CONTINUOUS DIAGNOSTICS AND MITIGATION PROGRAM

IDENTITY AND ACCESS MANAGEMENT – Who is on the Network?

OVERVIEW OF IDENTITY AND ACCESS MANAGEMENT

The Cybersecurity and Infrastructure Security Agency's Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of government networks and systems. The CDM Program provides cybersecurity tools, integration services, and dashboards to participating agencies to help them improve their respective security postures. The CDM Program ultimately reduces the threat surface and improves federal cybersecurity response through four capability areas: Asset Management, Identity and Access Management (IDAM), Network Security Management, and Data Protection Management.

The IDAM capability is intended to manage the access and privileges of agency network users. Managing who is on the network requires the management and control of account and access privileges, trust determination for people granted access, credentials and authentication, and security-related behavioral training. IDAM is deployed within the CDM Program through four component capabilities: trust determination for people granted access (TRUST), security-related behavioral training (BEHAVE), credentials and authentication (CRED), and management and control of account and access privileges (PRIV). These four capabilities have significant interdependencies and are managed together as part of the IDAM capability area. IDAM encourages enhanced cyber hygiene through the utilization of identification, authentication, and authorization.

BENEFITS OF IDENTITY AND ACCESS MANAGEMENT

The CDM Program implements the IDAM capability to properly identify and validate users needing to access network resources and information. IDAM allows agencies to validate identities so that the right individuals have access to resources and information at the right time. This capability provides visibility for privileged and non-privileged users. Network users are verified using a credentialing mechanism (digital certificate, personal identity verification [PIV] card, etc.) that contains their user authentication.

IDENTITY AND ACCESS MANAGEMENT CAPABILITIES

The following four IDAM capabilities have significant interdependencies that must be coordinated closely to ensure full understanding of who is on the network:

Trust determination for people granted access

The TRUST capability reduces the loss of availability, integrity, and confidentiality of data by aggregating and validating information on user identity. This capability determines whether a user will be given access to systems and credentials. TRUST ensures that attributes such as user background investigations and related determinations are vetted, current, and monitored per agency policies and applicable statutes.

Security-related behavioral training

The BEHAVE capability ensures that authorized users have appropriate security-related training. This capability applies parameters around training associated with IDAM. BEHAVE mandates that agencies train their employees, track those who have been trained, and deny network access to those that have not been trained.

Credentials and authentication

The CRED capability verifies that only those with proper credentials are allowed access to systems, services, facilities, and information. CRED also ensures that credentials are properly monitored and renewed by agency policies. CRED helps agencies make certain that access is assigned to, and only used by, authorized users that need access to perform their job functions.

Management and control of account and access privileges

The PRIV capability establishes the privileges associated with the credentials and, in turn, the individual or service. This capability provides agencies with insight into the risks associated with authorized users being granted excessive privileges to facilities, systems, and information. The PRIV capability reduces an agency's risk by helping to ensure that authorizations and accounts do not exceed privileges required by a user's job function.

CURRENT STATE OF CDM IDENTITY AND ACCESS MANAGEMENT DEPLOYMENT

IDAM has been largely implemented at all agencies, and plans are underway to continue to adapt the above capabilities to include mobile and cloud environments. The CDM Program will continue working with its agency partners to identify and prioritize the deployment of IDAM capabilities when necessary. Ultimately, IDAM data will be reported to the CDM Agency Dashboard (which enables agencies to manage authorized users) and the Federal Dashboard (which provides summary information about account privilege management across the Federal Government).

For more information on IDAM capabilities or the CDM Program, please contact the CDM Program Management Office at CDM@cisa.dhs.gov.