Identity, Credential, and Access Management Subcommittee

May 2018

Draft April-release FY18 FISMA icam metrics guidance

**Table of Contents**

[**Introduction** 3](#_Toc513200667)

[**Approach** 5](#_Toc513200668)

[**How to Navigate** 6](#_Toc513200669)

[**Tools & Tips** 7](#_Toc513200670)

[**FISMA Definitions** 7](#_Toc513200671)

[**Searching Active Directory** 9](#_Toc513200672)

[**Searching Active Directory - PIV** 10](#_Toc513200673)

[**Unprivileged Network Users** 11](#_Toc513200674)

[**Collecting Metric 2.4.1** 12](#_Toc513200675)

[**Collecting Metric 2.4.2** 13](#_Toc513200676)

[**Collecting Metric 2.4.3** 14](#_Toc513200677)

[**Collecting Metric 2.4.4** 15](#_Toc513200678)

[**Privileged Network Users** 16](#_Toc513200679)

[**Collecting Metric 2.5.1** 17](#_Toc513200680)

[**Collecting Metric 2.5.2** 18](#_Toc513200681)

[**Collecting Metric 2.5.3** 19](#_Toc513200682)

[**Collecting Metric 2.5.4** 20](#_Toc513200683)

[**Collecting Metric 2.5.5** 21](#_Toc513200684)

[**Section Resources** 22](#_Toc513200685)

[**Network and Local System Accounts** 23](#_Toc513200686)

[**Collecting Metric 2.6.1** 24](#_Toc513200687)

[**Collecting Metric 2.6.2** 25](#_Toc513200688)

[**Collecting Metric 2.7** 26](#_Toc513200689)

[**Collecting Metric 2.7.1** 27](#_Toc513200690)

[**Next Steps** 28](#_Toc513200691)

# **Introduction**

There are **13** ICAM-related metrics in the [FY18 CIO FISMA Metrics](https://www.dhs.gov/sites/default/files/publications/FY%202018%20CIO%20FISMA%20Metrics_V2_Final.pdf), including several new metrics that have not been collected in previous years. FY18 ICAM-related metrics can be found under Section 2 (Protect) of the guidance and below:

|  |  |
| --- | --- |
| **Metric** | **Description** |
| [2.4.1](#_Collecting_Metric_2.4.1) | Number of unprivileged users with [network accounts](#_FISMA_Definitions).1 (Exclude [non-user accounts](#_FISMA_Definitions)) |
| [2.4.2](#_Collecting_Metric_2.4.2) | Number of unprivileged users (from 2.4.1) that are required to authenticate to the network through the [machine-based](#_Searching_Active_Directory) or [user-based enforcement](#_Searching_Active_Directory) of a two-factor PIV credential2 or other NIST 800-63 r3 Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3/Federated Assurance Level (FAL) 3 credential.3 |
| [2.4.3](#_Collecting_Metric_2.4.3) | Number of unprivileged users (from 2.4.1) that use a username and password as their primary method for network authentication. Please describe compensating controls for limiting these users’ access in the comments field. |
| [2.4.4](#_Collecting_Metric_2.4.4) | Number of unprivileged users (from 2.4.1) covered by a centralized dynamic access management solution that controls and monitors users’ access. [(NIST SP 800-53r4 AC-2(6))](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) |
| [2.5.1](#_Collecting_Metric_2.5.1) | Number of privileged users with [network accounts](#_FISMA_Definitions). 1 (Exclude [non-user accounts](#_FISMA_Definitions)) |
| [2.5.2](#_Collecting_Metric_2.5.2) | Number of privileged users (from 2.5.1) that are required to authenticate to the network through the [machine-based](#_Searching_Active_Directory) or [user-based enforcement](#_Searching_Active_Directory) of a two-factor PIV credential2 or other NIST 800-63 r3 Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3/Federated Assurance Level (FAL) 3 credential. 3 |
| [2.5.3](#_Collecting_Metric_2.5.3) | Number of privileged users (from 2.5.1) that use a username and password as their primary method for network authentication. Please describe compensating controls for limiting these users’ access in the comments field. |
| [2.5.4](#_Collecting_Metric_2.5.4) | Number of privileged users (from 2.5.1) covered by a centralized dynamic access management solution that controls and monitors users’ access. [(NIST SP 800-53r4 AC-2(6))](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) |
| [2.5.5](#_Collecting_Metric_2.5.5_1) | Frequency with which privileged user privileges are reviewed, according to agency policy. |
| [2.6.1](#_Collecting_Metric_2.6.1) | Number of users with [privileged local system accounts](#_FISMA_Definitions). 4 |
| [2.6.2](#_Collecting_Metric_2.6.2) | Number of users with [privileged local system accounts](#_FISMA_Definitions) (from 2.6.1) are accessible through the Agency’s network in which the privileged user is required to authenticate to the network through the [machine-based](#_Searching_Active_Directory) or [user-based enforcement](#_Searching_Active_Directory) of a two-factor PIV credential or other NIST 800-63 r3 IAL3/AAL3/FAL3 credential. |
| [2.7](#_Collecting_Metric_2.7) NEW | Number of High Value Asset (HVA) systems5 that require all government and contractor users (100% privileged and unprivileged) to authenticate through the [machine-based](#_Searching_Active_Directory) or [user based enforcement](#_Searching_Active_Directory) of a two-factor [PIV](#_FISMA_Definitions) credential or other NIST 800-63 r3 IAL3/AAL3 credential. ([OMB M-18-02](https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/oct2017/cs2017_OMB.pdf), [NIST SP 800-63](https://pages.nist.gov/800-63-3/)) |
| [2.7.1](#_Collecting_Metric_2.7.1_1) NEW | Number of HVA systems assessed by DHS, a third-party, or independent entity (per [M-17-09](https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-09.pdf)) that determined machine-based or user-based enforcement of a two-factor PIV credential (as described in 2.7.) is not required due to mitigating security capabilities. |

Data collected from these metrics can help your agency prioritize and guide decisions around resource allocation to assure ICAM Program effectiveness. The ultimate goal of these metrics is to enable your agency to ensure the right people have the right access to the right data at the right time. ICAM program advancement is an incremental process and unique to each agency’s mission and business needs.

The GSA FICAM Program has worked with DHS, OMB, and others to develop practical guidance to help your agency collect the data for the ICAM-related FISMA metrics. This guidance is intended to help you logically navigate and interpret the metrics to decrease your reporting time and increase usability and understanding. We hope that senior leadership will have a better “apples-to-apples” comparison across agencies if all agencies have a clearer understanding of what the metrics represent and how to collect and report them.

1An unprivileged network account is any account that is not a [privileged network account](#_FISMA_Definitions).

2For a person with one or more unprivileged network accounts, the person should be counted in the total only if a two-factor PIV Credential is necessary to authenticate to all network accounts. The enforcement of authentication may be accomplished via either user-based or machine-based configuration settings.

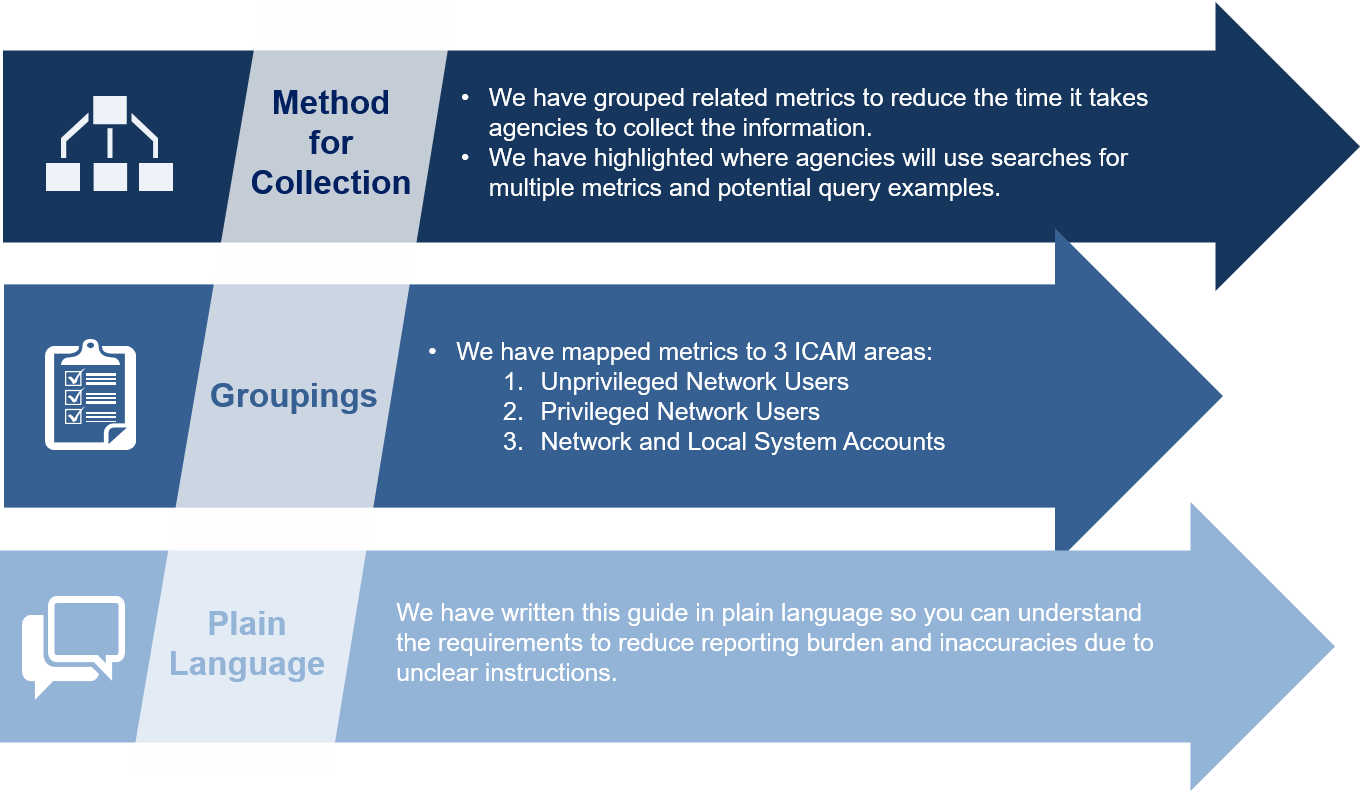
3For additional information, refer to [NIST SP 800-63.](https://pages.nist.gov/800-63-3/)

4 Do not report [privileged local system accounts](#_FISMA_Definitions)that are not accessible on the network.

5 HVA as defined in [M-17-09](https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-09.pdf). OMB will leverage existing data sources for the denominator of HVA related metrics.

# **Approach**

The approach detailed below describes the methodology behind this guidance document and explains the organization and sequencing of the collection process.



# **How to Navigate**

The purpose of this document is to provide your agency assistance and guidance with understanding, interpreting, and collecting information for the FY18 ICAM-related Metrics, to reduce the overall reporting burden.

Use this document as a How-to-Guide:

Ribbon logoRecycle logoThe recycle icon next to steps throughout the pages highlights when you should save the numbers collected because those numbers will be used for other metrics. 

The “why” is included for informative purposes only and provides insight into why these metrics are important and provide value at the program, agency, and government-wide level.

Pencil logoExamples are provided on several of the metrics to give you additional context for interpreting the metric.

Tips are included to give you ideas for collection methods.

Focus logoAssumptions, definitions and references are included to provide you with additional context and information.

*This guidance provides you starting steps for collecting the information in the FISMA metrics. Examples are provided to help you. We encourage you to contact us* [*icam@gsa.gov*](mailto:icam@gsa.gov) *with any questions or input!*

# **Tools & Tips**

## Focus logo**FISMA Definitions**

**Enterprise level**   
The entire reporting organization or each organizational component with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance.

**Local System Account**   
A predefined local account used by service control manager that has extensive privileges on a local system.1

**Network Account**   
A user account that provides access to the network.

**Non-User Account**  
An account that is not intended to be controlled directly by a person (or group). The account is either (a) intended to be used by the system or an application, which presents credentials and performs functions under the management of the person (or group) that owns the account, or (b) created to establish a service (like a group mailbox), and no one is expected to log into the account.

**Personal Identity Verification (PIV) credentials**   
A physical artifact (e.g., identity card, “smart” card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation, etc.) such that a claimed identity of the cardholder may be verified against the stored credentials by another person (human-readable and verifiable) or an automated process (computer-readable and verifiable). The Federal standard for this is specified as Federal Information Processing Standard Publication 201 (FIPS 201).

**Privileged Local System Account**   
A user account with elevated privileges which is typically allocated to system administrators, database administrators, developers, and others who are responsible for system/application control, monitoring, or administration functions. In Linux or other Unix-like operating systems, these are typically referred to as root account, root user, or super-user accounts.

**Privileged Network Account**   
A network account with elevated privileges, which is typically allocated to system administrators, network administrators, and others who are responsible for system/application control, monitoring, or administration functions.

**Unprivileged Network Account**   
An unprivileged network account is any account that is not a privileged network account, also known as a standard account.

1 <https://msdn.microsoft.com/en-us/library/windows/desktop/ms684190(v=vs.85).aspx>

******Searching Active Directory**

**Using The GUI**

You can use the find command in Active Directory Users and Groups application to search for network users and groups. This interface allows you to inspect groups and group membership individually.

**PowerShell**

PowerShell commands can be used to find members of administrative groups and members of child groups for the domain. Here’s an example command to list the members of a group for the example.gov domain:

dsget group “CN=Domain Admins,CN=Users,DC=example,DC=gov” -members

Sample results:   
“CN=Test Admin,CN=Users,DC=example,DC=gov”   
“CN=Administrator,CN=Users,DC=example,DC=gov”

Other scripts can be created to search Active Directory for membership to many groups at once. Active Directory understands LDAP filters. Here is an example script to find accounts who are part of one or both of the identified groups. It also takes into consideration only users with -admin at the end of their username.

$DomainsAdminsDn = (Get-ADGroup ‘Domain Admins’).DistinguishedName $AdminsDn = (Get-ADGroup ‘Administrators’).DistinguishedName Get-ADUser -LDAPFilter “(&(SamAccountName=\* admin) (|(memberof=$DomainsAdminsDn)(memberof=$AdminsDn)))”

To count the resulting objects instead of listing them, add this to the end of the Get-ADUser command:

-ResultSetSize $null | Measure-Object

This command uses variables to improve the readability of the filter. If you want to use the filter above in the GUI, from the find dialog, choose “Custom Search” and “Advanced”. You can’t use variables in there like in PowerShell, so make sure you use the full DN of the group.

Here are some references to help to identify built-in Windows (Active Directory) groups:

<https://technet.microsoft.com/en-us/library/cc978401.aspx>

<https://support.microsoft.com/en-us/kb/243330>

## book logo**Searching Active Directory - PIV**

**Machine Based Enforcement (MBE):**   
The user is required to use their PIV credential to authenticate to each device where the policy is applied.

**User Based Enforcement (UBE):**   
The user is required to use their PIV credentials to authenticate to all networks and devices. Your users’ Active Directory password hash values have been replaced with hash values of long (120 character) randomized strings.

**How do I know if accounts are required to login with their PIV (UBE)?**   
You can use LDAP filters to search Active Directory for accounts that do or do not enforce PIV to log onto networks. Here’s an example filter that you can use in a PowerShell script or Active Directory advanced search to find users based on User Account Control – Smart Card Login Enforced on The User.

To find users where the Smart Card Login is enforced on person objects:   
(& (objectCategory=person) (userAccountControl:1.2.840.113556.1.4.803:=262144))

To find users where the Smart Card Login is not enforced on person objects:   
(& (objectCategory=person) (!userAccountControl:1.2.840.113556.1.4.803:=262144))

More details on User Account Control LDAP filters can be found here:

<http://social.technet.microsoft.com/wiki/contents/articles/5392.active-directory-ldap-syntax-filters.aspx>

More info on AD Queries can be found here:

<https://blogs.msdn.microsoft.com/muaddib/2008/10/08/how-to-query-individual-properties-of-the-useraccountcontrol-active-directory-user-property-using-ldap/>

# **Unprivileged Network Users**

This section covers FISMA metrics around unprivileged network users (2.4.1-2.4.4).

Focus logo

Please refer to the following guidance for Metrics 2.4.1-2.4.4:

[OMB M-18-02,](https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/oct2017/cs2017_OMB.pdf)[NIST 800-53r4 IA-2(2),](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)[NIST SP 800-63](https://pages.nist.gov/800-63-3/)

|  |  |
| --- | --- |
| [2.4.1](#_Collecting_Metric_2.4.1) | Number of unprivileged users with [network accounts](#_FISMA_Definitions).1 (Exclude [non-user accounts](#_FISMA_Definitions)) |
| [2.4.2](#_Collecting_Metric_2.4.2) | Number of unprivileged users (from 2.4.1) that are required to authenticate to the network through the [machine-based](#_Searching_Active_Directory) or [user-based enforcement](#_Searching_Active_Directory) of a two-factor PIV credential2 or other NIST 800-63 r3 Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3/Federated Assurance Level (FAL) 3 credential.3 |
| [2.4.3](#_Collecting_Metric_2.4.3) | Number of unprivileged users (from 2.4.1) that use a username and password as their primary method for network authentication. Please describe compensating controls for limiting these users’ access in the comments field. |
| [2.4.4](#_Collecting_Metric_2.4.4) | Number of unprivileged users (from 2.4.1) covered by a centralized dynamic access management solution that controls and monitors users’ access. [(NIST SP 800-53r4 AC-2(6))](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) |

1An unprivileged network account is any account that is not a [privileged network account](#_FISMA_Definitions).

2For a person with one or more unprivileged network accounts, the person should be counted in the total only if a two-factor PIV Credential is necessary to authenticate to all network accounts. The enforcement of authentication may be accomplished via either user-based or machine-based configuration settings.

3For additional information, refer to [NIST SP 800-63.](https://pages.nist.gov/800-63-3/)

## **Collecting Metric 2.4.1**

**Unprivileged Network Users**

**Where do I start?**

1. Identify the characteristics that make your agency’s network accounts privileged. We’ll exclude those accounts from this metric.

* See [Section Resources](#_Section_Resources) for examples of these characteristics. They are typically groups in Active Directory.

1. Search the user repository (Active Directory) for and exclude accounts with the values identified in Step 1.

* See [Tools & Tips for Active Directory](http://127.0.0.1:4000/icam-fisma/tools-tips/searchAD) or [Tools & Tips for Active Directory-PIV](http://127.0.0.1:4000/icam-fisma/tools-tips/searchAD-PIV) for example searches.

1. Count the accounts in step 2 that are assigned to/ used by individual people (non-system).

* See [Tools & Tips for Active Directory](http://127.0.0.1:4000/icam-fisma/tools-tips/searchAD) for an example of how to count objects using PowerShell.

1. Identify the number of users of the accounts. Take care to eliminate duplicates from the count if two accounts are researched and identified to be assigned to the same person. Record this number for **Metric 2.4.1.**

Recycle logo

**Save the result from Metric 2.4.1!**

You'll use the user information found here again for metrics 2.4.2, 2.4.3,

John.smith.1 and john.smith.2 might both belong to the same person!

## **Collecting Metric 2.4.2**

**Unprivileged Network Users and Authentication**

**Where Do I Start?**

1. Start with the users identified in [Metric 2.4.1](#_Collecting_Metric_2.4.1,) and exclude users that can log onto the network with *anything other* than through the machine-based or user-based enforcement of a two-factor PIV credential or other NIST 800-63 r3 Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3/Federated Assurance Level (FAL) 3 credential. (i.e., one time password tokens, sms pin & password, username and password). Please see [Tools & Tips for Active Directory-PIV](#_Searching_Active_Directory) for information on querying for these users.

a. Some users have multiple accounts - a user must be excluded if even one of their accounts lets them log onto the network with something other than a PIV or NIST approved credential.  
  
b. Users who have the option of a two-factor PIV credential or Username/Password should also be excluded since two-factor PIV credential is not ***required***.

1. Count the total number of unique users who have not been excluded in previous steps on this page and record number for **Metric 2.4.2.**

Ribbon logo

**Why is Metric 2.4.2 important?**

It is important to authenticate credentials when a user accesses a new network. Additionally, users must use a two-factor PIV credential to log onto the networks to mitigate attacks such as *Pass the Hash*.

## **Collecting Metric 2.4.3**

**Unprivileged Network Users and Authentication**

**Where Do I Start?**

**Part 1:**

1. Take the users identified in [Metric 2.4.2](#_Collecting_Metrics_2.4.4) and *exclude* the users from [Metric 2.4.1](#_Collecting_Metric_2.4.1,).
2. For each remaining account, does the account have the ability to log onto the network using a username & password? If it does, the user of the account should be counted.
3. Count the total number of users identified in step 2 and record the number for the first part of **Metric 2.4.3.**

**Part 2:**

1. If you *do* have users that use their username and password as their primary authentication method, identified in Step 2 above, please describe the policies, technologies, and controls in place that limit the users’ access when this login method is used. Record this information under the comments field of **Metric 2.4.3**.
2. If you *don’t* have a policy, technology, and controls in place that limit users’ access when this login method is used, please respond with *No controls implemented*.

Ribbon logo

**Why is Metric 2.4.3 important?**

It is important to authenticate credentials when a user accesses a new network. Additionally, users must use a two-factor PIV credential to log onto the networks to mitigate attacks such as *Pass the Hash*.

## **Collecting Metric 2.4.4**

**Unprivileged Network Users Covered by a Centralized Dynamic Access Management Solution**

Your agency may have implemented a centralized dynamic access management solution that controls and monitors access for its users. This type of solution is commonly known as attribute-based access control (ABAC).

**Where Do I Start?**

1. If your agency is not leveraging an ABAC like model, please respond with N/A.
2. If your agency does leverage an ABAC like model, determine the data sources providing dynamic information used to make access decisions in your model.
3. Determine what attributes are associated with these sources and associated with the accounts in your directory(ies).
4. Ribbon logoFocus logoCount the number of users (starting with the population identified in [Metric 2.4.1](#_Collecting_Metric_2.4.1,)) who are authorized to access resources using this model and report for **Metric 2.4.4**.

**Why is Metric 2.4.4 important?**

A centralized dynamic access management solution model is similar to an Attribute Based Access Control (ABAC) model. These types of models provide an attribute-based approach to accommodate a wide breadth of access control policies and help simplify access control management.

**Additional Information**

**•** Please refer to [Use Case 18: Authorize Access - Dynamic](https://arch.idmanagement.gov/usecases/36_access_authorize_dynamic/) from the FICAM Architecture to understand the process behind a centralized dynamic access management solution.

• Per NIST SP 800-162, ABAC is a logical access control model that controls access to objects by evaluating rules against the attributes of the entities actions, and based on the environment relevant to a request. All ABAC solutions contain capabilities to evaluate attributes and environment conditions. To learn more about ABAC, please refer to [NIST SP 800-162 - Guide to Attribute Based Access Control (ABAC) Definition and Considerations.](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf)

• In December 2011, the [FICAM Roadmap and Implementation Plan v2.0](https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FICAM_Roadmap_and_Implem_Guid.pdf) included ABAC as a recommended access control model for promoting information sharing between diverse and disparate organizations. ABAC provides an attribute-based approach to accommodate a wide breadth of access control policies and helps simplify access control management.

# **Privileged Network Users**

This section covers FISMA metrics around privileged network users (2.5.1-2.5.5)

Focus logo

Please refer to the following guidance for Metrics 2.5.1-2.5.6:

[OMB M-18-02,](https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/oct2017/cs2017_OMB.pdf)[NIST 800-53r4 IA-2(1),](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)[NIST SP 800-63](https://pages.nist.gov/800-63-3/)

|  |  |
| --- | --- |
| [2.5.1](#_Collecting_Metric_2.5.1) | Number of privileged users with [network accounts](#_FISMA_Definitions). 1 (Exclude [non-user accounts](#_FISMA_Definitions)) |
| [2.5.2](#_Collecting_Metric_2.5.2) | Number of privileged users (from 2.5.1) that are required to authenticate to the network through the [machine-based](#_Searching_Active_Directory) or [user-based enforcement](#_Searching_Active_Directory) of a two-factor PIV credential2 or other NIST 800-63 r3 Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3/Federated Assurance Level (FAL) 3 credential. 3 |
| [2.5.3](#_Collecting_Metric_2.5.3) | Number of privileged users (from 2.5.1) that use a username and password as their primary method for network authentication. Please describe compensating controls for limiting these users’ access in the comments field. |
| [2.5.4](#_Collecting_Metric_2.5.4) | Number of privileged users (from 2.5.1) covered by a centralized dynamic access management solution that controls and monitors users’ access. [(NIST SP 800-53r4 AC-2(6))](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) |
| [2.5.5](#_Collecting_Metric_2.5.5_1) | Frequency with which privileged user privileges are reviewed, according to agency policy. |

1An unprivileged network account is any account that is not a [privileged network account](#_FISMA_Definitions).

2For a person with one or more unprivileged network accounts, the person should be counted in the total only if a two-factor PIV Credential is necessary to authenticate to all network accounts. The enforcement of authentication may be accomplished via either user-based or machine-based configuration settings.

3For additional information, refer to [NIST SP 800-63.](https://pages.nist.gov/800-63-3/)

## **Collecting Metric 2.5.1**

**Privileged Network Users**

**Where Do I Start?**

1. Identify the characteristics that make your agency’s network accounts privileged.

* See [Section Resources](#_Section_Resources) for examples of these characteristics. They are typically groups in Active Directory.

1. Search the user repository (Active Directory) for accounts with the values identified in Step 1.

* See [Tools & Tips for Active Directory](#_Searching_Active_Directory_1) or [Tools & Tips for Active Directory-PIV](#_Searching_Active_Directory) for example searches.

1. Count the accounts in step 2 that are assigned to/used by individual people (non-system).

* See [Tools & Tips for Active Directory](#_Searching_Active_Directory_1) for an example of how to count objects using PowerShell.

1. Identify the number of users of the accounts. Take care to eliminate duplicates from the count if two accounts are researched and identified to be assigned to the same person. Record this number for **Metric 2.5.1**.

Recycle logo

John.smith.1 and john.smith.2 might both belong to the same person!

**Save the result from Metric 2.5.1!**

You'll use the user information found here again for metrics 2.5.2, 2.5.3, and 2.5.4.

## **Collecting Metric 2.5.2**

**Privileged Network Users and Authentication**

#### **Where Do I Start?**

1. Start with the users identified in [Metric 2.5.1](#_Collecting_Metric_2.5.1) and exclude users that can log onto the network with *anything other* than through the machine-based or user-based enforcement of a two-factor PIV credential or other NIST 800-63 r3 Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3/Federated Assurance Level (FAL) 3 credential. (i.e., one time password tokens, sms pin & password, username and password). Please see [Tools & Tips for Active Directory-PIV](#_Searching_Active_Directory) for information on querying for these users.
2. Some users have multiple accounts - a user must be excluded if even one of their accounts lets them log onto the network with something other than a PIV or NIST approved credential. b. Users who have the option of a two-factor PIV credential or Username/Password should also be excluded since two-factor PIV credential is not ***required***.
3. Count the total number of unique users who have not been excluded in previous steps on this page and record number for **Metric 2.5.2**.

Ribbon logo

#### **Why is Metric 2.5.2 important?**

It is important to authenticate credentials when a user accesses a new network. Additionally, users must use a two-factor PIV credential to log onto the networks to mitigate attacks such as *Pass the Hash.*

## **Collecting Metric 2.5.3**

**Privileged Network Users and Authentication**

#### **Where Do I Start?**

Part 1:

1. Take the users identified in [Metric 2.5.2](#_Collecting_Metric_2.5.2) and *exclude* the users from [Metric 2.5.1](#_Collecting_Metric_2.5.1).
2. For each remaining account, does the account have the ability to log onto the network using a username & password? If it does, the user of the account should be counted.
3. Count the total number of users identified in step 2 and record the number for the first part of **Metric 2.5.3.**

Part 2:

1. If you *do* have users that use their username and password as their primary authentication method, identified in Step 2 above, please describe the policies, technologies, and controls in place that limit the users’ access when this login method is used. Record this information under the comments field of **Metric 2.5.3**.
2. If you *don’t* have a policy, technology, and controls in place that limit users’ access when this login method is used, please respond with *No controls implemented*.

Ribbon logo**Focus logo**

#### **Why is Metric 2.5.3 important?**

It is important to authenticate credentials when a user accesses a new network. Additionally, users must use a two-factor PIV credential to log onto the networks to mitigate attacks such as *Pass the Hash.*

#### **Additional Information**

For recommended compensating controls, please review the [Best Practices for Privileged User PIV Authentication Guidelines.](https://csrc.nist.gov/csrc/media/publications/white-paper/2016/04/21/best-practices-for-privileged-user-piv-authentication/final/documents/best-practices-privileged-user-piv-authentication.pdf)

## **Collecting Metric 2.5.4**

**Privileged Network Users Covered by a Centralized Dynamic Access Management Solution**

Your agency may have implemented a centralized dynamic access management solution that controls and monitors access for its users. This type of solution is commonly known as attribute-based access control (ABAC).

**Where do I Start?**

1. If your agency is not leveraging an ABAC like model, please respond with N/A.
2. If your agency does leverage an ABAC like model, determine the data sources providing dynamic information used to make access decisions in your model.
3. Determine what attributes are associated with these sources and associated with the accounts in your directory(ies).
4. Count the number of users (starting with the population identified in [Metric 2.5.1](#_Collecting_Metric_2.5.1)) who are authorized to access resources using this model and report for **Metric 2.5.4**.

Focus logoRibbon logo

**Why is Metric 2.5.4 important?**

A centralized dynamic access management solution model is similar to an Attribute Based Access Control (ABAC) model. These types of models provide an attribute-based approach to accommodate a wide breadth of access control policies and help simplify access control management.

**Additional Information**

**•** Please refer to [Use Case 18: Authorize Access - Dynamic](https://arch.idmanagement.gov/usecases/36_access_authorize_dynamic/) from the FICAM Architecture to understand the process behind a centralized dynamic access management solution.

• Per NIST SP 800-162, ABAC is a logical access control model that controls access to objects by evaluating rules against the attributes of the entities actions, and based on the environment relevant to a request. All ABAC solutions contain capabilities to evaluate attributes and environment conditions. To learn more about ABAC, please refer to [NIST SP 800-162 - Guide to Attribute Based Access Control (ABAC) Definition and Considerations](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf).

• In December 2011, the [FICAM Roadmap and Implementation Plan v2.0](https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FICAM_Roadmap_and_Implem_Guid.pdf) included ABAC as a recommended access control model for promoting information sharing between diverse and disparate organizations. ABAC provides an attribute-based approach to accommodate a wide breadth of access control policies and helps simplify access control management.

## **Collecting Metric 2.5.5**

**Frequency of Privileged User Privilege Review**

**Where Do I Start?**

The target frequency of user privilege reviews may be dictated by your enterprise-level ICAM policy.

1. If you don’t have a target frequency specified by an enterprise-level policy, please respond with N/A.
2. If you do have a target frequency specified, please review your enterprise-level ICAM policy and provide that frequency for **Metric 2.5.5**.

Focus logoRibbon logo

**Important Terms**

A (*User) Privilege* is a right granted to an individual, a program, or a process [Source: CNSSI-4009]. Privileges can pertain to both a *person* user and a *system* user, and allow that user to access information in accordance with their duties and a valid *“need to know.”* Different agencies have different needs based on their size, turnover, and other determining factors.

**Reviewing user privileges is important to managing risk in an organization because;**

• It is essential to identifying and neutralizing user access vulnerabilities or violations; and

• It enables the core information security principles of segregation of duties, least privilege, and need-to-know.

## focus logo**Section Resources**

How do I find Privileged Accounts?

**By Name:** Your agency may have a naming convention for its accounts to identify privileged users.

*For example,* some names may have -admin or -domainadmin as part of their usernames (jdoe-admin). This shouldn’t be the only way to find administrators since access can change over time.

**By Privileges:** Privileged network accounts have elevated access rights, typically in Active Directory, accounts are added to groups. Look through Active Directory to identify the groups that grant elevated permissions.

**By Inspection:** Occasionally, accounts are assigned elevated privileges individually. You will need to know your user population and find the fringe cases.

Take care to remove duplicate accounts from the results! These metrics are counting unique accounts and users. For more information on assurance levels, refer to [NIST SP 800-63-3.](https://doi.org/10.6028/NIST.SP.800-63-3)

**Examples:**   
For most agencies, network accounts are managed in Active Directory. Examples of shared accounts are accounts used for helpdesk, test, and training or guest accounts.

# **Network and Local System Accounts**

This section covers FISMA metrics around Network and Local System Accounts (2.6.1-2.6.2 and 2.7-2.7.1)

Focus logo

Please refer to the following guidance for Metrics 2.6.1-2.6.2:

[NIST 800-53r4 IA-2(3)](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)

|  |  |
| --- | --- |
| [2.6.1](#_Collecting_Metric_2.6.1) | Number of users with [privileged local system accounts](#_FISMA_Definitions). 4 |
| [2.6.2](#_Collecting_Metric_2.6.2) | Number of users with [privileged local system accounts](#_FISMA_Definitions) (from 2.6.1) are accessible through the Agency’s network in which the privileged user is required to authenticate to the network through the [machine-based](#_Searching_Active_Directory) or [user-based enforcement](#_Searching_Active_Directory) of a two-factor PIV credential or other NIST 800-63 r3 IAL3/AAL3/FAL3 credential. |

Focus logo

Please refer to the following guidance for Metrics 2.7-2.7.1:

[OMB M-18-02,](https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/oct2017/cs2017_OMB.pdf) [NIST SP 800-63](https://pages.nist.gov/800-63-3/)

|  |  |
| --- | --- |
| [2.7](#_Collecting_Metric_2.7) NEW | Number of High Value Asset (HVA) systems5 that require all government and contractor users (100% privileged and unprivileged) to authenticate through the [machine-based or user based enforcement](#_Searching_Active_Directory) of a two-factor [PIV](#_FISMA_Definitions) credential or other NIST 800-63 r3 IAL3/AAL3 credential. ([OMB M-18-02](https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/oct2017/cs2017_OMB.pdf), [NIST SP 800-63](https://pages.nist.gov/800-63-3/)) |
| [2.7.1](#_Collecting_Metric_2.7.1_1) NEW | Number of HVA systems assessed by DHS, a third-party, or independent entity [(per M-17-09)](https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-09.pdf) that determined machine-based or user-based enforcement of a two-factor PIV credential (as described in 2.7.) is not required due to mitigating security capabilities. |

4 Do not report [privileged local system accounts](#_FISMA_Definitions) that are not accessible on the network.

5 HVA as defined in [M-17-09](https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-09.pdf). OMB will leverage existing data sources for the denominator of HVA related metrics.

## **Collecting Metric 2.6.1**

**Users with Privileged Local System Accounts**

**Where Do I Start?**

1. Identify the user population with privileged local system accounts.

* These users will typically support the administration of systems that run and make up the infrastructure.
* These users may have *groups* or some other *access rights* associated with the account that gives them privileged access to the local system.
* The accounts may be built-in administrative accounts such as root on Unix-like systems.
* Take note of whether the above matches what is listed on the APL. Some local system accounts may have elevated privileges through built-in utilities such as SUDO. These accounts should be identified as well.

1. Count the number of individual users (people) with these accounts. A user with 5 privileged accounts counts once. Record this number for **Metric 2.6.1**.

**Don't Forget!**

* Network Administrators
* Database Administrators
* UNIX System Administrators
* Mainframe Administrators
* Web Server Administrators
* Email Server Administrators

#### **Save the result from Metric 2.6.1!**

You'll use the user information found here again for metric 2.6.2.

Recycle logo

## **Collecting Metric 2.6.2**

**Users with Privileged Local System Accounts and Authentication**

**Where Do I Start?**

1. For each of the users’ accounts identified in [Metric 2.6.1](#_Collecting_Metric_2.6.1), determine if the local system that allows a user to authenticate to the account requires authentication through the machine-based or user-based enforcement of a two-factor PIV credential or other NIST 800-63 r3 IAL3/AAL3/FAL3 credential.
2. If yes, for all of the user’s privileged local accounts, count this user. If no for 1 or more of a user’s accounts, do not count the user. Record this number for **Metric 2.6.2**.

Ribbon logo

**Why is Metrics 2.6.1 and 2.6.2 important?**

* Understanding this user population helps to validate that they have the appropriate access across information systems.
* Issuing the appropriate credentials to user populations is meaningless unless agencies are requiring the use of these credentials.

## **Collecting Metric 2.7**

**Number of High Value Asset (HVA) Systems and Authentication**

**Where Do I Start?**

1. Please refer to your agency’s High Value Asset (HVA) list to determine the total number of HVA systems at your agency and which systems those are.
2. Work with the System Owner or Information System Security Officer (ISSO) for each HVA system identified in step 1 to determine the number of HVA systems that require all users to authenticate through the machine-based or user based enforcement of a two-factor PIV credential or other NIST 800-63 r3 IAL3/AAL3 credential. This information may be available in the System Security Plan for each HVA, and potentially in control IA-2(12). Record this number for **Metric 2.7**.

Recycle logo

#### **Save the result from Metric 2.7!**

You'll use the user information found here again for metric 2.7.1.

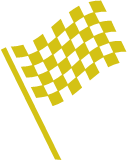
## **Collecting Metric 2.7.1**

**Number of High Value Asset (HVA) Systems and Authentication**

**Where Do I Start?**

1. Using the information collected in 2.7, identify the number of HVA systems that do not enforce users to authenticate through the machine-based or user-based enforcement of a two-factor PIV credential or other NIST 800-63 r3 IAL3/AAL3 credential.
2. For each of these systems, work with the System Owner and ISSO to determine if the system has been granted a security waiver due to an approved audit or similar agency risk acceptance procedure. These forms may exist as artifacts within the Authority to Operate package associated with the system’s FISMA ID. Record this number for **Metric 2.7.1.**

# **Next Steps**

Congratulations! You’ve collected all the data for the FISMA ICAM-related metrics.

As a reminder, your agency is required to report against FISMA metrics **every quarter**.

**Per the released memo**[M-18-02](https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-18-02%20%28final%29.pdf)**, the reporting deadlines are:**

|  |  |  |
| --- | --- | --- |
| **Reporting Period** | **Deadline** | **Responsible Parties** |
| FY 2018 Q1 CIO FISMA Reporting | January 15, 2018 | CFO Act Agencies |
| FY 2018 Q2 CIO FISMA Reporting | April 16 2018 | All Civilian Agencies |
| FY 2018 Q3 CIO FISMA Reporting | July 16, 2018 | CFO Act Agencies |
| FY 2018 Annual CIO, IG, and SAOP FISMA Reporting | October 31, 2018 | All Civilian Agencies |

We value your feedback - please send us an email at [icam@gsa.gov](mailto:icam@gsa.gov) to let us know if this guide was helpful and if you have any tips on how to improve it!