IDENTITY CRISIS: DEFINING THE PROBLEM AND FRAMING A SOLUTION FOR TERRORISM INCIDENT RESPONSE

Mark Landahl

INTRODUCTION

The date is July 17, 1996. Emergency services personnel from Suffolk County, NY and the United States Coast Guard respond to a report of a catastrophic explosion and the crash of a passenger airliner over the ocean off the southern coast of Long Island. The initial assumption is a nexus to terrorism. The East Moriches Coast Guard Station is designated as the operations command post, staging area, and evidence collection point. As the incident shifts from response to recovery, personnel from various response disciplines and levels of government stream into the station. Among them is Lieutenant Colonel David Williams of the U.S. Army Reserve. LTC Williams, dressed in his U.S. Army Reserve flight suit, presents identification, enters the site, and assists in the operation by landing helicopters on the designated helipads. On the third day of his work, LTC Williams is questioned concerning his identity and affiliation. Following a brief investigation, LTC Williams is identified as an impostor, escorted from the property, and charged by the Suffolk County Police.[1]

Identity is defined as the "the collective aspect of the set of characteristics by which a thing is definitively recognizable or known."[2] In the incident described above, the set of characteristics that assumed an identity consisted of a uniform, unverifiable paper credentials, and a demeanor consistent with a military officer. These characteristics allowed the impostor to pass a brief security inspection and work within a 'secured' site for several days. This incident, although a rare but serious example, highlights the limits of current methods for identifying response personnel. The infiltration of the Flight 800 response and recovery operation evidences only one of several dimensions of a comprehensive identity management capability gap for response and recovery operations that can be traced through an examination of historical terrorism incident response in the United States.

The current identity management system for first responders has left a nation-wide capability gap. The decentralized system has resulted in as many different forms of first responder identification as there are federal agencies and state and local governments. The lack of standardization and interoperability among forms of identification is problematic when confronting a large-scale, multi-jurisdictional response to a suspected incident of terrorism. In addition to the response to the crash of TWA Flight 800, this lack of capability is documented in the after-action reports of the response to every major domestic incident of terrorism, specifically the 1995 Oklahoma City Bombing and the 9/11 responses to both the World Trade Center and the Pentagon. This article seeks to define the scope of the problem, identify the elements of a potential solution, and briefly evaluate two alternative approaches to solving the problem. First, the failures of identity management through the response to previous incidents of terrorism and other

catastrophic incidents will be traced. Once cataloged, these 'failures' form the necessary framework for potential solutions to the problem. Finally, two alternative approaches to the problem will be evaluated for potential to improve identity management for terrorism incident response.

As will be revealed, the problem of identity management for terrorism incident response is multi-faceted. There are two main elements that contribute to the problem. The first element is related to the definition of identity presented in the second paragraph and introduced through the opening vignette – identity authentication. Identity authentication essentially answers two questions: first, simply, "who is this?" and second, "how certain are we that a person is who they say they are?" The second element is related to a second part of the definition of identity. Identity is also defined as "the set of behavioral or personal characteristics by which an individual is recognizable as a member of a group."[3] Group identity as it relates to terrorism incident response is essentially the training credential of an individual. This aspect of identity answers the question "what tasks is this individual trained to perform?"

Although the two elements of identity can be studied separately, for the purpose of this article they are examined together. The elements are bundled because successful terrorism incident response is dependent upon both aspects of identity. The purpose of this article is to begin the discussion of identity management for terrorism incident response; it is not intended to be an exhaustive study of the two elements of identity. The article is intended to examine the scope of the problem, frame the elements of potential solutions, and identify areas for additional research.

DEFINING THE PROBLEM: IDENTITY MANAGEMENT LESSONS LEARNED FROM TERRORISM INCIDENT RESPONSE

The identity management capability gap for terrorism incident response is a pervasive but solvable problem. The post-9/11 focus on the development of capabilities related to incident response, including acquisition of CBRNE (Chemical, Biological, Radiological, Nuclear, Explosive) detection equipment, response apparatus, and personal protective equipment have left out the essential component of identity management. Despite the glaring lack of capability, it has been all but ignored in homeland security preparedness efforts targeted at first response personnel.

Discussion of identity management is also hampered by the absence of an extensive body of knowledge or current debate on the issue. This section begins to address this shortcoming by examining the question: Is first responder identity management really a problem? Current accessible information bulletins and the After-Action Reports (AAR) of the response to domestic incidents of terrorism will be examined to develop the answer to this essential question.

The problem of identity management for terrorism incident response begins prior to the TWA Flight 800 disaster and has several dimensions beyond simple authentication of personal identity. The problem was identified in the response to the nation's first major domestic terrorist incident requiring a large multi-jurisdictional response: the bombing of the Murrah Federal Building in Oklahoma City, OK. On April 19, 1995, Timothy McVeigh detonated 4,800 pounds of ammonium nitrate mixed with fuel oil loaded in a Ryder box truck outside the Murrah Federal building. The blast caused a catastrophic collapse of the building, resulting in the deaths of 168 people and injuries

to 500 others. The ensuing public safety response and recovery efforts revealed major gaps in identity management capabilities at all levels of government.

Within two hours of the blast, the Oklahoma City Police Department (OCPD) had established a controlled perimeter around the incident site.[4] Identification of personnel immediately became an issue. Initially, the OCPD moved its permit and identification section equipment to the scene to issue identification badges. The operation lasted only a few hours as supplies were quickly exhausted.[5] The OCPD continued to issue alternative forms of identification. Due to rain and lighting, the location of the identity station changed three times. When agents from the Federal Bureau of Investigation (FBI) arrived, they also began issuing identification, causing confusion for those manning the perimeter. FBI and OCPD finally consolidated their operations and issued one form of identification, operating from a vacant warehouse building. The building was large enough to hold the up to 100 people who were waiting for identification after filling out permit forms and completing necessary identification checks. The combined identification operation issued approximately twenty thousand passes over a seventeen-day period.[6] In the publication *Oklahoma City – Seven Years Later: Lessons Learned for Other Communities*, an unnamed Oklahoma City law enforcement officer claimed: "Over 28,000 identity badges were issued during the Oklahoma City response and recovery effort. It took days to establish a central issuing agency. A predetermined ID system would have greatly reduced ID chaos."[7] Included among the lessons learned in the document is the important recommendation to "establish a Site ID System…Controlling access to the site is an immediate and on-going need."[8]

The need for a comprehensive identity management solution was also evident in the 9/11 response to the Pentagon. Understanding the lessons learned from the 1995 Oklahoma City bombing, the Arlington County Police Department pre-planned an identification system for incident scene security and accountability. The system consisted of 2,000 colored wristbands to be used for entry to an incident scene. In the tremendous public safety response to the terrorist attack at the Pentagon, Arlington County deployed its identity management system two days into the response. Once the system was utilized, the wristband supply was exhausted within two hours.[9]

The on-scene identity management efforts that followed included a system that took up to two hours to process and provide credentials to relief crews for entry into the site because of limited computers and lack of a central database.[10] The lack of a comprehensive identity management system also led one Arlington County firefighter to observe, "A volunteer firefighter tee shirt was the only required identification."[11] At the request of the incident commander, the United States Secret Service instituted a more efficient credentialing system several days into the response.

The identity management recommendations from the Pentagon AAR are similar to the lessons learned first reported in the Oklahoma City AAR. The Pentagon AAR concluded, "Arlington County should work with…emergency response and volunteer organizations to implement a uniform identification system. Such a system should be in place and used routinely."[12] These incidents indicate the need for a comprehensive identity management system that delivers the necessary capabilities to support incident response operations.

The September 11, 2001 response to the World Trade Center terrorist attacks is not documented by an official after-action report and, as a result, there is limited documented information concerning identity management at the incident scene. The

McKinsey & Co. report prepared for the New York City Police Department, entitled *Improving NYPD Emergency Preparedness and Response,* does provide some information regarding the problems associated with identity management on the WTC incident scene.

The report asserts that it took several days to secure the perimeter. It also details the problems caused by this delay. The report states that "due to inconsistent control of access and absence of an effective credentialing system, perimeter security [was] not adequately established, allowing large numbers of unnecessary personnel to enter site."[13] Although the report does not contain a sanctioned set of recommendations or lessons learned, the challenges faced during the response and recovery operation can be discerned from the content of the report. Based on the report, perimeter security and identity management proved to be significant challenges without an effective solution.

The previous sections identify many of the gaps associated with past responses to domestic terrorism incidents. Knowing identity management is a problem, in the past and in the future, but avoiding steps to solve the problem, would once again demonstrate that the nation suffers from a "failure of imagination" as described in the *9/11 Commission Report*.[14] If we reasonably know what is possible, it should be included in our planning and preparation.

The vignette in the introduction of this article revealed the opportunity to exploit current identity documents for secure site infiltration. This security gap could be exploited to perpetrate a secondary attack. *Improving NYPD Emergency Preparedness and Response* points out that the "risk of secondary attack was not made a priority."[15] The possibility of secondary attacks at incident scenes such as the WTC response must be considered. The May 2005 issue of the *FBI Law Enforcement Bulletin* identifies the two components of a secondary attack as follows: "The first one draws in emergency responders, regardless of the extent of deaths and injuries. In the second, the responders themselves become the target and include not only law enforcement, fire and rescue, and emergency medical personnel but civilian Good Samaritans as well."[16] The exploitation of lax identity procedures to perpetrate a secondary attack is a plausible conclusion based on pervasive failures in previous incident response. The potential utilization of this gap for terrorist activity is also advanced by the Department of Homeland Security and Federal Bureau of Investigation joint bulletin released in December 2004 titled *Potential Terrorist Use of Public Safety or Service Industry Uniforms, Identification, or Vehicles*.[17] The bulletin warns of the potential exploitation of the unverifiable identity characteristics of the public safety and service industry (uniforms, paper identification, vehicles, etc.) for terrorist activity. Possible scenarios include the use of public safety and service industry uniforms or vehicles to perpetrate a secondary attack on first responders. The exploitation of these unverifiable identity characteristics could allow access to critical sites, such as staging areas, where a secondary attack would prevent rescue efforts and potentially cause mass casualties to first responders. Although a secondary attack can also come from a pre-placed device, the possibility exists for an attack precipitated by infiltration through the unverifiable flash identification, uniform, and vehicle paradigm.

The after-action and related reports detailing the response to the three major domestic terrorist attacks reveal a common problem that to date has not been effectively resolved. The common element among the lessons learned from the responses to each incident reveals that identity management failure is endemic to terrorism incident

response. From Oklahoma City to Arlington to New York City, identity management is a glaring response capability gap. Despite AAR recommendations regarding improvements needed in identity management dating back to 1995, little has been accomplished in the recognition and development of a solution. Identity management is not simply a local, state, or regional problem, but a national problem that has been largely ignored.

ELEMENTS OF AN IDENTITY MANAGEMENT SOLUTION

The previous section served to define the scope of the identity management problem for incident response. In this section these common identity management failures are organized and explained as the elements of a potential solution. These elements are derived from the analysis of the response to previous incidents of terrorism and the consideration of future incident scenarios. In the paragraphs that follow the four elements of a potential identity management solution are defined.

1. Identity Authentication

In *Identity Fraud: A Critical National and Global Threat*, the key to identity authentication is described as "access to data to assist in the validation, verification, and authentication of personal identifiers."[18] Validation of the data is predicated on trust. The heart of identity management lies in the creation and maintenance of trust. Trust allows for a consumer to have a defined level of certainty in the authenticity of a credential based on the process by which it was issued and the security of the token. The trust model provides a level of certainty for the consumer in answer to the question, "Who is this?" Certainty and trust are measured through a two-pronged test of product and process.

In order to provide certainty and trust in an identity credential, it must be sound in both product and process. The process must provide assurances that an individual has been vetted through an identity-proofing process. The process should include common criteria and assurances prior to enrollment and token issuance. The more stringent the criteria and assurances are, the higher the level of certainty and trust. Strong criteria may include elements such as background investigations, collection and verification of biometric information, and requirements for presentation of certain identity documents prior to issuance.

The second prong of the test is the product, or identity token (document, card, or item that is used to establish identity) itself. Trust and certainty are developed through a product that is counterfeit resistant. The ability of the product to resist change and/or duplication develops certainty and trust. The stronger the product is to resist counterfeit, the higher the level of trust and certainty in the answer to the question, "Who is this?"

Process and product come together to form a trust model. Both aspects must be sound to develop certainty. A stringent vetting process backed with a token that can be easily reproduced and altered does not create trust. Likewise an identity token that is strongly resistant to tampering, but was issued without criteria or assurances, also creates uncertainty and is not trusted. Identity authentication is marrying sound process and a tamper-resistant product to create certainty and trust.

President Ronald Reagan often quoted the Russian proverb "doveryai no proveryai," which translates to "trust, but verify," to describe his foreign policy dealings with the

Soviet Union in the late 1980s.[19] "Trust, but verify" is an appropriate mantra for first responder identity. The solution requires a framework that can provide verification. The infiltration of the response to the TWA Flight 800 disaster illustrated the vulnerability and limitation of trust in our current identity schema. Our visual (uniform, paper credential, vehicle) and behavior (acting in conformance with identified office) based identity management system must be replaced with identity authentication through verifiable credentials. If the TWA disaster had been a terrorist attack, the current system would not have mitigated the threat of secondary attack against first responders.

2. Rapid In-Processing

In-processing for incident response requires that identity and affiliation be verified, the responder be enrolled or logged into the scene, the level of site access determined, and accountability be maintained by tracking personnel on-scene. Rapid in-processing for identity management is the ability to perform these tasks efficiently with minimal impact on the completion of tactical objectives for incident response. The lack of rapid in-processing to incident scenes is documented as a failing of identity management for terrorism incident response. The AAR's for both the Oklahoma City and Pentagon responses indicate that it took hours to provide credentials to personnel for entry into the scenes. Speed of processing, however, competes with identity authentication in an incident response setting. Perimeter personnel must weigh security against the immediate need for personnel at an incident scene. Due to the inadequacies of the current identity management system, perimeter personnel are forced to revert to unverifiable credentials and the uniform, emergency vehicle, and demeanor consistent with the identity construct. Any identity management solution must provide a level of security and speed that does not hinder, but enhances, incident response. The speed of processing should be consistent with the time required for perimeter personnel to check "flash" identification and ask follow-up questions.

3. Interoperability

The Department of Homeland Security SAFECOM program defines interoperability as "the ability of emergency responders to work seamlessly with other systems or products without any special effort."[20] An identity solution for terrorism incident response must have this important capability. The problems of radio interoperability are well documented. They are found among the lessons learned of every AAR and became a central focus of the *9/11 Commission Report*. The same gaps would be found if technology had been broadly applied to identity management for first responders. The implementation of identity management technology for first responders is in its infancy. In its current state, it is the communication equivalent of smoke signals. This can be seen as a problem or an opportunity. Unlike communications, there is not a proliferation of proprietary technology that has been implemented for identity management. This presents an opportunity to create a standards-based interoperable system. Interoperability is a necessary element in authentication of responders from varied disciplines and levels of government who converge on incident scenes.

4. Data Storage / Retrieval and Promulgation Capability

Data storage/retrieval and promulgation is the ability to store or link to data in a manner that it can be brought forward for utilization in other processes. An identity management system for improved terrorism incident response must include the capability to store or link data in a manner that can be distributed to and utilized by incident commanders. Data storage/retrieval and promulgation addresses two aspects deficient in previous response to incidents of terrorism. The first deficit involves the matter of the training credential.

The group affiliation, or training credential in this case, is essential information for incident commanders to adequately deploy and coordinate appropriate assets to achieve incident objectives. In *Information, Technology, and Coordination: Lessons from the World Trade Center Response*, the importance of information for deployment and coordination of responders is highlighted: "Effective deployment and coordination depend on many kinds of information from the roles and capabilities of response and support organizations to the identity of individual responders."[21] While the effective utilization of assets is a problem of incident management, providing the information concerning the characteristics, group affiliation, or training credential of assets is a function of identity management.

The second deficiency in terrorism incident response that can be addressed through data storage/ retrieval and promulgation is accountability. In the National Commission on Terrorist Attacks upon the United States *Staff Statement No. 14*, the following outlines the deficiency in accountability: "Once units arrived at the WTC they were not accounted for comprehensively and coordinated."[22] Providing this information is a function of a comprehensive identity management system. Would the resources have been uncoordinated and unaccounted had an effective identity management system been in place? A properly structured and effective identity management system would provide real-time usable information to incident commanders concerning the number, location, and qualifications of assets at his/her disposal. With regards to personnel resources, the answers to questions such as: "Who is this?" and "What can they do for me?" are critical to incident commanders. An effective identity management system for incident response must provide incident commanders with the data to answer those critical questions.

TWO APPROACHES TO A SOLUTION: INCIDENT RESPONSE RESOURCE OR COMPREHENSIVE NATIONWIDE PROGRAM

The previous sections detail the problem of identity management for terrorism incident response as pervasive, but not without potential solution. The framework revealed by the analysis of the After-Action Reports of domestic incidents of terrorism identifies the elements of an identity management solution necessary to improve incident response. These elements can be achieved through two possible options: the on-scene resource or a nationwide comprehensive identity solution for first responders. In the following sections the two options will be developed and examined for their potential application to improve identity management for terrorism incident response.

DEFINING AN INCIDENT RESPONSE RESOURCE: THE IDENTITY MANAGEMENT TEAM

The concept of identity management teams for incident response is not novel. A version of this solution has been implemented at every major incident of terrorism out of necessity, utilizing available materials and untrained personnel and resulting in repeated and unnecessary mistakes. The need to control access and positively identify personnel on terrorism incident scenes was recognized with our first domestic attack on the World Trade Center in 1993. The impetus in 1993 was the need to control access to the crime scene.[23] The additional threat of secondary attack, as described previously in this article, increases the urgency for implementing effective incident scene control and credentialing. The failings of identity credentialing during the 1995 Oklahoma City Murrah Federal Building bombing, and the 2001 responses to the World Trade Center and the Pentagon, were pervasive and discussed earlier to illustrate and define the problem of identity management for terrorism incident response. In this section the Arlington County and Oklahoma City After-Action Reports will be revisited in greater detail. They are instructive because the failings of identity management early in the incidents were tempered with later success. The systems that were instituted over the course of the incidents, through trial and error, provide best practices and a concept of operations at the heart of what should comprise an on-scene identity management team for terrorism incident response.

As established through the previous analysis of historical responses to incidents of terrorism, identity management is deficient for terrorism incident response. Despite this deficiency, there is currently no defined response asset under the FEMA National Mutual Aid and Resource Management Initiative to address this important function. The National Mutual Aid Resource Management Initiative "supports the National Incident Management System by establishing a comprehensive, integrated, national mutual aid and resource management system that provides the basis to type, order, and track all (federal, state, and local) response assets."[24] The resource definitions are typed so the level of capability of resources can be readily determined before an asset is requested. The problem is that there is no resource definition that performs the function of identity management for incident response. Currently, if an incident commander needed assistance in managing access to the scene through a credentialing system, there are no typed assets to order through mutual aid or other process to perform this function, forcing ad-hoc solutions. The intent of this section is twofold: first, to develop a typed resource definition based on lessons learned from two selected case studies of previous incident response; second, to evaluate the definition across the previously developed framework for improved terrorism incident response.

Identity Management Team Case Studies

The development of the resource definition for identity management begins with the examination of the 1995 Oklahoma City Murrah Federal Building bombing and the 2001 response to the attack on the Pentagon. These incidents and after-action reports provide significant detail regarding the development of ad-hoc identity management capabilities as the incidents unfolded. Parallels will be drawn utilizing other published documents that highlight identity management efforts but do not provide enough significant detail for a case study. An analysis of these incidents reveals a baseline structure to construct a typed identity management resource.

1995 Oklahoma City Murrah Federal Building Bombing

In the response to the 1995 Oklahoma City bombing incident many lessons were learned concerning the structure, function, concept of operations, importance of site access control, and the need for dedicated identity management resources. The Oklahoma City incident provides the background for the first large-scale terrorist incident that required a robust capability for identity management and scene control. Through trial and error, and utilizing only available resources, an ad-hoc identity management capability was developed and sustained that allowed for the issuance of over 28,000 identity credentials over the course of the incident.

The initial failure of identity management at the incident scene was due to the lack of any pre-planned credentialing option. This lesson learned is captured in the recommendations of the after-action report. Although the capability gap is clearly identified in the report, eleven years later there still remains no guidance or nationally defined resource to perform this critical function. This subsection seeks to close the gap first exposed in the Oklahoma City response by defining a response asset for this critical function.

The development of on-scene identity credentialing first requires the establishment of a perimeter. In the case of the Oklahoma City bombing, establishing a controlled perimeter around the incident site occurred within two hours of the blast.[25] Once the perimeter was established the Oklahoma City Police Department (OCPD) utilized its only available asset to issue identification by moving its Permit and Identification Section equipment to the scene to issue identification badges. The Permit and Identification Section was not a deployable asset; however, it was the only available option for credentialing. Once established, the operations of the Permits and Identification Section lasted only a few hours as identity supplies were quickly exhausted.[26]

The OCPD continued to issue alternative forms of identification: "different colored passes were issued for each day after April 20th to discourage people from returning to the site when they had no current assignment."[27] Due to rain and lighting conditions, the location of the identity station changed three times. When agents from the FBI arrived, they also began issuing identification, causing confusion for those manning the perimeter. The FBI and OCPD finally consolidated their operations and issued one form of identification, operating from a vacant warehouse building. This is an important concept of operation in the employment of an identity management resource: it must be integrated and maintain a permanent location throughout the incident.

In *Oklahoma City – Seven Years Later: Lessons Learned for Other Communities*, it is reported that early in the response "the ID process was a major issue due to lack of controls and systems in place. No one had been designated to issue ID's and the system was hit and miss."[28] This is instructive in defining an identity asset as it must include controls and systems, and be specifically designated to perform the function with a direct link to on-scene unified command.

The after-action report also details the process utilized for credentialing volunteers and rescue workers.

> The process was as follows: volunteers appeared at the Permits and ID location and filled out a permit form with their name, agency, and destination. This permit form was submitted along with a photo ID. The Investigator would inquire as to

> reasons for accessing the scene. The permit would be approved or denied based on the reason and destination. The Investigator entered the information into a logbook, signed the permit, and sent the volunteer to the FBI photo section for their photo ID. If there were questions about the admittance of a person, the FBI made the final determination.[29]

The excerpt from the after-action report gives detail on the process for issuing on-scene identity credential documents. This process included examination of identity documents, affiliation and destination, collection of a photograph, and recording of the issued document. These elements form the basis of a minimum inspection necessary for entrance to a terrorism incident scene. Another essential element of the identity management function is communications equipment. Credentialing staff utilized "a cellular phone and a police radio…when trying to check on whether a volunteer should gain access to the scene."[30] Communications equipment and the aforementioned direct contact with on-scene incident command are essential elements in a response asset for identity management.

The process was not without criticism. "Due to the number of persons requesting entry, the limited resources for processing permits, and lack of guidelines, this process generated complaints. Complaints came from rescue workers and volunteers about the length of time to obtain a permit and the restrictions on the permit."[31] The identity process undertaken during the Murrah Federal Building bomb response was completed by hand, not utilizing computerized processes. The after-action report advises "The entire process would probably have gone more smoothly had investigators been able to utilize lap top computers to enter the necessary data on the volunteers."[32] The defined response resource must include computerized processes that allow data and biometric information to be quickly captured and stored to allow access at later times to facilitate processing for re-entry into the scene.

The Oklahoma City bombing response provides baseline information on the development of a defined resource to improve identity management for terrorism incident response. The lessons learned from that response suggest seven elements for the concept of operations and necessary equipment for an identity management asset for incident response. The elements related to the concept of operations of a defined resource include a pre-planned solution, an established perimeter, a defined location for distribution, and systems and controls (including a defined issuance process and tracking of issued credentials). The lessons learned also revealed the equipment and identity supplies needed for identity management: mechanisms for receiving replenishment, communications equipment (interoperable radios, internet, and database access), and computer equipment for identity document production (digital cameras, computers, identification printers). The lessons learned from, and ad hoc developments during, the response to the Oklahoma City bombing form the basis of a defined resource for identity management for incident response.

2001 Pentagon Response

The response to the terrorist attack on the Pentagon on September 11, 2001 also offers many lessons learned concerning the structure, function, concept of operations, importance of site access control, and the need for dedicated identity management resources. The Pentagon attack provides additional background for large-scale terrorist incident response that requires a robust capability for identity management and scene

control. As with the Oklahoma City bombing, credentialing at the Pentagon developed through trial and error, utilizing available resources. The Pentagon response also tested the boundaries of a limited credentialing solution developed by the Arlington County Police Department in the wake of the identity failures in the Oklahoma City response. The development of the credentialing function at the Pentagon incident site is also instructive as its evolution informs the development of a resource definition for an identity management team for improved terrorism incident response.

Understanding the lessons learned from the 1995 Oklahoma City bombing, the Arlington County Police Department pre-planned an identification system for incident scene security and accountability. The system consisted of 2,000 red, yellow, blue, and green colored wristbands to be used for entry to an incident scene. In the tremendous public safety response to the terrorist attack at the Pentagon, Arlington County deployed its identity management system two days into the response. Once the system was utilized, the wristband supply was exhausted within two hours.[33] This failure is instructive in that it took two days to implement an access control system and demonstrated that identity supplies must be significant to support issuance to thousands of responders. This critical failure further enhances the argument that a defined deployable identity management resource, staffed by trained personnel who possess the appropriate equipment and supplies, is essential for improved terrorism incident response.

On the third day of the response, the Defense Protective Service (DPS), using a tactic similar to that employed by Oklahoma City Police in 1995, utilized its available badging equipment to produce identity credentials. The DPS system is described in the after-action report as "burdensome"[34] and "inadequate for a task of this magnitude."[35] In addition, the badging process "took too long, delaying shift changes inordinately."[36] The AAR also claims that "because of the limited computers to create badges and lack of a single database, processing added an additional burden to crew relief."[37] A defined identity management resource must have adequate computer stations and utilize a single database. This also emphasizes the need for a defined asset. Ad-hoc solutions waste valuable time as lessons are learned in identity management for incident response time and again, at the cost of safety, force protection, and lost on-scene work hours.

At the request of DPS and the FBI, the identity system was bolstered by the addition of United States Secret Service (USSS) identity assets. The AAR describes that the USSS trained members of the Army Band to operate its five portable badge-making workstations.[38] After the incorporation of the USSS equipment the system was described as "effective."[39] The addition of more appropriate equipment and trained personnel resulted in a system that was more effective. This is instructive in the development of a defined resource, as the number of workstations must permit sufficient throughput not to hamper on-scene operations.

The 9/11 Pentagon response provides further validation of the baseline information provided by the study of the Oklahoma City bombing for the development of a defined resource to improve identity management for terrorism incident response. In addition to the lessons learned from the response to the Oklahoma City incident, the Pentagon response provides information for the construction of a defined identity management resource. Lessons learned indicate the need for adequate supplies, sufficient workstations to provide reasonable throughput, and the need for a central database. These additional factors, when combined with the elements revealed in the response to

the Oklahoma City incident, provide the baseline for a defined resource for identity management functions on incident scenes.

Identity Management Team Typed Resource

The lessons learned and basic necessary elements of an identity management team were revealed through examination of the 1995 Oklahoma City Murrah Federal Building bombing and the 2001 response to the Pentagon. The elements related to the concept of operations of a defined asset include a pre-planned solution, an established perimeter, a defined distribution location, a direct link to on-scene incident command, and systems and controls (including a consistent issuance process and tracking of issued credentials). The lessons learned also revealed necessary equipment, including: a significant amount of identity supplies and mechanisms to acquire additional materials, communications equipment (interoperable radios, internet, and database access), computer equipment sufficient for significant throughput for identity document production (digital cameras, computers, identification printers), and a single centralized database. The following resource definition (Table 1) and concept of operations (Figure 1) were developed utilizing these lessons learned and basic elements,

RESOURCE:	IDENTITY MANAGEMENT TEAM (IDMT)					
CATEGORY:	Law Enforcement/Security			KIND:	Team	
MINIMUM CAPABILITIES:		TYPE I	TYPE II	TYPE III	TYPE IV	OTHER
COMPONENT	METRIC					
Equipment	Computer Equipment	5 Identity Issuance Stations (5 Computers, 5 Digital Cameras, 5 ID Printers, Multi-Technology Readers)	3 Identity Issuance Stations (3 Computers, 3 Digital Cameras, 3 ID Printers, Multi-Technology Readers)			
Equipment	Communications	Team Radio Communication Equipment (portable radios, extra batteries, battery charger, cellular phones)	Team Radio Communication Equipment (portable radios, extra batteries, battery charger, cellular phones)			
Equipment	Communications	Wireless Internet Access, external LE database access	Wireless Internet Access, external LE database access			
Equipment	Software	Database accessible by Incident Command	Database accessible by Incident Command			
Equipment	Computer Equipment	Hand-held remote verification capability	Hand-held remote verification capability			
Equipment	Identity Supplies	10,000 interoperable Identity Tokens Extra printer cartridges Mechanism to obtain additional supplies	5,000 interoperable Identity Tokens Extra printer cartridges Mechanism to obtain additional supplies			

RESOURCE:	IDENTITY MANAGEMENT TEAM (IDMT)					
CATEGORY:	Law Enforcement/Security			KIND:	Team	
MINIMUM CAPABILITIES:		TYPE I	TYPE II	TYPE III	TYPE IV	OTHER
COMPONENT	METRIC					
Equipment	Generator	Able to work at location without land line electricity	Able to work at location without land line electricity			
Personnel	Training	Team Trained to Operate Equipment and perform identity functions	Team Trained to Operate Equipment and perform identity functions			
Personnel		1 Officer in Charge (OIC) 1 Supervisor 6 Officers	1 Supervisor or OIC 4 Officers			
Vehicles		Integrated in mobile asset or deployable to a fixed location	Integrated in Mobile Asset / or deployable to fixed location			
COMMENTS:	Type I – A pre-designated team consisting of one OIC, one supervisor and six officers in an integrated mobile response asset. The team has the ability to manage identity management functions for large-scale incidents. The team engages in routine training to maintain advanced skill level. Type II – A pre-designated team consisting of one supervisor or OIC and four officers in an integrated mobile response unit or deployable to a fixed location. The team has the ability to manage identity functions for small to mid-sized events. Team engages in routine training to maintain advanced skill level.					

TABLE 1: IDENTITY MANAGEMENT TEAM RESOURCE DEFINITION

The function of the IDMT is to provide identity authentication and accountability support to incident command through the implementation of a comprehensive on-scene credentialing system. The IDMT function is dependent upon the establishment of a strong perimeter, as evidenced by the analysis of the Oklahoma City and Pentagon Incidents. The concept of operations also must include deferment of un-requested assets to a secondary staging area. The FEMA report *Responding to Incidents of National Consequence: Recommendations for America's Fire and Emergency Services Based on The Events of September 11, 2001, and Other Similar Incidents* recommends "There should be a separate marshalling area at the incident base for unrequested/unverified resources. This 'corral' concept was used in Oklahoma City. For added security, law enforcement should manage the perimeter of these areas."[40] This recommendation is incorporated into the IDMT concept of operations outlined in Figure 1.

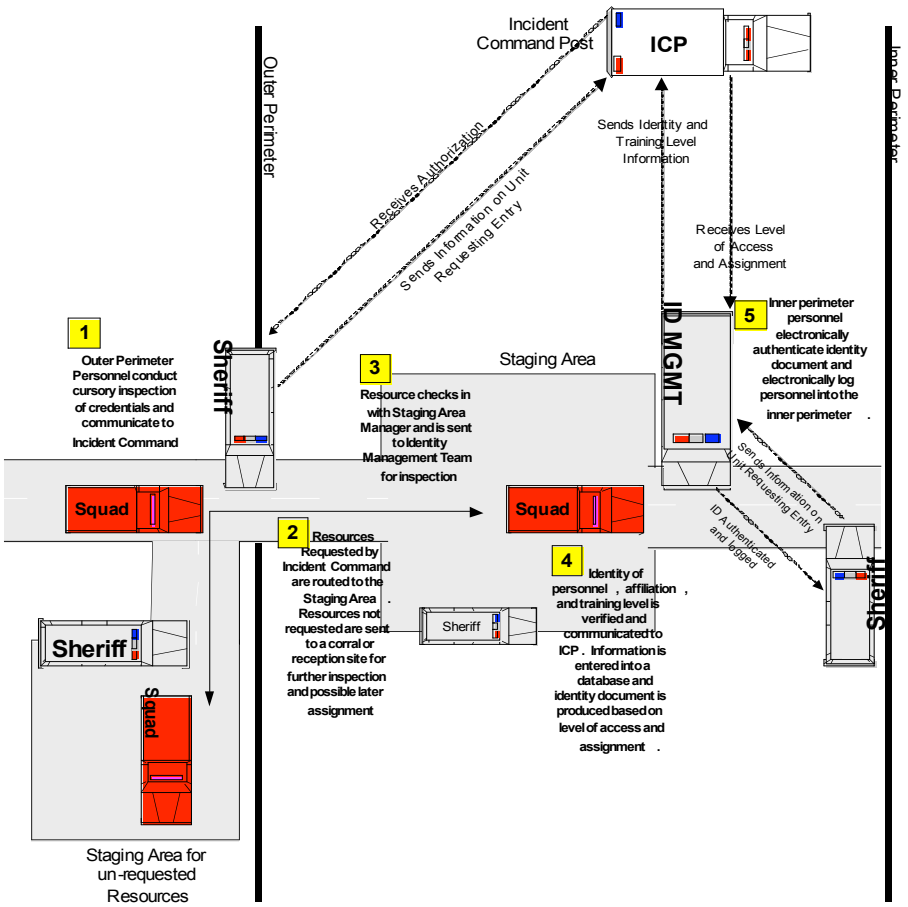

FIGURE 1: IDENTITY MANAGEMENT TEAM CONCEPT OF OPERATIONS

The study of the Oklahoma City bombing and the Pentagon attack also revealed the need for a consistent system of identity issuance. The Oklahoma City AAR detailed the process that was utilized to issue credentials; however, the Pentagon AAR does not provide sufficient detail that describes the mechanisms of the issuance process. The paper-based system that was developed out of necessity and availability of materials can be greatly enhanced with the advent of readily available technologies that can transfer data from existing identity credentials, such as readers for 2D barcodes or magnetic stripes that have been incorporated into many state drivers' licenses. In addition, the need to maintain connectivity to law enforcement and other databases allows for further inspection of identity as outlined in the resource definition (Table 1). This allows for verification of identity through other sources, should inspection and electronic implementation of available credentials require additional investigation.

Utilizing exploitable features of existing identity credentials, coupled with agency issued credentials, can greatly enhance the ability to examine documents and rapidly populate data into a database for a smooth and rapid process for credential issuance. In some jurisdictions it may also be possible to pre-populate the database with responder information/ biometrics that can be utilized in emergency response situations requiring tight scene controls. Individual jurisdictions or regions may choose to issue responder

credentials with exploitable technology that can further improve the on-scene credentialing process.

The Department of Defense program Defense Cross Credentialing Identification System (DCCIS) has developed a web-base option for identity verification for non-government personnel requiring access to government resources.[41] The Federation for Identity and Cross-Credentialing Systems (FiXS) maintains the ability to authenticate identity through the maintenance of a system that allows companies to keep their employee data in their own system that is only accessed when a credential is presented for authentication. The structure of the system alleviates privacy concerns as data is not maintained in a single accessible database. This model is not a strong option for applicability to identity management for incident response; communications have traditionally failed during response to incidents of terrorism. The dependence on a web-based system would require assurances of continued access throughout the evolution of an event. This is not a dependable option based on previous response experience.

The implementation of an interoperable or technology-based solution at the local or state level will continue to require a dedicated resource to manage identity. A technological solution does not eliminate the need for the function to be managed and maintained on-scene. In addition, not all responders will be issued the same credential, particularly across private-sector agencies that are critical to the success of response and recovery operations. Those not issued credentials pre-event will require the on-scene identity issuance capability of a defined identity management team.

COMPREHENSIVE NATIONWIDE IDENTITY SOLUTION FOR FIRST RESPONDERS

It would be reasonable to believe that the identity management problem – detailed in the after-action reports on every major incident of domestic terrorism – must have been resolved, considering the many reports of the many panels and commissions investigating terrorism response following 9/11. This is not the case. Although the gap has been identified and documented, these reports barely make mention of it. An implementable solution to the identity management gap for terrorism incident response has been mentioned in the reports, but is not included by any panel among its final recommendations. The following represents a summary of the identify management concepts outlined in post-9/11 homeland security reports. Many of the suggested solutions are limited to technological possibilities such as biometric identifiers, bar-codes, RFID, and smart cards, but fall short of providing concrete implementable solutions.

The concept of addressing identity through a comprehensive enterprise solution first appeared as a "standardized emergency responder identification and accounting system" to be coordinated by FEMA. This was first proposed in the National Emergency Management Association's October 2001 *White Paper on Domestic Preparedness*.[42] The explanation was limited to a bulleted point that provided no suggestion for the scope or methodology of the program. A "universal identification card" for positive identification of response personnel also appeared as an "area for future research and analysis, and subsequent conclusions and policy recommendations" in the third report of the *Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Gilmore Commission) published in December 2001.[43]

The explanation was also limited to a bulleted point that did not provide further description of the proposed program.

In the fourth Gilmore Commission report a "nation-wide law enforcement/first responder identification system" is proposed as a solution to the problem of inadequate authentication of identities for personnel operating systems and working in critical facilities.[44] In addition, the report suggests that "smart card" technology be included in a system that "must be able to be effectively used during mutual aid operations and other cooperative efforts between different levels of government and between different government entities at the same governmental level."[45] The proposed identity system solution is located in an appendix to the document and is not listed among the key recommendations of the panel. The placement in an appendix, lack of substantive explanation, and relative unimportance given to this solution in the report is perplexing. Additionally, the nexus between a system for the identification of law enforcement/first responders and the stated problem of authentication of the identity of personnel operating systems and working in critical facilities is unclear. This solution, identified in "Appendix L: Protecting Critical Infrastructure Against Terrorist Attacks" of the fourth Gilmore Commission, serves as a critical response capability, and should have been further developed and included among the key recommendations of the panel.

The necessity for standardized response identification is also cited in the Department of Homeland Security (DHS) Universal Task List (UTL). The UTL is one component of the DHS planning "tool-box" for its capabilities-based preparedness planning process. The UTL is a comprehensive list of seventeen hundred tasks and sub-tasks required to respond to the fifteen event scenarios outlined in the national planning scenarios. The UTL common task: Communication and Information Management contains the task "Establish role of operation area satellite system (OASIS) at the EOC."[46] As a sub-task "Establish a national authentication and security identification certification system for emergency responders, Federal, State, local and tribal personnel and other non-government personnel requiring access to affected areas" is listed.[47] The placement of the identity management concept is once again perplexing as it is listed as a sub-task to a disconnected overarching task regarding satellite systems. There is a pattern in the development of the first responder identity concept: although considered critical, it has been obscured under irrelevant and unrelated tasks and objectives. The importance of the concept warrants its direct recognition and inclusion as an overarching task.

The UTL serves to inform the companion planning document in the capabilities based planning process the Target Capabilities List (TCL).[48] The TCL is comprised of those three hundred tasks listed in the UTL that are deemed "critical" and grouped into thirty-six target capabilities.[49] The identified sub-task concerning emergency responder identification certification was not included among the three hundred UTL tasks that were deemed as critical and migrated into thirty-six critical capabilities in the TCL. The need for identity management at incident scenes is an essential response capability, a documented capability gap, and should be included as target capabilities, or at a minimum to be included as a sub-task.[50]

The identity management for first responder concept is also included in the RAND Corporation publication *Protecting Emergency Responders Volume 3: Safety Management in Disaster and Terrorism Response*. The publication outlines the recommendation to "develop personnel identification and credentialing systems better suited to major disaster response operations."[51] The document outlines several options

for achievement of the recommendation. Traditional solutions including color-coded event badges, armbands, and/or vests as identification are recognized as deficient because they offer only visual recognition and do not provide additional capabilities for accountability and training credentials.[52] Any identification and credentialing system must be part of pre-event preparedness and should include "their certifications, training levels, and other information on their general skills relevant to operating in a hazardous environment."[53] Technology options to achieve the recommendation include smart cards, bar-code identifiers, RFID, and biometric systems. The report contains the most comprehensive explanation of any of the listed programs; however, it falls short of providing a specific framework for implementation.

The National Memorial Institute for the Prevention of Terrorism, in *Project Responder: National Technology Plan for Emergency Response to Catastrophic Terrorism,* proposes a responder identity solution related to training and credentialing. The report calls for "a digital smart card/chip 'electronic transcript' system that securely verifies identification, levels of training/certification, and currency, for the multitude of responders that converge on the scene of a high-visibility CBRNE event."[54] The report recommends research, development, and piloting of a GPS-enabled "smart card" tested through multi-jurisdictional response exercises. The overarching goal is to provide the on-scene commander with technology that could broadcast "a rapid, accurate, and verifiable picture of resource and skill availability, and ensure the qualifications of each responder at the scene."[55] The report outlines a four-year process that includes research, implementation in three jurisdictions, evaluation, and standards development. While it seems comprehensive, the report does not provide specific information concerning implementation.

The literature related to identity management for incident response shows it as a clear and protracted problem. The AAR reports also show a clear capability gap for terrorism incident response. The post-9/11 panel and commission reports present a limited range of solutions that neglect specifics for implementation. The challenge presented by incident response identity management has only been included as a secondary or tertiary recommendation in numerous reports, and has not been the primary subject of investigation or research for incident response application. The solutions presented in the literature include standardized or universal identification for first responders that may include the use of technology such as biometric identifiers, bar-codes, RFID, and smart cards.

Opportunity Knocks: Federal Implementation of Smart Card Technology

The federal government is shifting its identity paradigm under *Homeland Security Presidential Directive-12: Policy for a Common Identification Standard for Federal Government Employees and Contractors* (HSPD-12). The goal of HSPD-12 is "to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors."[56] HSPD-12 further clarifies secure and reliable identity as consisting of the following criteria.

> Secure and reliable forms of identification for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering,

> counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application.[57]

The program being developed under HSPD-12 seeks to create a government-wide trust model. Ensuring that identification issued by any federal agency meets the same minimum standard in both process and product.

The Secretary of Commerce, through the National Institute for Standards and Technology (NIST), released the HSPD-12 directed government-wide standard on February 25, 2005. *Federal Information Processing Standard Publication 201: Personal Identity Verification (PIV) of Federal Employees and Contractors* (FIPS-201) outlines a two stage process to meet the listed criteria for a "secure and reliable form of identification." The stated goal of FIPS-201 is "to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to federally controlled government facilities and electronic access to government information systems."[58]

The initial implementation stage, Personal Identity Verification One (PIV-I), includes the description of required processes to meet security and control mandates for identify proofing of individuals for issuance of federal identification cards under HSPD-12. The federal PIV card will only be issued by accredited agencies and will utilize a process consisting of three necessary components.[59] First, the applicant will personally appear. Second, the applicant will present two forms of identity source documents as certified by the Office of Management and Budget[60] (with at least one being issued by a state or federal authority) and submit to necessary biometric screening.[61] Finally, the applicant will be screened through a National Agency Check with Written Inquiries (NACI), Office of Personnel Management (OPM), or National Security community background investigation including fingerprint identification.[62]

The second stage of implementation outlined by FIPS-201, Personal Identity Verification Two (PIV-II), includes the physical and technical elements to support interoperability aspects of HSPD-12. The federal PIV card bases identity authentication on a three-tiered system: the real-time comparison of biometrics (fingerprint and/or photographic), "something you are;" combined with the card itself, "something you have;" and a PIN numerical, "something you know."[63] The tiers backed by the distribution and identity-proofing standards outlined by PIV-I provide a secure identity solution that meets the requirements mandated by HSPD-12. The addition of PKI enabled digital certificate remote network verification architecture provides an additional level of security for both physical and logical access, as the status can be revoked without requiring the physical collection of the PIV card.

The PIV card mandated by FIPS-201 consists of common physical characteristics and appearance elements with allowances for slight variation for specific agency purposes. In an effort to standardize, the physical make-up of the card is consistent with International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) requirements. FIPS-201 contains five slightly varied approved models for card fronts and three variations for the back of approved PIV cards. In addition to the Integrated Circuit Chip (ICC) standardization aspects, the models allow flexibility for the inclusion of magnetic stripe and/or bar code technology for agency-

specific applications. Certain fields are mandated on the front of the PIV card, such as name, photograph, affiliation, agency, and expiration date. Required elements on the back of the card include card serial number and agency issuer identification

FIPS-201 (PIV-II) also describes the technical requirements for PIV interoperability, with further detail provided in a series of related NIST and industry technical publications. There are five basic technical requirements governing the federal PIV card. FIPS-201 provides standardization requirements for the card ICC, a Card Holder Unique Identifier (CHUID), PIV Card Activation, the PIV authentication data (one asymmetric key pair and corresponding certificate), and biometric data. FIPS-201 requires that the PIV card contain both contact and contactless ICC interfaces. The ICC interfaces are mandated to be consistent with ISO/IEC and *FIPS 140-2: Security Requirements for Cryptographic Modules Standards* which, when coupled with card reader standardization required by FIPS-201, achieves government-wide interoperability.[64]

The required CHUID must include an expiration date, asymmetric signature field, and Federal Agency Smart Credential Number (FASC-N) that uniquely identifies and tracks each card. The CHUID must be readable from both contact and contactless interfaces. FIPS-201 mandates that the specific technical requirements outlined by NIST SP800-73: *Interfaces for Personal Identity Verification* for the CHUID and FASC-N be incorporated into PIV cards. The requirements for the asymmetric signature field must be encoded as a Cryptographic Message Syntax (CMS) as outlined in the Internet Engineering Task Force report RFC 3852 and NIST SP 800-78: *Cryptographic Algorithms and Key Sizes for Personal Identity Verification.*

The PIV card is required to include personal identification number (PIN) based cardholder activation. The PIN must be accepted by the card before it will activate for release of biometric and asymmetric key information. The PIN must meet the standards outlined in FIPS PUB 140-2. The inclusion of a PIN activated system allows for greater card security as the information is not transmitted until contact interface is successful and the correct PIN has been entered.

The PIV card authentication data must, at minimum, consist of one asymmetric private key and a corresponding X.509 public key certificate stored on the card. [65] All keys are accessed only through the contact ICC interface and must not be exportable from the card. The card may also contain additional keys and PKI certificates based on specific agency needs. The X.509 PKI certificate allows for remote network verification through Online Certificate Status Protocol (OCSP) and the Certificate Revocation List (CRL) that must in routine situations be updated by agencies at least every eighteen hours. The inclusion of authentication data allows for the card certificate status to be verified through a secure remote network adding a strong layer of security.

The final technical requirement of FIPS-201 is the inclusion of biometric data on the PIV card. The following biometric information is collected during the card issuance process: full-set of fingerprints, electronic facial image, and two electronic fingerprints. The full set of fingerprints is not electronically stored and is utilized only for law enforcement background checks. An electronic facial image is printed on the card face and may, but is not required to be, stored on the card. Two electronic fingerprints (right and left index finger) are required to be included on the card for biometric authentication. The technical specification mandates for collection and inclusion of

biometric data on the PIV card are located in NIST SP-800-76: *Biometric Data Specification for Personal Identity Verification*.

The federal Personal Identity Verification project mandated by HSPD-12 and described by FIPS-201 provides the basis for a secure identity program far surpassing any current efforts to provide identity management solutions to government employees. The federal program is being implemented in two stages. Under PIV-I the process for identity proofing including background investigations, document requirements, and agency accreditation is administered. The second stage, PIV-2, outlines the technical and interoperability requirements for the federal smart PIV card. The reliance on interoperable smart card technological capabilities such as inclusion of biometric identifiers and encrypted PKI certificates provides identity verification at levels far beyond currently employed solutions (Figure 2). The PIV project and its inherent flexibility provide a secure identity model that could be replicated and applied to first responder identity for terrorism incident response applications at the state and local level.

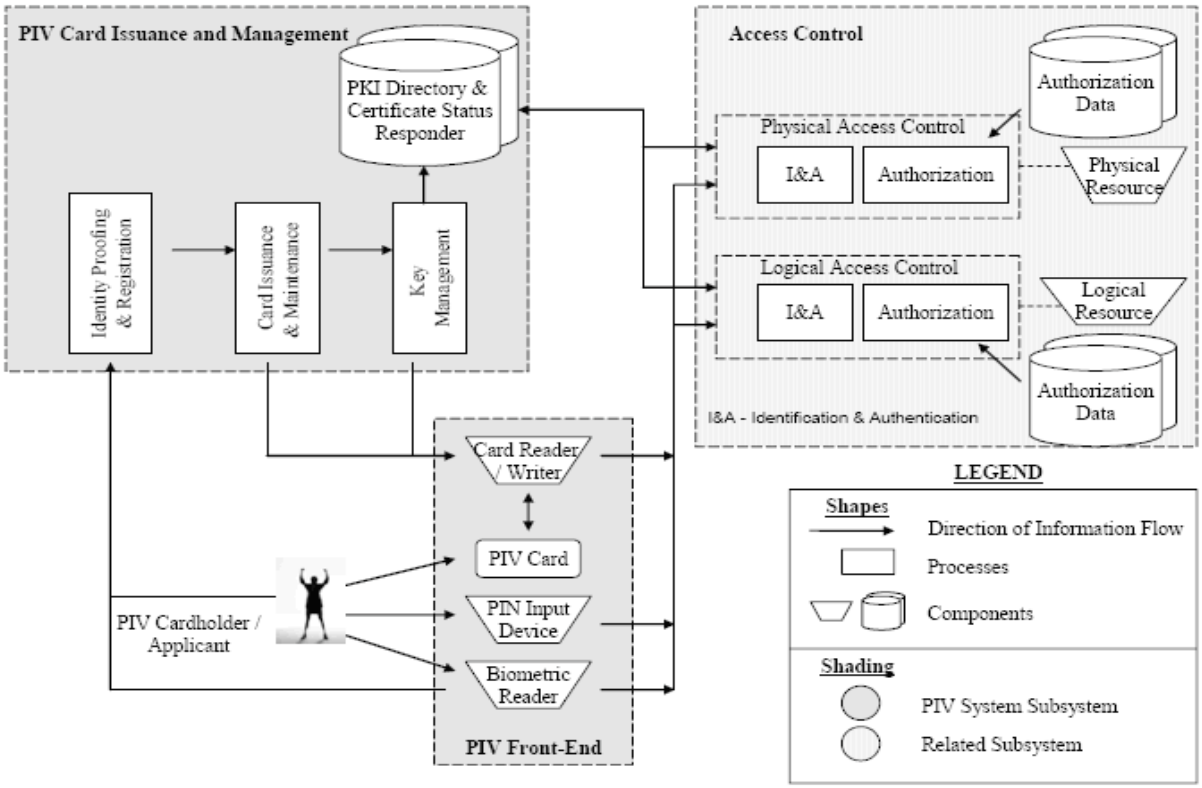

FIGURE 2: PIV CARD SYSTEM COMPONENT MODEL[66]

Local Implementation of HSPD-12 programs: The National Capital Region

The unique multi-jurisdictional nature of the National Capital Region (NCR) has made it the first region to recognize the need to develop a comprehensive project to implement an HSPD-12/FIPS-201-based identity smart card for first response personnel. The NCR consists of the District of Columbia and bordering counties from Maryland and Virginia. HSPD-12 has required federal agencies to implement FIPS-201;

implementation of the standard has not been mandated for state and local governments. The NCR is the first entity to attempt to replicate the federal program on the state and local level. The blurred lines of federal, state, and local responsibility that are unique to the region make a common identity standard capable of electronic authentication a necessity. The multi-jurisdictional nature of incident response in the region necessitates a common interoperable platform to authenticate identity and affiliation across levels of government. The NCR project, titled the First Responder Authentication Card (FRAC), utilizes the standards outlined in FIPS-201 PIV-II to develop a platform capable of interoperability with federally issued smart identity cards.

The NCR FRAC is based entirely on the standards outlined by FIPS-201 PIV-II. One of the major impediments to the implementation of a pure FIPS-201 PIV-I and PIV-II compliant identity card for state and local first responders is the background check requirement. As described in previous sections, FIPS-201 requires a fingerprint check and National Agency Check with Written Inquiries (NACI) for all personnel to be issued a federal identity credential. The heart of an identity trust model is the security of both the issuance process and the product (token). If the model is vulnerable to infiltration during the issuance process, or the finished product is subject to counterfeit, there is no trust and authentication will be suspect. At the state and local level the cost of conducting FIPS-201-compliant background investigations on all first responders would be exorbitant.

In many communities only the background investigations conducted on law enforcement officers may meet the standard outlined by FIPS-201. The pre-employment identity verification procedures of other response disciplines, including fire, EMS, public works, public health, and clinical care, would not meet the standard. In order to meet PIV-I enrollment standards, additional investigation of employees would be required. This raises numerous concerns ranging from personal privacy to the significant additional and associated costs. The NCR FRAC has addressed this problem by delineating levels of authentication based on the scope of enrollment procedures. This allows for a graduated trust model where four increasing levels of authentication are defined based upon the depth of procedures prior to credential issuance. It does not preclude agencies with minimal procedures from inclusion in the program; however, when the card is electronically authenticated the level of authentication is displayed allowing the user to determine if additional scrutiny is necessary. The graduated model ensures maximum participation among local governments (due to limited additional financial commitments) while maintaining a level of trust.

The NCR was ground-zero on 9/11. The response to the terrorist attack on the Pentagon revealed a pervasive identity gap, as documented in previous sections of this article. In addition, the NCR also has the unique and frequent need for identity authentication of first responders from dozens of agencies across all levels of government for daily operations. The FRAC is a necessary element in the NCR for both daily operations and response to critical incidents such as those created by terrorist attacks.

The NCR FRAC program is moving through the research and evaluation stage. In February 2006, interoperability was tested through a limited enrollment and multi-jurisdictional exercise dubbed "Winter Fox." The interoperability and authentication capability was targeted by the exercise that took place in four locations including the Pentagon, Port of Baltimore, Virginia Department of Transportation, and Frederick

County, MD. The exercise sought to examine the ability to electronically validate PKI certificates of FIPS 201 standardized smart cards through four different back-end architectures. The cards used in the exercise included the NCR FRAC, Maryland FRAC, Transportation Security Administration Transportation Worker Identity Credential (TSA TWIC), and the Department of Defense Common Access Card (DoD CAC). Each of the identified cards is maintained through different back-end infrastructures. The exercise sought to test the capability to validate personnel identity across the disparate infrastructures.

The exercise utilized hand-held readers that received satellite downloads of certificate revocation lists every twenty-four hours. The readers were utilized to read and validate PKI-enabled FIPS-201 smart cards. The Winter Fox exercise resulted in 285 scans of the smart cards with disparate back-end architectures. Of the scans, seventy-nine resulted in PIN verification failures.[67] This means that 28% of the attempts were unable to be validated by the back-end architecture because of incorrect PIN entry, or more simply cardholder error. The 206 scans where the user did not err in PIN entry resulted in 100% validation. This provides strong evidence of the interoperable capability of FIPS smart cards. The hand-held reader also has the ability to read, but not validate, 2D barcodes contained on most driver licenses. Several driver licenses were read, but were not validated as part of the exercise.

Opportunity Knocks: Personnel Certification and Credentialing under the National Incident Management System

The National Incident Management System (NIMS) also describes the need for personnel certification and credentialing. NIMS describes personnel certification and credentialing as:

> Personnel certification entails authoritatively attesting that individuals meet professional standards for the training, experience, and performance required for key incident management functions. Credentialing involves providing documentation that can authenticate and verify the certification and identity of designated incident managers and emergency responders.[68]

The NIMS Integration Center (NIC) is working toward solutions for part of the identity management problem for incident response identified earlier in this article. The NIC has formed working groups to develop standards for training, experience, and currency for specific positions within each response discipline. When developed, these standards will ensure standardization across jurisdictions and provide common terminology for determining personnel qualified to assist in the accomplishment of objectives on incident scenes.

The program to date has fallen short on prescribing a method to verify identity. The lack of an identity-authentication solution to couple with training standards limits the effectiveness of the program. Without verification the program fails to develop trust. The current direction of the program is strengthening only the vetting process and fails to back that more stringent process with a trusted identity token. The NIC efforts to implement personnel certification standards, backed by an identity token than can be authenticated and is strongly resistant to counterfeit, would vastly improve identity management for terrorism incident response

CONCLUSIONS

The previous sections detail the pervasive failures of identity management in the response to incidents of domestic terrorism. The failures are significant and potentially high-consequence for future responses, but not so insurmountable nor without solution that they need be repeated again. The first step in solving the problem is recognition and comprehension of the problem. This article serves as a first step in recognizing and defining the problem of identity management for terrorism incident response. The analysis of incident after-action reports and other related documentation reveals a pattern of identity management failure in the response to large-scale incidents of terrorism that, when analyzed, provides a framework for a solution. It must be recognized that examining response in the past does not provide a complete solution for the future; the possible hazards of the future must also be considered. The consideration of plausible scenarios, such as the threat of secondary attack, serves to inform a proposed solution to potential threats in the future.

The success or failure of the federal government and the National Capital Region in the implementation of HSPD-12 and the NCR FRAC will impact the future of identity management at the state and local level. Although the HSPD-12 program was developed for the purpose of security, efficiency, fraud protection, and privacy, the program could potentially mitigate the previous failures of terrorism incident response if broadly applied to the first-response community across levels of government. The exercise and evaluation of the NCR FRAC program is critical in determining the potential of the program for mitigating identity management problems endemic to the historical incident response to terrorism.

Although the focus of this article was limited specifically to terrorism incident response, secure verifiable identity has benefits beyond this limited scope. Identity management for the full spectrum of the homeland security mission is in desperate need of attention and creative problem solving. A potential solution must incorporate the identity management issues of other homeland security mission areas in order for it to be comprehensive.[69] Incident response is just one dimension of need as it relates to identity management for overall homeland security. A comprehensive solution can also bolster terrorism prevention and protection mission capabilities.

For example, the HSPD-12/NCR FRAC smart card program can provide additional benefits through the ability to improve physical access control at government facilities nationwide. The United States General Accounting Office report *Security: Breaches at Federal Agencies and Airports* details the success of undercover agents in penetrating nineteen federal buildings and two commercial airports without screening, through the use of fraudulent law enforcement credentials. "At the 21 sites that our undercover agents successfully penetrated, they could have carried in weapons, listening devices, explosives, chemical/biological agents, devices, and/or other such items/materials."[70] The report details another dimension of the identity management capability gap that can be addressed by the broad application of credentials capable of electronic authentication. This is possible through the implementation of PKI-enabled smart card technology for the protection of critical infrastructures. A comprehensive identity management program utilizing HSPD-12/NCR FRAC framework would prevent those agents or terrorists of the future from penetrating secure sites through unverifiable fraudulent credentials.

The HSPD-12/NCR FRAC program also provides the ability to improve information system security by incorporating card readers into computer access. Incorporated physical access control provides two layers of security for logical systems. The first hurdle for a potential assailant is entering the physical location; the computer card reader option provides a second level of security. An incorporated smart card option decreases the potential for cyber attack through on-site infiltration with this two-layer process.

The FIPS-201/NCR FRAC program can also benefit other government operations. According to the *CIO/ PKI Smart Card Project: Approach for Business Case Analysis of Using PKI on Smart Cards for Government-wide Applications*, implementing smart card technology with digital forms improves efficiency because it "reduces paperwork, eliminates redundant data entry, and improves data accuracy as transcribing and data entry errors are eliminated"[71] A smart card-based system implemented with e-government initiatives creates public value and cost savings in other areas of government processes. The many additional benefits of the implementation of smart card technology can help address some of the concerns of cost relative to the public value it creates.

There are several impediments to the nationwide implementation of a comprehensive HSPD-12/NCR FRAC model identity solution. The first impediment is problem recognition. This article has explored the problem of identity management for terrorism incident response for the purpose of increasing awareness. If the success of the NCR FRAC program continues, the solution will likely develop awareness about the problem it solves before the problem itself is broadly recognized. An NCR FRAC type program may appear to those unaware to be a solution searching for a problem.

The second impediment is cost. One problem the NCR FRAC program has been unable to mitigate is the continuing cost of program maintenance. The program is dependent upon back-end infrastructure (PKI certificates) provided by private sector certificate authorities. Each digital certificate requires an enrollment fee and a yearly maintenance fee for the three-year life of the certificate. The cost of the card and digital certificate for the three year life of the card is approximately $125-$150.[72] The continuing cost associated with the program is a major impediment to broad implementation by local governments.

The State of Illinois provides an example for reducing the costs of private sector management of digital identity certificates. Illinois has established itself as a certificate authority to lower the long-term costs associated with management of digital identity. The program was originally established for financial transactions with the state, but has application to first responder identity. The state is currently developing a project to credential its first responders with PKI enabled smart cards. The Illinois example, of states serving as certificate authorities, could potentially drive down the continuing costs for broad local implementation of smart card technology for first responder identity. The success or failure of implementation in Illinois could also have far-reaching implications for first responder identity management.

The efforts of the NIMS Integration Center (NIC) program to define personnel certification for incident response must be joined with efforts to provide secure verifiable identity. Personnel position definitions without a method for identity verification provide only minimal incremental improvement for incident response. The efforts of the NIC must be joined with interoperable identity initiatives.

The past failures of identity management in the response to incidents of terrorism must be recognized and brought to the forefront of homeland security policy and planning at the state and local level. Creating a mechanism to positively answer the critical the questions "who is this?" and "what can they do for me?" can have benefits far beyond incident response to terrorism. A comprehensive solution could potentially be incorporated into the hardening of physical and logical facilities bolstering terrorism prevention and protection capabilities. The cost of continued ignorance could potentially be catastrophic.

Mark Landahl leads the Homeland Security Section of the Frederick County (Maryland) Sheriff's Office in suburban Washington, D.C. In that capacity he oversees the full spectrum of homeland security activities including policy and plan development, the delivery of related training, and homeland security investigations and intelligence. He received his bachelor's degree in political science/education from the State University of New York College at Cortland and is a 2006 graduate of the Center for Homeland Defense and Security's master degree program at the Naval Postgraduate School. Mr. Landahl also serves as an adjunct assistant professor at University of Maryland University College (UMUC). He is currently developing courses for the new major in homeland security at UMUC. Mr. Landahl can be reached at mlandahl@fredco-md.net.

---

[1] Joe Haberstroh and Steve Wick, "Military Impostor Fools Coast Guard," *New York Newsday*, July 27, 1996.

[2] *The American Heritage Dictionary of the English Language*, 4th ed., s.v. "Identity."

[3] Ibid.

[4] City of Oklahoma City, *Alfred P. Murrah Federal Building Bombing April 19, 1995: Final Report* (Stillwater, OK: Fire Protection Publications, 1996), 369.

[5] Ibid, 39.

[6] Ibid, 219-220.

[7] Oklahoma City National Memorial Institute for the Prevention of Terrorism, *Oklahoma City - Seven Years Later: Lessons Learned for Other Communities* (Oklahoma City: MIPT, 2002), 11.

[8] Ibid, 10

[9] Titan Systems Corporation, *Arlington County: After Action Report on the Response to the September 11 Terrorist Attack at the Pentagon* (Arlington, VA: n.d.), C-23.

[10] Ibid, A-69.

[11] Ibid, A-20.

[12] Ibid, C-28.

[13] McKinsey & Company, *Improving NYPD Emergency Preparedness and Response* (New York: McKinsey & Company, 2002), 17.

[14] National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: Norton & Co, 2004), 336.

[15] McKinsey & Company, *Improving NYPD Emergency Preparedness and Response*, 17.

[16] Brian Houghton and Jonathan Schacter, "Coordinated Terrorist Attacks Implications for Local Responders," *FBI Law Enforcement Bulletin* 74, no. 5 (May 2005), http://www.fbi.gov/publications/leb/2005/may2005/may05leb.htm

[17] U.S. Department of Homeland Security and the Federal Bureau of Investigation, *Information Bulletin: Potential Terrorist Use of Public Safety or Service Industry Uniforms, Identification, or Vehicles* (Washington, DC: DHS, n.d.), 1-4, http://www.iafc.org/associations/4685/files/DHSFBI%20alert.pdf

[18] Gary R. Gordon and Norman A. Wilcox, *Identity Fraud: A Critical National and Global Threat* (Utica, NY: Utica College, Economic Crime Institute, 2003), 6.

[19] AP Foreign Desk, "Excerpts from the Reagan Interview with 4 Correspondents," *New York Times*, December 4, 1987.

[20] U.S. Department of Homeland Security SAFECOM Program, "Interoperability," http://www.safecomprogram.gov/SAFECOM/interoperability/default.htm

[21] Sharon S. Dawes, et. al., *Information, Technology, and Coordination: Lessons from the World Trade Center Response* (Albany, NY: University at Albany, SUNY, Center for Technology in Government, 2004), 9.

[22] National Commission on Terrorist Attacks upon the United States, *Staff Statement No. 14* (Washington, DC: n.p., n.d.), 8.

[23] Federal Emergency Management Agency, United States Fire Administration, *The World Trade Center Bombing: Report and Analysis* (Emmitsburg, MD: USFA, 1993), 135.

[24] U.S. Department of Homeland Security, Federal Emergency Management Agency, *Typed Resource Definitions: Law Enforcement and Security Resources* (Washington, DC: FEMA, 2005), 2.

[25] City of Oklahoma City, *Alfred P. Murrah Federal Building Bombing*, 369.

[26] Ibid., 39.

[27] Ibid., C-217

[28] Oklahoma City National Memorial Institute for the Prevention of Terrorism, *Oklahoma City - Seven Years Later*, 11.

[29] City of Oklahoma City, *Alfred P. Murrah Federal Building Bombing*, C-217.

[30] Ibid.

[31] Ibid.

[32] Ibid.

[33] Titan Systems Corporation, *Arlington County: After Action Report*, C-23.

[34] Ibid., A-69.

[35] Ibid.

[36] Ibid., C-58.

[37] Ibid., A-69.

[38] Ibid., C-23.

[39] Ibid.

[40] Federal Emergency Management Agency, United States Fire Administration, *Responding to Incidents to National Consequence: Recommendations for America's Fire and Emergency Services Based on the Events of September 11, 2001, and Other Similar Incidents* (Washington, DC: FEMA, 2004), 50.

[41] *Federation for Identity and Cross Credentialing Systems*, "Welcome to FiXS," http://www.fixs.org/

[42] *White Paper on Domestic Preparedness* (Lexington, KY: National Emergency Management Association, 2001), 3, http://www.nemaweb.org/Library/Documents/Preparedness.PDF

[43] *Third Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Arlington, VA: Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, 2001), 60.

[44] *Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Arlington, VA: Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, 2002), L-12.

[45] Ibid.

[46] *Universal Task List: Version 2.1* (Washington, DC: U.S. Department of Homeland Security, Office of State and Local Government Coordination and Preparedness, 2005), 16. Additional Note: There is a new version of the Universal Task list that has additional tasks related to identity management under the heading of common tasks. It is located on www.llis.gov, but contains no date or official markings and is not in the same format as other documents related to the National Preparedness Goal. The author utilizes the UTL 2.1 document dated May 23, 2005.

[47] Ibid.

[48] *Target Capabilities List: Version 1.1* (Washington, D.C.: U.S. Department of Homeland Security, Office of State and Local Government Coordination and Preparedness, 2005), 3-4. Additional Note: The author utilizes the TCL 1.1 dated April 23, 2005 as it is the only non-draft version. There are also two draft versions of TCL 2.0, one dated December 2005 and a more recent draft dated September 2006. Both exist as draft versions and contain more information related to identity management including the recognition of a credentialing capability in a TCL phase two under development. The author utilizes the current accepted policy which is guided by TCL 1.1 as the other versions are in draft format.

[49] The TCL defines critical tasks as those prevention, protection, response, and recovery tasks that require coordination among an appropriate combination of federal, state, local, tribal, and private-sector, and non-governmental entities during a major event in order to minimize the impact on lives, property, and the economy. The identified critical tasks must be performed to prevent occurrence prior to a major event or respond by reducing a loss of life or serious injuries, mitigate significant property damage, or are essential to the success of the Homeland Security mission.

[50] The September 2006 Draft of the TCL contains more information related to identity management including the recognition of a credentialing capability to be included in TCL phase two (under development). The draft indicates the recognition of the importance of identity management, but as it is not present in current guiding policy (TCL 1.1) the recommendation is made by the author.

[51] Brian A. Jackson et al., *Protecting Emergency Responders Volume 3: Safety Management in Disaster and Terrorism Response* (Arlington, VA: RAND, 2004), 34-35.

[52] Ibid., 34.

[53] Ibid., 35.

[54] Thomas M. Garwin, Neal A. Pollard, and Robert V. Tuohy, eds., *Project Responder: National Technology Plan for Emergency Response to Catastrophic Terrorism* (Oklahoma City, OK: MIPT, 2004), 116.

[55] Ibid.

[56] *Homeland Security Presidential Directive HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors* (Washington, DC: The White House, August 2004), 1.

[57] Ibid.

[58] U.S. Department of Commerce, National Institute of Standards and Technology, *Federal Information Processing Standards Publication 201: Personal Identity Verification (PIV) of Federal Employees and Contractors* (Washington, DC: NIST, 2005), 1.

[59] In order to be accredited agencies will be required to implement the guidelines set forth in NIST Special Publication 800-79 Guidelines for Certification and Accreditation of PIV Card Issuing Organizations.

[60] Acceptable identification documents are described on Form I-9, OMB No. 1115-0136 Employment Eligibility Verification.

[61] National Institute of Standards and Technology, *Publication 201*, 6.

[62] Ibid.

[63] Ibid., 10-11.

[64] The Associated technical publications include ISO/IEC 7816, ISO/IEC 10373 (1&3), ISO/IEC 14443 (1-4), ISO/IEC 10373 (6), Crypto-Modules FIPS 140-2.

[65] The specifications for X.509 certificates are contained in Federal Identity Credentialing Committee Publication: *X.509 Certificate and CRL Extensions Profile for the Common Policy*.

[66] National Institute of Standards and Technology, *Publication 201*, 11.

[67] Craig Wilson, "Winter Fox Interoperability Demonstration," presentation at the meeting of the Government Smart Card Interagency Advisory Board, 15 March 2006, 14, http://www.smart.gov/iab/presentations/IABmeetingMarch2006.pdf.

[68] U.S. Department of Homeland Security, *National Incident Management System* (Washington, DC: DHS, 2004), 46

[69] The homeland security mission areas are described in the Department of Homeland *Security Target Capabilities List*. The mission areas include prevention, protection, response, and recovery.

[70] U.S. General Accounting Office, Office of Special Investigations, *Security: Breaches at Federal Agencies and Airports* (Washington, D.C.: GAO, 2000), 3.

[71] U.S. General Services Administration, *CIO PKI/Smart Card Project: Approach for Business Case Analysis of Using PKI on Smart Cards for Government-wide Applications* (Washington, DC: GSA, 2001).

[72] Jason Miller, "GSA Sets HSPD-12 Price Point" *Federal Computer Week*, July 15, 2007, http://www.fcw.com/article103084-06-25-07-Print/