Illinois Integrated Justice Information Systems (IIJIS)
Concept of Operations for an Illinois Homeland Security Scenario

I. Overview

For many years, public safety providers have been able to respond to events that threatened the security and well-being of our nation – natural disasters, fires, riots, and even conventional hijackings. The nature and extent of those threats changed drastically September 11, 2001, when suicidal terrorists hijacked four airliners and used them as massive weapons to attack innocent civilians and disrupt our world. In light of these unprecedented events, a host of legislative and policy measures have been planned or implemented to bolster the nation's security in airports, international borders, key government buildings, and critical infrastructure. In addition to these direct enhancements of physical security, there are growing calls for improved information and communication capabilities to anticipate and deter terrorist threats, and to respond quickly when those threats might materialize.

The IIJIS Homeland Security Scenario for Information Sharing represents a concerted effort by a number of Illinois agencies working together to achieve this common goal. By continuing our work toward the vision outlined in IIJIS Strategic Plan 2003-2004, we will develop a Homeland Security scenario that will allow us to identify and resolve the information and communication deficiencies that exist today. Through the efforts of the government agencies originally engaged in our scenario planning, as well as the addition of public safety and private partners whose responsibilities are identified in Illinois terrorism plans, we hope to provide a forum for planning and exercise activities that will develop, maintain, and enhance our terrorism response capability. Because the challenges of securing the homeland are formidable, information becomes the key element in designing strategies and solutions. IIJIS is committed to applying information and communication technology in its quest to make Illinois and the nation safer.

II. Purpose

The purpose of the Illinois Homeland Security Scenario is to identify the future functions, range of information exchanges, and interactions needed among public safety and private partners to prevent and respond to a homeland security event. This scenario will serve as a guideline for public safety entities in Illinois to govern the collection, use, retention, and distribution of information in the event of an anticipated or actual terrorist attack. Once developed, current and planned technology for public safety information and communication systems can be validated against Illinois' scenario to identify the gaps that exist today.

Our work will allow us to answer many questions, including:

- How do we analyze intelligence information to assess our vulnerabilities?
- How will we handle sensitive information while protecting privacy and preventing unauthorized disclosure?
- What information will be shared? with whom?
- How do we prioritize the information to be shared during a terrorist event and ensure timely delivery of the information?

- What barriers exist today to prevent information sharing?
- What changes are needed in Illinois to improve the process?
- How will we ensure ongoing communication?
- What information and communication needs are most pressing?
- What solutions are most critical?
- What factors will contribute to solutions?
- What factors will constrain solutions?

III. Scope

The Illinois Homeland Security Scenario(s) will be a strategic planning tool that:

- Will apply to a variety of threats or acts of terrorism within Illinois;
- Provides guidance and outlines operational concepts for both **prevention** and **crisis and consequence management response** to a threatened or actual terrorist incident within Illinois;
- Serves as the foundation for further development of detailed State, and local operational plans and procedures;
- Acknowledges the unique nature of each incident, the capabilities of the local jurisdiction, and the activities necessary to prevent or mitigate a specific threat or incident; and
- Illustrates ways in which State and local agencies can most effectively unify and synchronize their information and communication capabilities.

IV. Method

Our Planning Committee has been expanded to include several homeland security professionals to help us better understand the HS environment. With their help, we will attempt to define and prioritize a set of HS threats. Our vision is to examine a variety of threats and focus on closing critical information and communication gaps that terrorists could exploit to maximize the impact of their attacks. We will design strategies to manage events, but will not try to define them all, as the universe of current and potential threats is large and changing. Such strategies must consider not only existing but potential scenarios and provide the best processes for prevention, detection, and response. We will collaboratively plan to manage the largest risks in the most effective manner, including:

- Weapons of Mass Destruction and Disruption (WMD),
- Public Health, and
- Physical Infrastructure

V. Participating Agencies

Defining a scenario for Homeland Security is a complex task involving many agencies, levels of government, jurisdictions, public/private organizations, systems, and management structures. The scope of the problem, the need for rapid solutions, and the complexity of those solutions present an unprecedented need for cooperation. Since terrorism threatens both the public and private sectors, cooperation will maximize the investment in security solutions while minimizing their complexity and redundancy. Without cooperation and collaboration, we may be able to develop improved solutions, but they may not be interoperable or integrated.

VI. Expected Outcomes

Enhanced communications and public alerts.

- Improved dissemination of government-issued threat warnings and alerts
- Improved public/private knowledge distribution of homeland security information
- Expanded wireless and communications systems

Strengthened information assurance and reliability:

- Ensure the confidentiality, integrity, and availability of public and private sector data
- Enhanced surveillance and intelligence

Improved information integration:

- The coordination among government agencies to manage threats and the integration of systems and data to share information
- Increased ability to create and share actionable and relevant information

Improved response management

- Increased ability to discern indicators of terrorist activity amid overwhelming amounts of information

VII. Conclusion

While we believe the federal government should be the leader in Homeland Security, they should not be the sole source of leadership. Strategies and solutions must emerge from among the broad array of stakeholders. State and local governments and commercial providers need to plan for and implement solutions that improve security based upon cross-enterprise requirements.