

# The November CDM Webinar

## We will begin at 12:00PM EST

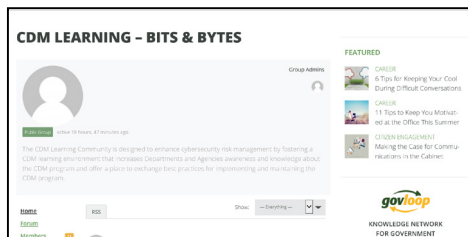
## Welcome to the CDM Webinar: PRIVMGMT: The First Step Toward CDM Phase 2 Capabilities

While you wait, check out:



### Our CDM Homepage

<https://www.us-cert.gov/cdm/training>



### Our CDM Bits and Bytes Blog

<https://www.govloop.com/groups/cdm-learning-bits-bytes/>

*Have a topic suggestion for a future event or blog post? Want to join our membership list? Please reach out to [cdmlearning@hq.dhs.gov](mailto:cdmlearning@hq.dhs.gov)*



Homeland  
Security

Federal Network Resilience

# PRIVMGMT: The First Step Toward CDM Phase 2 Capabilities

November 17, 2016

12:00 – 1:00 PM EST



A CDM Learning Webinar



Homeland Security

Federal Network Resilience

# Welcome Ross Foard, PMP, CISSP, CIAM, ITIL

## Continuous Diagnostics and Mitigation (CDM) Phase 2 Engineer and ICAM SME



Ross re-joined the Department of Homeland Security in 2016 to share his expertise on identity management, strong authentication, PIV card, access management, and account management.



## Today's Topics

- CDM Phase 2 Definition for “Who is on your network?”
- Our Focus Today is  
*PRIVMGMT Overview and Core Concepts*
- Important Agency PRIVMGMT Considerations

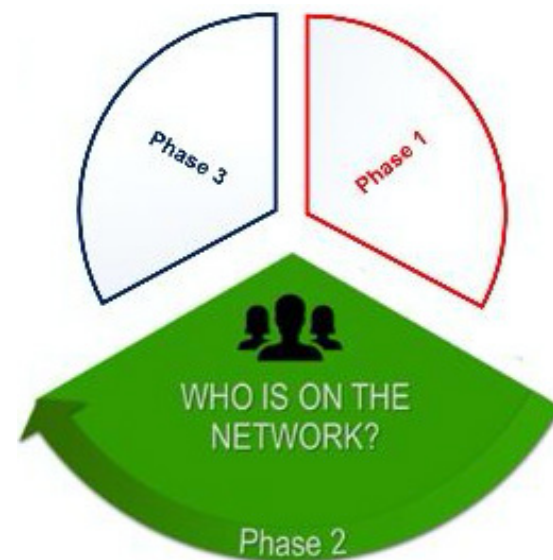


# CDM Phase 2 Tool Functional Areas (TFA)

## Phase 2 – Who is on Your Network

### Four Tool Functional Areas

- TRUST - Were they properly vetted?
- BEHAVE – Have they been trained?
- CRED – Are they using their PIV card for access?
- **PRIV – What Access does a user have [aka privileges]?**



# Key Concepts of the Phase 2 Tool Functional Areas

- Before we talk about the PRIVMGMT Solution, lets discuss the PRIV Tool Functional Area. **All users of IT have some level of privileges.** Additionally, there is a **specific class of users that is viewed as “Privileged”**
- **Master User Record** - Elements of PRIV are contained in a Master User Record (MUR)
- **Policy Decision Point** – Compares the Desired State with the Actual State to determine if they are in alignment
- **Identity and Account Information** – Attributes associated with each user and the accounts the users have been authorized
- **Policy Information** – Policy-based attributes associated with each account type



# What is PRIV (Manage Account Access)

An agency is responsible for managing the privileges of all users with access to agency resources to ensure that employees can fulfill their assigned duties efficiently and securely.

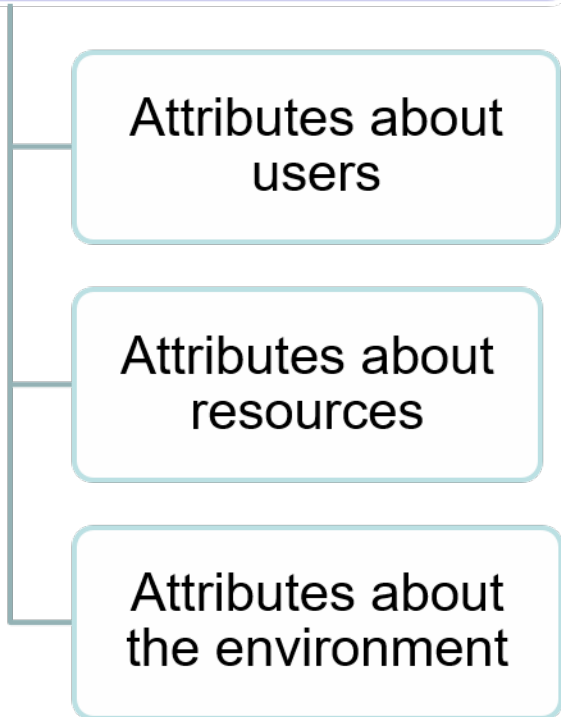
Group 1	Domain Controller (DC) Admins	Full Control	Read	Write	Create All Child Objects	Delete All Child Objects	Add GUID
	Kelly Wilson	X					
	Riley Smith						
Group 2	DC Admin-Read Only						
	Mary Lee		X				
	Robert Sycor		X				
	Allie Harshel		X				



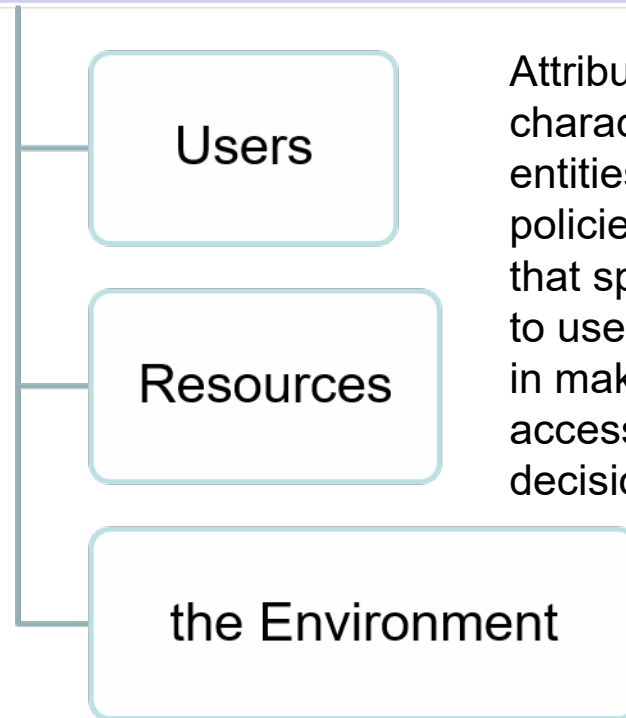
# PRIV = Attribute and Policy Management

Reference: NIST IR 7657

**Attribute Management**  
*Attributes* are distinguishable characteristics of users or resources, conditions defined by an authority, or aspects of the environment.



**Policy Management**  
*Policies* are rules that specify how to use attributes to render an access decision.



Attributes are characteristics of entities, while policies are rules that specify how to use attributes in making an access control decision.





# Levels of Assurance (LOA) 1-4

---

As a reminder, OMB 04-04 (December 2003) known as HSPD-12:

- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Some confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- **Level 4: Very high confidence in the asserted identity's validity.**

...describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity.

...the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the credential was issued.

...the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

**For Highly Privileged Users only LOA-4 is appropriate**

Reference: OMB M-04-04, E-AUTHENTICATION GUIDANCE FOR FEDERAL AGENCIES



# Master User Record (MUR)

The MUR is intended to consolidate a person's comprehensive set of job functions and system roles and his or her associated accesses and privileges in one place.



Sandy has the following access:

- Can create new employees in the HR system.
- Cannot view, create, change configuration settings.
- Can view all employee records in the learning management system; cannot create, change, or delete records.

Sandy is a human resource officer.



Justin has the following access:

- Can view audit logs in the HR system.
- Can view all transactions in the HR system.
- Cannot create, change, or delete records.
- Can view configuration settings, cannot make configuration changes.
- Must have a Secret security clearance.

Justin is the ISSO for the human resource department.



# Our Focus Today:

## Tighten Policies and Practices for Privileged Users



Tony Scott told reporters on July 9, 2015...

agencies have “dramatically increased” two-factor authentication for privileged users and “a number of agencies have hit 100 percent.”

Government-wide, two-factor authentication increased 20 percent during the sprint.

### Cybersecurity Sprint June 2015

To the greatest extent possible, agencies should:

- minimize the number of privileged users,
- limit functions that can be performed when using privileged accounts,
- limit the duration that privileged users can be logged in,
- limit the privileged functions that can be performed using remote access,
- and ensure that privileged user activities are logged and that such logs are reviewed regularly.



# Our Focus Today: Tighten Policies and Practices for Privileged Users

OMB M-16-04

*“All agencies will improve the identity and access management of user accounts on Federal information systems to drastically reduce vulnerabilities and successful intrusions.”*

*Cybersecurity Strategy and Implementation Plan (CSIP for the Federal Civilian Government, October 30, 2015)*



THE DIRECTOR

EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503

October 30, 2015

M-16-04

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan  
Director

Shaun Donovan  
2015.10.30 14:22:10  
-04'00'

Tony Scott  
Federal Chief Information Officer

Anthony Scott  
2015.10.30 14:05:55  
-04'00'

SUBJECT: Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government

*Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government, October 30, 2015*

*“DHS will accelerate the deployment of Continuous Diagnostics and Mitigation (CDM)... capabilities to all participating Federal agencies to enhance detection of cyber vulnerabilities and protection from cyber threats.”*



Homeland  
Security

Federal Network Resilience

## CDM Phase 2 - Responding to the Focus

---

- Situational Awareness from Cyber Sprint drives Use Cases:
  - Managing Privileged Users
  - Active Directory-centric network logon
- Deliver on the imperative for **strong authentication** and especially for the HSPD-12 (PIV)
- Agency participation is self-determined based on fit of Use Cases to the Agency's situation and abilities
- Focused on tool solution set with necessary installation and configuration services
- Operations and Maintenance by Agencies
- Defers integration into CDM solution (e.g., metrics and reporting)



# What is the danger?

**According to the 2016 Verizon Data Breach Report, 63% of confirmed data breaches involved weak, default, or stolen passwords.**

The use of stolen credentials... targeting traditional username and password authentication are prevalent across numerous patterns.

## **Static Credentials**

Static credentials in the form of username and password continue to be targeted by several of the top hacking action varieties and malware functionalities.



# PRIVMGMT Solution Addresses Managing Privileged Users

## PRIVMGMT

Phase 2 Task Order that procures tools, sensors, and services on behalf of participating Federal Agencies to strengthen policies and practices for privileged users in particular.

### Key Elements are:

- Provides MUR for Privileged Users
- Strong authentication via PIV card
- Privileged User Management



...supports the objectives for privileged management as defined from the 2015 Cyber Sprint and documented in OMB M-16-04.



# PRIVMGMT Solution Overview

- What it provides
  - Use of PIV card for privileged access to the Privileged Access Manager
  - Agencies have prerequisite to provide the PIV card and PIV validation infrastructure
  - Level of Assurance (LOA) 4 authentication for privileged access to target devices
  - Scalable solution architecture to accommodate Agency variations
  - MUR and PDP and Phase 2 elements of TRUST, PRIV, CRED, and BEHAVE to support future CDM Dashboard integration
- What it doesn't provide
  - CMaaS integration services to the CDM dashboard
  - Ongoing maintenance and operations support
- What is needed by each Agency
  - Infrastructure resources (post-SDR)
  - Identification of support personnel
  - Complete and return Readiness Survey (already distributed) and As-Is Questionnaires (when received)
- PoP 12 Jul 2016 – 11 Jul 2018



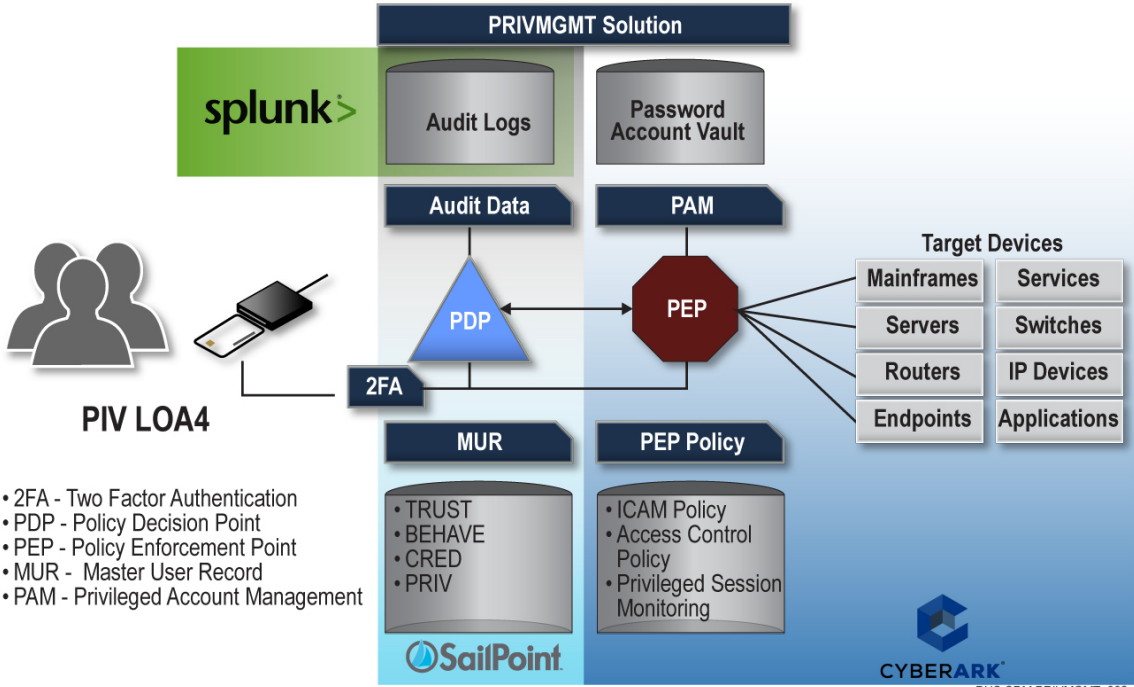


# Overview of the PRIVMGMT Solution

## PRIVMGMT Solution Overview

The solution is composed of three Commercial Off-the-Shelf (COTS) tools: **SailPoint**, **CyberArk**, and **Splunk**

- SailPoint IdentityIQ** - is the Master User Record (MUR) for privileged users, which includes data elements for TRUST, BEHAVE, CRED, and PRIV, and acts as the PDP to define the desired state and perform defect checks on the actual state
- CyberArk** - acts as the PEP to ensure proper execution of access control policies and provides a Password Account Vault
- Splunk** - repository for all event and audit logs



- 2FA - Two Factor Authentication
- PDP - Policy Decision Point
- PEP - Policy Enforcement Point
- MUR - Master User Record
- PAM - Privileged Account Management

DHS CDM PRIVMGMT\_002

# Password Account Vault - CyberArk

- Access to the Password Account Vault is only allowed using the PIV card
- Controls access to privilege account passwords and certificates
- Protects privileged account credentials using multiple layers of security
- Account credentials generated based on policy and are not known to the user
- Prevents unauthorized users from accessing privileged account credentials
- Provides detailed audit and reporting
- Can proactively rotate account credentials automatically



# MUR AND PDP – SAILPOINT

CDM Functional Area	Target Attributes	Target Data Sources
TRUST	<ul style="list-style-type: none"> <li>A common identifier for all privileged users</li> <li>The manager of the privileged user</li> <li>Whether or not the user has a valid PIV assigned</li> </ul>	<ul style="list-style-type: none"> <li>Agency-specific</li> </ul>
BEHAVE	<ul style="list-style-type: none"> <li>Whether or not the user has taken annual security training</li> <li>Whether or not the user has taken any additional training required for privileged users</li> </ul>	<ul style="list-style-type: none"> <li>Agency-specific</li> <li>Learning Management Systems or flat file</li> </ul>
CRED	<ul style="list-style-type: none"> <li>Does the user have a credential assigned? (includes PIV and other credential types)</li> <li>If credential type is not PIV, does it meet complexity requirements?</li> <li>Does the credential meet age requirements?</li> <li>Are other accounts entitled to use the same credential?</li> </ul>	<ul style="list-style-type: none"> <li>Active Directory, LDAP, Agency-specific</li> </ul>
PRIV	<ul style="list-style-type: none"> <li>To which privileged credentials does a user have access?</li> <li>To which credential vaults does a user have access?</li> </ul>	<ul style="list-style-type: none"> <li>Active Directory, LDAP, Agency-specific</li> </ul>

# Auditing Logs - Splunk

---

Provides a repository for all event and audit logs

Can utilize Phase 1 Splunk implementation if available



# PRIVMGMT: The First Step Toward CDM Phase 2 Capabilities

---

## Today's Topics

Important Agency PRIVMGMT Considerations



# Considerations - People

---

## IT Executive / Management

- Program Sponsorship and Announcements
  - Document and communicate commitment
    - Document the working relationship with already existing CDM TO2 Activities
    - Consider creating an Integrated Project Team (IPT) to include key stakeholders
    - Charter the PRIVMGMT effort internally
- Communication and Awareness
  - Respond to the Readiness Survey and As-IS Questionnaire (when received)
  - Foster adoption of the ICAM and CDM programs via proactive communication and awareness



# Considerations - People

---

## IT Organization and Staff Planning

### –Personnel Site/System Access

- Contractor will carry DHS suitability

### •Reciprocity will facilitate access and logistics for contractors

- Logical/Physical
- Prepare for Agency-specific security considerations

### » Identify Key Stakeholders

### » Coordinate with Security Ops

## IT Sourcing

### –Evaluate existing resources availability to assist with implementation activities

### –PRIVMGMT is a turn-key solution where the Agency will be responsible for Operations and Maintenance



# Considerations - Process

---

## Program / Project Management

–Awareness and preparation to work through change management process

- Understand realistic timelines and approval durations
- Required documentation

–Logistics

- License Transfer Process is same as TO2 process
- Property accountability and financial implications
- Transfer to operations

–IT Governance

- Review existing governance processes
- Understand Authority to Operate (ATO) process

–IT Service Management

- Existing service contracts





# Considerations - Technology

---

## Existing ICAM Infrastructure

- Be prepared to update Attachment G during as-is validation
- Update Privileged User Management documentation
  - Current Architecture, deployments, and versions
  - Current operational status
    - New implementations, changes in infrastructure configurations, etc.

## Facility \ Data Center

- Plan for installation
  - Ping, Power, and Pipe
    - Existing Bandwidth and limitations
- Be prepared to provide hardware and/or virtual machines to support PRIVMGMT solution



# Questions and Answers

***What is the impact of...??***

***What about....??***

***How did the stakeholders adjust to ....??***

***What would you do differently about....??***

***What should I do about ....??***

***What would you recommend for....??***

***How much time did it take to....??***

***How are you maintaining 95% compliance with CSM CAP....??***

***How did you handle... (latency, centralization, control issues, etc.)??***



# The CDM Learning Program

## CDM Learning Program

- Monthly Learning Community Event (CDM-LCE)
- Monthly Webinars
- Weekly CDM Bits & Bytes
- Online Vignettes

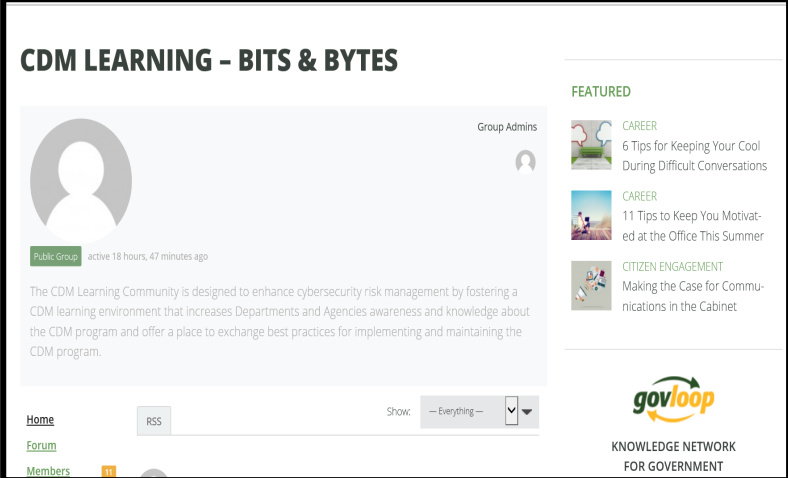
Resources Available:

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

Sign up to receive event  
information:

[cdmlearning@hq.dhs.gov](mailto:cdmlearning@hq.dhs.gov)

Sign up for the CDM learning blog:  
<https://www.govloop.com/groups/cdm-learning-bits-bytes>



The screenshot shows the 'CDM LEARNING - BITS & BYTES' group page on Govloop. The page features a profile picture placeholder, a 'Public Group' status, and a description: 'The CDM Learning Community is designed to enhance cybersecurity risk management by fostering a CDM learning environment that increases Departments and Agencies awareness and knowledge about the CDM program and offer a place to exchange best practices for implementing and maintaining the CDM program.' A 'Featured' section on the right lists three articles: '6 Tips for Keeping Your Cool During Difficult Conversations', '11 Tips to Keep You Motivated at the Office This Summer', and 'Making the Case for Communications in the Cabinet'. The Govloop logo and 'KNOWLEDGE NETWORK FOR GOVERNMENT' tagline are visible in the bottom right corner.



Homeland  
Security

Federal Network Resilience

# The CDM Learning Program

## Sign up for December 8th, 2016 Event:

### ***Best Practices for Privileged User PIV Authentication: Getting Ready for PRIVMGMT***

*With Ms. Hildegard (Hildy) Ferraiolo, a Computer Scientist and PIV expert from NIST*



[https://dhsconnect.connectsolutions.com/privmgmt-bpfpupa-signup/event/event\\_info.html](https://dhsconnect.connectsolutions.com/privmgmt-bpfpupa-signup/event/event_info.html)



U.S. DEPARTMENT OF  
Homeland  
Security

Federal Network Resilience

# Event Conclusion

---

Thank you for attending today's  
CDM Webinar!

- A certificate of attendance will be available to download on the CDM Learning Program website at [www.us-cert.gov/cdm/training](http://www.us-cert.gov/cdm/training), within one week of today's event
- Visit our website to learn more about the CDM Learning Program and upcoming events at [www.us-cert.gov/cdm](http://www.us-cert.gov/cdm)
- For any questions, comments, or suggestions for future topics, please email us at [cdmlearning@hq.dhs.gov](mailto:cdmlearning@hq.dhs.gov)

