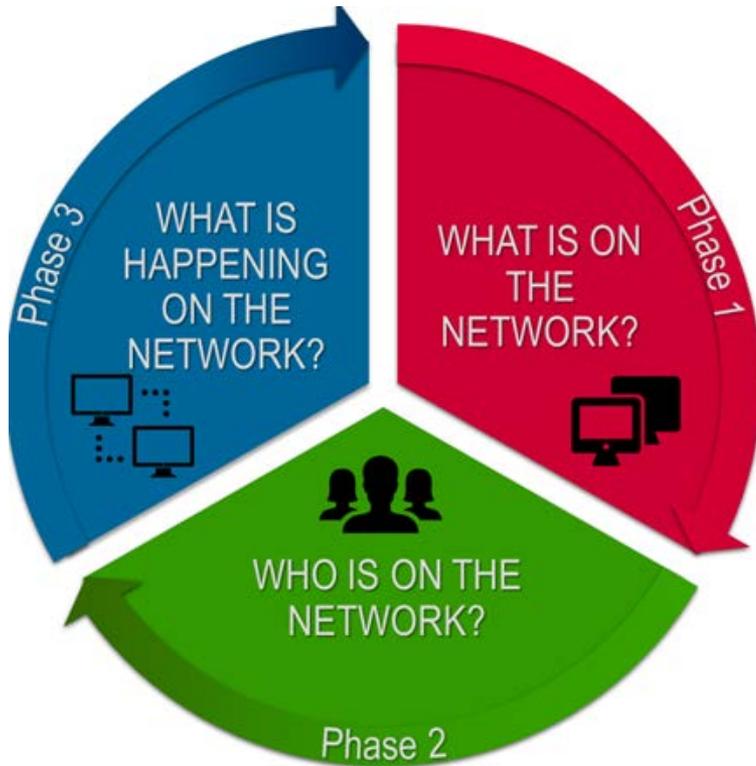
# FICAM

- Provides architecture and implementation guidance to address concerns related to:
  - Identity
  - Credential
  - Access Management



Homeland  
Security

# Summary



**Who is on the Network?**

**Trust**

**Behave**

**Credentials**

**Privileges**



Homeland  
Security

# Additional Resources

## GSA Site

- <http://www.gsa.gov/cdm>

## US-Cert Site

- <http://www.us-cert.gov/cdm>

## Additional Upcoming Activities

- January 21, 2016
  - CDM Learning Community Event  
CDM: Awakening the Force of Automated Assessments  
Time: 1:00 pm – 3:00 pm  
Location: Arlington, VA  
Registration Information - <https://www.us-cert.gov/cdm/training>



Homeland  
Security

# CDM PMO Program Managers

*No discussion or questions regarding CDM acquisition or procurement activities – this is strictly a CDM learning community activity. For agency-specific queries, contact:*

- **Group A – DHS**
  - Betsy Proch ([betsy.proch@hq.dhs.gov](mailto:betsy.proch@hq.dhs.gov))
- **Group B – DOE, DOI, DOT, USDA, VA, OPM**
  - Derrick Williams ([derrick.Williams@hq.dhs.gov](mailto:derrick.Williams@hq.dhs.gov))
- **Group C – DOC, DOJ, DOL, State, USAID**
  - Paul Loeffler ([paul.loeffler@hq.dhs.gov](mailto:paul.loeffler@hq.dhs.gov))
- **Group D – GSA, HHS, NASA, SSA, Treasury, USPS**
  - Odell Blocker ([odell.blocker@hq.dhs.gov](mailto:odell.blocker@hq.dhs.gov))
- **Group E – Educ, EPA, HUD, NRC, NSF, SBA**
  - Matt Hartman ([matthew.Hartman@hq.dhs.gov](mailto:matthew.Hartman@hq.dhs.gov))
- **Group F – Non-Chief Financial Officer (CFO) Act Agencies**
  - Geri Clawson ([geraldine.clawson@hq.dhs.gov](mailto:geraldine.clawson@hq.dhs.gov))
- **Unsure?**
  - [CDM.FNR@hq.dhs.gov](mailto:CDM.FNR@hq.dhs.gov)



Homeland  
Security

# Questions and Answers



Homeland  
Security

# Survey Questions

- Please help us improve these events by answering the 5 survey questions



Homeland  
Security

# CUE/CPE Information

- Thanks for attending today's session!
- A generic Webinar completion certificate can be downloaded from the following site:  
[https://www.us-cert.gov/sites/default/files/cdm\\_files/course\\_certs/Phase2OverviewCourseCompletionCertificate\\_nofitsi.pdf](https://www.us-cert.gov/sites/default/files/cdm_files/course_certs/Phase2OverviewCourseCompletionCertificate_nofitsi.pdf)
- Hold onto the following:
- Completion certificate after filling in your name
- A copy of the email confirmation showing you registered for the Webinar



Homeland  
Security

# Contact Information

*THANK YOU FOR  
ATTENDING OUR WEBINAR.*

Contact: [cdm.fnr@hq.dhs.gov](mailto:cdm.fnr@hq.dhs.gov)



Homeland  
Security