

---

# Comprehensive Resource Management and Credentialing System

---

Policy

---

South Dakota Office of Emergency  
Management

---

# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v1Dec14

### Table of Contents

- Policy Outline..... iv**
- Website Information ..... v**
  - Privacy Agreement.....7
  - Access and Permissions.....7
- Policy..... 9**
- Procedure..... 10**
  - Identification..... 10
  - Identification / Credential Card..... 10
  - Identification / Credential Card Appearance ..... 11
    - Front of Card..... 11
    - Back of Card ..... 15
      - Verification ..... 18
      - Revocation ..... 18
      - Card Disposal..... 18
- Deployment ..... 19**
  - Access ..... 19
  - Affiliation ..... 19
  - rapidTAG..... 19
    - Personnel rapidTAG..... 20
    - Equipment rapidTAG..... 21
    - Company rapidTAG ..... 22
  - Passport Tags..... 23
- Attachments**
  - Attachment 1: Organization Name Template ..... 25
  - Attachment 2: Law Enforcement Card Definitions..... 26

# **Comprehensive Resource Management and Credentialing System**

## **Resource Manager Web Credentialing Policy**

**v1Dec14**

This document was drafted by the Comprehensive Resource Management and Credentialing System (CRMCS) project advisory committee. This committee was established by the South Dakota Office of Emergency Management (SDOEM) and includes representatives from SDOEM, Midwest Card and ID solutions, Office of Homeland Security, Department of Public Safety, South Dakota Fire Marshall's office, Department of Health, EMS and each South Dakota Homeland Security Regional Council. This group will meet annually to review and revise this document. Email [Laurie.Morrison@state.sd.us](mailto:Laurie.Morrison@state.sd.us) or telephone 605-773-3231 to request a copy.

### **Policy time line:**

**Drafted: 05 Dec 2014**

**Finalized: 14 Jan 2015**

**Revised:**

**Revised:**

**Revised:**

**Revised:**

# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v1Dec14

### Policy Outline

The Comprehensive Resource Management and Credentialing System (CRMCS) is a tool created to enhance the resource management efforts of county, city, and state organizations. This tool allows emergency response agencies, county emergency managers, state and private/not for profit resource managers the ability to credential personnel, provide information on availability of assets and personnel prior to and during an emergency, the ability to track those assets on scene, and near real-time incident visibility via the internet. The resource information is housed in **resourceMGR web™** (RMW) and the **interTRAX® exchange** system.

This credentialing policy outlines the establishment and intended use of the credentials that are to be stored within the CRMCS and printed on the credential cards.

The CRMCS provides a platform to facilitate the following Homeland Security strategic goals:

- Expand, strengthen, and / or sustain capabilities and resources, ensuring a flexible, reliable, and effective response
- Resource Tracking
- Credentialing of Personnel
- Improve / enhance resource management and accountability
- Establish and improve a system for developing and deploying specialized resources
- Continue and enhance local, regional, and inter-state collaborative initiatives for prevention, preparedness, response, and recovery
- South Dakota is part of the EMAC and will continue to support its efforts
- Develop a working template to deploy logistical support to communities post disaster

The CRMCS supports the South Dakota Emergency Operations Plan (SEOP) by providing for consistent application of ESF standards in preparation for response to and recovery from an incident. The CRMCS provides accountability for personnel and resources on-scene at an incident using the **interTRAX® exchange** system or manual accountability. It provides the opportunity to shorten the timeline for response and improve situational awareness of available local and state resources.

# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v1Dec14

### Website Information:

resourceMGR web™ – [www.southdakota.responders.us](http://www.southdakota.responders.us)

WebEOC – <https://webeoc.sd.gov>

South Dakota Office of Emergency Management -  
[http://dps.sd.gov/emergency\\_services/emergency\\_management/](http://dps.sd.gov/emergency_services/emergency_management/)

bReady – <http://bready.sd.gov>

This page left intentionally blank

# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v4Jan2013

### Resource Manager Web Privacy Agreement:

**ATTENTION: resourceMGR web™ (RMW) contains personal information on individuals whose information is stored in it. The use of this information is strictly for Emergency Management purposes inside the State of South Dakota. By entering into this system, you agree to not release any personal information to include, but not limited to: names, home addresses, telephone numbers, or personal medical information outside of RMW without prior written approval of SDOEM – Director, Tina Titze or Deputy Director – (vacant).**

Requests for information on this system from any outside entity should be forwarded to Laurie Morrison for its consideration. Questions on this policy should be directed to Laurie Morrison at email: [Laurie.Morrison@state.sd.us](mailto:Laurie.Morrison@state.sd.us) or telephone: 605-773-3231. Any violation of this policy may subject you to the loss of use of this system.

### Access and Permissions for RMW:

***A county CRMCS lead, typically the emergency manager, as well as agency representatives must receive training on the system before being granted access to RMW. Once training is completed the county lead/agency representative will be given a username and password and granted permissions for the organization(s) within their jurisdiction.***

Access to information in RMW is managed in a parent-child hierarchy. See figure 1:

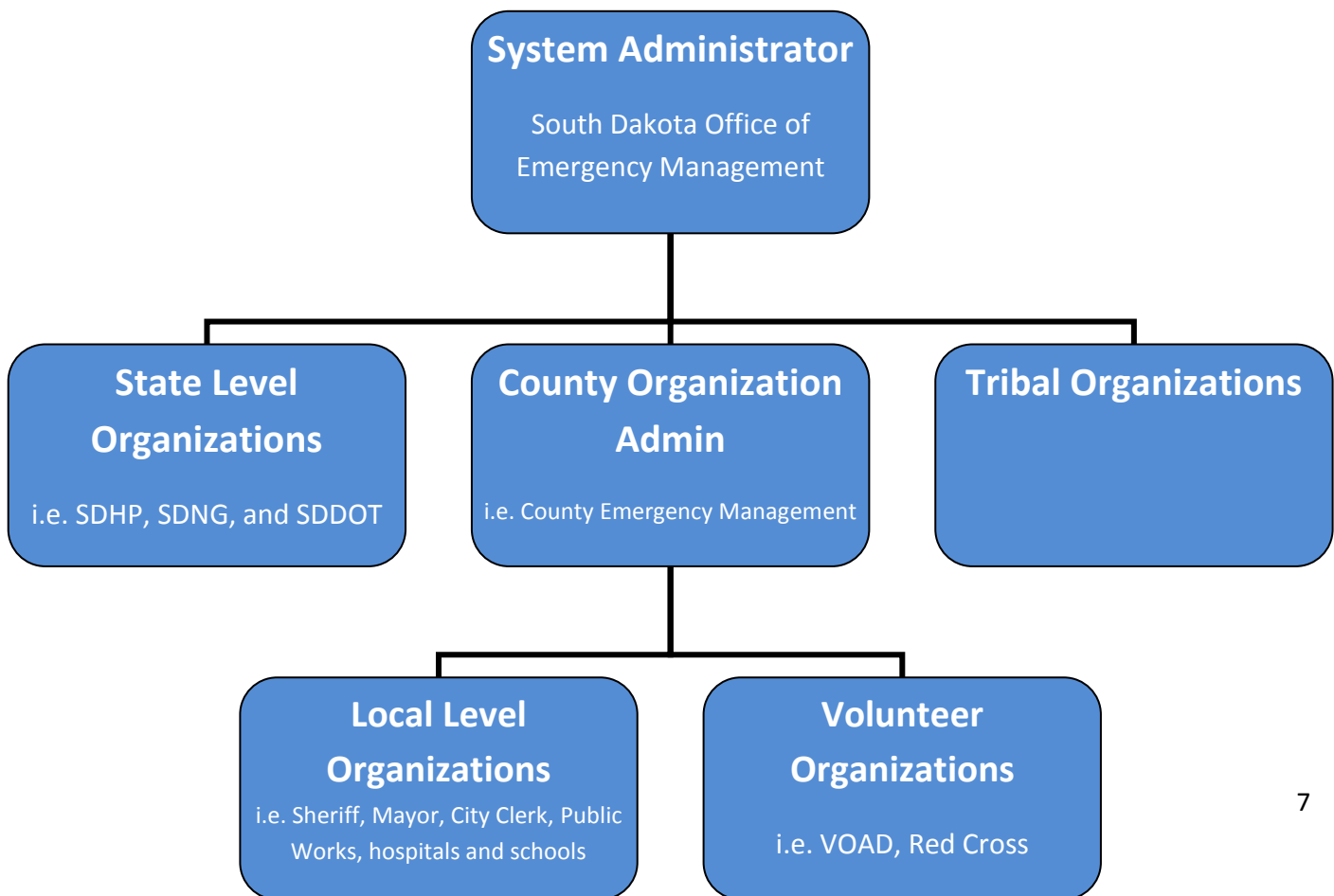


Figure 1

# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v4Jan2013

There are five levels of permission in RMW. From greatest system responsibility to least they are: Resource Admin, Admin No Delete, Data Input / Print, View Only and Incident View.

**Resource Admin:** This allows the user admin access to a specific organization. They can create, read, update, delete, and print all information in that organization only.

**Admin No Delete:** This allows the user the same permission as the Organization Admin EXCEPT that they cannot delete any information for a specific organization. This would be used to ensure information integrity by only allowing the Organization Admin the permission to delete information.

**Data Input / Print:** This permission allows for data entry without admin permissions for a specific organization. An example of who could be granted this permission would be part-time staff or intern whose only responsibility would be to input data or print Identification / Credential Cards.

**View Only:** This allows for View Only of information for a specific organization EXCEPT for medical data. An example of who could be granted this permission would be SDOEM Regional Coordinators or someone from outside that specific organization like a neighboring county.

**Incident View:** This allows for incident specific reporting and situational awareness. (Incident View will be granted for the Organization of "South Dakota" only.)

Permissions are granted for specific organizations. A user will not be able to see data in an organization they do not have permission to view. Permission follows the parent-child hierarchy, in that, a user can only see data in organizations that are below (children) of the organization that user has permission to if granted permission to "include all children". This is done to ensure visibility to organizations in the user's jurisdiction.

**In order to view another organizations data the user must make a request to an administrator with permission at least one step above (parent) of the organization they are requesting access to.**

Different levels of permission can be granted for different organizations. A user can have organization admin access to one (or more) organization(s) and have view only (or other level) into another organization.



# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v4Jan2013

### I. Policy

A. The Secretary of the South Dakota Department of Public Safety authorizes the South Dakota Division of Emergency Management (SDOEM) to be the jurisdiction having authority, to develop, direct, and maintain a system of issuing cards to emergency personnel in South Dakota, in accordance with the National Incident Management System (NIMS).

B. SDOEM shall institute a program to grant authority to agencies and organizations to issue Identification / Credential Cards for persons in specific positions to be deployed for intrastate mutual aid.

C. There are specific certification and licensure requirements for numerous positions that people fill in response to a disaster. These positions fall under the licensing and certification authority of several state agencies in South Dakota. This policy is not an individual agency policy, but the coordination of those positions that individual agencies are currently providing credentials for.

D. Credentialing validates the identity and attributes (such as affiliations, skills, or privileges) of individuals or members of teams. Credentialing is essential to the emergency management community. It allows the community to plan for, request, and receive resources needed for emergency assistance. Credentialing ensures that personnel resources match requests and supports effective management of officially dispatched responders.

E. Credentialing involves providing documentation that identifies, authenticates, and verifies the qualifications of emergency response personnel. The FEMA NIMS standards call for typing of incident management personnel, emergency response providers, other personnel (including temporary personnel), and resources needed for emergency response.

F. The credential cards are the property of the agency / department that issues them. It is the responsibility of each individual participating agency/department to ensure their training programs adequately prepare personnel for the appropriate certification program. The Advisory Committee shall not oversee individual training programs or the training policies of any department as the responsibility for verifying a person's qualifications lies ultimately with the agencies / organizations that issue the card.

G. Requests for changes to be made to this document can be sent to [Laurie.Morrison@state.sd.us](mailto:Laurie.Morrison@state.sd.us) . This document will be reviewed and revised annually by the CRMCS project advisory committee.

## II. Procedure

### A. Identification

The State issued driver's license or ID number will be used as the "personnel ID" unique identifier for personnel in [resourceMGR web™](#).

### B. Identification / Credential Card (IDCC)

Authorized agencies shall issue IDCC based on the positions within one of the following eight discipline areas. **If an individual works for more than one organization, they will have an IDCC for each organization that they work for. One IDCC covering multiple organizations is not permitted due to liability and qualification management.** (More than one IDCC or passport tag is recommended if manual accountability is employed):

1. "Fire" shall be utilized for those individuals to be credentialed in Fire Fighting positions
2. "Law" shall be utilized for individuals to be credentialed in Law Enforcement Positions.
3. "Health & Med" shall be utilized for individuals verified to be credentialed in a Medical position.
4. "EM" shall be utilized for individuals to be credentialed in Emergency Management positions
5. "Vol" shall be utilized for individuals to be credentialed as Volunteers
6. "Gov" shall be utilized for Government positions
7. "Private" shall be utilized for those individuals to be credentialed as Private Industry
8. "Mil" shall be utilized by those individuals to be credentialed as Military members as determined by the South Dakota National Guard.

# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v4Jan2013

### C. Identification / Credential Card Appearance

#### 1. Front of Card

##### a) Picture

The IDCC shall not be valid unless a picture is included on the card.



(1) Photos should include head and shoulders and be on a white or blue background (DL or passport style photo). Hats are not to be worn. (Federal recommendation)

(2) Photos need to be cropped to meet the requirements of the system. An example is listed below. More information on how to crop photos is listed on the [www.SouthDakotaResponder.com](http://www.SouthDakotaResponder.com) website.

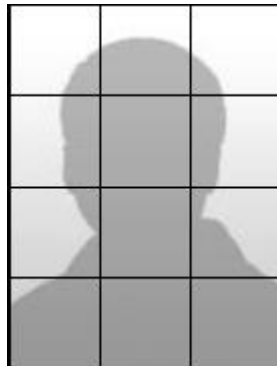
(3) Cropping Guide:

<http://southdakota.responders.us/resources/crmcs/cropping-guide/>

Photo Elements	Crop to 4:3 ratio	Resize to 640x480 (if needed)
----------------	-------------------	-------------------------------



Head, shoulders, no hat, and on a white background



3

4



480 pixels

640 pixels

# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v4Jan2013

### b) Organization Logo

There are three categories of logos that shall be used for an organization logo. Final decisions will be made by the system card issuer. Order of preference is as follows:

- (1) Organization specific Logo
- (2) City or County Logo (if applicable)
- (3) Nationally recognized logo (Fire, Public Health, EMS, Etc.)

### c) Rank / Title

This field will be designated for position titles. Some options will be preloaded into the system. If the NIMS job title is appropriate it should be listed here.

### d) Organization Name

If the organization is affiliated with a county, city or regional group, that affiliation must be noted in this field. The **Organization Name** field should have the name of the organization if it is a private group. This field is limited to a maximum of 25-28 characters including spaces. Only commonly accepted abbreviations will be accepted. This information will be tied to the header of the card. Whatever is entered here will be printed at the top of the card as the header.

### e) Issue Date

The **Issue Date** is to be set when the qualifications are verified. If a reprinted card is issued for the same individual it must contain the original issue date. (I.e. use existing issue and expiration date)

### f) Expire Date

The **Expire Date** is to be set on the day of printing, and shall not exceed 4 years from the issue date. **NO card is to be printed without an expire date.** The date can be set shorter than 4 years to expire at the same time as a qualification such as a license or certification. This does NOT include card re-prints for lost, stolen, or damaged cards. If a reprint card is issued for the same individual, it must contain the original expire date. At the end of the 4-year (or shorter) period, credentials and qualifications must

# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v4Jan2013

be reviewed and re-vetted. Only then can a new card be printed with a new Expire Date.

### g) Color Coding

Card colour scheme is set by each card design. These colours are not changeable. Schemes will be as listed in table 1:

### h) Text Classification

Clear-text classification is set by each card design. These classifications are not changeable. The purpose is to provide a non-color clear text definition of an individual's discipline. Classifications will be as listed in Table 1:

Table 1

Color	Discipline	Text Classification	Organization examples
Red	Fire	Fire	City Fire, County Fire, Volunteer Fire Services
Blue	Law Enforcement	Law	Police, Sheriff, Patrolman
Green	Medical	Health & Med	Verified medical personnel
Yellow	Emergency Management	EM	Designated EM offices, Recognized IMAT groups
White	Volunteer	Vol	Red Cross, CERT, MRC, Salvation Army, etc.
Gray	Government Officials and employees	Gov	Governor, Senator, Representative, State Agencies, County Commissioner, County Clerk, Dispatcher, (any state or local government employee not included in other discipline), Schools, Hospitals, etc.
Brown	Pre- Identified Private Industry Responders	Private	Electric Co., Gas Co.
Black	Military	Mil	National Guard members

# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v4Jan2013

### i) Personnel barcode

The barcode on the front of the card is automatically generated in Resource Manager. An example of the QR Barcode is below. (See the [resourceMGR web™ User Guide for more information on what is included in each item in the barcode](#)) It contains as a minimum:

- (1) Barcode Expiration
- (2) Organization Country Code
- (3) Organization State Code
- (4) Organization Type Code
- (5) Organization ID
- (6) Organization Name
- (7) Personnel ID
- (8) Last Name
- (9) First Name
- (10) Rank
- (11) Date of Birth



# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v4Jan2013

County Emergency Mgmt



### j) Other ID

Other ID is assigned in the software as an optional field. This can be used as place to display a radio number, patrol number, or any other pertinent reference number for that individual. (This is not an option on Passport tags)

### k) Security Features

The IDCC will not be valid without the EDI Secure Cardwaves hologram laminate. This laminate provides an additional level of security for the card. It also enhances the durability of the card.

### l) Footer

The Footer along the bottom of the card will read the name of the state / jurisdiction where the card was issued. This will be used to assist in identification when responders are called to cross jurisdictional boundaries and / or state lines for aid and assistance. The South Dakota IDCC will have "South Dakota" as the footer.

## 2. Back of Card

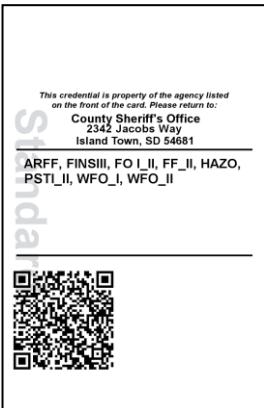
The back of the law enforcement IDCC will look different than all other cards. It will have the commission statement "THE HOLDER OF THIS CARD IS A COMMISSIONED LAW ENFORCEMENT OFFICER AND HAS STATUTORY POWERS OF ARREST AND IS AUTHORIZED TO CARRY A FIREARM" printed at the top of card. **This does not apply to any non-sworn employees of a law enforcement agency.**

### a) Qualification Field

The qualification field contains **qualifications** as identified by both the card holder, and the card holder's organization of affiliation. There is a high-to-low hierarchy in qualifications of Federal then State then Local. **State qualifications shall not supersede federal qualifications and Local qualifications shall not supersede State or Federal qualifications.** If a person or piece of equipment meets a Federal qualification then that will be the qualification it is given.

(1) State, local and tribal qualifications are developed by various defined groups.

(2) Requests to add local qualifications to RMW can be made by filling out the "[Qualification Addition Spreadsheet](#)" listed under the resource tab of [www.SouthDakotaresponder.com](http://www.SouthDakotaresponder.com) and sending it to [Laurie.Morrison@state.sd.us](mailto:Laurie.Morrison@state.sd.us).



# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v4Jan2013

(3) All qualifications can have a deadline of membership, or expiration date put into RMW, however, these qualifications will remain active on the IDCC until the card itself expires. It is the organization's responsibility to track the qualifications of the personnel they are creating credentials for to ensure that they still maintain the assigned level of qualification.

(4) NIMS guidance on credentialing does not confer the authority or privilege to practice any profession. Only the receiving department, agency or jurisdiction can extend that privilege or authority after evaluating the person's information.

(5) Two key elements in the qualification process include typing personnel and resources and certifying that personnel, in fact possess, at least the minimum level of training, (experience, licensure, certification and fitness) to perform the job.



# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v4Jan2013

### b) Medical Barcode

The Medical Barcode is automatically generated from the “Resource Manager” software. (See the [resourceMGR web™ User Guide for more information on what is included in each item in the barcode](#)) It contains the following **OPTIONAL** information:

- (1) Gender
- (2) Blood Pressure
- (3) Blood Type
- (4) Allergy Conditions
- (5) Medical Conditions
- (6) Physician
- (7) Insurance
- (8) Height
- (9) Weight
- (10) Emergency Contact Name
- (11) Emergency Contact Phone

\* Card holders should be advised that the information contained in the barcode is not encrypted and can be read. It is not protected should you choose to disclose it. When using **Mobile express™** only personnel with the STI MED qualification can read the information in the medical barcode.

# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v4Jan2013

### D. Verification

Verification of personnel ensures “... personnel possess a minimum level of training, experience, physical and medical fitness, and capability appropriate for a particular position...” This requires organizations to test and evaluate their personnel against the qualifications established by the typing efforts. Additionally organizations must “...authenticate qualifications...” through a formal process to approve and provide signature for personnel qualifications.

Reference: [http://www.fema.gov/pdf/emergency/nims/NIMS\\_core.pdf](http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf)

### E. Revocation

A critical component of identity and qualifications is revocation. Organizations need to have a process in place to revoke credentials when certain events occur. **No more than 18 hours** after a person is relieved of their position, no matter the condition of their release, it is the organization that issued that card’s responsibility to get the card back and destroy it using the guidelines listed in paragraph F. Likewise, if an individual’s qualifications change, their credentialing information should also be updated in the affected databases or records **within 30 days**.

### F. Card Disposal

Expired, revoked, or returned credential cards should be shredded if possible but will be destroyed by cutting through the barcode as a minimum so that the card can no longer be read by the system. NOTE: If the credential is printed on a proximity card it will be destroyed in the same way as the standard card.

### III. Deployment

In addition to the legally mandated requirements of the credentialing effort, there are other aspects that need to be addressed in the credentialing process. Under NIMS, these include the authorization to deploy, control of access to an affected area, affiliation of personnel deploying as part of an organization, and revocation of IDCCs when necessary. Appropriately issued credentials do not authorize an individual or a team to self deploy. Each agency authorized to issue credentials shall have a policy in place that dictates how credentialed staff associated with their agency are authorized to deploy to an incident.

#### A. Access

NIMS intentionally limits access to a disaster to only personnel who have been credentialed and authorized to deploy through a formal agreement between the requesting and providing agencies. The agreements can range from automatic mutual aid agreements, the Emergency Management Assistance Compact and mission assignments to Federal agencies to provide Direct Federal Assistance. Personnel that arrive to check in that have not been credentialed, requested, and authorized are to be turned away at the discretion of the Incident Commander. No one should be granted access to an incident that has not been credentialed, either with an IDCC or a rapidTag, to ensure accountability.

#### B. Affiliation

SDOEM recognizes the need for processes to address the full range of access control, both for individuals who provide support to the incident command structure and for those who require access for specific purposes outside of the NIMS/ICS structure. It may not be practical to confirm the qualifications of individuals or groups of people responding to an event. In these cases, documented affiliation (identification) with an organization or entity responding to or affected by the event provides proof of qualification and authorization to deploy.

#### C. **rapidTAG™**

RapidTag cards are incident specific IDCCs that are used to account for personnel, equipment, or companies that have not been issued or do not have the RMW IDCC on hand. An individual's qualifications and mission tasking need to be verified prior to issuing a rapidTag.

# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v4Jan2013

### The Personnel rapidTag contains:

- (1) Incident Name
- (2) Organization
- (3) Organization Type specific icon
- (4) First Name Last Name
- (5) Rank
- (6) Role
- (7) Location
- (8) Expiration

### The Personnel barcode will contain the following:

- (9) Organization Country
- (10) Organization State
- (11) Organization Type
- (12) Organization ID
- (13) Personnel ID
- (14) First and Last Names
- (15) Rank
- (16) Date of Birth
- (17) Qualifications



# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v4Jan2013

### The Equipment rapidTag contains:

- (1) Incident Name
- (2) Organization
- (3) Organization Type specific icon
- (4) Description
- (5) Make Model
- (6) Role
- (7) Location
- (8) Expiration

### The Equipment barcode will contain the following:

- (9) Organization Country
- (10) Organization State
- (11) Organization Type
- (12) Organization ID
- (13) Organization Name
- (14) Equipment ID
- (15) Make
- (16) Model
- (17) Description
- (18) Manufacture Date
- (19) Equipment Type



# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

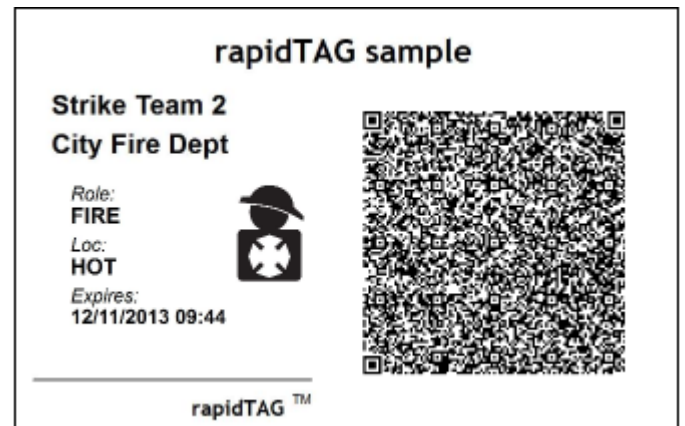
v4Jan2013

(20) Date in Service

(21) Qualifications

### The Company rapidTag contains:

- (1) Incident Name
- (2) Company Name
- (3) Organization
- (4) Role
- (5) Location
- (6) Expiration



### The Company barcode will contain the following:

- (7) Organization Country
- (8) Organization State
- (9) Organization Type
- (10) Organization ID
- (11) Company ID
- (12) Company Name
- (13) Qualifications
- (14) Equipment and Personnel Barcode data from contained Equipment and Responders

# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v4Jan2013

### D. Passport Tags

Passport Tags are a three on one perforated card. They are printed on special card stock so you end up with a keychain sized ID (similar to a grocery store loyalty card or library card). They allow you to use interTRAX in conjunction with your velcro or magnetic passport accountability system. **These tags are not a substitute for the IDCC printed from RMW.** They are to be used for manual accountability or ID label (attached to collar or helmet).

The 3-tag passport cards are printing using the “People” option selecting the card printer, selecting the design “R\_Card\_3\_tag”. **Make sure the laminator is OFF for printing this design.**



This page left intentionally blank



# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v4Jan2013

### Attachment 1: Organization Name Template

**State organizations** will be prefaced with “SD” i.e. SD Office of Emergency Mgmt, SD Dept of Health, SD Dept of Agriculture, SD Highway Patrol, SD Dept of Transportation.

**County organizations** County names should be spelled out, with the Co. abbreviated at the end. i.e. Minnehaha Co., McPherson Co.

**City organizations** will be the city name then organization i.e. Yankton EMS or Hot Springs VFD

**Township organizations** will be written “Twp” i.e. Cottage Grove Twp PD

**Private Industry** will use their organization name.

**Volunteer organizations** will use their organization name. I.e. Red Cross, United Way

Common abbreviations will be allowed. Some examples are listed below. These should be used when applicable:

Dept = Department (only when not accounting for a fire, police or public health department)

Dist = District

Div = Division

EMS = Emergency Medical Services

Env = Environment

FD = Fire Department

HD = Public Health Department

Mgmt = Management

PD = Police Department

PU= Public Utilities

PW= Public Works

Twp = Township

VFD = Volunteer Fire Department

# Comprehensive Resource Management and Credentialing System

## Resource Manager Web Credentialing Policy

v4Jan2013

### Attachment 2: Law Enforcement Card Definitions

- In order to have a blue “law enforcement” background badge- the holder must be a sworn or certified law enforcement officer fitting into one of the two law enforcement officer (LEO) “types” listed below. Credentials issued will serve as commissioning cards and are required to have the following language on the back; "THE HOLDER OF THIS CARD IS A COMMISSIONED LAW ENFORCEMENT OFFICER AND HAS STATUTORY POWERS OF ARREST AND IS AUTHORIZED TO CARRY A FIREARM"
- The “types” are:
  - Full Time/Part Time Law Enforcement Officer- Includes those officers who are certified by South Dakota Law Enforcement Officers Standards and Training Commission as law enforcement officers and those officers who are serving as law enforcement officers under a provisional certification pending completion of a basic training course.
  - Reserve Officer- Includes all other sworn personnel that may respond to an incident such as uncertified reserve law enforcement officers, correctional officers, special deputies, process servers and other personnel who serve a sworn law enforcement support role but are not certified by South Dakota Law Enforcement Officers Standards and Training Commission.
- Support personnel who are members of law enforcement agencies (e.g. non- sworn jailers, administration, dispatchers, etc) who are not sworn officers should be credentialed with badges displaying the grey “Government” background.
- Private security personnel, even if contractors for public entities should be credentialed with the brown “Private Industry” background. Private security should not be confused with law enforcement.