EMERGENCY SERVICES SECTOR COORDINATING COUNCIL

Charting A Path Forward On Crisis Reentry

For the Emergency Services Sector:

Report of the

Emergency Services Sector Coordinating Council

March 21, 2012

REPORT TRANSMITTAL COVER MEMORANDUM

The lack of a standard national protocol for coordinated multi-jurisdictional crisis reentry is unquestionably one of the top concerns of the Nation's critical infrastructure firms as well as public and private sector emergency responders.

This gap is highly relevant to the Mission of the Emergency Services Sector Coordinating Council (ESSCC) to "protect and promote the capability of the Emergency Services Sector to provide services to the public, the other sectors, and the nation", and its Strategy of communicating to DHS and others relevant Emergency Services Sector "policies, guidelines, programs, standards and best practices".

In furtherance of the ESSCC's Mission and Strategy, an ESSCC Working Group ("Working Group") prepared a report on a plan for bringing Sector-wide leadership, nationally, to meet the Nation's need for a standardized and coordinated national approach to Emergency Responder cross-jurisdictional disaster reentry. That report has now been adopted by the ESSCC as an ESSCC Report, approved by the ESSCC Association Members listed on its first page, and transmitted by means of this Transmittal Cover Memorandum.

This ESSCC Report includes both technical and policy recommendations to the ESSCC's Association Members, as well as policy recommendations to DHS and Congress.

This Report includes a model Joint Standard Operating Procedure (JSOP) which is recognized as a best practice and National Template for Nationwide Adoption, but, for budgetary and other reasons, is not proposed as a national mandate at this time. ESSCC does not support a national mandate at this time, either through grant guidance or legislation. Adoption of the model should be at the discretion of localities/states, with the ability to modify based on their unique needs.

The ESSCC has come together to craft a path forward on crisis reentry access for the Emergency Services Sector and other affected Sectors. The ESSCC and its Association Members are working together to achieve the Report's recommendations, and we welcome and urge efforts of others to enhance the Nation's all hazard response and recovery capabilities through coordinated support for the Report, its recommendations, and the JSOP.

John Thompson, Chair | Shawn Kelley, Vice Chair

March 21, 2012

Table of Contents

Attachments

###

ASSOCIATION MEMBERS OF THE EMERGENCY SERVICES SECTOR COORDINATING COUNCIL

American Ambulance Association

American Public Works Association

Central Station Alarm Association

Electronic Security Association

International Association of Chiefs of Police

International Association of Emergency Managers

International Association of Fire Chiefs

National Association of State EMS Officials

National Association of Security Companies

National Association of State Fire Marshalls

National Emergency Management Association

National Sheriffs' Association

National Native American Law Enforcement Association

Security Industry Association

EMERGENCY SERVICES SECTOR COORDINATING COUNCIL
Initial Report of the
Credentialing & Disaster Reentry Working Group

Executive Summary

The lack of a standard national protocol for coordinated multi-jurisdictional crisis reentry is unquestionably one of the top concerns of the Nation's critical infrastructure firms and both public and private sector emergency responders.

This gap is highly relevant to the Mission of the Emergency Services Sector Coordinating Council (ESSCC) to "protect and promote the capability of the Emergency Services Sector to provide services to the public, the other sectors, and the nation", and its Strategy, which includes "determining and communicating the vulnerabilities, needs and requirements" of the Emergency Services Sector, and "communicating to DHS and all CIP sectors regarding [Emergency Services Sector] policies, guidelines, programs, standards and best practices".

In furtherance of its Mission and Strategy, the ESSCC formed a Credentialing & Disaster Reentry Working Group ("Working Group") with a Mission to "bring Sector-wide leadership, nationally, to meet the Nation's need for a coordinated standardized national approach to Emergency Responder cross-jurisdictional credentialing and disaster reentry."

The work of the Working Group was carried out through a series of meetings between May and December 2011. A key decision of the Working Group was to use the FEMA "Building Resilience Through Public-Private Partnerships" Conference After Action Report ("AAR") as the "road map" for the work of the Working Group and for its recommended path forward for the Emergency Services Sector.

This Initial Report reflects the findings and recommendations of the Working Group, including policy recommendations to the ESSCC that it approve and adopt this Initial Report, and make certain recommendations to DHS and to Congress. In addition to technical and phased adoption recommendations, the Working Group recommends[1] that the ESSCC:

-Recognize a Template Joint Standard Operating Procedure ("Template JSOP") attached to the Initial Report as a National Template for nationwide adoption and urge ESSCC Association Members to approve and adopt this Initial Report;

-Recast the Working Group as a permanent Committee of the ESSCC tasked with organizing and supporting a National Crisis Reentry Governance Board;

-Support a series of activities associated with governance, adoption, training and exercising of the Template JSOP;

-Make recommendations to DHS regarding activities in support of governance, adoption, training and exercising of the Template JSOP; and

-Recommend and urge that Congress support use of the Template JSOP as a National Template for nationwide adoption, and explore the possibility of providing Federal grants to support its nationwide adoption

[1] See "**Policy Recommendations for The Path Forward on Crisis Reentry**", p. 35 below, for actual language.

EMERGENCY SERVICES SECTOR COORDINATING COUNCIL
Initial Report of the
Credentialing & Disaster Reentry Working Group

Introduction

Coordinated All Hazards/All Sector Cross-Jurisdictional Crisis Reentry: A National Imperative

The lack of a standard national protocol for coordinated multi-jurisdictional crisis reentry is unquestionably one the top concerns of the Nation's critical infrastructure firms and both public and private sector emergency responders. Over the past decade, the Nation's critical infrastructure firms have developed a corps of emergency management professionals charged with minimizing the impact of disasters on their firms, the communities they serve, and the Nation's financial and Homeland Security. These private sector emergency managers, ultimately responsible for managing many aspects of the Nation's response and recovery from many different types of crises, want and need a common, standardized, all hazard approach to managing entry by their essential personnel into any crisis zone in the Nation. However, because no such common national approach exists today, and because most reentry planning now occurs, if at all, at the county level, and then to address a specific type of hazard (e.g., hurricanes), critical infrastructure firms must approach each crisis as a new, after-the-fact, ad hoc response.

The consequent confusion and delays not only impacts private sector emergency response, but also creates an unnecessary burden on the public sector emergency services personnel who implement disaster reentry or themselves respond into restricted areas. The current lack of a standard protocol not only retards recovery, but has the potential to increase the disaster's casualties and damage (e.g. by hindering containment and damage repair at nuclear or chemical facilities). Further, since communities disrupted by a disaster are more vulnerable to terrorist and criminal adversaries, and since premature return of citizens to a disaster area puts such citizens at risk, the lack of a consistent, easily understood basis for decision-making by law enforcement personnel controlling access increases the danger of inappropriate persons circumventing security measures, to the jeopardy of the communities, the inappropriate entrants themselves, and authorized emergency services responders within the restricted area.

The lack of a common, standardized national approach, formally incorporated into the National Incident Management System (NIMS), is a major national problem, not only for Federal policymakers, but also for on-the-ground emergency responders. Many, many, local leaders responsible for managing entry into emergency zones after a major crisis have themselves seen failures caused by lack of a common crisis reentry protocol operating across multiple jurisdictions, and have been, themselves, required to make very difficult crisis reentry decisions fraught with unnecessary risks for themselves and for their communities.

> All disasters are local.
>
> …
>
> The private sector is what gets communities back up and running.
>
> FEMA Deputy Administrator Richard Serino, Nov. 14, 2011

Because local officials have the initial authority and responsibility for every disaster, as well as some level of on-going authority for every disaster, regardless of scale, crisis reentry is viewed as a problem to be addressed first by local and state officials. As state and local decision-makers balance the need to admit critically needed responders and exclude inappropriate personnel, a common, standardized approach would both assist their decision-making process and better ensure that their decisions are effectively and expeditiously implemented, to the benefit of the public. Since every state and locality is at risk of suffering a natural or man-made disaster, the public benefits of such an improvement in emergency management would be national in scope.

The Emergency Services Sector Coordinating Council: Crafting a Path Forward for the Nation's Public & Private Emergency Responders

Recognizing the critical nature and scale of this national problem, the unique experience of the Emergency Services Sector in past disaster response, the dependence of this Sector on resolution of this issue if it is to improve the effectiveness of and protection for emergency services responders in future disasters, and the need and opportunity to make a difference in addressing it, the Emergency Services Sector Coordinating Council (ESSCC) has exercised leadership to collaboratively craft a path forward for the Nation's public and private emergency responders by formulating a national standard on disaster reentry as an essential step in fulfilling its assigned Mission.

The vehicle selected by the ESSCC in crafting this path forward is a Credentialing & Disaster Reentry Working Group ("Working Group") led by Lenny Millholland, Sheriff of Winchester, VA, Chair, and John Walsh, International Association of Emergency Managers, Vice Chair. Over several months, the Working Group heard from law enforcement, emergency management and emergency response field operations personnel, considered the relevant issues with input from Subject Matter Experts made available for the effort, developed and finalized this Initial Report, and recommended that it be approved, adopted and advanced by the ESSCC.[2]

As this Initial Report makes clear, the recommendations set forth here, and the actions to be taken pursuant to those recommendations, do not represent completion of the task of charting a path forward on crisis reentry for the Emergency Services Sector—they

[2] For purposes of this Initial Report, the Working Group members do not purport to speak for the organizations with whom they are affiliated. Accordingly, this Initial Report does not necessarily reflect the views of any organization that has not adopted it.

represent the first step. Accordingly, this Initial Report recognizes that the work of the Emergency Services Sector Coordinating Council will extend into the future, until the path forward has been fully charted and a solid foundation has been laid for coordinated crisis reentry, nationwide, by public and private emergency response and recovery personnel.

The Emergency Services Sector Coordinating Council ("ESSCC")

As context for this Report's findings and recommendations, this Section provides background information on the Emergency Services Sector and the ESSCC, including its strategy, goals and organizational components. For accuracy, this Section quotes extensively from ESSCC authoritative source documents.

The Emergency Services Sector

> The Emergency Services Sector (ESS) … forms the Nation's first line of defense for preventing and mitigating day–to–day incidents as well as catastrophic situations. The ESS encompasses a wide range of emergency response functions with the primary mission to save lives, protect property and the environment, assist communities impacted by disasters (natural or manmade), and aid recovery from emergency situations. In the ESS, owners and operators represent multiple distinct disciplines and systems that inherently reside in the public safety arena within State and local government agencies, but which also include private, for–profit businesses.[3]
>
> As the first line of defense and primary protector or of the public and—in the direct context of national CIKR protection efforts, the other CIKR sectors—the loss or incapacitation of ESS capabilities would clearly impact the Nation's security, public safety, and morale.
>
> The emergency services sector encompasses all fire, rescue and emergency, sworn law enforcement, EMS, and emergency management personnel. The extent of the sector extends beyond "first responders" to those who provide specialized, prevention, or investigative capabilities, and personnel and services that directly support emergency services capabilities, including but not limited to emergency services administrative/operational staff, public safety answering points and dispatch, corrections and public works. The sector is primarily a public sector, but does include private sector holdings such as industrial fire departments, sworn private security officers, private EMS providers, etc. It should be noted that the ESS does not include emergency rooms and their personnel, which are healthcare sector assets.[4]

ESSCC Mission[5]

> The mission of the ESSCC is to protect and promote the capability of the ESS to provide services to the public, the other sectors and the nation.

ESSCC Strategy[6]

[3] Taken from "Critical Infrastructure Partnership Advisory Council, 2011", ("CIPAC"), at p. 1.

[4] See http://www.sheriffs.org/about/ESSCC2.asp, accessed July 22, 2011. Note that the "ESSCC and the Health Care SCC are in agreement that the transfer of a patient to definitive care represents a transfer point between the two very-interdependent sectors." Id.

[5] This section quotes extensively from the ESSCC's authoritative governance document, "Emergency Services Sector Coordinating Council (ESSCC) Organizational And Governance Structure" (July 2008).

The ESSCC will accomplish its mission by:

- determining and communicating the vulnerabilities, needs and requirements of the ESS to protect its infrastructure to DHS, and other sectors and stakeholders;
- communicating to DHS and all CIP sectors regarding ESS policies, guidelines, programs, standards and best practices;
- providing realistic, all–hazard, locally–oriented public safety and emergency management information to DHS and other C IP sectors; and
- establishing effective mechanisms for information sharing among and between DHS and the ESS.

ESSCC's Strategic Goals[7]

To enact the strategy and accomplish the mission, the ESSCC cooperative activity must undertake a series of short and long-term goals. The sector's organizational structure is framed to support the following goals.

- Gather data, information, or feedback from public safety and emergency services leadership across the country on issues identified by the sector, DHS, other federal agencies, or other critical infrastructure sectors.
- Work within the diverse community of the ESS and with other sectors to identify and examine issues, and recommend courses of action regarding critical infrastructure protection. Specifically, identifying ways public safety can protect themselves, and what public safety needs to protect other critical infrastructure.
- Provide access to experienced practitioners, best practices, and the emergency services leadership at the local level.
- Educate and inform the emergency services community on federal, state, and local initiatives relating to critical infrastructure protection.
- Communicate the critical infrastructure protection needs and ideas of the emergency services sector to the federal government.
- Support [an] emergency services sector Information Sharing and Analysis Center (ISAC) to gather, analyze and disseminate to its members alerts, warnings, advisories and an integrated view of information system and other infrastructure vulnerabilities.
- Work in cooperation with DHS and other federal agencies to contribute to the National Infrastructure Protection Plan and Emergency Services Sector Specific Plan.

Community Representation in the ESSCC[8]

The organization of the ESSCC is structured to both maximize the wealth of diverse perspectives, and maintain an effective, collaborative decision–making process.

[6] Id.

[7] Id.

[8] Id.

The scope of the emergency services sector is state and local officials who have a direct ("on the ground"/incident scene) responsibility and accountability for emergency management and response; and who have the ability to prevent an emergency or coordinate a response to such an emergency. This includes volunteer, career and industrial fire service (and the full range of diverse response capabilities those responders have, e.g. HazMat, search and rescue, EMS, etc.), sworn law enforcement and their private–sector counterparts, state and local emergency managers, and pre-hospital medical services including public, private and volunteer providers.

Role of Associations in the ESSCC[9]

The public safety and emergency service community will be involved primarily through associations. There are 2 reasons for this approach: (1) the associations represent the leadership of their respective constituencies and parent 2) associations are a proven vehicle for reaching out to a wide representation of a given sector. A sector organized through professional organizations representing the various types of emergency service providers can, with the proper support, provide a number of services.

- Dissemination of information to hundreds–of–thousands of emergency service workers.
- Information gathering from national and international emergency service workers.
- Facilitating sector collaboration and cross–sector outreach.

All participants are expected to serve as stewards within their organizations or agencies to educate colleagues and constituencies about various efforts to prevent and respond to incidents–natural or man–made–involving critical infrastructure or key national assets. Participants will serve as an outreach tool, while concurrently providing input back to the sector.

This Initial Report, which aims at charting a path forward on crisis reentry for the Nation's emergency services sector, is intended to advance the ESSCC's mission, strategy and strategic goals by building on the diverse perspectives of the emergency services sector represented by the ESSCC's Association Members.

[9] Id.

ESSCC Working Group Mission, Composition & Processes

Recognizing the critical nature and scale of the national problem of crisis reentry, and the need and opportunity to make a difference in addressing it, the ESSCC formed the Credentialing & Disaster Reentry Working Group ("Working Group") and charged it with the task of collaboratively developing and proposing a path forward for the Nation's public and private emergency responders. This Section provides information on the Working Group.

Working Group Mission Statement

The Mission of the Emergency Services Sector Credentialing & Disaster Reentry Working Group is to bring Sector-wide leadership to bear, nationally, to meet the Nation's need for a coordinated standardized national approach to Emergency Responder cross-jurisdictional credentialing and disaster reentry.

The Working Group will meet this Mission by vetting, refining and promoting adoption of national standards, processes, protocols and best practices in credentialing and disaster reentry affecting the Emergency Services Sector, working with other Sector Coordinating Councils whenever possible.

In doing so, the Working Group will seek out approaches that are practical for adoption and implementation by public and private Emergency Service Sector agencies and firms, and will specially focus on building blocks for a coordinated and standardized national approach, including credentialing and disaster reentry standards and protocols, and a standard approach to emergency responder job titles and/or certifications.

Members of the Working Group

Lenny Millholland - Sheriff, Winchester, VA/ National Sheriffs' Association, Chair

John Walsh - International Association of Emergency Managers, Vice Chair

Steve Amitay – National Association of Security Companies

John Chwat – Electronic Security Association

Pat Credeur – National Rural Water Association

Richard T. Garcia – FBI InfraGard National Members Alliance (SME)

Shawn Kelley - International Association of Fire Chiefs

Dennis Kelly - Pegasus Program/InfraGard National Members Alliance (SME)

Vincent MacNeill – Securitas USA, Inc.

David McBath - International Association of Chiefs of Police

Tom Rhatigan - National Sheriffs' Association (staff)

Lance Ross -National Emergency Managers Association

Leslee Stein-Spencer - National Association of EMS Officials

Jim Willey - American Dental Association

Working Group Processes

The Working Group was formed by the ESSCC's leadership during the Spring of 2011, following prior internal ESSCC discussions and consultation with stakeholders. Once chartered, the Working Group held a series of meetings between May and December of 2011, at which Subject Matter Experts organized presentations by field operations personnel and presented information to the Working Group members regarding credentialing and disaster reentry. Working Group Subject Matter Experts (SMEs), understood to have a different set of perspectives and interests than other Working Group Members and ESSCC Association Members, were not considered voting members of the Working Group.

Working Group meetings were conducted in accordance with pre-published Agendas[10], and, in most cases, with pre-distributed presentation materials. Following formal presentations, Members were given the opportunity to ask questions and share their own perspectives. Every effort was made to assure broad-based participation and to achieve Working Group consensus on Working Group decisions and recommendations.

Perhaps the most important of the Working Group's decisions was its decision to use the FEMA "Building Resilience Through Public–Private Partnerships" Conference After Action Report as the "road map" for the work of the Working Group and for the path forward on crisis reentry for the Emergency Services Sector.

FEMA AAR: Strategic Road Map for the Working Group and the Path Forward

In August, 2011, FEMA published its "Building Resilience Through Public–Private Partnerships" Conference After Action Report ("AAR"), summarizing findings and recommendations reached at that Conference.

A key section of that AAR, entitled "The Road Best Taken is Best Without Boundaries", focuses on the problem of crisis reentry, and was found by the Working Group to be entirely on–point to the work of the Working Group, and extremely well–grounded in its approach.

After review and discussion of the AAR, the Working Group, by consensus, agreed to utilize "The Road Best Taken is Best Without Boundaries" as the road map for its work going forward, and as the road map for the path forward on crisis reentry for the Emergency Services Sector. In this context, the following section discusses and quotes extensively from "The Road Best Taken is Best Without Boundaries".

[10] Copies of Working Group Meeting Agendas and Minutes are available upon request to the ESSCC Secretariat.

"The Road Best Taken is Best Without Boundaries": Road Map for the Work of the Working Group

As noted above, the FEMA After Action Report on the "Building Resilience Through Public–Private Partnerships" Conference ("AAR")[11] contains a key section, entitled "The Road Best Taken is Best Without Boundaries". That section of the AAR focuses on the problem of crisis reentry, and, after review, the Working Group adopted it as the "road map" for its work and for the path forward on Crisis Reentry for the Emergency Services Sector.

The FEMA AAR

This section contains the findings of "The Road Best Taken is Best Without Boundaries" FEMA AAR, quoting directly and extensively from that document.

> **Vision:** All government jurisdictions nationwide offer the private sector consistent credentialing, access and waivers across jurisdictional lines nationwide, in support of a disaster.[12]
>
> **Background**
>
> Access to disaster sites by non-emergency responders is a long-standing challenge that has been hard to resolve – in large part due to the vast number of jurisdictions involved at all levels of government nationwide.
>
> This [AAR] vision session included a cross-section of about 30 of the nation's top retail, shipping, finance, grocery, home-building, sporting and utility companies; state and city emergency managers; Urban Area Security Initiatives and regional partnerships; standards organizations; and members of sector advisory councils. Following a brief overview of the current status of credentialing efforts by the facilitators, this highly experienced group discussed disaster relief credentialing (providing ID's to businesses and individuals for disaster site access), weight restrictions and general access issues.
>
> The focus of the discussion quickly gravitated to the broader issue of access and how to develop a system that local jurisdictions can use to govern the ability of the private sector to enter restricted areas without hindering the disaster response. Credentials are cards that can be provided ahead of time, but any such access management system must be able to provide just-in-time access. Weight restrictions may also limit a disaster response by restricting the flow of resources to a disaster zone. Participants expressed that they deal with weight restriction conflicts episodically, but were not sure if these restrictions actually impeded the ability to respond. Nevertheless, there was broad agreement that a process for requesting receiving waivers should be developed in each state and made known to all local jurisdictions.

[11] FEMA,"Building Resilience Through Public–Private Partnerships" After Action Report (August 2011).

[12] Id. at 12.

Challenges

- *Tackling the Right Problem – Credentialing vs. Access*: Before the discussion could move too far down the road, the group had to decide whether the real issue at hand actually involved credentialing, or whether it was really a broader issues of access within which credentialing might just be one of many tools.
- *Consistent Processes*: Several participants in both the public and private sectors shared good practices they had either instituted or experienced, demonstrating that there are solutions – but the major challenge is establishing broader, more consistent practices. Related barriers include building trust, access management system, process and protocols.
- *Bottom-Up or Top-Down Approach*: There was much discussion regarding how to best implement common access protocols - from the top down (with the federal government creating the guidance) or from the bottom up (with local and state jurisdictions setting the guidance). Some participants believed that the process had to be top down, because the issue crosses state and other jurisdictional lines, while others were adamant that a federal approach cannot be enforced effectively at the local level.

Solutions

- *Focus on Access*: After initial discussion about credentialing, the group rapidly came to agreement that the actual issue is not credentialing, but the broader issue of access.
- *Create Process-Driven Solution*: The solution to access issues should be driven by process, rather than by technology or distribution of cards. Part of the process should be a just-in-time mechanism for providing access; this could be as simple as sharing contact lists in a database system or could include interoperable credentials.
- *Document and Train*: Regardless of the process developed, it must be committed to writing, turned into protocols, placed into a General Order by the relevant jurisdiction. Relevant public and private entities would then need training. Furthermore, these processes must then be collected, aggregated, shared, and updated. By documenting, collecting, and sharing these processes, it will become easier to foster broader, more consistent practices across the board.
- *Use a Collaborative Approach*: Building trust is another important part of the solution, and along with this effort, a collaborative approach. Ultimately, participants determined that access issues could only be move toward resolution through a combination of top-down and bottom-up approaches. Rather than set rules that need to be enforced, build consensus and buy-in by demonstrating good examples and offering templates, tools, resources and even mentoring.
- *Organize Nationally, Implement Locally*: The group agreed that a national organization like NEMA, IAEM, NGA or similar could play an important role in

implement any recommendations. This organization would help convene the various stakeholders, be the authoritative resource for research and catalogue efforts, and be a rallying point for future efforts by the private sector and non-federal organizations, should they wish to promote legislative or policy changes. To ensure appropriate regional adaptation, national and regional, state, and local associations could all be key factors in synthesizing the effort.

Conclusion and Actions

Despite the known complexities of the issue of disaster site access and credentialing, the group delivered several productive and decisive recommendations for a way forward, including:

- *Multi-Tiered Approach:* Any strategy must include all levels of government- federal, state, tribal, territorial, and local
- *Communication and Outreach Strategy:* At the crux of the access issue is trust and knowledge. The strategy must go beyond laws or mandates, and include avenues that foster ongoing, long- term networking and collaboration between those who need access and those in charge of maintaining the security and integrity of a disaster site. Additionally, outreach to educated specific groups will be an important component – for example, sheriffs and emergency management associations.
- *Tools and Resources:* A successful strategy will be supported by collection of tools and resources that are readily available to the public and private sectors. Suggested items include:
    - A nationally accessible collection of good practices from the private sector and government
    - An umbrella initiative to identify and connect existing efforts to resolve this issue
    - Dedicated points of contact at the state/tribal/territorial/local levels, who can maintain the networks year around and handle emergency requests.
    - A reference catalogue of existing state regulations and authorities impacting access
    - Sample enabling legislation from states that have put this in place
    - Standards to provide general guidelines
    - A collaborative web site, such as a Wiki, where the public and private sectors can post the disaster site best practices related to access issues and work together to build newer, better solutions.[13]

Application of the FEMA AAR by the Working Group

Consistent with the guidance of the AAR and "The Road Best Taken is Best Without Boundaries", after discussion, the Working Group determined by consensus that it would:

[13] Id. at 12-14 (emphasis supplied).

- **Focus on Access Issues, not Credentialing:** The Working Group determined that it would focus on issues surrounding Access Control, and would cooperate with other initiatives that are focusing on Credentialing.[14]
- **Focus on a Solution Driven by Reentry Operational Processes.** The Working Group concurred with the AAR's view that access solutions should be driven by crisis reentry operational processes, rather than by technology or new credentials.
- **Focus on a Documented Template Protocol on Which Responders Can Be Trained.** In view of the JSOP's adoption and implementation in Louisiana and Mississippi, the Working Group, by consensus, undertook to evaluate and vet the JSOP as a possible template for nationwide adoption, as a common multi-jurisdictional crisis reentry protocol. In that effort, the Working Group heard from members of the Louisiana Working Group, and from law enforcement, emergency management, and public and private emergency responders who reported on the process by which the JSOP was initially developed and was subsequently implemented in Louisiana and Mississippi.
- **Focus on Building Trust and Buy-In through Collaboration instead of Mandates.** In addition, in crafting this Report, the Working Group sought to craft a path forward built on collaborative approaches rather than mandates, all in accordance with the AAR.
- **Focus on A Key Role for National and State Associations to Implement Recommendations.** The ESSCC, which itself is organized around national associations serving the emergency services sector, fully recognizes the value of working through associations, as recommended by the AAR. As part of its efforts to evaluate and vet the Template JSOP as a national template, the Working Group sought to identify and validate key roles for national and state associations as a key implementation strategy.

In addition, the Working Group concurred with and had additional comments on the AAR's recommendations on the following points:

- **Multi-Tiered Approach:** While the Working Group concurs that any strategy must include all levels of government—federal, state, tribal, territorial, and local—all involved must recognize the special roles and authorities of local government in crisis reentry: elected local officials and local emergency managers ordinarily establishes reentry policy, and local law enforcement ordinarily operates checkpoints and emergency zones. In addition, the Working Group is especially concerned that any national strategy must

[14] The ESSCC is aware of and is cooperating with several credentialing initiatives, including the following:

- State, Local, Tribal, Territorial Government Coordinating Council (SLTTGCC)–developing a common credentialing program for non-federal government personnel
- International Association of Fire Chiefs (IAFC)– developing a common credential for the Fire Service.
- PIV–I FRAC Technology Transfer Working Group (TTWG)–promoting adoption of PIV–I Standard Credentials for public and private sector personnel.
- National Sheriff's Association Credentialing Standard–PIV–I, RFID and Basic Credential (varying costs), available for adoption by any industry or sector group.

See Working Group Memorandum to PIV-I/FRAC Technology Transition Working Group (TTWG), entitled "Comments Proposed for Consideration by the TTWG", dated Oct. 7, 2011, at Attachment A.

include private sector response and recovery personnel, a constituency whose reentry needs are vitally important and valued on par with those of government. Finally, the Working Group is concerned that long-term viability of any strategic approach is not realistic unless there is on-going "ownership" of the governance effort by an identified entity or set of entities.

- **Communication and Outreach Strategy:** The Working Group concurs that any strategy must be built on trust and must foster ongoing, long- term networking and collaboration between those who need access and those in charge of maintaining the security and integrity of a disaster site. The Working Group also especially concurs with the AAR's view that outreach to sheriffs and emergency management associations is particularly critical. The Working Group is concerned that long-term viability of any communications and outreach strategy is not realistic unless there is on-going "ownership" of the effort by an identified entity or set of entities.
- **Tools and Resources:** The Working Group concurred with the AAR's view that any strategy must be supported by tools and resources that are readily available to public and private sector entities and essential personnel. The Working Group is concerned that long-term availability of tools and resources is not realistic without on-going "ownership" of the "best practices" effort by an identified entity or set of entities.

The JSOP: Background and Status

This section discusses the development and current implementation of the JSOP, and outlines the Working Group's evaluation of the Template JSOP as a template for nationwide adoption.

Background on the JSOP's Development

The JSOP is the product of efforts initiated shortly after Hurricane Katrina to address the significant problems created for law enforcement and critical infrastructure firms in managing reentry into the Katrina emergency zone in Louisiana and Mississippi.

Starting in 2006, leadership of the National Sheriff's Association ("NSA") and of the InfraGard National Member's Alliance ("InfraGard National"), separately began the processes of seeking solutions for the problem of crisis reentry. An initial approach to the problem, focusing on credentialing, was pursued, but it became clear that, though definitely related, the solutions to problem of crisis reentry access control are truly different from the solutions to the problem of credentialing, and that a solution focusing on a standard crisis reentry protocol was needed.

2009 Multi-State Full Scale Exercise: Texas and Louisiana

In 2008, InfraGard National and NSA began working together on developing a prototype protocol that could be tested and refined in the field. Based on a strategic partnership with NSA announced in January of 2009, subsequently joined by the Association of Contingency Professionals and other stakeholders, InfraGard National sponsored a Multi-State Full Scale Exercise conducted in Harris and Galveston Counties, Texas and in St. John and St. Charles Parish, Louisiana on May 19, 2009.

An overview of the 2009 Multi-State Full Scale Exercise follows.[15]

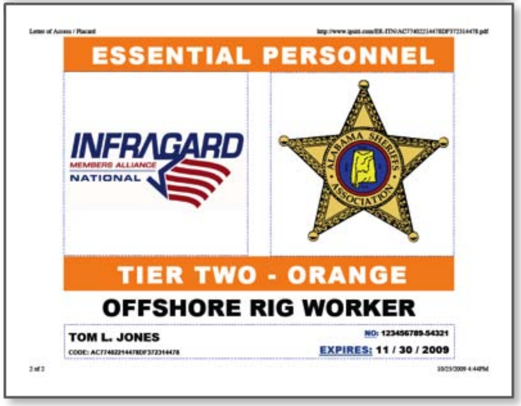
[15] The 2009 Multi-State Full Scale Exercise was conducted in conformance with the DHS HSEEP Program. The Exercise AAR and other Exercise documents are available through the ESSCC Secretariat.

Overview: INMA-sponsored Offshore/Energy Sector Crisis Area Reentry Exercise
May 19, 2009

The Offshore/Energy Sector Crisis Area Reentry Exercise was sponsored by the InfraGard National Members Alliance. It was conducted on May 19, 2009 through three Exercise Scenarios based on real-world hurricane recovery activities conducted by Offshore/Energy Sector emergency responders during the "Tier 2" period—after the most critical disaster response activities have ceased and before the general public is allowed to reenter.

Exercise stakeholders were led by oil & gas industry leaders and the Energy Security Council. The exercise involved law enforcement checkpoints very professionally operated by the Louisiana State Police, St. John Parish, LA Sheriff's Office, St. Charles Parish, LA Sheriff's Office, Harris County, TX Sheriff's Office and Galveston County, TX Sheriff's Office.

The Exercise grew out of the tremendous problems experienced by oil and gas and other large commercial firms with tremendous assets and operations in reentering disaster areas after Hurricane Katrina in 2005 and Hurricane Ike in 2008.



Letter of Access / Placard

http://www.ipsiti.com/ER-ITN/AC77402214478DF372314478.pdf

ESSENTIAL PERSONNEL

INFRAGARD
MEMBERS ALLIANCE
NATIONAL
ALABAMA SHERIFFS ASSOCIATION

TIER TWO - ORANGE

OFFSHORE RIG WORKER

TOM L. JONES
CODE: AC77402214478DF372314478

NO: 123456789-54321
EXPIRES: 11 / 30 / 2009

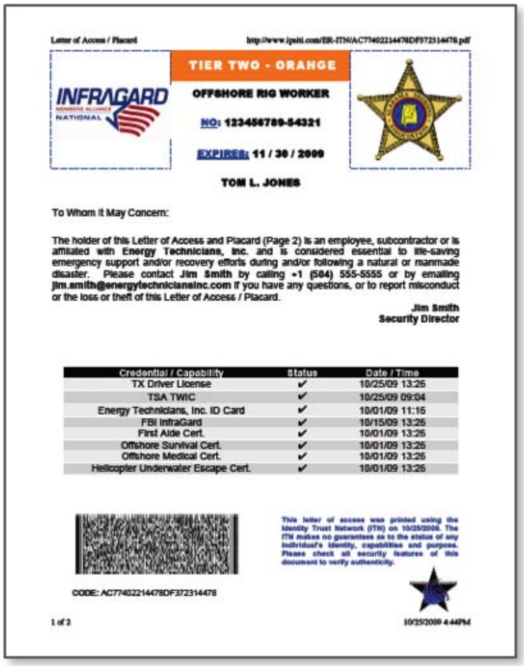
2 of 2

10/25/2009 4:44PM

The Exercise tested a Pegasus-provided system that enables large-scale commercial firms in the oil and gas, telecommunications, and other critical infrastructure sectors to go to one place to apply for reentry authority from law enforcement anywhere in the Nation and to provide law enforcement with verified information about the persons seeking reentry. Key to the Exercise was the testing of a common vehicle Placard format to supplement placards available at the county level, which might be recognized by all counties in a disaster area after a major national event, and a Letter of Access that contains information about the identity and credentials of persons authorized to reenter.

The System and approach developed and utilized as part of the Exercise were very well-received, and, based on the success of the Exercise, InfraGard is pursuing a follow up pilot project and exercise for the healthcare industry and a National Level Exercise (NLE) involving InfraGard's 30,000 members nationwide.

For additional information, please contact:
Rich Garcia, INMA Exercise Lead, 713.241.1870
Sheriff Tommy Ferrell (Ret.), NSA Past President, 601.431.0101
Lee Colwell, President, Pegasus Research Foundation, 501.442.0790
Dennis Kelly, President, InfraGard New Orleans, 504.251.0240



Letter of Access / Placard

http://www.ipsiti.com/ER-ITN/AC77402214478DF372314478.pdf

INFRAGARD
MEMBERS ALLIANCE
NATIONAL

TIER TWO - ORANGE

OFFSHORE RIG WORKER

NO: 123456789-54321

EXPIRES: 11 / 30 / 2009

TOM L. JONES

To Whom It May Concern:

The holder of this Letter of Access and Placard (Page 2) is an employee, subcontractor or is affiliated with **Energy Technicians, Inc.** and is considered essential to life-saving emergency support and/or recovery efforts during and/or following a natural or manmade disaster. Please contact **Jim Smith** by calling **+1 (504) 555-5555** or by emailing **jim.smith@energytechniciansinc.com** if you have any questions, or to report misconduct or the loss or theft of this Letter of Access / Placard.

Jim Smith
Security Director

Credential / Capability	Status	Date / Time
TX Driver License	✔	10/25/09 13:26
TSA TWIC	✔	10/25/09 09:04
Energy Technicians, Inc. ID Card	✔	10/01/09 11:16
FBI InfraGard	✔	10/15/09 13:26
First Aide Cert.	✔	10/01/09 13:26
Offshore Survival Cert.	✔	10/01/09 13:26
Offshore Medical Cert.	✔	10/01/09 13:26
Helicopter Underwater Escape Cert.	✔	10/01/09 13:26

This letter of access was printed using the Identity Trust Network (ITN) on 10/25/2009. The ITN makes no guarantees as to the status of any individual's identity, capabilities and purpose. Please check all security features of this document to verify authenticity.

CODE: AC77402214478DF372314478

1 of 2

10/25/2009 4:44PM

INMA-Sponsored Offshore/Energy Sector Crisis Area Reentry Exercise
Exercise Stakeholders

InfraGard National Members Alliance

- **InfraGard Chapters**
- **New Orleans, Baton Rouge,**
- **Lafayette & Houston**

Major Oil Company

LA GOHSEP

St. Charles Parish OEP

St. John Parish OEP

Galveston County Sheriff's Office

FBI-New Orleans Field Office

Port of South Louisiana

MS River Maritime Association

Securitas Security Services

NALCO Company

National Sheriffs' Association

Pegasus Program

Energy Security Council

LA State Police

St. Charles Parish Sheriff's Office

St. John Parish Sheriff's Office

Harris County Sheriff's Office

FBI-Houston Field Office

Port of St. Bernard OHS-EP

Crescent River Port Pilots

Blue Marine Security

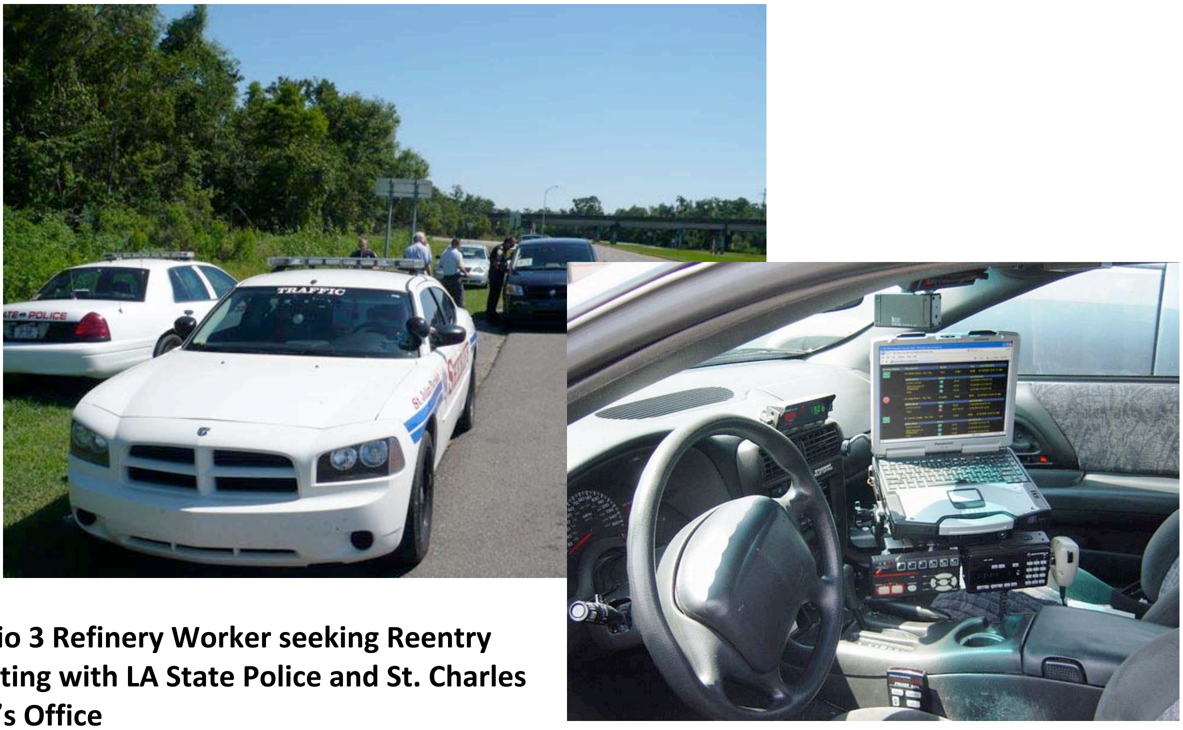
Rob Muller, MD

Exercise Crisis Response Center

Scenario 2 Offshore Rig Worker Seeking Checkpoint Reentry

Scenario 3 Refinery Worker seeking Reentry at St. John Sheriff's Office Checkpoint

Scenario 3 Refinery Worker seeking Reentry at St. Charles Sheriff's Office Checkpoint



Scenario 3 Refinery Worker seeking Reentry interacting with LA State Police and St. Charles Sheriff's Office

2010 Multi-State Full Scale Exercise: Texas/Louisiana/Mississippi/Alabama

Based on lessons learned from the 2009 Multi-State Full Scale Exercise, and other activities following up on it, InfraGard National sponsored a second Multi-State Full Scale Exercise in 2010. The 2010 Multi-State Full Scale Exercise was conducted in Galveston County, Texas, Lafourche Parish, Louisiana, Harrison County, MS and Calhoun County, AL on April 6 and 7, 2010.

Based on the results of the 2010 Multi-State Full Scale Exercise, the county emergency managers of Harrison, Hancock, and Jackson Counties, MS, led by Rupert Lacy, Harrison County, MS Emergency Management Agency, implemented the prototype protocol used for the 2010 FSE as a voluntary reentry protocol for those counties for the 2010 Hurricane Season.

An overview of the 2010 Multi-State Full Scale Exercise follows.[16]

[16] The 2010 Multi-State Full Scale Exercise was conducted in conformance with the DHS HSEEP Program. The Exercise AAR and other Exercise documents are available through the ESSCC Secretariat.

2010 Gulf South Disaster Reentry Full Scale Exercise

April 6 and 7, 2010

The 2010 Gulf South Disaster Reentry Full Scale Exercise was sponsored by the InfraGard National Members Alliance. It was conducted on April 6 and 7, 2010 through four Exercise Scenarios (locations) based primarily on real-world hurricane recovery activities conducted by emergency responders, critical infrastructure and support personnel from a variety of industry sectors. The processes and data system utilized for the Exercise were very well received, and, based on the success of the Exercise, us being operationally-deployed in the Gulf Coast Region prior to the 2010 Hurricane Season. A summary of the Exercise follows:

Goals

- Test the Emergency Responder ID Trust Network® designed to improve the ability of emergency responder, critical infrastructure and support organizations to 1) discover access requirements and operating procedures for law enforcement jurisdictions where they have facilities or operations; 2) inform law enforcement checkpoints of which essential personnel have been dispatched for duty; 3) easily and quickly share updated, validated and required identity information for each of their essential personnel to demonstrate qualifications and confirm identity.
- Test the Pegasus Emergency Responder ID Card as an optional second photo ID for those responders that require a stronger method to verify their identity nationwide.
- Test a Joint Standard Operating Procedure (Joint SOP) as a candidate to be used by multiple law enforcement agencies within a large region such as the Gulf Coast.

Scenarios and Locations

- Hurricane Response (Galveston, Lafourche and Harrison Counties)
- Tornado Response (Calhoun County)

Recovery Phases

- Reentry Condition 1 – immediate, critical disaster response activities underway prior to recovery and rebuilding
- Reentry Condition 2 – after the most critical disaster response activities have ceased and before the general public is allowed to reenter

Checkpoint Communications

- Full Internet Access via Computer in Vehicle or Handheld Device
- Full Internet Access via Radio Relay to Dispatch Center or Command Post
- No Internet or Radio Communications Available (Printed Documents Used Only)

Participants and Represented Sectors

- Approximately 190 individuals from more than 65 organizations (various roles)
- 7 law enforcement agencies and multiple Fortune 500 companies
- Oil, Gas & Chemical, Electric Utility, Telecom, Banking & Financial Services, Insurance, Healthcare, Information Technology, Transportation, Maritime, Pipeline, Debris & Waste Removal, Manufacturing, Private Security, Government, Education and Volunteers

For additional information, please contact:

Rich Garcia, INMA Exercise Lead, 713.241.1870
Sheriff Tommy Ferrell (Ret.), NSA Past President, 601.431.0101
Lee Colwell, President, Pegasus Research Foundation, 501.442.0790
Dennis Kelly, President, InfraGard New Orleans, 504.251.0240

INFRAGARD
MEMBERS ALLIANCE
NATIONAL

Partial List of Participants

Law Enforcement

Galveston County, TX Sheriff’s Office
Galveston, TX Police Department
Lafourche Parish, LA Sheriff’s Office
Louisiana State Police
Harrison County, MS Sheriff’s Office
Gulfport, MS Police Department
Calhoun County, AL Sheriff’s Office
FBI-Houston Field Office (Observer)
FBI-New Orleans Field Office (Observer)

Associations and Other Stakeholders

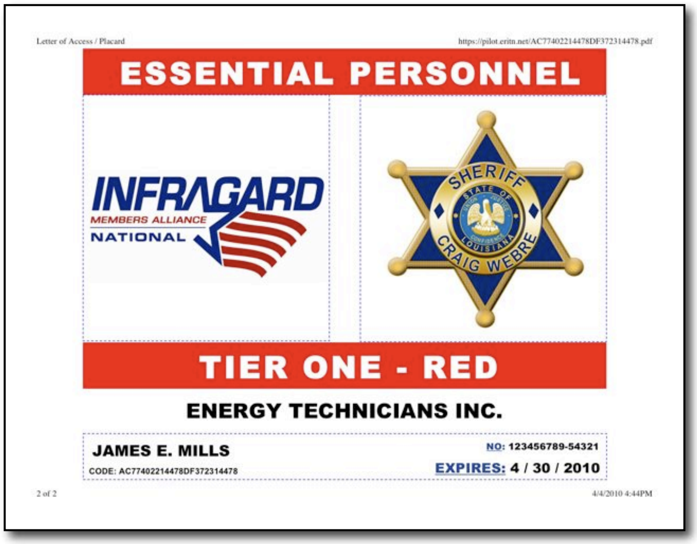
National Sheriff’s Association
Alabama Sheriff’s Association
Energy Security Council
Association of Contingency Planners
Port of South Louisiana
Port of St. Bernard
Mississippi Department of Transportation
Mississippi State Port Authority
Mississippi River Maritime Association

Responder Organizations / Corporations (Partial Listing – 25 Total)

Bunge North America
Chevron
Global Elite Group
J. Ray McDermott
Mississippi Commission for Volunteer Service
Mississippi Voluntary Organizations Active in Disaster
Nord-Sud Shipping
G4S Wackenhut
Securitas USA
Shell Oil Company
Waste Management, Inc.
Enterprise Products, LLP
Southern Companies

Emergency Managers (Observers)

Galveston County, TX
Lafourche Parish, LA
Harrison County, MS
Calhoun County, AL
State of Texas
State of Mississippi
Department of Homeland Security



Letter of Access / Placard https://pilot.eritn.net/AC77402214478DF372314478.pdf

ESSENTIAL PERSONNEL

INFRAGARD
MEMBERS ALLIANCE
NATIONAL
SHERIFF
STATE OF LOUISIANA
CRAIG WEBRE

TIER ONE - RED

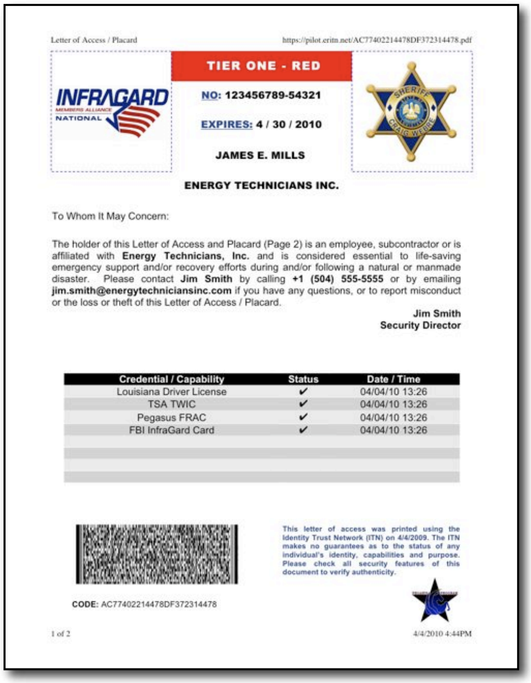
ENERGY TECHNICIANS INC.

JAMES E. MILLS
CODE: AC77402214478DF372314478

NO: 123456789-54321
EXPIRES: 4 / 30 / 2010

2 of 2 4/4/2010 4:44PM

The ER-ITN prints a Vehicle Placard (above) tied to an individual for traffic management, and a Letter of Access (right) in case there is no Internet access at the checkpoint.



Letter of Access / Placard https://pilot.eritn.net/AC77402214478DF372314478.pdf

INFRAGARD
MEMBERS ALLIANCE
NATIONAL
SHERIFF
CRAIG WEBRE

TIER ONE - RED

NO: 123456789-54321

EXPIRES: 4 / 30 / 2010

JAMES E. MILLS

ENERGY TECHNICIANS INC.

To Whom It May Concern:

The holder of this Letter of Access and Placard (Page 2) is an employee, subcontractor or is affiliated with **Energy Technicians, Inc.** and is considered essential to life-saving emergency support and/or recovery efforts during and/or following a natural or manmade disaster. Please contact **Jim Smith** by calling **+1 (504) 555-5555** or by emailing **jim.smith@energytechniciansinc.com** if you have any questions, or to report misconduct or the loss or theft of this Letter of Access / Placard.

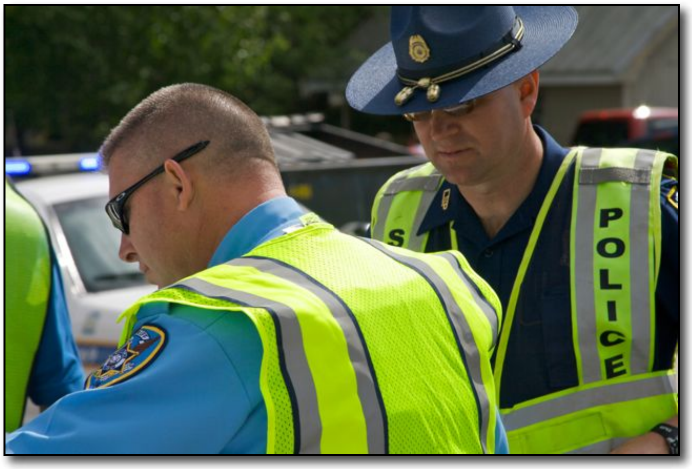
Jim Smith
Security Director

Credential / Capability	Status	Date / Time
Louisiana Driver License	✔	04/04/10 13:26
TSA TWIC	✔	04/04/10 13:26
Pegasus FRAC	✔	04/04/10 13:26
FBI InfraGard Card	✔	04/04/10 13:26

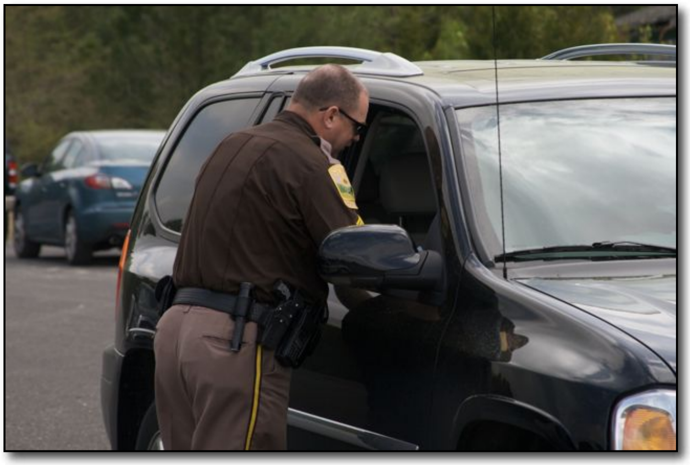
This letter of access was printed using the Identity Trust Network (ITN) on 4/4/2009. The ITN makes no guarantees as to the status of any individual's identity, capabilities and purpose. Please check all security features of this document to verify authenticity.

CODE: AC77402214478DF372314478

1 of 2 4/4/2010 4:44PM



Lafourche Deputy and LA Trooper explain to a responder that his status in the ER-ITN has changed since he had printed his placard several days ago. Access denied.



Calhoun Deputy explains to a healthcare worker that his nursing license is not showing as valid in the ER-ITN. The Deputy feels the risk is too high. Access denied.

Fox News captures a Galveston Deputy using his cell phone to advise another Deputy of the responder's status in the ER-ITN. All credentials shown as ‘valid.’ Access granted.

Lafourche Parish and the State Police had three vehicles at two checkpoints all with access to the ER-ITN. Radio relay to Dispatch, the Placard and Letter of Access were also tested.

Calhoun County had two checkpoints, each with access to the ER-ITN. However, the primary checkpoint relied on the Placard and Letter of Access before sending to secondary.

Galveston County had two checkpoints, one of which had access to the ER-ITN. Only the Placard and Letter of Access was examined at the primary checkpoint.

Development of the Template JSOP

During the Spring of 2010, the Gulf of Mexico Oil Spill created a number of problems associated with law enforcement control and management of emergency zones. In response, InfraGard National, through Rich Garcia, Chair, InfraGard National Crisis Reentry/Exercise Committee, asked the FBI New Orleans Field Office to convene a meeting of coastal Louisiana law enforcement to discuss the value of a standard crisis reentry protocol used by all law enforcement agencies along the Gulf Coast. As an outcome of this meeting, during the summer of 2010, the Louisiana Sheriff's Association (LSA) and the Louisiana Association of Chiefs of Police (LACP), with support of the Louisiana State Police, convened a LSA-/LACP-led Working Group (the "LA Working Group") to develop a formal standard crisis reentry protocol that could be adopted statewide in Louisiana and in any other state.

The LA Working Group, consisting of representatives of law enforcement, critical infrastructure firms and emergency managers, came together under the leadership of Sheriff Craig Webre, Lafourche Parish Sheriff, Chair, to provide broad-based stakeholder input and consensus to law enforcement as to "How" law enforcement and security personnel should manage and coordinate multi-jurisdictional crisis reentry by public and private sector Essential Personnel. The LA Working Group's premise was that local elected officials and emergency managers would determine "Who" would reenter "When", and that the purpose of the law enforcement protocol was to provide a common protocol and information tools that would assist law enforcement and security personnel in answering "How" law enforcement and security personnel would manage and coordinate multi-jurisdictional crisis reentry.

The LA Working Group had as its starting point a Standard Operating Procedure developed and published by the Louisiana State Police in 2006 (the "2006 LSP SOP"). The LA Working Group sought to update the 2006 LSP SOP and produce a "next generation" protocol based on lessons learned from the 2009 and 2010 InfraGard National-sponsored Full Scale Exercises and the broad range of experience and perspectives brought to the LA Working Group by its members.

In a series of meetings and work sessions over a 5-month period in 2010 and 2011, the LA Working Group developed and published a template Joint Standard Operating Procedure (JSOP) for coordinated statewide disaster reentry.[17] As discussed below, that JSOP, which is the model for the Template JSOP, contemplates that Working Groups in each adopting State or region will develop and adopt Statewide or regional administrative measures based on "lessons learned". That JSOP is also technology- and vendor-neutral, allowing adopting agencies to implement the JSOP using any technology, vendor, or vehicle, provided that standard "Guidelines for Data Systems" are met, including common interoperability, real-time access to data, common data formats, and other neutral functional specifications.[18] A current list of the Members of the LA Working Group follows.

[17] As discussed below, that template JSOP has been adopted statewide in Louisiana and Mississippi and forms the basis for the Template JSOP considered by the ESSCC Working Group.

[18] See Template JSOP Section 3, "Guidelines for Data Systems".

Coordinated Statewide Disaster Reentry Working Group
Membership List
April 2, 2011

Sheriff Craig Webre	Sheriff, Lafourche Parish Sheriff's Office, Co-Chair
Sheriff Jack Stephens	Sheriff, St. Bernard Parish Sheriff's Office, Co-Chair
Chief Harry Brignac	President, LACP/Chief, French Settlement, LA
Chief Nick Congemi	Greater New Orleans Causeway Police Department
Chief Harold Klibert	St. John Sheriff's Dept.
Paul Miller	Union Pacific Railroad Police
Major Mark Poche	St. Bernard Parish Sheriff's Office
Pat Santos	GOHSEP
Clay Rives	GOHSEP
Mark Harrel	GOHSEP
Chief Ken Scott	LSUHSC PD
LTC Brian Wynne	LA State Police
Maj. David Staton	LA State Police
Capt. Duane Schexnayder	LA State Police
Fabian Blache	LA Association of Chiefs of Police
Chuck Hurst	LA Sheriff's Association
Richard Hackmann	Hancock Bank
Chris Boudreaux	Lafourche Parish Office of Emergency Management
Bonnie Canal	SE LA Chapter, Association of Contingency Planners
Lt. Louis A. Dering	U. S. Coast Guard Sector New Orleans
Chrissy Chantaarasopak	U. S. Coast Guard Sector New Orleans
Mike Derrick	Enterprise Products
Dr. Monica Farris	UNO Center for Hazards Assessment, Response and Technology
Richard T. Garcia	InfraGard National Members Alliance
Bill Gillespie	Shell Oil Company
Will Hatcher	FBI InfraGard Coordinator
Ron Reed	FBI InfraGard Coordinator
Kent Lirette	J. Ray McDermott
Vincent MacNeill	Securitas USA, Inc.
Dr. Robert Marier	LA State Board of Medical Examiners
Lester Millet, III	Port of South Louisiana
Dr. Rob Muller	FBI InfraGard Medical SIG
Lou Munson	Louisiana Association of Broadcasters
Karla Long	Louisiana Ambulance Alliance
Dawson Primes	Tangipahoa Parish OHSEP / LEPA President
Dennis Quijano	Bunge Corp.
Pat Day Rainey	LSU Health Care Services Division, Baton Rouge (Ret.)
Stacy Hall	LA Department of Health & Hospitals
Dr. John Renne	UNO Transportation Institute
Wayne Rogillio	Louisiana State Board of Private Security Examiners
Kenneth Scott	LSU Health Sciences Center
Jay Smith	Mississippi River Maritime Association
Vice Chancellor Ronnie Smith	LSU Health Science Center, New Orleans
Commander Paul Stocklin	U. S. Coast Guard Sector New Orleans
Doug Dodt	City of Kenner Office of Emergency Preparedness
Francis Hymel	St. James Parish Office of Emergency Preparedness
Richard Bordner	FBI InfraGard
Elvin Thibodeaux	Cox Communications
Dennis Kelly	Pegasus Program, Staff
Darrell Geusz	Pegasus Program, Staff

Initial Adoption and Implementation of the JSOP

During the Spring and Summer of 2011, the JSOP was adopted, first, by the Louisiana Sheriff's Association, the Louisiana Association of Chiefs of Police, and the Louisiana State Police[19]. Shortly after adoption in Louisiana, the JSOP was adopted by the Mississippi Highway Patrol with the support of the Mississippi Sheriff's Association[20].

In each State, shortly after JSOP adoption, adopting law enforcement agencies were trained in operations under the JSOP, and critical infrastructure and other firms seeking reentry were enabled to register their essential personnel for reentry and to apply for reentry rights from local officials with reentry requirements.

In order to assure data system interoperability, standard compliance and business practice accountability, the State Sheriff's Associations for Louisiana and Mississippi have chosen the Pegasus Program to manage the technology vendors who implement the JSOP and associated credentialing programs in their states; currently two vendors provide these services and other vendors are expected to apply as technology standards and a meaningful market for these services further develop.[21]

Overview of the Template JSOP

The Template JSOP is built on the fact that all crises start locally and, as both legal and practical matters, local elected officials and emergency management personnel ultimately determine "who" reenters their local areas, and "when" they reenter. Within that legal, policy and operational framework, the Template JSOP attempts to provide a common, standardized, protocol which law enforcement and security personnel managing checkpoints and emergency zones, and the public and private emergency managers and emergency response and recovery personnel seeking to reenter those checkpoints and emergency zones, jointly use and refer to in determining "how" reentry is to be conducted.[22]

[19] See http://www.lsp.org/lscap.html, last accessed December 17, 2011.

[20] See http://www.dps.state.ms.us/dps/dps.nsf/webpages/EmergencyOperations_Credentialing?OpenDocument, last accessed December 17, 2011.

[21] For the vendor management task, the Pegasus Program brings three distinct groups to the table: a policy governance board ("Pegasus Advisory Board"), chaired by Sheriff Tommy Ferrell (Ret.), presently composed of leaders from among the Nation's Sheriffs; a policy administrative body ("Pegasus Research Foundation"), led by Dr. Lee Colwell, former Associate Director of the FBI, that builds policy consensus, administers policy guidance and certifies Pegasus Program vendors for compliance with applicable technology standards and acceptable business practices; and a technology group ("Pegasus Technology Consortium"), led by Dennis Kelly, SME to the ESSCC Working Group, that manages vendors for technology and business practice compliance within Pegasus Program policy guidance. The Pegasus Program was initiated by the National Sheriffs' Association in 2001 because local law enforcement data systems do not "talk to each other", and to provide a vendor neutral voice to advance standard compliance and data interoperability for the benefit of local law enforcement and their partners in public safety and emergency response. Pegasus Program policy is grounded in support of data standard compliance, data system interoperability, and vendor neutrality.

[22] See Section 1.2, "Purpose", which states:

> This SOP is NOT intended to address the "Who" or "When" issues of Disaster Reentry: the policy decisions regarding "Who" will be allowed to reenter an emergency zone, and "When" they will be

In addition, the Template JSOP is a "baseline" plan for Statewide or regional adoption and implementation, and "does not prohibit internal jurisdictions from adopting additional requirements or more stringent procedures regarding 'How' checkpoints and emergency zones are operated for or within that jurisdiction."[23]

Further, the Template JSOP expressly "DOES NOT impose any requirement on anyone seeking to reenter or access an emergency zone, nor does it guarantee complying emergency responders or essential personnel will be authorized checkpoint reentry or access to emergency zones"[24], making it clear that

> Decisions regarding checkpoint reentry and emergency zone access are always subject to the "Who" and "When" Disaster Reentry policy decisions, typically made at the Parish/County level, and to operational decisions of incident managers and checkpoint/emergency zone security personnel.[25]

Within this context, a principal function of the Template JSOP is to provide a standard phased four tier reentry structure, terminology and visual cues[26], and standard technical specifications for JSOP-compliant traffic management Placards and Letters of Access that document the holder's identity, capabilities, affiliations, and purpose, all as contemplated by Homeland Security Presidential Directive-12[27] and FEMA's "NIMS Guideline for the Credentialing of Personnel"[28]. Another key function of the Template JSOP is to provide vendor-neutral functional specifications for Template JSOP-compliant data systems, to assure that law enforcement and security checkpoint and emergency zone operations are not confounded, yet again, by competing data systems that "don't talk to each other", by requiring data system interoperability, real-time access to data, common data formats, and other neutral functional data system specifications.[29]

---

allowed to reenter, are determined by elected officials and emergency managers, ordinarily at the parish/county level, as determined by applicable law. Rather, this SOP focuses on providing a standardized statewide approach to the operational decisions made by security personnel, typically law enforcement and National Guard, operating checkpoints and emergency zones; that is, this SOP addresses "How" checkpoints and emergency zones are to be operated by security personnel, addressing issues such as [Traffic Management, Vehicle Management, Verification of Credentials, Coordination Between Checkpoints, and Emergency Zone Operations].

[23] See Template JSOP Section 1.2, "Purpose".

[24] Id.

[25] Id.

[26] The Template JSOP provides for four phased reentry Tiers: Tier ER—Immediate/Unrestricted Access (Color Code Red), Tier 1—Response Support (Color Code Blue), Tier 2—Recovery Support (Color Code Green), and Tier 3—Rebuild/Repopulate (Color Code Grey). See Template JSOP Subsection 2.1, "Unified Phased Reentry Protocol".

[27] See Homeland Security Presidential Directive-12 (August 27, 2004), http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm#1, accessed November 20, 2011.

[28] See FEMA, "NIMS Guideline for the Credentialing of Personnel" (July 2011), http://www.fema.gov/pdf/emergency/nims/nims_alert_cred_guideline.pdf, accessed November 20, 2011.

[29] See Template JSOP Section 3, "Guidelines for Data Systems".

This standard phased tier reentry structure and associated terminology and visual cues, when supported by vendor-neutral functional specifications designed to assure data interoperability, and when adopted Statewide by multiple States, is intended to facilitate multi-state adoption and implementation of the Template JSOP and to standardize law enforcement and security checkpoint and emergency zone operations. Key expected outcomes are: 1) coordinated reentry across jurisdictional boundaries, 2) safer and more effective and efficient law enforcement and security personnel management and operation of checkpoints and emergency zones, regardless of the home jurisdiction of deployed personnel, and 3) more effective and efficient management of reentry operations by private sector, as well as public sector, critical infrastructure and other entities needing reentry access, especially for entities seeking access into multiple jurisdictions.

The Template JSOP also provides a single authoritative repository for Statewide or regional standard rules or procedures for law enforcement and security personnel regarding checkpoint and emergency zone operations[30], and a non-exclusive list of IDs that provide a reasonable level of identity assurance, to serve as a standard and trusted resource for law enforcement and security personnel.[31] These provisions are intended to help achieve the key outcomes listed in the preceding paragraph, especially by enabling pre-planning by entities likely to need reentry access and by reducing confusion within large reentry areas caused by inconsistent or conflicting reentry rules or procedures.

A copy of the Template JSOP is attached as Attachment B. The Template JSOP is composed of nine (9) substantive sections, organized as follows:

Acknowledgments[32]
1. Introduction[33]
    - 1.1 Overview
    - 1.2 Purpose
    - 1.3 Scope / Applicability
    - 1.4 Administrative Provisions
2. Concept of Operations[34]
    - 2.1 Unified Phased Reentry Protocol [35]
        - *2.1.1 Tier ER – Immediate / Unrestricted Access (Color Code = Red)*
        - *2.1.2 Tier 1 – Response Support (Color Code = Blue)*
        - *2.1.3 Tier 2 – Recovery Support (Color Code = Green)*

[30] See, e.g., Template JSOP Subsections 2.3.1, "Disaster/Incident Preparations" (providing a list of pre-incident preparedness activities) and 2.3.2, "Checkpoint Operations" (providing standard terminology for different types of checkpoint operations, specifying access requirements and procedures, and providing standard rules regarding spot checks, curfew requirements and tethering requirements).

[31] See Template JSOP Section 7, "Appendix D-List of Recognized IDs".

[32] The "Acknowledgments" Section is intended for the adopting entity's use for inclusion of non-substantive comments.

[33] Section 1, "Introduction", provides generic background information about the JSOP, which may be changed without affecting the operation of the JSOP.

[34] Section 2, "Concept of Operations", provides substantive information at the heart of the JSOP.

[35] Subsection 2.1, "Unified Phased Reentry Protocol", defines the four (4) Tiers (Tier ER, Tier 1, Tier 2 and Tier 3), and the terminology and visual cues associated with each Tier.

        2.1.4 Tier 3 – Rebuild / Repopulate (Color Code = Grey)
    2.2 Partial Evacuation Reentry for CBRNE
    2.3 Identification / Credentialing Guidelines
        2.3.1 Disaster / Incident Preparations[36]
        2.3.2 Checkpoint Operations[37]
3. Guidelines for Data Systems[38]
4. Appendix A – Tiered Reentry Quick Reference Guide[39]
    4.1 ESF Reference Table and Standardized Icons
5. Appendix B – Sample Vehicle Placard [40]
6. Appendix C – Sample Letter of Access [41]
7. Appendix D – List of Recognized IDs[42]
8. Appendix F – Glossary of Terms and Abbreviations[43]
9. Appendix G – Sample Text for SOP Adoption[44]

The Template JSOP's treatment of several key items are worth special note:

1. As noted in the next Section, the Template JSOP anticipates that, after adoption, follow-on governance and other activities will be carried out at the adopting State or regional level to act on "lessons learned" during implementation.
2. The Template JSOP is technology- and vendor-neutral, neither specifying nor even mentioning any particular technology, vendor, or vehicle. The Template JSOP allows adopting agencies to implement the JSOP using any technology, vendor or vehicle of their choice, provided that standard "Guidelines for Data Systems" are met,

[36] Subsection 2.3.1, "Disaster/Incident Preparations", contains substantive provisions that are essential to the Template JSOP Concept of Operations.

[37] Subsection 2.3.2, "Checkpoint Operations", provides recommended checkpoint operational procedures that adopting State or regional entities may adopt as-is or revise to reflect State or regional conditions or practice.

[38] Section 3, "Guidelines for Data Systems" provides general specifications for data systems that support implementation of the Template JSOP, once adopted. Though general in nature, these general specifications should be identical nationwide, in order to assure maximum interoperability across State and county boundaries, and to encourage vendor interest.

[39] Section 4, "Appendix A—Tiered Reentry Quick Reference Guide" should be identical nationwide, in order to facilitate service by anyone trained in the Template JSOP anywhere in the Nation.

[40] Section 5, "Appendix B—Sample Vehicle Placard", provides technical specifications for JSOP-compliant Placards. Section 5 should be identical nationwide, in order to facilitate adoption across jurisdictional boundaries and recognition by anyone trained in the Template JSOP anywhere in the Nation.

[41] Section 6, "Appendix C—Sample Letter of Access", provides technical specifications for JSOP-compliant Letters of Access. Section 6 should be identical nationwide, in order to facilitate adoption across jurisdictional boundaries and recognition by anyone trained in the Template JSOP anywhere in the Nation.

[42] Section 7, "Appendix D – List of Recognized IDs" provides a starting point for a list of recognized IDs that adopting State or regional entities may adopt as-is or revise to reflect State or regional conditions or practice.

[43] Section 8, "Appendix F – Glossary of Terms and Abbreviations", provides a starting point for a Glossary that adopting State or regional entities may adopt as-is or revise to reflect State or regional conditions or practice.

[44] Section 9, "Appendix G – Sample Text for SOP Adoption" provides sample language for adoption by other agencies and entities within the jurisdiction of the adopting State or region, and is not necessary to the JSOP. Adopting State or regional entities may delete this Section 9, adopt this language as-is or revise to reflect State or regional conditions or practice.

including Internet connectivity, common interoperability, real-time access to data, common data formats, and other neutral functional specifications.[45]

3. As noted above, the Template JSOP contains a non-exclusive list of nearly thirty types of IDs, representing hundreds of different issued physical ID cards, that are generally recognized by law enforcement as providing a reasonable level of identity assurance. This non-exclusive list was developed to serve as a standard and trusted resource for law enforcement and security personnel[46], and is open to addition of any ID on which law enforcement within the adopting State or region develops consensus that the ID provides a reasonable level of identity assurance. It is fully expected that this list of IDs may vary from State to State and will change over time, as consensus regarding the adoption of credentialing standards further develops among the emergency services sector, the government sector, and critical infrastructure firms.

[45] See Template JSOP Section 3, "Guidelines for Data Systems".

[46] See Template JSOP Section 7, "Appendix D-List of Recognized IDs."

Considerations Regarding the JSOP as a Template For Nationwide Adoption

The Template JSOP

As noted above, the Working Group undertook to evaluate and vet the JSOP adopted for Statewide implementation in Louisiana and Mississippi as a template for nationwide adoption. The form of the Template Joint Standard Operating Procedure ("Template JSOP")[47] considered by the Working Group is the form of JSOP adopted in Louisiana and Mississippi, with minor editorial changes to language in the "Acknowledgments" Section that are specific to adoption in Louisiana or Mississippi, to standardize "parish" and "county" references, and to update references to DHS standard documentation.

The Template JSOP contemplates that it will serve as a template for adoption by multiple States and regions, anticipating adoption of "key components" 'as-is' and customizing or expanding "other components":

> The purpose of this SOP is to describe in concept the joint Federal, State, Parish/County and Local/Municipal infrastructure strategy to permit access into restricted areas (emergency zones) after an incident, crises or disaster. The following guidelines are also intended to serve as a template (operational model) for States and regions to allow seamless transition (transit) through multiple jurisdictions in order to restore critical municipal functions and CI / KR as quickly and safely as possible.
>
> This SOP was developed such that local, county, state government, as well as the US Federal government, can implement key components 'as-is' to accomplish coordinated reentry and transit across an entire region of the country. Other components can be customized or expanded for state, local or regional needs without frustrating coordinated reentry and transit of CI / KR and other essential and support personnel.[48]

The Working Group recognizes that the Template JSOP provides no guidance as to what "key components" should be adopted 'as-is' and what "other components can be customized or expanded for state, local or regional needs". Accordingly, the Working Group recommends that additional technical documentation be developed for distribution along with the Template JSOP to provide this kind of guidance, as outlined below[49].

In addition, the Template JSOP anticipates that, after adoption, follow-on governance and other activities will be carried out at the adopting State or regional level to act on "lessons learned" during implementation:

[47] See Attachment B, "Template Joint Standard Operating Procedure". The Working Group recommends that the above-quoted language in the Template JSOP be revised in future versions to include Tribal and Territorial Governments as well as Federal, State and Local Governments.

[48] Template JSOP, Section 1.2 "Purpose".

[49] See Table 1, "Recommended Classification of Sections of the Template JSOP" in the following Section of this Initial Report.

> The integrity of SOP administrative processes is vital to coordinated reentry. Accordingly, law enforcement and other agencies which adopt this SOP, or which honor Placards and Letters of Access issued under it, undertake to make every effort to maintain the integrity of those administrative processes, and to include lessons learned about the SOP from incidents in which the SOP comes into operation in applicable After Action Reports. Statewide Working Groups responsible for the development and refinement of this SOP will be called upon to provide responsive follow-up based on those After Action Reports and other relevant information.[50]

The responsive follow-up actions contemplated by the Template JSOP are not limited by it. Examples of actions contemplated would include implementing revisions to the form of the Template JSOP adopted for the State or region consistent with Template JSOP guidance. Such actions might also include taking action external to the Template JSOP to maintain integrity in the crisis reentry process; e.g., revoking or conditioning the participation of agencies, firms or individuals found to have abused either the processes for applying for or granting reentry privileges or the privileges themselves.

Working Group Consideration of the Template JSOP

As noted above, the Working Group concluded that, in order to serve as a template for national adoption, guidance should be provided along with the Template JSOP as to which "key components" should be uniform nationally, which components should be uniform at a Statewide or regional level, and which components should be characterized as "best practices" but need not be uniform at either the national or State/regional level. The Working Group also reached consensus that the Template JSOP should be accompanied by a separate document providing policy guidance for adopting agencies and that, after adoption, the Template JSOP would need to be supported at the adopting State or regional level by governance and other follow-up action.

In addition to the foregoing, the Working Group felt that some governance activity would be needed at the national level, in order to assure that versions of the Template JSOP that are adopted by various States and regions meet a minimal level of conformity needed to assure seamless reentry processes nationwide, and to assure "best practices" that support the Template JSOP are developed and promoted nationally.

This Initial Report is subject to approval of the ESSCC and, ultimately, will be subject to action of individual Statewide or regional working groups that meet to consider adopting and implementing the Template JSOP. Accordingly, the initial recommendations contained herein are recognized to be subject to experience in the field, and experience in the field will determine whether the recommendations below should be revised or deleted and new subjects covered.

[50] Template JSOP, Section 1.4 "Administrative Provisions" (emphasis supplied).

Discussion of Recommendations Regarding Use of the Template JSOP as a National Template

After deliberation, the Working Group came to the consensus that the Template JSOP is a reasonable starting point document to serve as a national template for adoption and implementation by any State or large region in the Nation. This consensus recognized that the Template JSOP will evolve over time and that adopting State and regional agencies will have some flexibility to adjust elements that are not National Standard Elements, so as to reflect State or regional circumstances and conditions. In keeping with the foregoing, the Working Group recommends that the Template JSOP be adopted by the ESSCC and others as a National Template for Nationwide Adoption.

The Working Group also developed consensus that elements of the Template JSOP should be considered either:

- National Standard Elements (elements that must be standard or uniform nationally),
- Statewide/Regional Standard Elements (elements that should be standard or uniform within the adopting State or region), or
- Best Practice Elements (elements that are recommended for adoption and implementation, "as is", but which may be changed).

Recognizing that the Working Group's recommended guidance will evolve over time, Table 1 on the following page provides recommended initial guidance as to classifications of Sections of the Template JSOP as either National Standard Elements, Statewide/Regional Standard Elements, or Best Practice Elements.

Table 1: Recommended Classification of Sections of the Template JSOP

Acknowledgments	[Adopting Agency Text]
1. Introduction	Best Practice Element
1.1 Overview	Best Practice Element
1.2 Purpose	Best Practice Element
1.3 Scope / Applicability	Best Practice Element
1.4 Administrative Provisions	National Standard Element[51]
2. Concept of Operations	National Standard Element
2.1 Unified Phased Reentry Protocol	National Standard Element
2.1.1 Tier ER – Immediate / Unrestricted Access (Color Code = Red)	National Standard Element
2.1.2 Tier 1 – Response Support (Color Code = Blue)	National Standard Element
2.1.3 Tier 2 – Recovery Support (Color Code = Green)	National Standard Element
2.1.4 Tier 3 – Rebuild / Repopulate (Color Code = Grey)	National Standard Element
2.2 Partial Evacuation Reentry for CBRNE	Statewide/Regional Element
2.3 Identification / Credentialing Guidelines	Statewide/Regional Element
2.3.1 Disaster / Incident Preparations	National Standard Element
2.3.2 Checkpoint Operations	Statewide/Regional Element
3. Guidelines for Data Systems	National Standard Element
4. Appendix A – Tiered Reentry Quick Reference Guide	National Standard Element
4.1 ESF Reference Table and Standardized Icons	National Standard Element
5. Appendix B – Sample Vehicle Placard	National Standard Element
6. Appendix C – Sample Letter of Access	National Standard Element
7. Appendix D – List of Recognized IDs	Statewide/Regional Element
8. Appendix F – Glossary of Terms and Abbreviations	Best Practice Element
9. Appendix G – Sample Text for SOP Adoption	Best Practice Element

[51] The Working Group recommends that, in future versions of the Template JSOP, Section 1.4 should be broken into two sections, separately treating "Honoring Letters of Access & Placards For Cross-Jurisdictional Transit", as a National Standard Element, and "Administrative Provisions", as a Statewide/Regional Element.

Recommendations On Technical Matters and Phased Adoption

As noted above, the Working Group makes several recommendations regarding technical matters relating to the Template JSOP, as follows:

- Terminology in the Template JSOP should be revised in future versions to include Tribal and Territorial Governments as well as Federal, State and Local Governments;[52]
- The Working Group recommends that additional technical documentation be developed for distribution along with the Template JSOP to provide guidance on which elements of the Template JSOP should be treated as National Standard Elements, as State/Regional Standard Elements or as Best Practice Elements;[53].
- In future versions of the Template JSOP, Section 1.4 should be broken into two sections, separately treating "Honoring Letters of Access & Placards For Cross-Jurisdictional Transit", as a National Standard Element, and "Administrative Provisions", as a Statewide/Regional Element.[54]

In addition, while the Working Group recommends expeditious national adoption and implementation of the Template JSOP, the Working Group also recognizes that simultaneous national adoption and implementation at the State or regional level likely will not occur. The Working Group sees several benefits in phased adoption, including:

- First priority adoption efforts can be given to States and regions where large natural disasters tend to be common every year, and where the terrorist threat is perceived to be highest;
- Adoption and governance activities taken in early-adopting States and regions may be observed by personnel from later-adopting States and regions, to maximize efficiency and outcomes in subsequent adoption and governance activities;
- Administrative and other lessons learned by early-adopting States and regions can be shared with later-adopting States and regions, for enhanced efficiency and outcomes; and
- Scarce Federal resources made available to support Template JSOP adoption, governance and training may be applied based on national priorities.

In line with the foregoing, the Working Group recommends that consideration be given to phased adoption based on the probability and consequences of man-made and natural disasters.

[52] See Footnote 45.

[53] See text at Footnote 47.

[54] See Footnote 49.

Discussion of Working Group Policy Recommendations

Recommendations to the ESSCC

Consistent with the guidance of the FEMA AAR, the Working Group concluded that, in order to achieve sustained national adoption and implementation of the Template JSOP, some level of follow-on consensus-building and training (including Exercise) activity, as well as on-going governance activity, should be conducted at the adopting State or regional level, and that this activity should be commenced promptly and aggressively. The Working Group is recommending that follow-on consensus-building activity be carried out through a series of State-level crisis reentry consensus-building conferences, starting in 2012, at an accelerated pace.

The Working Group also concluded that, in addition to the necessity of some level of governance activity at the adopting State or regional level, some level of on-going governance activity at the national level will be needed to assure standardized adoption and implementations of the Template JSOP, as well as development and dissemination of best practices in closely-related areas such as traffic management, vehicle management, credentials verification, coordination between checkpoints, and emergency Zone operations. The Working Group's recommendation is that this national level governance activity be carried out by a National Crisis Reentry Governance Board, to be formed.

Consistent with the guidance of the FEMA AAR, the Working Group further concluded that this follow-on and on-going consensus-building, training and governance activity must be "owned" by the Emergency Services Sector, and that the ESSCC is the appropriate vehicle to bring National and State Associations to bear to carry out the tasks needed to carry out these tasks. In addition, the Working Group came to the consensus that there is a need for an on-going vehicle within the ESSCC to organize and assure that this activity is carried out, and recommends that the Working Group be recast as a permanent Committee of the ESSCC tasked with serving as the organizing committee for the recommended National Crisis Reentry Governance Board. Finally, the Working Group is recommending that Association Members of the ESSCC, along with the ESSCC itself, be urged to adopt and support the recommendations of this Report.

Recommendations To DHS

Consistent with the guidance of the FEMA AAR, and with the FEMA Mission Statement, the Working Group also concluded that there are a number of vital tasks that can and should be carried out by DHS/FEMA. In addition to recommending that DHS FEMA adopt the Template JSOP for operational purposes, the Working Group is recommending that DHS incorporate the Template JSOP into the National Incident Management System (NIMS). The Working Group is recommending that DHS review existing grant programs for ways to support adoption and implementation of

FEMA Mission Statement

FEMA's mission is to support our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.

the Template JSOP, and convene and provide grants in support of the National and State-level consensus-building, training and governance activity recommended above. The Working Group also is recommending that DHS inform Congress on the Template JSOP, and urge Congress to review and support use of the Template JSOP as a national template for all hazards reentry for nationwide adoption.

Recommendation to Congress

The Working Group is recommending that the ESSCC recommend and urge Congress to review and support use of the Template JSOP as a national template for all hazards reentry, for nationwide adoption, and explore the possibility of providing Federal grants to support its adoption nationwide.

Policy Recommendations for The Path Forward on Crisis Reentry

Recommendations to ESSCC

Recommendation 1:

The Working Group recommends that the ESSCC

- Approve and adopt this Initial Report and its Findings & Recommendations;
- Recognize the Template JSOP as National Template for Nationwide Adoption; and
- Urge ESSCC Association Members to approve and adopt this Initial Report and its Findings and Recommendations alongside the ESSCC, and support adoption of this Report's Findings and Recommendations by DHS and the Congress.

Recommendation 2:

The Working Group recommends that this Working Group be recast as a permanent Committee of the ESSSCC tasked with serving as Organizing Committee for a National Crisis Reentry Governance Board and charged with developing and submitting annual After Action Reports and Best Practices for approval by the National Crisis Reentry Governance Board.

Recommendation 3:

The Working Group recommends that the ESSCC support:

- The organization and convening of National Crisis Reentry Governance Board;
- The organization and convening of up to 20 Coordinated Statewide Crisis Reentry Consensus-Building Conferences intended to develop consensus regarding coordinated crisis reentry, and adoption of the Template JSOP for Statewide adoption, using a program of phased adoption;
- Carrying out law enforcement training sessions in all adopting States;
- Conducting a series of regional Multi-State Crisis Reentry Full Scale Exercises, starting in 2012; and
- Initiatives by ESSCC Member Associations to adopt and support this Report's Findings and Recommendations.

Recommendation to DHS

Recommendation 4:

The ESSCC recommends and urges that the Department of Homeland Security:

- Adopt the JSOP and incorporate the Template JSOP into the National Incident Management System;
- Assure that existing Grant programs supporting consensus-building, training, and equipment may be used to support efforts to adopt, implement, and provide governance of the Template JSOP;
- Convene and provide Grants in support of the following types of activities aimed at nationwide Crisis Reentry consensus-building, training and governance:
  - Statewide Consensus-Building Conferences;
  - Statewide Law Enforcement Training;
  - Organization of State-level Crisis Reentry Governance Boards;
  - Organization & Initial Meeting of the National Crisis Reentry Governance Board;

    - A series of Multi-State Crisis Reentry Full Scale Exercises in different regions of the country.
- Inform Congress on the Template JSOP, and urge Congress to review and support use of the Template JSOP as a national template for all hazards reentry for nationwide adoption.

<u>Recommendation to Congress</u>

Recommendation 5:

The ESSCC recommends and urges Congress to review and support use of the Template JSOP as a national template for all hazards reentry for nationwide adoption, and explore the possibility of providing Federal grants to support adoption of the Template JSOP nationwide.

ATTACHMENTS

Attachment A: Working Group Memorandum to PIV-I/FRAC Technology Transition Working Group (TTWG), entitled "Comments Proposed for Consideration by the TTWG", dated Oct. 7, 2011

Attachment B: Template Joint Standard Operating Procedure

Attachment C: Sample Template JSOP-Compliant Placard & Letter of Access

Attachment A
Working Group Memorandum to PIV-I/FRAC Technology Transition Working Group (TTWG), entitled "Comments Proposed for Consideration by the TTWG", dated Oct. 7, 2011

ESSCC

Emergency Services Sector Coordinating Council (ESSCC)
Credentialing & Disaster Reentry Working Group (CDRWG)

TO: PIV-I/FRAC Technology Transition Working Group (TTWG)
FROM: ESSCC CDRWG, Sheriff Lenny Millholland, Chair
DATE: October 7, 2011
SUBJECT: Comments Proposed for Consideration by the (TTWG)

This document responds to the TTWG's invitation to the ESSCC CDRWG to participate in or observe the deliberations of the TTWG.

In essence, the ESSCC CDRWG is interested in having an observer participate in the deliberations on the TTWG and keep the CDRWG informed of developments. Because the TTWG is focused on credentialing and the CDRWG is focused on disaster reentry and access, the two efforts do not conflict and should not be viewed as conflicting.

<u>Explanatory Comments</u>
Materials provided by the TTWG state as follows:

> The [TTWG] is focused on exploring PIV-I credentials as the standard that enables interoperability between local and State emergency response officials. PIV-I is a trusted identity and credentialing standard developed by the Federal Government for non-Federal issuers. Non-Federal entities that elect to conform to the PIV-I standard will be trusted by and interoperable with Federal agencies ….

The CDRWG is principally focused on the issue of disaster reentry and access by Essential Personnel from the private as well as the public sector. In this connection, the CDRWG has recently voted to adopt the FEMA "Building Resilience Through Public-Private Partnerships" AAR, and its section on disaster reentry entitled "The Road Best Taken … Is Best Without Boundaries" as the "road map" for its work going forward. This section of the AAR, which focuses especially on "Access to disaster sites by non-emergency responders", contains two "Recommended Solutions" that are highly relevant here, namely:

- ***Focus on Access Control***: The AAR notes that the conferees discussed credentialing issues in depth and concluded that the "actual issue is access, not credentialing"
- ***Create Process-Driven Solution:*** The AAR proposes that solutions to the reentry problem be driven by reentry business processes, not "technology or distribution of cards"

Based on these "Recommended Solutions" contained in the FEMA AAR, the CDRWG will be focusing on access, not credentialing, and will be seeking solutions that are driven by reentry business processes—both of which issues are separate from and outside the credentialing focus on the TTWG.

Additional Comments

The CDRWG has been provided with information indicating that the TTWG is well aware of the many issues involved in adopting a PIV-I national credentialing system or program built on the PIV-I standard, or, indeed, any national system or program, including, in particular, the following:

- Cost of Credentials, Supporting Data System and Data Readers
- A National Standard for Card Design and Layout, Complying With and Further Refining FIPS 201
- The Value of Using Standard Job Titles
- A Plan that addresses Essential Personnel from the Private Sector as well as the Public Sector
- Absent new Federal Statutory Mandates, A Plan that Proceeds Based on Bottom-Up Consensus Rather Than Top-Down "Guidance" or Voluntary Compliance
- A Migration Plan Addressing Non-Compliant IDs

The CDRWG looks forward to receiving information regarding your efforts to establish a national credentialing system or program.

###

Attachment B
Template Joint Standard Operating Procedure ("Template JSOP")

INSERT STATE OR OTHER OFFICIAL AGENCY SEAL(S) HERE

STATE OF [STATE_NAME]

JOINT STANDARD OPERATING PROCEDURE

STATEWIDE CREDENTIALING / ACCESS CONTROL PROGRAM
ALL HAZARDS REENTRY AND TRANSIT

[PUB DATE]

Table of Contents

Acknowledgements

[Insert State-specific acknowledgments]

1. Introduction

1.1 Overview

Recent large-scale disasters have demonstrated the critical need for a universally acceptable all hazard disaster reentry and transit Standard Operating Procedure (SOP) that can be adopted across a region, the entire State and/or in multiple States. The current lack of consistent reentry access requirements and operating procedures between local jurisdictions have greatly hampered the recovery efforts of critical utilities, services, and communications, as well as the Critical Infrastructure / Key Resources (CI / KR) that supply the rest of the Nation.

1.2 Purpose

The purpose of this SOP is to describe in concept the joint Federal, State, Parish/County and Local/Municipal infrastructure strategy to permit access into restricted areas (emergency zones) after an incident, crises or disaster. The following guidelines are also intended to serve as a template (operational model) for States and regions to allow seamless transition (transit) through multiple jurisdictions in order to restore critical municipal functions and CI / KR as quickly and safely as possible.

This SOP was developed such that local, county, state government, as well as the US Federal government, can implement key components 'as-is' to accomplish coordinated reentry and transit across an entire region of the country. Other components can be customized or expanded for state, local or regional needs without frustrating coordinated reentry and transit of CI / KR and other essential and support personnel.

This SOP is NOT intended to address the "Who" or "When" issues of Disaster Reentry: the policy decisions regarding "Who" will be allowed to reenter an emergency zone, and "When" they will be allowed to reenter, are determined by elected officials and emergency managers, ordinarily at the parish/county level, as determined by applicable law. Rather, this SOP focuses on providing a standardized statewide approach to the operational decisions made by security personnel, typically law enforcement and National Guard, operating checkpoints and emergency zones; that is, this SOP addresses "How" checkpoints and emergency zones are to be operated by security personnel, addressing issues such as:

- Traffic Management
  - Expediting approval, denial and further investigation decisions when appropriate
  - Handling self-dispatchers and other exceptions
- Vehicle Management
  - Handling multi-vehicle tethering/escort requests
- Verification of Credentials (IDs, Qualifications and Affiliations)
  - What IDs and other tokens will be honored (e.g. Letter of Access and Vehicle Placard)
  - How one or more credentials are verified for authenticity and validity
- Coordination between Checkpoints

  - Handling of traffic in transit to another Parish/County
  - Adoption of common standardized statewide "Tier" terminology
  - Adoption of standardized statewide format for Letters of Access and Vehicle Placards
- Emergency Zone Operations
  - Conducting "spot checks" within the emergency zone or at muster locations
  - Operations during emergency zone curfew periods

This Joint SOP is a Statewide "baseline plan"; requirements "over and above" these requirements may be, and will be, made at the county/parish or local level by elected officials, emergency managers and incident managers to address local or exigent circumstances. Specifically, this SOP is NOT intended to, and DOES NOT, prohibit a particular jurisdiction from implementing additional requirements or more stringent operating procedures regarding "How" checkpoints and emergency zones are operated for or within that jurisdiction. For example, this SOP does not preclude municipal and parish/county requirements that persons seeking to reenter their jurisdiction have a specific or proprietary ID, placard or reentry permit for that particular jurisdiction; in those cases, checkpoint and emergency zone security personnel for that particular jurisdiction, and persons seeking entry into that particular jurisdiction, must comply with the additional jurisdictional requirements.

Similarly, this SOP is NOT intended to, and DOES NOT, impose any requirement on anyone seeking to reenter or access an emergency zone, nor does it guarantee that complying emergency responders or essential personnel will be authorized checkpoint reentry or access to emergency zones. Decisions regarding checkpoint reentry and emergency zone access are always subject to the "Who" and "When" Disaster Reentry policy decisions, typically made at the Parish/County level, and to operational decisions of incident managers and checkpoint/emergency zone security personnel.

Rather, this SOP establishes a Statewide protocol for checkpoint and emergency zone operations that enables security personnel to operate in a more standard and coordinated manner, Statewide, within Parish/County requirements, while also providing emergency responders and essential personnel who must cross Parish/County boundaries with an established Statewide protocol that may be followed: when local authorities decide who needs to be provided access, this SOP is designed to facilitate the ability of those critical personnel to respond in the most efficient, effective, and expeditious manner, to benefit the public good.

The intersection of these "Who" and "When" Disaster Reentry policy decisions with the "How" checkpoint and emergency zone operational security decisions is discussed in **Section 1.4** Administrative Provisions.

1.3 Scope / Applicability

This SOP is intended for Federal, State, Parish/County and Local/Municipal government representatives and private sector companies (CI / KR owners, operators and managers) with presence in or that support local needs in [STATE_NAME].

This SOP references the following Federal or State directives:

- Homeland Security Presidential Directive (HSPD-5)
    - NIMS / ICS
- Homeland Security Presidential Directive (HSPD-7)
    - Identifies and prioritizes seventeen (17) CI / KR Sectors. Other valid CI / KR sectors may exist and may not be listed (based on local / regional needs)
- Homeland Security Presidential Directive (HSPD-8)
    - All Hazard approach for improved coordination between local, state, and federal agencies
- Homeland Security Presidential Directive (HSPD-12)
    - Use of identity verification or identification methods (including ID cards) that are strongly resistant to identity fraud, are issued by reliable, trusted sources and that can be validated through electronic means
- NIMS Guideline for the Credentialing of Personnel (July 2011)
    - A person is considered 'credentialed' if the person meets four fundamental elements including 1) identity, 2) qualification, 3) affiliation and 4) authorization for deployment.
- Uniform Emergency Volunteer Health Practitioner Act (UEVHPA) (if enacted in [STATE_NAME]
    - Health care workers that have been confirmed as 'credentialed' may operate within [STATE_NAME] after an emergency declaration has taken place
- Emergency System for Advanced Registration of Volunteer Health Providers (ESAR-VHP)
    - Guidelines and standards for the registration, credentialing, and deployment of medical professionals in the event of a large-scale national emergency

1.4 Administrative Provisions

All operational decisions made at checkpoints or in the emergency zone must give effect to applicable Disaster Reentry Policy decisions. As stated in **Section 1.2** Purpose, the reentry policy decisions regarding "Who" will be allowed to reenter an emergency zone, and "When" they will be allowed to reenter, are determined by elected officials and emergency managers, ordinarily at the parish/county level, as determined by applicable law. Once "Who" and "When" Disaster Reentry Policy are determined, security personnel operating at checkpoints and within emergency zones are left to determine "How" they will conduct those operations within Disaster Reentry Policy, depending on local practice and procedure or exigent circumstances.

The integrity of SOP administrative processes is vital to coordinated reentry. Accordingly, law enforcement and other agencies which adopt this SOP, or which honor Placards and Letters of Access issued under it, undertake to make every effort to maintain the integrity of those administrative processes, and to include lessons learned about the SOP from incidents in which the SOP comes into operation in applicable After Action Reports. Statewide Working Groups responsible for the development and refinement of this SOP will be called upon to provide responsive followup based on those After Action Reports and other relevant information.

Consistent with the foregoing, and to facilitate coordinated Statewide reentry, security personnel conducting checkpoint/emergency zone operations—Sheriffs' Offices and municipal and State Police and National Guard—will honor LOAs and Placards compliant with this SOP and issued to personnel seeking to transit through their jurisdictions, subject to published Disaster Reentry Policy and exigent incident/emergency manager authority.

2. Concept of Operations

All participants agree that the following concept of operations, components and criteria are essential elements for access into a restricted area (emergency zone) during an incident, crises or disaster and will be administered ONLY:

- in the event of a Declaration / State of Emergency from the Governor, or affected County/Parish/Local President/Chief Executive or Mayor
- in the event Life Safety or Public Safety is at risk as determined by State or Local emergency manager or law enforcement under applicable law

2.1 Unified Phased Reentry Protocol

For a quick reference guide on the All Hazards Tiered Reentry Process, please see Appendix A – Tiered Reentry Quick Reference Guide.

For a complete listing of recognized IDs, please see Appendix D – List of Recognized IDs.

Based upon lessons learned from previous incidents, reentry shall occur using a phased or 'tiered' approach. The following Statewide Tier descriptions serve as a baseline for 'All Hazards' and may be amended based upon defined incidents or incident types.

Note: Local Jurisdictions may be precluded from Statewide coordinated reentry timelines due to the following assumptions:

- Imminent Threat to Life and Property has not ceased.
- Road Access: Road Closures
- Public Health
- Search and Rescue / Recovery Efforts

Important: Life Safety shall always take precedence during all reentry phases and will dictate both Tier 1 and 2 Reentry Timelines (i.e. Reentry Timelines shall be dictated by the incident; therefore, cannot be predetermined), as well as any exceptions or overrides.

Important: Authority and/or privilege to practice a profession may only be conferred by the appropriate Jurisdictional Authority (State licensing board, State Police, Local Law Enforcement, Local OEP, etc.).

2.1.1 Tier ER – Immediate / Unrestricted Access (Color Code = Red)

Immediate and unrestricted access will be granted to:

- Search and Rescue Agents
- Parish / Municipal Fire and EMS
- Local, State and Federal Law Enforcement, Homeland Security and Emergency Management
- Military (including National Guard and Coast Guard)
- All other Emergency Response Personnel providing support of CI / KR (based upon the discretion of local authorities)

2.1.2 Tier 1 – Response Support (Color Code = Blue)

- Critical Infrastructure / Key Resources Rapid Response Teams and Subject Matter Experts including, but not limited to, municipal utilities, public works, public health, water, lighting, transportation and communications (at the discretion of local authorities, with preregistered and prequalified CI / KR contracted to support Tier ER as first priority)
- Personnel on the staff of Hospitals with Emergency Departments
- Security Personnel (preregistered / prequalified)
- Official Damage Assessment Teams (FEMA, State, and Local)
- Critical Infrastructure / Key Resources Damage Assessment Teams
- Other designated personnel at the discretion of local authorities (i.e. First Aid, EMACs, Mutual Aid, CERT, etc.)

2.1.3 Tier 2 – Recovery Support (Color Code = Green)

- Relief Workers
- Healthcare personnel not included in Tier 1
- Animal Rescue, Research & Care Organizations
- Other CI /KR and business operators considered critical to recovery efforts (based upon the Discretion of Local authorities)
- Other personnel approved at the discretion of the local authorities

2.1.4 Tier 3 – Rebuild / Repopulate (Color Code = Grey)

- All other business operators and residents (as appropriate, subject to safety issues)

2.2 Partial Evacuation Reentry for CBRNE

Reentry Guidelines for partial evacuations (CBRNE[1] Events-deliberate and / or otherwise) shall be determined at the local level (Local OEP), with consideration of the following:

- Only Tier ER shall be allowed into the Hot Zone until the incident has been resolved (Imminent threat to life has ceded)
- Pre-registration of all EMAC (Emergency Management Assistant Compact) / Mutual Aid Providers with local, state, and federal stakeholders is required (see Section 2.3.1 Disaster / Incident Preparations)

[1] Chemical, Biological, Radiological, Nuclear, Explosive

2.3 Identification / Credentialing Guidelines

Federal, State, and local government agencies and law enforcement officials agree to recognize specific forms of identification and evidence that an individual is considered 'credentialed' as provided by critical infrastructure owners and operators, and their contractors, subcontractors and assigns as they seek access into a restricted disaster area.

Relying parties (e.g. law enforcement, National Guard) will require constant communications with local and State EOCs so that proper admittance is granted. Once identity and attributes are authenticated, access is granted at the discretion of the relying parties.

In furtherance of this access program, Federal, State, Parish/County, Local/Municipal and private sector partners all agree to take action in support of this SOP. The following actions are required:

2.3.1 Disaster / Incident Preparations

Pre-Incident Coordination between local, state, federal and private sector stakeholders shall include the following:

- Pre-registering essential personnel with local, state, and federal stakeholders for seamless transition.
  - Stakeholders are defined as emergency managers and law enforcement at a minimum.
- Updating / Maintaining essential personnel rosters prior to any incident, including listing essential personnel's current credentials (IDs, qualifications and affiliations) essential for ICS Resource Typing
  - **Affiliation Examples:** Employer or sponsor, member of a specialty team, member of a government or industry (trade) association, union memberships, etc.
  - **Qualification Examples:** Licenses, certifications, permits, training and skills, equipment/tool operator ratings, criminal vetting, etc.
- Pre-Identifying essential personnel and their Tier levels (Tier ER, Tier 1, Tier 2, etc.). Different Tier Levels may be assigned to different response personnel (assessment team vs. recovery person, for example)
  - Note: Some organizations may be restricted regarding which Tier levels they are authorized to use
  - Note: Some facilities may want to conduct a phased reentry of their facility
- Preparing Vehicle Placards and Letters of Access (LOA) for essential personnel
  - These should be prepared prior to an incident whenever possible (e.g. hurricane or storm event). *Special Note: for redundancy reasons, at the discretion of parish/county/local Office of Emergency Preparedness officials, Tier ER and Tier One (1) Placards and Letters of Access may be printed annually for "All Event" access.*
  - Vehicle Placards must have the following printed on them (see Appendix B – Sample Vehicle Placard):
    - State-Designated Logo (Default is State Sheriff's Association Logo)
    - Organization Logo

        - Organization Name
        - Tier Designator (Including Color)
        - Person’s Name (First and Last)
        - Name of Event (e.g. “Hurricane X”)
        - Unique Number (for reference in the issuing registration system)
        - OPTIONAL: Standard icon for the corresponding ESF (see Appendix A – Tiered Reentry Quick Reference Guide)
    - Letters of Access must have the following printed on them (see Appendix C – Sample Letter of Access)
        - State-Designated Logo
            - Default is State Sheriff’s Association Logo
        - Organization Logo
        - Organization Name
        - Tier Designator (Including Color)
        - Person’s Name (First and Last)
        - Name of Event (e.g. “Hurricane X”)
        - Destination or Purpose (e.g. Facility Name (specific or generic) – “Port Fourchon” or “Oil Refinery”)
        - Unique Number (for reference in the issuing registration system)
        - Letter Body stating the person is essential to the organization for response, recovery or rebuilding
        - Point of Contact, such as a Security Officer, Manager or Supervisor (can be included within the letter body)
        - Basic listing of the person’s IDs and attributes (credentials)
        - OPTIONAL: Standard icon for the corresponding ESF (see Appendix A – Tiered Reentry Quick Reference Guide)
        - OPTIONAL: Photograph of the individual
        - OPTIONAL: 1D or 2D barcode
        - OPTIONAL: Location for the application of proprietary stickers to indicate various things regarding the person or the person’s organization. Examples include, but are not limited to:
            - A sticker to indicate the letter of access had been verified as authentic or belonging to the carrier using the data system
            - A sticker to indicate the person has passed or has been interviewed at a given checkpoint
            - A sticker to indicate the person was vetted using one or more criminal history resources

2.3.2 Checkpoint Operations

Three types of ‘checkpoints’ are considered in this SOP:

- **Outer Perimeter Checkpoint**
    - This is a checkpoint where traffic management is a priority and risk remains relatively low.
    - Typically a cursory review of the individual and his or her vehicle is conducted.

  - Vehicle Placards can be leveraged to form multiple lanes of traffic segmented by priority (no placard vs. placard, by Tier level, by ESF, etc.) as the roadway permits.
  - Individuals can be directed to a second officer located at the Outer Perimeter Checkpoint or to the command post for a further, more detailed review as needed
- **Inner Perimeter Checkpoint**
  - This is a checkpoint where a more detailed (or scrutinized) review of a person's identity details and documents is appropriate and where risk remains high or higher
  - An inspection of IDs and Letters of Access, as well as inspection of the person's record in the issuing registration system, is appropriate
- **Spot Check**
  - This is a roaming checkpoint where a more detailed (or scrutinized) review of a person's identity details and documents is appropriate and where risk remains high or higher
  - This typically occurs due to the person's actions or geographic location within the emergency zone
  - This also typically occurs at a muster point where the person is or will be assuming or being asked to fulfill certain job roles, assignments or responsibilities
  - An inspection of IDs and Letters of Access, as well as inspection of the person's record in the issuing registration system, is appropriate

2.3.2.1 Access Requirements / Procedures

For a quick reference guide on the Tiered Reentry Process, please see Appendix A – Tiered Reentry Quick Reference Guide.

For a complete listing of recognized IDs, please see Appendix D – List of Recognized IDs.

Tier	Access Requirements / Procedures
Tier ER	**IN UNIFORM / MARKED VEHICLE** Access will be granted without restriction. **IN CIVILIAN DRESS / UNMARKED VEHICLE** Access will be granted after: • Visual inspection of the person's Vehicle Placard. • RECOMMENDED: Visual inspection of at least two (2) personal IDs, one of which must have a photo and have been issued by a US State or the US Federal government, Canadian Provincial or Canadian Federal government. Unrestricted Foreign Passports with a US Entry Stamp and required Visa (as required for non-Visa waiver countries) are also acceptable.[2]

[2] The US State Department may issue restrictions on specific foreign governments and their passports

Tier	Access Requirements / Procedures
	• OPTIONAL: Visual inspection of the person's Letter of Access, or inspection of the person's record in the issuing registration system.
Tier One (1) **and** **Tier Two (2)**	**OUTER PERIMETER CHECKPOINT** Access will be granted after: • Visual inspection of the person's Vehicle Placard. • AS NEEDED: Visual inspection of at least two (2) personal IDs, one of which must have a photo and have been issued by a US State or the US Federal government, Canadian Provincial or Canadian Federal government. Unrestricted Foreign Passports with a US Entry Stamp and required Visa (as needed) are also acceptable. • OPTIONAL: Visual inspection of the person's Letter of Access or inspection of the person's record in the issuing registration system. **INNER PERIMETER CHECKPOINT** Access will be granted after: • Visual inspection of the person's Vehicle Placard. • Visual inspection of at least two (2) personal IDs, one of which must have a photo and have been issued by a US State or the US Federal government, Canadian Provincial or Canadian Federal government. Unrestricted Foreign Passports with a US Entry Stamp and required Visa (as needed) are also acceptable. • Visual inspection of the person's Letter of Access • OPTIONAL: Inspection of the person's record in the issuing registration system.
Tier Three (3)	**OUTER PERIMETER CHECKPOINT** Access will be granted after: • Visual inspection of the person's Vehicle Placard. • AS NEEDED: Visual inspection of at least one (1) photo ID, which may or may not have been issued a US State, the US Federal or an unrestricted foreign Federal government (i.e. Foreign Passport). • OPTIONAL: Visual inspection of the person's Letter of Access or inspection of the person's record in the issuing registration system. **INNER PERIMETER CHECKPOINT** Access will be granted after: • Visual inspection of the person's Vehicle Placard. • Visual inspection of at least one (1) photo ID, which may or may not have been issued a US State, the US Federal or an unrestricted foreign Federal government (i.e. Foreign Passport). • Visual inspection of the person's Letter of Access • OPTIONAL: Inspection of the person's record in the issuing registration system.

2.3.2.2 Spot Checks

Spot checks of the person's IDs and Letter of Access (or inspection of the person's record in the issuing registration system) may be conducted within the emergency zone or at a muster location on a case-by-case basis, as needed or appropriate.

2.3.2.3 Curfew Requirements for CI/KR

In order to maintain Public Safety, the Governor, or affected County/Parish President or Chief Executive or Mayor may institute curfews for the emergency zone.

CI/KR organizations will instruct essential personnel to follow all curfews enacted in the emergency zone. CI/KR essential personnel may be instructed to check in with a checkpoint, command center or the EOC on their way out of the emergency zone.

2.3.2.4 Tethering Requirements for CI/KR

In order to better facilitate movement of personnel between checkpoints, tethering shall be allowed with the following stipulations:

- The primary (lead) vehicle must be a Marked Company Vehicle (With clearly visible serial number), or a Company Vehicle that has standardized markings (Logos) and colors (Bus, Van, etc.)
- Pre-registration and vetting (as required) for all tethered personnel in the same or tethered vehicle (no last minute additions without pre-approval of local authorities)
- A Vehicle Placard must be issued to at least one qualified occupant of each tethered vehicle
- A Letter of Access must be issued to each occupant of each tethered vehicle
- A defined destination or purpose must be provided (i.e. affected CI/KR).
- No Family Members or non essential personnel will be allowed, except for when Tier 3 status condition is present

3. Guidelines for Data Systems

A Statewide essential personnel registration and management system (for First Responders, Mutual Aid, Essential Personnel, etc.) that allows seamless transition through multiple jurisdictions following all mandatory evacuations (partial and /or otherwise) should be used.[3]

This Management Interface shall incorporate the following capabilities:

- Web Based Application (Internet Connectivity)
- Common Interoperability
- Real Time Access to Information
- User Friendly
- Secure Hosting (Personal Data is only used to verify Identity Claims)

[3] This is a general specification for entry; internal checkpoints within emergency zones may implement biometric authentication or other security requirements.

- Commercial Off the Shelf (COTS)
- Supports Existing Infrastructure and Legacy Technology
- Common Data Formats
- Fully Operable under any local communications condition

4. Appendix A – Tiered Reentry Quick Reference Guide

Accepted IDs

ID 1 - Must have a photo and was issued by a US State, the US Federal, a Canadian Provincial, or the Canadian Federal government. Unrestricted Foreign Passports must have Valid Entry Stamp (and US Visa for non-Visa waiver countries).

ID 2 - Must meet the requirements of ID1, OR have a sponsoring organization's (employer's) logo. The photo of the cardholder printed on the ID is recommended.

Spot Checks

Spot checks of the person's IDs and Letter of Access (or inspection of the person's record in the issuing registration system) may be conducted within the emergency zone or at a muster location on a case-by-case basis, as needed or appropriate.

Tier	OUTER PERIMETER / BASIC CHECK	INNER PERIMETER / DETAILED CHECK
Tier ER **Response** 🟥 **RED**	**IN UNIFORM / MARKED VEHICLE** **Access will be granted without restriction.** **IN CIVILIAN DRESS / UNMARKED VEHICLE** • Visual inspection of the person's Vehicle Placard. • **AS NEEDED:** Visual inspection of at least two IDs, one of which must have a photo. • **OPTIONAL:** Visual inspection of the person's Letter of Access, or inspection of the person's record in the issuing registration system.	
Tier One (1) **Response Support** 🟦 **BLUE**	• Visual inspection of the person's Vehicle Placard. • **AS NEEDED:** Visual inspection of at least two IDs, one of which must have a photo. • **OPTIONAL:** Visual inspection of the person's Letter of Access or inspection of the person's record in the issuing registration system	• Visual inspection of the person's Vehicle Placard. • Visual inspection of at least two IDs, one of which must have a photo. • Visual inspection of the person's Letter of Access • **OPTIONAL:** Inspection of the person's record in the issuing registration system.
Tier Two (2) **Recover** 🟩 **GREEN**	• Visual inspection of the person's Vehicle Placard. • **AS NEEDED:** Visual inspection of at least two IDs, one of which must have a photo. • **OPTIONAL:** Visual inspection of the person's Letter of Access or inspection of the person's record in the issuing registration system.	• Visual inspection of the person's Vehicle Placard. • Visual inspection of at least two IDs, one of which must have a photo • Visual inspection of the person's Letter of Access • **OPTIONAL:** Inspection of the person's record in the issuing registration system.
Tier Three (3) **Rebuild** ◼ **GREY**	• Visual inspection of the person's Vehicle Placard. • **AS NEEDED:** Visual inspection of at least one photo ID • **OPTIONAL:** Visual inspection of the person's Letter of Access or inspection of the person's record in the issuing registration system.	• Visual inspection of the person's Vehicle Placard. • Visual inspection of at least one photo ID • Visual inspection of the person's Letter of Access • **OPTIONAL:** Inspection of the person's record in the issuing registration system.

4.1 ESF Reference Table and Standardized Icons[4]

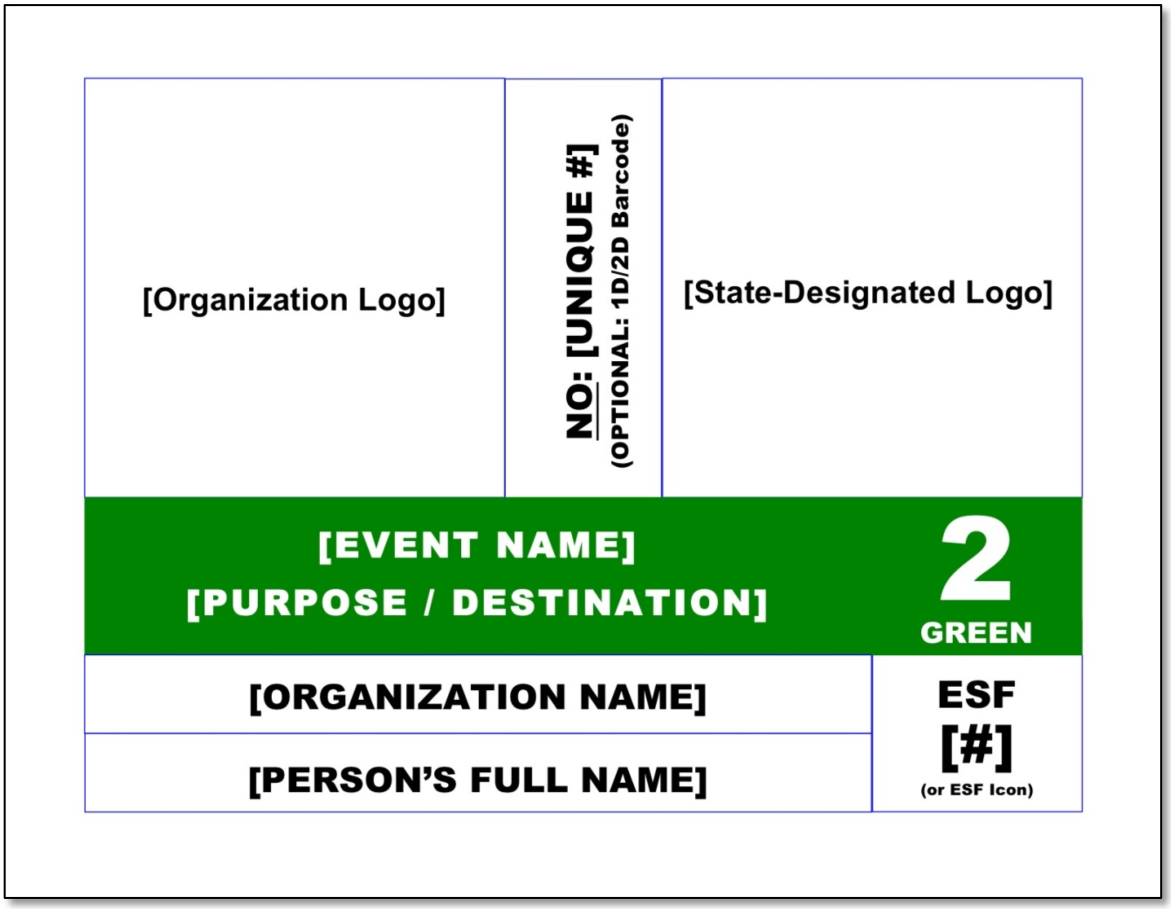
ESF	Description	Icon
ESF 1	Transportation	Future Version
ESF 2	Communications	Future Version
ESF 3	Public Works and Engineering	Future Version
ESF 4	Firefighting	Future Version
ESF 5	Emergency Management	Future Version
ESF 6	Mass Care, Emergency Assistance, Housing, and Human Services	Future Version
ESF 7	Logistics Management and Resource Support	Future Version
ESF 8	Public Health and Medical Services	Future Version
ESF 9	Search and Rescue	Future Version
ESF 10	Oil and Hazardous Materials Response	Future Version
ESF 11	Agriculture and Natural Resources	Future Version
ESF 12	Energy	Future Version
ESF 13	Public Safety and Security	Future Version
ESF 14	Long-Term Community Recovery	Future Version
ESF 15	External Affairs	Future Version
	STATE SPECIFIC	
ESF XX	[STATE_NAME]	Future Version

[4] As of the date of publication of this SOP, DHS is still in the process of developing standardized ESF Icons. Future versions of this SOP will incorporate standardized icons for each ESF.

5. Appendix B – Sample Vehicle Placard

Tier 2 All Hazards Depicted. Adjust accordingly, including corresponding color banners and Tier designation, for other tiers. Font sizes must be as large as possible while still fitting in text.

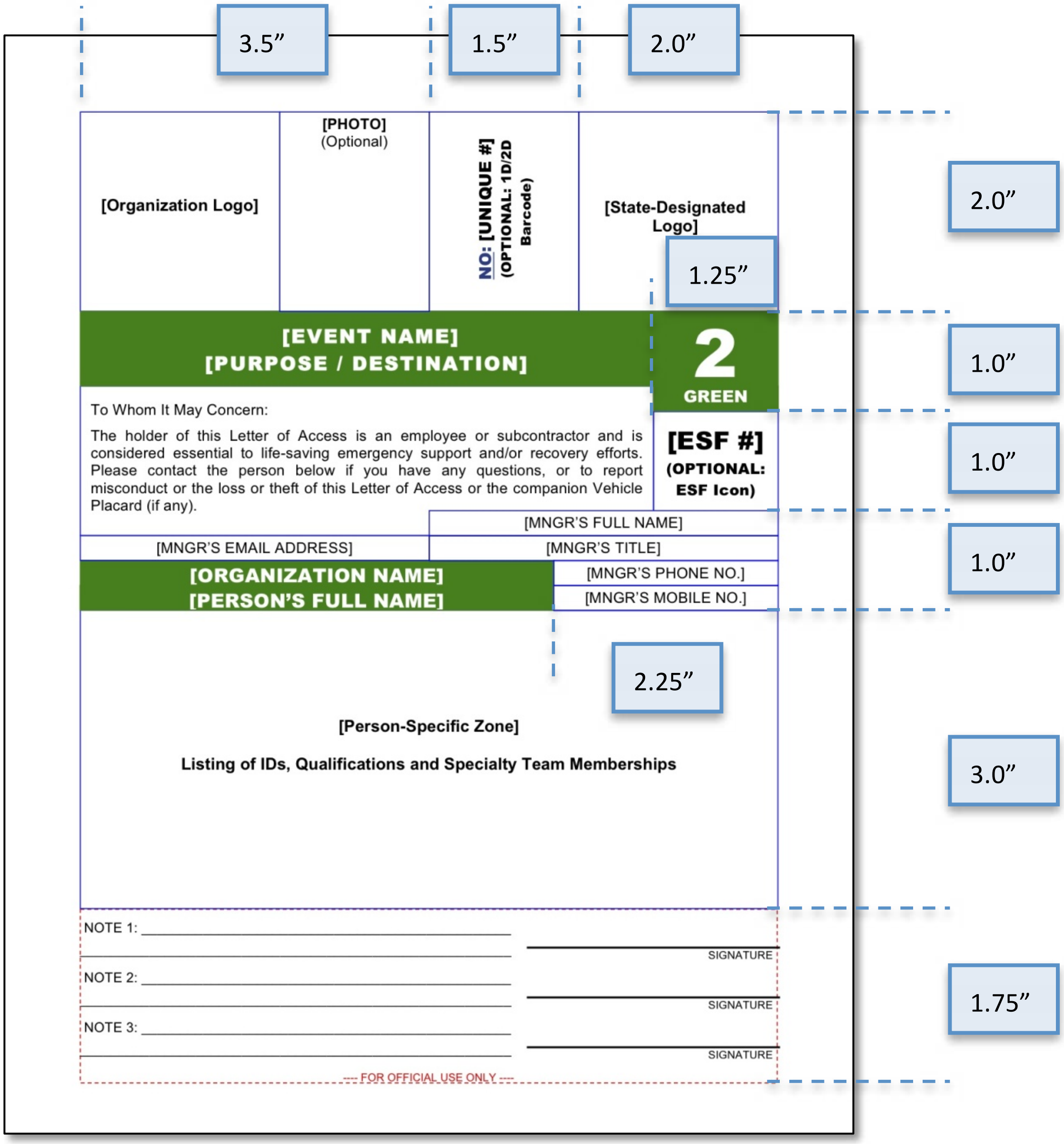
- Placard shall have a ½" margin. All fonts shall be "Arial Black" and Bolded, all capitalized and shall be a minimum of 24pt font size, except for the Tier and ESF Indicator Zones.
- Event Name and Purpose / Destination Zone shall be white colored text on the corresponding tier color background (bounding box 8" (w) by 1.5" (h))
- The Tier Designator zone shall be 2" (w) x 1.5" (h) in size and have the corresponding tier color background. The font for the letters "ER" or the numerical digit ("1", "2", or "3") shall be 80pt font size, white in color and do not have to be bolded. The color will be spelled out directly underneath and shall be 20pt font size.
- ESF Indicator Zone / icon shall be 2" (w) by 1.5" (h) in size. The letters "ESF" will appear on top of the ESF numerical digit and shall be 26pt font size. The numerical digits shall be 36pt font size
- Logos shall not exceed 4" x 4" in size.
- The unique number of the placard shall appear in between the two logos, rotated 90 degrees counter-clockwise. An **optional** 1D or 2D barcode can appear below or above this.



6. Appendix C – Sample Letter of Access

Tier 2 All Hazards Depicted. Adjust accordingly, including corresponding color banners and Tier designation, for other tiers. Font sizes must be as large as possible while still fitting in text.

- All fonts shall be “Arial Black” and Bolded
- Event Name, Purpose/Destination, Organization Name and Person’s Full Name shall be Bold, Arial Black font and 14pt in size, white in color with the corresponding tier color background.
- Letter Body, Manager’s Contact Info and Person-Specific Zone must be Arial 11pt font (bolded font not necessary)
- Tier Designator text shall be a minimum of 48pt in size, white in color with the corresponding tier color background. The color name will appear underneath in 12pt Arial Black font, white in color.



[Organization Logo]

[PHOTO]
(Optional)

NO: [UNIQUE #]
(OPTIONAL: 1D/2D Barcode)

[State-Designated Logo]

[EVENT NAME]
[PURPOSE / DESTINATION]

2
GREEN

To Whom It May Concern:

The holder of this Letter of Access is an employee or subcontractor and is considered essential to life-saving emergency support and/or recovery efforts. Please contact the person below if you have any questions, or to report misconduct or the loss or theft of this Letter of Access or the companion Vehicle Placard (if any).

[ESF #]
(OPTIONAL: ESF Icon)

[MNGR’S FULL NAME]
[MNGR’S EMAIL ADDRESS] [MNGR’S TITLE]

[ORGANIZATION NAME]
[PERSON’S FULL NAME]

[MNGR’S PHONE NO.]
[MNGR’S MOBILE NO.]

[Person-Specific Zone]

Listing of IDs, Qualifications and Specialty Team Memberships

NOTE 1: ____
____
SIGNATURE

NOTE 2: ____
____
SIGNATURE

NOTE 3: ____
____
SIGNATURE

---- FOR OFFICIAL USE ONLY ----

7. Appendix D – List of Recognized IDs

All IDs should have the following information printed on the surface of the ID:

ID Card Element	Explanation
Cardholder's Color Photo	Current Color Photo
Cardholder's Name	First and Last Name (Middle Name Optional)
Agency Name	Name of Issuing Authority (e.g. Employer / Sponsor, Government Agency)
Agency / Organization Seal	Seal / Logo of Issuing Authority (e.g. Employer / Sponsor, Government Agency)
OPTIONAL: Tier Designator / Color	Red, Blue, Green or Grey Banding and Tier Indicators (ER, 1, 2, or 3)
OPTIONAL: NIMS ESF Standardized Icon	Standardized Icon representing the corresponding ESF category of the individual or the issuing authority
OPTIONAL: Electronic Validation Capability	ID may possess electronic validation technology. Examples include, but are not limited to: • AAMVA / Nat'l Sheriffs' Assoc. Standard for Magnetic Stripe • AAMVA / Nat'l Sheriffs' Assoc. Standard for 2D Barcodes • FIPS 201 Standard for Magnetic Stripe, Barcode or Contact / Contactless Smart Cards • TSA TWIC Standard for Magnetic Stripe, or Contact / Contactless Smart Cards • Proximity Technology (e.g. for Physical Access Control Systems)

The following IDs have been evaluated to provide a reasonable level of identity assurance. Most of the IDs listed are resistant to identity fraud, tampering and counterfeiting. Providers whose reliability has been established issue many of the IDs listed.

Credential Name	Description	Notes / Exceptions	Validation Source(s)
US State / US Territory Driver License	Issued by US State governments.	Photo Required.	Employer / Sponsor [State (DMV)]
US State / US Territory ID	Issued by US State governments.	Photo Required.	Employer / Sponsor [State (DMV)]
US State / US Territory Commercial Driver License (CDL)	Issued by US State governments.	Photo Required	Employer / Sponsor [State (DMV)]
US Passport	Issued by US Department of State	Includes Photo	Employer / Sponsor [ICAO (PKD)]
US Passport Card	Issued by US Department of State	Includes Photo	Employer / Sponsor [(DoS)]
Permanent Resident Card (Green Card)	Issued by US Citizen and Immigration Services	Includes Photo	Employer / Sponsor [US CIS (DHS)]
Employment	Issued by US Citizen and	Includes Photo and	Employer / Sponsor

Credential Name	Description	Notes / Exceptions	Validation Source(s)
Authorization Document (Form I-766)	Immigration Services. An ID card representing the ability to work in the US. New more secure version being issued starting May 11, 2010.	fingerprint on face of card. Newer card has machine-readable text zone.	[US CIS (DHS)]
Canadian Provincial ID / Driver License	Issued by Canadian Provincial Governments	Includes Photo	Employer / Sponsor [Province (DMV)]
Foreign Passport	Issued by foreign national governments around the world. Some moderate-risk countries do not have controlled registration and issuance practices. Some high-risk countries' passports (such as Cuba and Iran) are not accepted per the US Department of State.	Valid US entry stamp must be present in the passport.	Employer / Sponsor [ICAO (PKD)]
Employer / Sponsor ID Card	Issued by companies and organizations with offices and operations located in the US. Some moderate-risk and high-risk companies do not have controlled registration and issuance practices.	Requirement of a photo recommended…those IDs that do not have a photo should be accompanied by a US government-issued ID or passport.	Employer / Sponsor
Government-Issued Professional ID Card or Badge (Incl. Law Enforcement, Firefighter, etc.)	Issued by State, County and Municipal government organizations across the US. Some require prior professional certification.	Some do not have a Photo.	Employer / Sponsor [US Federal/State/City Govt.]
US Military ID (DoD CAC)	Issued by the US Department of Defense.	Includes Photo	Employer / Sponsor [DoD DMDC]
US Military Driver License	Issued by the US Department of Defense.	Requirement of a photo recommended.	Employer / Sponsor [DoD]
US Military Dependent's ID Card	Issued by the US Department of Defense.	Requirement of a photo recommended.	Employer / Sponsor [DoD DMDC]
US Transportation Worker	Issued by the US Transportation Security	Includes Photo.	Employer / Sponsor

Credential Name	Description	Notes / Exceptions	Validation Source(s)
ID Card (TSA TWIC)	Administration		[US TSA (DHS)]
US Coast Guard Merchant Mariner Card	Issued by the US Coast Guard	Requirement of a photo recommended…those IDs that do not have a photo should be accompanied by a US government-issued ID or passport.	Employer / Sponsor [US Coast Guard]
Form I-872 American Indian Card	Issued by US Department of State	Includes Photo	Employer / Sponsor [(US DoS)]
Indian and Northern Affairs Canada Card	Issued to Indian tribe members in Canada. Reasonably strong credential.	Includes Photo	Employer / Sponsor [Indian and Northern Affairs Canada]
ILO Seafarer's ID Card	Issued by foreign national governments around the world. Used by sailors aboard vessels registered abroad. Stringent standards set by the International Labor Organization. Some moderate-risk countries do not have controlled registration and issuance practices. Some high-risk countries' ID cards (such as Cuba and Iran) are not accepted per the US Department of State.	Includes Photo	Employer / Sponsor [Foreign Govt.]
US First Responder ID Card or Placard	Issued by State, County and City governments and the Pegasus Program throughout the US. The number and type of security features used in some of these ID cards is lacking.	Some do not have a photo…those IDs that do not have a photo should be accompanied by a US government-issued ID or passport.	Employer / Sponsor [US State/City Govt.]
US Personal Identity Verification ID Card (PIV/FIPS-201)	Issued by many US Federal agencies.	Includes Photo	Employer / Sponsor [US Federal/State/City Gvmt or Corporation]
NEXUS Card	Issued by US Customs and Border Protection. NEXUS cards are WHTI-compliant	Includes Photo	Employer / Sponsor [US CBP]

Credential Name	Description	Notes / Exceptions	Validation Source(s)
	documents for land and sea travel, as well as air travel when traveling to and from airports using the NEXUS program, and provide expedited travel via land, air or sea to approved members between the U.S. and Canada border.		
SENTRI Card	Issued by US Customs and Border Protection. SENTRI cards are WHTI-compliant documents for entry into the United States by land or sea, and also provide expedited travel to approved members between the U.S. and Mexico border.	Includes Photo	Employer / Sponsor [US CBP]
FAST/EXPRES Card	Issued by the Canadian Border Services Agency. The FAST/EXPRES card provides expedited travel to pre-approved, low-risk commercial truck drivers crossing either the U.S./Mexico or the U.S./Canada border.	Includes Photo	Employer / Sponsor [Canadian Border Services Agency]
State Dept Diplomatic Driver License	Issued by US Department of State to diplomats, family members and eligible embassy staff living in the US or in US territories.	Includes Photo	Employer / Sponsor [(US DoS)]
State Dept Diplomatic ID Card	Issued by US Department of State to diplomats, family members and eligible embassy staff living in the US or in US territories.	Blue Border for Diplomats and UN Officers. Green Border for Embassy Staff. Red Border for Career Consular Officers and Employees. Family members can also carry the same ID card.	Employer / Sponsor [(US DoS)]
Civil Air Patrol ID	Issued by Civil Air Patrol, an auxiliary of the US Air	Most include photo…those IDs that do	Employer / Sponsor [Civil Air Patrol]

Credential Name	Description	Notes / Exceptions	Validation Source(s)
	Force. The number and type of security features used in this ID card is lacking.	not have a photo must be accompanied by a US government-issued ID or passport.	
FBI InfraGard ID	Issued by the FBI. The number and type of security features used in this ID card is lacking.	Does not include photo. Must be accompanied by a US government issued photo ID or passport.	Employer / Sponsor [FBI InfraGard]

8. Appendix F – Glossary of Terms and Abbreviations

Term or Abbreviation	Definition or Explanation
Credentialing	All the administrative processes that result in issuing, using, monitoring, managing, or revoking any or all of the elements necessary for a person to be credentialed, to include: 1. Identity: Approved Identification Credentialing List (Appendix B) 2. Capabilities: Roles / Responsibilities, Certifications, Verifiable Training, Vetting 3. Affiliations: Employer, Memberships, Associations 4. Purpose: Have you been authorized by your Agency / Organization to respond to the incident at the present timeline (i.e. Tier 1 , Tier 2)

9. Appendix G – Sample Text for SOP Adoption

This SOP is primarily intended to serve the needs of law enforcement agencies and personnel in conducting law enforcement and security operations at checkpoints and within emergency zones during declared emergency events. Law enforcement agencies adopting this SOP may fully adopt it for purposes of implementing all aspects of this SOP, including issuance of Placards and LOAs, or, alternatively, may adopt it for coordination and transit purposes and to evidence intent to honor Placards and LOAs issued under this SOP by other jurisdictions. The following alternative sample language is provided for use by law enforcement agencies in adopting this SOP:

FULL ADOPTION BY LAW ENFORCEMENT

> This SOP has been developed primarily to facilitate coordinated emergency preparedness, response and recovery by law enforcement agencies statewide and across state boundaries, within controlling policy guidance established by elected officials and emergency managers under applicable law. [Law Enforcement Agency Name] has adopted this SOP for purposes of fully implementing all operational aspects of this SOP within [Jurisdiction Name] during emergency events, including issuance of Placards and Letters Of Access for reentry into and use within this agency's jurisdiction.

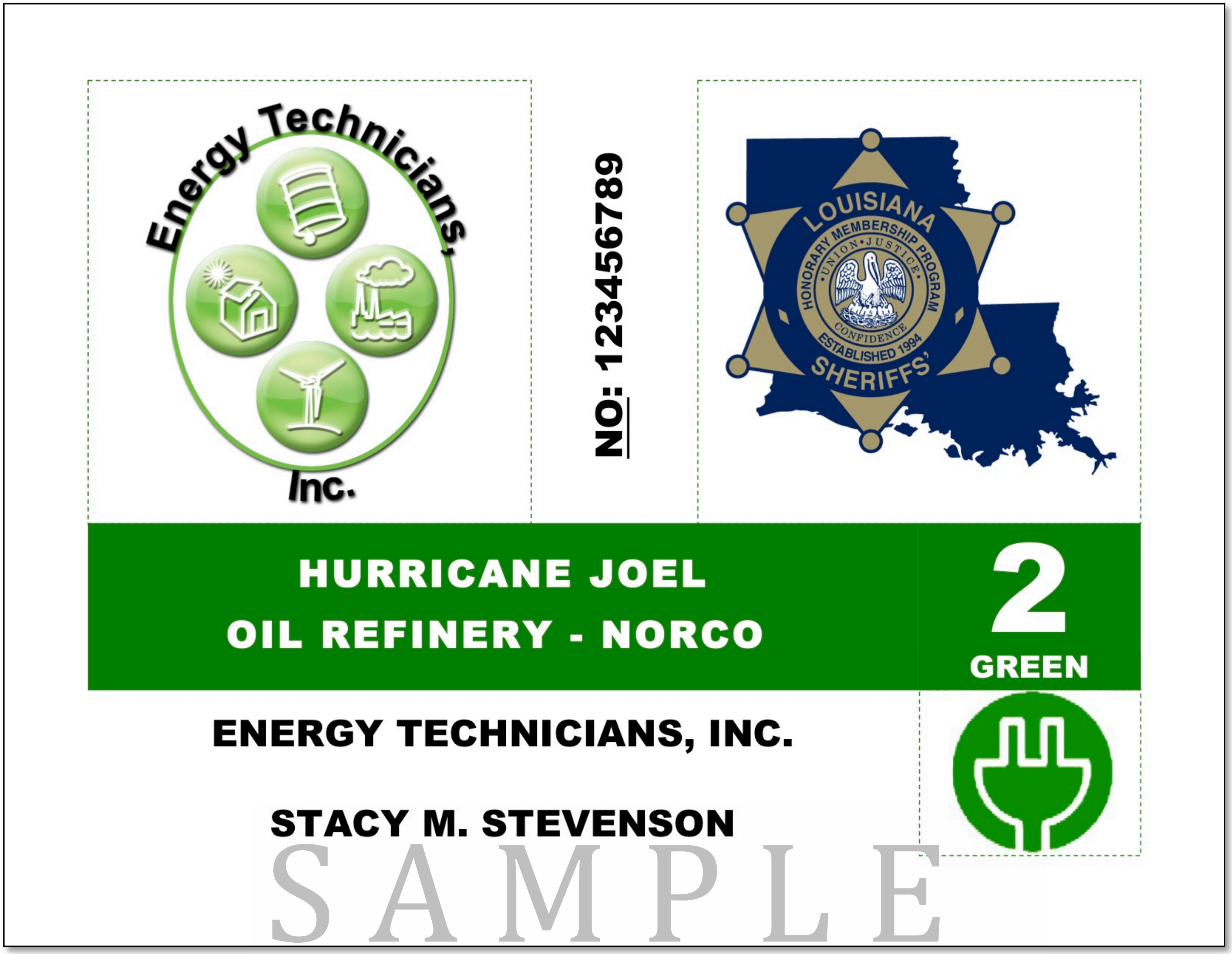
OR ADOPTION BY LAW ENFORCEMENT FOR COORDINATION & TRANSIT

> This SOP has been developed primarily to facilitate coordinated emergency preparedness, response and recovery by and between law enforcement agencies statewide and across state boundaries, within controlling policy guidance established by elected officials and emergency managers under applicable law. [Law Enforcement Agency Name] has adopted this SOP for coordination and transit purposes, to evidence intent to honor Placards and Letters Of Access issued under this SOP for purposes of transiting through [Jurisdiction Name] during emergency events, and for related operational purposes.

Public emergency managers and other types of agencies and entities also may adopt this SOP for purposes of facilitating interaction with adopting law enforcement agencies. The following sample language is provided for consideration by other agencies and entities.

> This SOP has been developed primarily to facilitate coordinated emergency preparedness, response and recovery by and between law enforcement agencies statewide and across state boundaries, within controlling policy guidance established by elected officials and emergency managers under applicable law. [Agency or Entity Name] has adopted this SOP for purposes of facilitating interaction with law enforcement agencies which have adopted it.

Attachment C
Sample Template JSOP-Compliant Placard & Letter of Access



NO: 123456789

HURRICANE JOEL

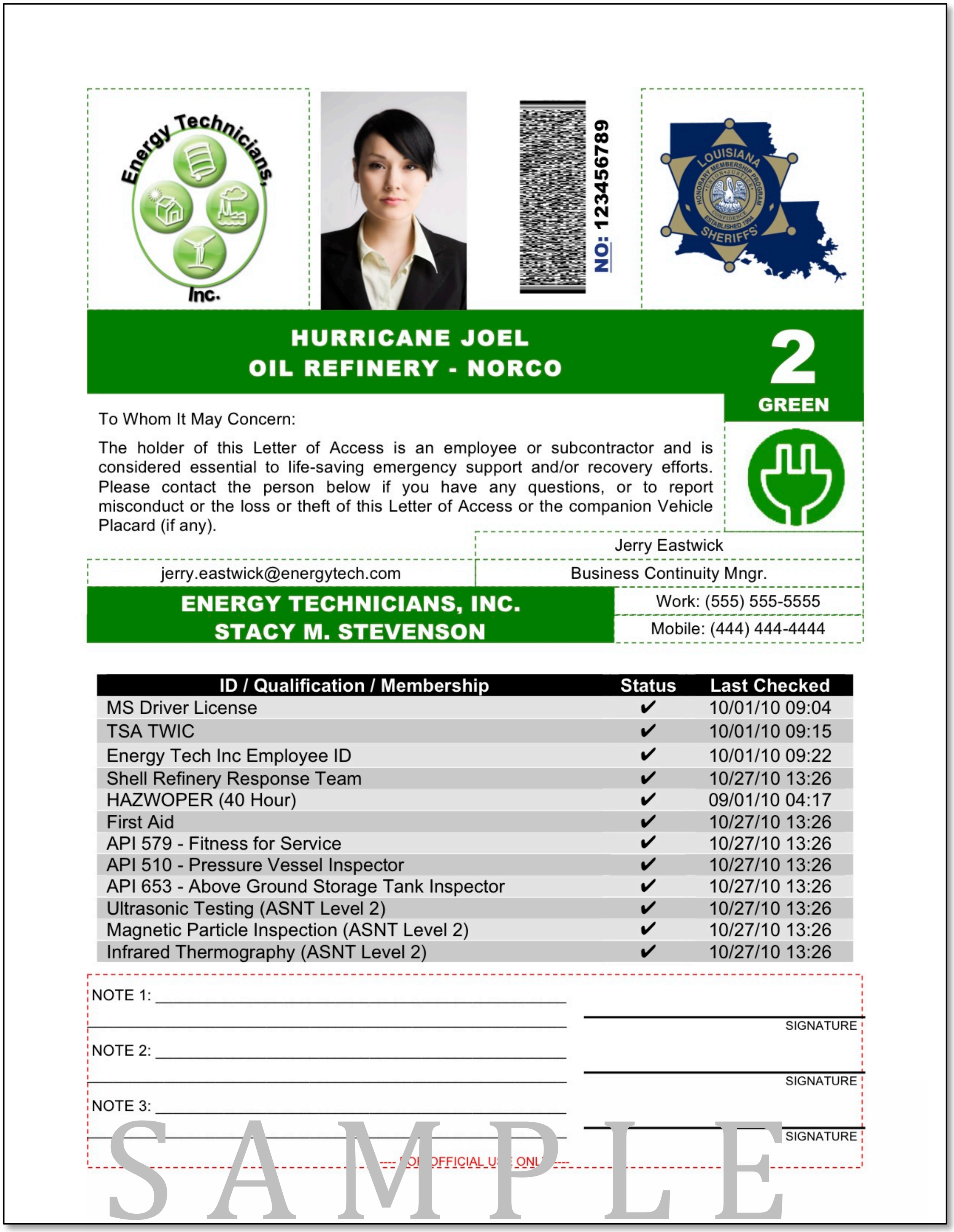
OIL REFINERY - NORCO

2

GREEN

ENERGY TECHNICIANS, INC.

STACY M. STEVENSON



NO: 123456789

HURRICANE JOEL
OIL REFINERY - NORCO

2
GREEN

To Whom It May Concern:

The holder of this Letter of Access is an employee or subcontractor and is considered essential to life-saving emergency support and/or recovery efforts. Please contact the person below if you have any questions, or to report misconduct or the loss or theft of this Letter of Access or the companion Vehicle Placard (if any).

	Jerry Eastwick
jerry.eastwick@energytech.com	Business Continuity Mngr.
ENERGY TECHNICIANS, INC.	Work: (555) 555-5555
STACY M. STEVENSON	Mobile: (444) 444-4444

ID / Qualification / Membership	Status	Last Checked
MS Driver License	✔	10/01/10 09:04
TSA TWIC	✔	10/01/10 09:15
Energy Tech Inc Employee ID	✔	10/01/10 09:22
Shell Refinery Response Team	✔	10/27/10 13:26
HAZWOPER (40 Hour)	✔	09/01/10 04:17
First Aid	✔	10/27/10 13:26
API 579 - Fitness for Service	✔	10/27/10 13:26
API 510 - Pressure Vessel Inspector	✔	10/27/10 13:26
API 653 - Above Ground Storage Tank Inspector	✔	10/27/10 13:26
Ultrasonic Testing (ASNT Level 2)	✔	10/27/10 13:26
Magnetic Particle Inspection (ASNT Level 2)	✔	10/27/10 13:26
Infrared Thermography (ASNT Level 2)	✔	10/27/10 13:26

NOTE 1: ____

____ SIGNATURE

NOTE 2: ____

____ SIGNATURE

NOTE 3: ____

____ SIGNATURE

---- FOR OFFICIAL USE ONLY ----