



## Credentialing Support Annex

Credentialing is a critical component in any jurisdiction's response to emergencies. It is imperative that authorized individuals be able to gain quick access to a site without having to undergo laborious and time-consuming background checks. No less important is the need to deny site access to individuals with questionable or non-mission critical motives, whose presence would be a hindrance at best.

In the Washington metropolitan area, where it is not unlikely that a regional incident or regional emergency could occur that requires assistance from neighboring jurisdictions, a reliable and regionally understood credentialing system is vital. In the optimal circumstance, a system would allow unimpeded site access to authorized responders from all metropolitan regional partners and federal partners.

The credentialing systems used by COG jurisdictions vary in their design, stage of development, and sophistication. Some jurisdictions have no formal credentialing system in place, relying instead on face or name recognition. Others are developing or reworking their credentialing system. The District of Columbia has recently launched a new credentialing initiative that incorporates state-of-the-art technology to facilitate site access for authorized responders. This Annex summarizes the major elements of the District's credentialing initiative.

### I. Purpose

The purpose of the District of Columbia Credentialing Initiative is two-fold:

To develop tamper-proof IDs for all District employees that will be recognized by federal and regional public safety partners and that will permit critical employees access to the District's Emergency Operations Center and other operation and response areas in the case of an emergency.

To develop mobile credentialing facilities that can be rapidly deployed in the event of an emergency.

These projects are described in more detail below.

### II. Employee IDs

The District has recently redesigned the standard ID badge issued to each employee. Although the primary purpose of the badge is to identify an individual as a District employee, the badge also contains information that further designates whether an individual is critical to any District emergency response.

The front side of a standard ID badge contains the following common elements:

**Expiration Date** – date access privileges expire

**Picture** – picture of the card holder

**Name** – full name of the card holder

**Employee Type** – District employees are designated as one of five categories:

- *Public Safety* – employees directly involved in ensuring public safety (excluding administrative and support staff)
- *Health Services* – employees directly involved in all health services (excluding administrative and support staff)
- *Employee* – general full-time classification (including administrative and support staff)
- *Temporary/Volunteer* – employees on loan from federal agencies, volunteers, or part-time employees
- *Contractor* – full-time and part-time contract employees

**Color Code** – These codes correspond to the employee types above, and are used to quickly distinguish employee type from a distance

- *Black* - Public Safety
- *Yellow* - Health Services
- *Blue* - Employee
- *Green* - Temporary/Volunteer
- *Red* - Contractor

**Agency** – agency of employment

**Security Hologram** – hologram to prevent tampering or fraudulent reproduction

**District Flag**

**Watermark** – matte finish overlay of the District government flag that covers the entire card to prevent fraud; visible when card is held at an angle

The elements contained on the back side of a standard ID card, listed below in order of their appearance on the card, depend on whether an employee is critical to any District emergency response. (Such elements are denoted with an asterisk.)

**Emergency Designation\*** – contains the words “EMERGENCY CRITICAL” in big block letters, and identifies employees, of any type, as critical to any District emergency response

**Name\*** - employee’s full name should be identical to the name printed on the front of the card

**Agency Symbol\*** - symbol of the agency with which an employee is affiliated

**Verification Number\*** - hotline to DCEMA for verification of the individual’s access privileges

**Bar Code\*** - unique number associated with the card holder that contains employee data

**Unauthorized Use Statement** – statement that unauthorized or fraudulent use of the card is punishable under US and District code

**Property Disclaimer** – address to which lost cards should be returned

**Tier Designation\*** - identifies the employee's level of criticality:

- *Executive* – highest criticality
- *Tier 1* – highest criticality
- *Tier 2* – mid-level criticality
- *Tier 3* – lowest criticality

**ESF Designation** – denotes one or more emergency support functions to which the employee is assigned; if the employee is critical to all ESFs, the designation will read “All ESFs”

The purpose of an “EMERGENCY CRITICAL” designation is to facilitate the transit of the card holder to the perimeter of the site. Such a designation would inform police and other security personnel assigned to restrict access to the city that the card holder should be allowed to pass. Once at the site, the card holder would still have to be screened and issued a credential before site access would be permitted.

### III. Mobile Credentialing Facilities

As part of its credentialing initiative, the District is arranging for the provision of two mobile credentialing facilities that could be deployed without delay in the event of an emergency. Each facility would be a tent shelter complete with a generator, electric power, and interior environmental control.

Each facility would contain a mini-Local Area Network, consisting of a server with a ruggedized case, ten work stations, one laptop, one camera, and one or more card printers. Networked bar code readers at all perimeter access points would track the entrance and exit of response personnel.

This page intentionally left blank.