



Fact Sheet

Privilege Management and Data-Level Access Control Pilot

PRIVILEGE MANAGEMENT AND DATA-LEVEL ACCESS CONTROL PILOT

- The Program Manager for the Information Sharing Environment (ISE) is exploring the use of privilege management technologies to enhance the quality and timeliness of information sharing across multiple jurisdictions and to ensure relevant information is made available more quickly to authorized users. These technologies will allow the ISE to accurately and uniformly enforce policy rules, while also supporting different jurisdictional policies and procedures resulting in increased accountability and trust within the ISE.
- Information flow within the ISE is presently controlled mostly by operational and management procedures. The technical controls to be developed in the Privilege Management and Data-Level Access Control Pilot will add more protections and accountability, and provide a means to give the right information to authorized users at the right time while complying with and enforcing Federal, State, local or tribal data access policies.
- Privilege management technologies permit or deny the requests of authorized *users or processes* (FBI analyst, State police, emergency responder, analytic software, etc.) to perform an *action* (read, write, share, etc.) on a *resource* (database, data element, network, NIEM IEPD data element, etc.). Policy decision and enforcement technology then uses this information to make an access control decision. The privilege management technology does not require one universal policy to be applied to all Fusion Centers; instead, this technology identifies the relevant policies to be applied to a particular request and reconciles these relevant policies to render a single access control decision.
- In July 2009 the Program Manager, Information Sharing Environment (PM-ISE) and the Department of Commerce's National Institute of Standards and Technology (NIST) signed a Memorandum of Understanding (MOU) to conduct a one-year Privilege Management and Data-Level Access Control Pilot.
- The Privilege Management and Data-Level Access Control Pilot focuses on evaluating the benefits of Privilege Management technologies, developing the tools needed to express and enforce data access control policies, ensuring interoperability of ongoing ISE-related standards efforts, providing a reference implementation, and accelerating the rate of adoption of these new technologies.
- These technologies are policy-neutral and can enforce any access control model (i.e. Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), Separation of Duties, Discretionary Access Control (DAC), Mandatory Access Control (MAC), Authorized Use, Chinese Wall, etc.). Privilege management technologies can reconcile

multiple policies to render an access control decision without requiring a one-size-fits-all policy to be adopted by all Fusion Centers.

PRIVILEGE MANAGEMENT BENEFITS

- Privilege management and data-level access control technologies offer a number of benefits to the ISE and support a number of business drivers, including:

Business Driver	Privilege Management Technology
Greater information sharing stemming from increased trust.	Local policies are enforced for access control decisions consistent with ISE-G-108 (IdAM Framework)
Accurate and uniform enforcement of policy rules.	Policy expressed in machine-readable format, repeatable, auditable, and testable.
Support for different jurisdictional policies and procedures, no need for a “one size fits all” policy.	Policies can be selected and enforced based on who is providing and who is requesting the information.
Relevant information becomes available in a timelier manner.	Access control decisions are made in real-time, authorized users have access as necessary, and required. Policies can change with situational means.
Increased accountability.	Authorized user requests and access control decisions are stored in audit logs

BACKGROUND ON THE INFORMATION SHARING ENVIRONMENT

- The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended, calls for the development of an ISE to facilitate the sharing of terrorism and homeland security information among Federal, State, local, and tribal governments and, as appropriate, foreign governments and the private sector. As part of implementing the Information Sharing Environment (ISE), the law requires the Program Manager to describe the functions, capabilities, resources, and conceptual design of the ISE, and the impact on the enterprise architectures of participating agencies.
- The IRTPA calls for the ISE to employ an information sharing and access management approach that controls access to data rather than just systems and networks, without sacrificing security; facilitates the sharing of information at and across all levels of security; incorporates protections for individuals’ privacy and civil liberties; and incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls.