

2015 Achievement Awards Virginia Association of Counties

APPLICATION FORM

All applications must include the following information. Separate applications must be submitted for each eligible program. **Deadline: June 1, 2015.** Please include this application form with electronic entry.

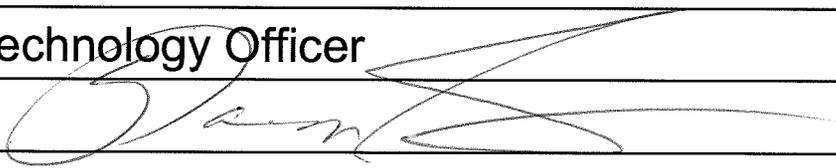
PROGRAM INFORMATION

Locality: Fairfax County
Program Title: Regional Identity and Access Management Service (IAMS)
Program Category: Regional Collaboration

CONTACT INFORMATION

Name: Michael Dent
Title: Chief Security Officer
Department: Department of Information Technology
Complete Mailing Address: 12000 Government Center Parkway, Suite 527, Fairfax, Virginia 22035
Telephone # 703-434-4778 Fax # 703-653-1300
E-mail: Michael.Dent@fairfaxcounty.gov

SIGNATURE OF COUNTY ADMINISTRATOR OR CHIEF ADMINISTRATIVE OFFICER

Name: Wanda M. Gibson
Title: Chief Technology Officer
Signature: 



Title: Regional Identity and Access Management Service (IAMS)

Program Category: 11 - Regional Collaboration

State the problem, challenge or situation faced by the locality and how the program fulfilled the awards criteria (innovation, partnering or collaboration and a model for other localities). Tell how the program was carried out, including financing and staffing, and the program's results.

Typically, as the number of IT applications grows in organizations, the number of usernames and passwords that an individual user must maintain grows along with it. This can lead to the potential for access to systems by unauthorized personnel because authorized users tend to reuse passwords across multiple applications, rarely changing them (depending on enforcement policy), and often writing them down on paper near their workstation. Such practices leave the organization, its data and applications, vulnerable to access by unauthorized persons, whether internal or external to the organization. The potential for compromise through this manner was a real risk when granting access to regional, public safety applications across the NCR used by thousands of Northern Virginia government personnel supporting fire, police, emergency management, public health, and other disciplines. A solution was required that facilitated uncompromised, shared access to disparate systems with the partners being able to retain their autonomy in administering users through their existing user access management systems.

The target audience for the regional Identity and Access Management Service (IAMS) is any governmental entity which has IT applications deemed necessary for access by personnel from a variety of partner organizations (government, commercial, non-profit, etc.), regardless of network reachability.

IAMS leverages existing user information, managed and protected by local governments, and fuses the authenticated identity with permissions to applications via the NCRnet, a private network interconnecting localities. Securing communications using accepted protocols between IAMS and the end user repositories in the localities ensures higher confidence in the system. Furthermore, when a user account is disabled by the managing local government (employee release, retirement, etc.), access to regional applications is terminated immediately. This allows agencies and emergency support functions across the NCR to share information and data in order to leverage resources to support mutual aid incident response across boundaries.

IAMS leverages the NCRnet, an essential component of the interoperability initiative used by regional applications such as the NCR Fire and Rescue Department CAD2CAD Service, to onboard localities and facilitate interconnection. Each local government interconnects to the NCRnet and manages the inbound and outbound traffic using a firewall it controls. This interoperable network asset, predicated on governance and adopted policies, opens up a variety of possibilities for cross-government communication, collaboration, and efficiencies for public safety.

IAMS relies on state-of-the-art capabilities, federal and industry security guidance and practices for access control and identity validation using a federated architecture and policy management model. It uses a virtual directory to interconnect with existing partner Microsoft Active Directory (AD) systems using digital certificates managed by each partner. This “least common denominator” connectivity approach uses the Lightweight Directory Access Protocol over Secure Sockets Layer (LDAPS) to ensure encryption of the read-only transaction to lookup and authenticate the user. The AD system of each locality is identified by a locality-issued digital certificate thereby establishing trust.

In addition to LDAPS, some localities deployed Microsoft AD Federation Services (ADFS) within their organization, simplifying integration with IAMS. The end user of a locality is directed to a sign-in page managed and operated by the locality, increasing trust with the organization, end user confidence,

and resiliency from dependencies on other services. This token-based form of authentication uses Security Assertion Markup Language (SAML) and never passes raw, user identity data (e.g., username and password) through IAMS.

Customizable workflow processes support request submission, review, and approve/reject functions for access to IAMS-enabled applications. While providing a centralized portal for end users, IAMS also decentralizes and streamlines the process for obtaining access; i.e., a single process marries the identification of available roles with authorized approvers. Supported by email notifications, user provisioning to applications can occur within minutes rather than days. This is essential in a fast-paced, public safety environment when new personnel often need to fill roles on a dynamic basis.

In production since June 2013, IAMS has the capacity for authentication of more than 50,000 personnel utilizing established interconnections with local governments. Using the GetAccess web-based application, IAMS has simplified end user access and reduced the administrative burden for the Northern Virginia Emergency Response System (NVERS), an early adopter of the service. IAMS has provisioned more than 200 users, including personnel from police, fire, emergency medical services (EMS), health, emergency management, 9-1-1, and other support disciplines, across Northern Virginia governments, the Virginia Department of Emergency Management, and the Northern Virginia Hospital Alliance, for streamlined access to the NVERS portal. NVERS staff no longer needs to perform identity validation processes or password resets for end users. All registration, request for access to NVERS, and password reset responsibilities are handled by IAMS instead of NVERS.

Additionally, IAMS has removed the administrative burden of username/password management from at least four additional, regional applications possessing more than 7,500 unique users from public safety entities in the NCR. As a result, application owners can focus on granting access to requesters instead of time consuming processes associated with validating user authenticity and resetting user passwords thereby reducing administrative transaction times and costs. End users can focus on using

critical applications to do their jobs, relying on a strong, complex, and frequently changed password (managed by the locality) rather than multiple or weak passwords, thereby improving employee efficiency, security and service to citizens.

One goal of the IAMS project was to take advantage of the investment in the existing interconnections between NCR entities to allow access to disparate governmental systems and data through automated trusted sources. In practice, IAMS provides seamless end user access utilizing an accepted federated service that leverages existing partner owned internal access management systems without the need for additional investment by the partners. IAMS is a key aspect of the NCR Interoperable Communications Infrastructure (ICI) facilitating public safety data sharing for real-time situational awareness and faster, more coordinated incident response for citizens. To date, in Northern Virginia IAMS has integrated with Fairfax County, the City of Fairfax, Prince William County, Loudoun County, and the City of Alexandria. Additionally, integration via ADFS with Arlington County is completed and the towns of Herndon and Vienna are actively engaged in IAMS planning.

Another goal, proliferation of the IAMS capability to existing and planned public safety applications, is well underway. Integration with the NVERS web application has been operational since June 2013. IAMS integration with the MugShots (NOVARIS) application is in place, allowing police personnel from participating localities to access this critical tool via their desktop workstation or other locality-managed mobile device.

Federal Urban Area Security Initiative (UASI) funds, issued by the Department of Homeland Security, were responsible for establishing the initial pilot of IAMS, its current operations, and the operations of the NCRnet.

Include a short overview of the program (no more than one page double-spaced) that can be used as a quick reference guide for judges.

The Identity and Access Management Service (IAMS) is an interoperable, authentication service providing secure access to applications and data for 50,000 authorized end users in the National Capital Region (NCR), which includes thirteen (13) localities in Northern Virginia supporting public safety and emergency response functions. IAMS integrates existing, independent data repositories using accepted industry protocols to allow end users to present one identifier (e.g. email address) and password, managed by their respective organization, to access regional applications and data. IAMS also supports registration by users external to the localities such as state and federal entities. Through a simple yet robust registration process, key information about the user is captured and viewable by various approvers for authorization.

This shared service effectively eliminates the need for applications and users to manage individual sets of usernames, passwords, and the permissions assigned to a user within the application. Furthermore, when the managing partner government disables a user account, access to regional applications is terminated immediately.

Include a brief summary of the program (3-4 paragraphs) that could be used for press releases, brochures, etc.

As part of the National Capital Region Interoperability Program (NCRIP), public safety agencies have developed regional data sharing applications to support operational coordination, situational awareness, and regional planning for catastrophic events. With thousands of local government personnel in the region, provisioning and controlling access to applications and data while maintaining a secure environment presents administrative and risk-management challenges. The solution, the Identity and Access Management Service (IAMS), implemented as part of the NCR Interoperable Communications Infrastructure (ICI), permits users within the member NCR jurisdictions and partner entities to access regional applications via their locality-issued credentials for secure authentication and authorization to regional applications across the NCRnet - the regional, fiber-optic network that is owned and operated by the NCR partners.

The NCR is comprised of thirteen (13) localities in Northern Virginia, the District of Columbia, and several jurisdictions in Maryland. The region is also home to many state and federal agencies and a population of nearly six million citizens who daily may move between localities which presents unique challenges for emergency preparedness planning and incident response. The goal of interoperability is to provide first responders with the ability to communicate with regional partners in real-time to mitigate risk and provide better response to emergency events. IAMS is a foundational piece of the interoperability solution in the NCR, providing end users with secure, identity-based access to systems, applications and data from any location or device and providing regional leadership with the functionality needed to maintain compliance with the Department of Homeland Security (DHS) cyber security standards. IAMS leverages existing investments in network infrastructure and technology to connect existing Microsoft Active Directory (AD) systems in the local governments. This approach

provides a framework of processes that increase compliance, security, and user productivity while reducing the administrative burden and costs on application owners and end users.

In its first year of operation, IAMS had services in place to authenticate over 50,000 users from over ten (10) NCR localities. While the initial deployment brought in major NCR entities with high concentrations of public safety personnel and active interoperable applications, with on-going proliferation many existing and planned public safety and other emergency support applications will be integrated. The enthusiasm of regional application owners and users who have embraced the IAMS solution validates IAMS as the means to enable the trusted partnership among disparate organizations and systems.