

## MEMORANDUM

**Date:** January 25, 2007

**To:** Chair and Members, COG Chief Administrative Officers Committee

**From:** Chair, COG Chief Information Officers Committee

**Subject:** Consideration of Establishing a National Capital Region Interoperability Services Program

The purpose of this memorandum is to present for consideration and approval by the COG Chief Administrative Officers Committee a proposal for the Council of Governments to (1) conceptually approve development of a National Capital Region interoperability services program, (2) designate of the CAO Committee as an interim governing body of this program on behalf of COG and its member governments, and (3) authorize COG, on behalf of the CAO's, to assume the responsibility of interim contracting and administrative agent.

### Timing

Action by the CAO's is desirable on February 7, 2007, and the COG Board on February 14, 2007, in order to facilitate use of FY 2005 UASI funds authorized for initial development of such a regional interoperability program. FY 2005 UASI funds must be utilized by March 2007.

### Background

In early October 2006, the MetroCIO's (CIO Committee) approved the establishment of the NCR Operational Framework Working Group (NOFWG or Working Group) to begin the effort of constructing a region-wide entity that would provide service and support to the applications, data exchanges and infrastructure created by the National Capital Region Interoperability Program (NCRIP or Interoperability Program) as the interoperability component of the NCR's homeland security plan. The CIO Committee, working with relevant ESF's and the NCRIP Project Management Office (PMO) recognized the high priority that the Department of Homeland Security, the NCR Senior Policy Group and the CAO's have assigned interoperability.

- At its October and November 2006 meetings, the CIO Committee considered the proposed structure, timing and processes leading to a long term entity that would coordinate delivery of region-wide service in support of an interoperability services program. This would establish a single point of contact that all NCR jurisdictions participating in the interoperability services program would use to report problems, request service, or seek support for the operation of applications, data exchanges and infrastructure.
- On November 14, 2006 the CIO Committee unanimously passed a resolution authorizing transmission of the substantive recommendation of the CIO

Governance Committee to establish a governance entity for interoperability services, to the CAO Committee.

### Two Stage Implementation

Because of the complexity of assembling a region-wide service delivery mechanism and the very short term deadline of March 2007 related to the expenditure of FY 2005/6 Homeland Security monies that have been allocated to the NCR for interoperability, and the pending completion of live data exchanges as part of the Data Exchange Hub (DEH) project, the CIO Governance Committee recommends a two-tier development process:

- By March 2007 creation of an interim governance entity to be composed of key managers and chief administrative officials of the NCR to provide the legal vehicle for the signing of region-wide interoperability contracts and region-wide grant applications – if appropriate – relating to the delivery of these services. The attached draft proposed COG resolution conceptually approves development of the interoperability services program as a COG-supported activity and establishes the CAO Committee as that interim body; and
- A key outcome of the work of the interim governance entity should be recommendations for the establishment of a long-term entity, including its governance, procedures, and intermediate and long term financing and sustainability.

### Need for a Governing Body

After conversations with many stakeholders, with the COG General Counsel, and others, the CIO Committee has determined that there needs to be an interim regional entity that will support the delivery of interoperability services. This entity is needed to:

- Establish and provide oversight of applicable regional policies governing interoperability services after consultation with the COG CIO Committee, EMA, Police, Fire and Public Health Officers and others as appropriate;
- Recommend a long term governance entity/structure for interoperability services and to recommend to that entity a long-term provider of services;
- Identify and assess methods of cost sharing among participants and users of these systems, and make recommendations, to such participants, users, the long term entity, and COG.
- Determine the priorities for the use of the systems created or designated as part of the interoperability services and determine how they will be set and managed;
- Set policies about systems quality control and on-going management of system quality; and
- Authorize grant applications and contracts as appropriate to carry out the mission of interoperability services as may be defined.

## Privacy and Security of Data Exchanges

The interoperability data function is a critical part of the NCR's mission to provide protection against all-threats situations. The exchange of data between and among jurisdictions and non-government organizations which are part of the NCR potentially exposes that data to privacy and security issues which, if not properly managed by the NCR's interoperability service function, could have serious consequences.

The Security Policy utilizes the management, operational and technical security control family developed by the Computer Security Division of the National Institute of Standards and Technology (NIST). Documentation was developed by NIST and contractor personnel, released for public review by the global security community, and then revised to address feedback prior to being released as official guidance. Guidelines have been established in multiple areas including risk management, security metrics, firewall implementation, and security control.

Each data exchange shall be evaluated from a security perspective based on the threats, vulnerabilities, and risks associated with the data exchange. The selection and application of management, operational, and technical security controls shall reduce the identified risks to a level acceptable to the interoperability services program and partners involved in the data exchange. As threats evolve, the risk assessment shall be refreshed to determine the effectiveness of existing security controls and to identify additional security controls.

Each component shall possess one or more security controls that shall, either in whole or in conjunction with other controls, ensure the confidentiality, integrity, and availability of data handled by the interoperability services program. Privacy controls shall also be identified based on the nature of the information being shared. The Security Policy is being developed recognizing that a loss or breakdown in data privacy controls can lead to public embarrassment, legal ramifications, and loss of citizen confidence in their local government.

Prior to March 2007, the DEH project (a component of the NCRIP) will complete live data exchanges for WebEOC and computer aided dispatch (CAD) applications.

## Organizational Proposal for an Interim Structure

The purpose of this entity is to effectively and efficiently sustain the operation of NCR interoperability capabilities, without excessive or burdensome financial or operational reliance on any one jurisdiction.

- The interim entity's title is proposed as the **Interoperability Council of the Metropolitan Washington Council of Governments** or Interoperability Council;
- The Interoperability Council's membership is recommended to be composed of the CAO's of each participating COG jurisdiction;
- The Interoperability Council will receive periodic recommendations from the CIO, EMA, Police, Fire and Public Health Committees of COG and may also

- receive recommendations or comments from other stakeholders on matters pending; and
- The Interoperability Council key duties, consistent with the section "Need for a Governing Body," above, will be spelled out in a Charter or Bylaws approved by the COG Board.

### Budget and Financing

To finance the operation of the interoperability services program between March 2007 and September 2007 when awarded FY 2007 HSGP monies are expected to be received, the NOFWG is working to develop an estimated budget for this period. It is anticipated that the efforts March 2007 through September 2007 can be supported from available FY 2006 UASI resources.

Amounts required for NCR-IS operations October 2007 to September 2008 will take into consideration warranty periods. The determination of the amount that is likely to be an NCR locality responsibility has not been calculated.

In addition the CIO Committee and COG will be preparing an application for FY 2007 UASI NCR interoperability monies for interoperability services operations in FY 2007.

The CIO Committee and COG staff will assemble fiscal information and a reasonable estimate of resources needed to sustain operations and maintenance of regional infrastructure, data exchanges and applications and to provide information about the possible local jurisdictional budget impacts. A proposed budget will take a look across several years, taking into consideration plans about how the continued deployment of the interoperability projects will occur, how warranties will be applied and the nature and scope of services acquired with grant monies.