# Preliminary Report on the Creation of the Information Sharing Environment

**Prepared Pursuant to Section 1016(c) of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458)**

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **JUN 2005** | | **00-06-2005 to 00-06-2005** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Preliminary Report on the Creation of the Information Sharing Environment** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **ISC Secretariat,2100 K Street NW,Washington,DC,20511** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT **unclassified** | b. ABSTRACT **unclassified** | c. THIS PAGE **unclassified** | | **9** | |

# Table of Contents

# I. Purpose of the Preliminary Report

Recognizing that successful counterterrorism efforts require effective information sharing, section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Public Law 108-458), building on Executive Order 13356 of August 27, 2004, "*Strengthening the Sharing of Terrorism Information to Protect Americans" (Executive Order*), requires the creation of the "Information Sharing Environment" (Environment) for terrorism information. In accordance with IRTPA, the Environment will be the combination of policies, procedures, and technologies linking, as appropriate, the resources (people, systems, databases, and information) of Federal, State, local, and tribal governments, the private sector, and potentially foreign allies to facilitate information sharing, access, and collaboration among users to combat terrorism more effectively. The Environment will support sharing and access to terrorism information, including information from the intelligence, law enforcement, military, homeland security, and other communities.

Consistent with section 1016(f)(1) of IRTPA, the President designated John A. Russack as the Program Manager (PM) for information sharing on April 15, 2005. As recommended by the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission), by Memorandum of June 2, 2005, the President directed the Director of National Intelligence (DNI) to exercise "authority, direction, and control over the PM." The President also directed the heads of all executive department and agencies to provide assistance and information to the DNI and the PM, which will assist the PM in implementing his government-wide statutory mandate in section 1016.

Section 1016(c) of IRTPA requires the PM, in consultation with the Information Sharing Council (ISC) established by IRTPA, to submit a preliminary report (Preliminary Report) describing the technical, legal, and policy issues presented by the creation of the Environment and the way in which these issues will be addressed to the President and Congress, within 180 days after the enactment of IRTPA (i.e. June 15, 2005). In addition, section 1016(c) requires the establishment of an initial capability to provide electronic directory services or the functional equivalent, and a review of relevant current Federal agency capabilities, databases, and systems for sharing and using information.

This document is the PM's Preliminary Report. The Information Systems Council, created by the Executive Order, is in the process of being reorganized as the Information Sharing Council, described in section 1016 of IRTPA. This report was coordinated extensively with representatives of departments and agencies who will participate in the Environment and who have been working on the Environment effort since the issuance of the Executive Order in August 2004. This Preliminary Report draws and builds upon the Information Systems Council's report, required by the Executive Order and titled, "Implementation Plan for the Interoperable Terrorism Information Sharing Environment."

It is important to emphasize that this Preliminary Report is only the first milestone in the process of developing the Environment. Subsequent reports will refine and advance the ideas raised here, as well as identify additional ones integral to building the Environment. Continued PM leadership, supplemented by close cooperation and coordination by all partners in this endeavor, will be essential ingredients for success.

# II. Introduction

The final report of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) described many instances in which, in the period leading up to September 11, 2001, potentially useful information (1) was available but no one knew to ask for it, (2) was distributed only in compartmented channels, or (3) was requested but withheld on the basis of a determination that it could not be shared. Improving information access and sharing is an essential element in winning the war on terror and protecting the homeland. We must better integrate information across our nation to support the needs of intelligence, homeland security, law enforcement, military, emergency responders, state, local, and tribal governments and the private sector.

The shortfalls we experience in information sharing require a staged interagency response. The PM will lead the effort to design and implement the Environment. In this effort, he will be assisted by the ISC. To the extent that additional interagency policy review becomes necessary, it will occur in accordance with Presidential guidance regarding policy development and coordination processes. These efforts will provide direction and help to facilitate the implementation of an effective program across the government. They bring together senior officials from across the Federal Government to work toward a common set of goals and objectives, and ultimately to implement a synergistic approach across the interagency establishment.

The Environment must be supported by the resources, policies, guidelines, and enterprise architecture(s) needed to broaden the secure sharing of terrorism information among Federal, State, local, and tribal entities, the private sector, and potentially foreign allies. To that end, this Preliminary Report broadly identifies some key issues that must be addressed from the outset if we are to achieve our objectives. We recognize, however, there are a multitude of other challenges that will have to be addressed during the tenure of the PM.

# III. Issues Attendant to the Creation of the Information Sharing Environment

The Environment represents a combination of policies, procedures, and technologies designed to facilitate the appropriate sharing of terrorism information across diverse sectors. It is neither one large database nor simply a technology solution. The PM, in consultation with representatives of departments and agencies who will participate in the Environment and relying upon the work of the Information Systems Council, has identified several key issues to be addressed in the implementation of the Environment. The remainder of this section describes these key issues along with a discussion of the initial steps identified to address them.

## *Issue 1: Current authorities and policies governing roles and responsibilities are in some instances ambiguous and conflicting.*

Individual departments and agencies have their own policies and procedures for information sharing, but there is no single government-wide agreement on what constitutes appropriate information sharing. Different standards exist among agencies (and even within agencies) for the designation and dissemination of terrorism information, resulting in different views on who

requires the information and when and how the information is needed and processed. Because information protection standards vary, decisions on reconciling the need to protect information and the need to share information have been inconsistent and have contributed to the creation of cultures that support information segregation. A fundamental change must occur so that, in the dynamic setting of the new Environment, the right information is available to the right people at the right time.

An interagency legal working group (LWG) supporting the information sharing effort identified certain governance roles and authorities that require clarification, including:

- the authorities for establishing business rules to govern the Environment;
- the authorities for creating the Environment architecture; and
- the roles of departments and agencies in sharing terrorism-related information with State, local, and tribal law-enforcement entities.

It is not clear at this point whether statutory changes will be required to clarify these governance issues. The PM, in consultation with the ISC, will review these issues and make recommendations through the interagency policy process for the best means to clarify the roles and authorities of participating agencies.

### *Issue 2: Organizations do not fully trust one another when sharing information.*

Trust is a major challenge in establishing the Environment. In part, this is due to the existence of individual organizational cultures that have been developed based on their mission. There are also legitimate concerns regarding how information will be handled and used once it moves beyond the disseminating agency's control. There is widespread concern that other users of the disseminating agency's information may not have the necessary skills, training, and knowledge to interpret and use it properly. A lack of understanding of organizational missions and a sense of competition between organizations can also lead to the belief that sharing will result in a lack of prestige, loss of control, or reduction in resources. Users are sometimes reluctant to share information because they fear that the information may be misused or misunderstood. A number of steps can be taken to drive systemic changes to foster confidence in broader communities of interest. Education, better audit controls, development and implementation of processes and procedures where none currently exist, and management accountability are paramount.

As a first step, the PM and the ISC will initiate a mission analysis to clarify roles and responsibilities, including identifying offices and people accountable for terrorism information sharing across the government. Additionally, trust will develop by enabling all key stakeholders to participate in the establishment and continued governance of the Environment.

### *Issue 3: Authorized users are not always able to access terrorism-related information in a timely manner. Originator controls, need-to-know requirements, and other restrictions limit access to and distribution of information and limit the ability to collaborate.*

In the current environment, actionable information does not always get to the people who need it when they need it. Users face a vast and confusing array of systems, databases, networks, and

tools that require different access methods and controls. Often, information can only be found in disparate locations, and access typically depends on the user's point of entry into the system. It must be made easier for the user to "enter" the new Environment and use its capabilities. The goal is to permit easy access to the information for appropriately cleared personnel with a need and authorization to access it, while preventing access by those who potentially would do us harm. A significant delay in pushing out critical information could result in missing a window of opportunity for action necessary to protect the homeland.

Although guidelines developed in response to Executive Order 13356 did prescribe limits on the use of originator controls on terrorism information, they have not yet been fully implemented. Moreover, the need-to-know principle, that has influenced information sharing decisions since the early days of the Cold War, can no longer be the exclusive criterion for such decisions in the era of the war on terror. Frequently, originators today do not know "who has the need to know what." As the WMD Commission stated, "it is unrealistic to think that we can achieve our information sharing goals without departing from the traditional approaches of the "need-to-know" principle," however, "one must not dismiss the risks of this approach" (Chapter 9). Moving to an Information Sharing Environment necessitates shifting the paradigm to find the appropriate balance between the need-to-know and the need-to-share and will require rigorous safeguards and significant changes to policies, processes, and cultures.

Under the requirements of Executive Order 13356, departments and agencies have been working to develop and implement data standards to support interoperability. Additional work must be done to expand upon these standards for network enterprises outside the Intelligence Community. In addition, emphasis must be placed on the development of processes and procedures to facilitate interoperability, as well as to rapidly identify users to enable timely access to relevant information.

A major impediment to information sharing is the difficulty associated with moving information and collaborating across various security domains. State and local agency networks, moreover, typically do not connect and communicate with each other or with Federal Government networks. Users have difficulty accessing information due to the tendency to compartmentalize data and the wide variety of systems governed by different policies, procedures, and access controls. Sharing information with and receiving information from foreign governments also present special issues that need to be further addressed and resolved.

The PM and the ISC will review the implementation of existing governmental arrangements for the protection and sharing of information, consistent with applicable law and Presidential guidance. In addition, mandatory guidelines must be developed that appropriately balance security risk with the need to facilitate expedited and efficient access to information for those appropriately cleared personnel with a need and authorization to access the information. These guidelines will also need to address issues concerning restrictions on sharing information with and receiving information from foreign governments.

## *Issue 4: The Environment must ensure the protection of information privacy and other legal rights of Americans in the Environment*

Protection of information privacy and other legal rights of all Americans is a fundamental concern when sharing information. The Environment must protect these rights while permitting access to necessary data. To enable and support information sharing between Federal, State,

local, and tribal entities, there is a continuing need to ensure and enforce information privacy and other legal rights.

A Privacy and Civil Liberties Oversight Board is in the process of being established in accordance with section 1061 of IRTPA to ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of laws, regulations, and Executive Branch policies related to efforts to protect the Nation against terrorism. The Board will build upon the good work of the President's Board on Safeguarding Americans' Civil Liberties, which was established by the President by Executive Order 13353 of August 27, 2004. The ISC will work in conjunction with the statutory Board to identify appropriate information privacy policies and controls for safeguarding Americans' information privacy and civil liberties.

### *Issue 5: The Environment must build on the work of the Information Systems Council in response to Executive Order 13356 to remove technology barriers to information sharing.*

Consistent with the work of the Information Systems Council under section 5 of Executive Order 13356, one of the Environment's goals is to remove technology as a barrier to improved information sharing. For the most part, the technology needed to improve interoperability and information sharing is available today; it should be an enabler rather than a barrier. It is the roles and responsibilities, policies, procedures, guidelines, rules, standards, and legal issues that impede our ability to use technology effectively. This connection and tension between policies and technical matters are highlighted above in the description of Issue 3-*Authorized users are not always able to access terrorism-related information in a timely manner*. While it is true that users face a vast and confusing array of systems, databases, networks and tools, in most cases this vast and confusing array is caused not by technological barriers, but by the policies, protocols, and sometimes security and legal concerns that prevent us from connecting the systems and sharing information in an optimal way.

As the four key issues described above are addressed, the PM, in coordination with the ISC, will work to address any remaining technology barriers that might arise during the implementation of the Environment. Since the implementation plan will be developed over the next six months, it is difficult to predict precisely what, if any, specific barriers of a purely technical nature will need to be addressed. The Information Systems Council identified some of the potential technical issues, including the following: scalability concerns; lack of collaboration tools; lack of interoperable analytic tools; lack of system support for directories and validations; inability to move information across various security level domains; and lack of connectivity between necessary partners. As noted above, however, many of these barriers can be addressed through the implementation of appropriate policies and procedures.

## IV. Capability to Provide Electronic Directory Services

A key component of the Environment is what the IRTPA refers to as "electronic directory services or the functional equivalent." Based in part on a concept articulated by the Markle Foundation's Task Force on National Security in the Information Age, electronic directory services will help authorized participants, including analysts, operators, responders, planners, and policy makers, to locate information, organizations, services, and personnel in support of their respective requirements.

At this point, substantive electronic directory services exist within several of the individual communities that will be associated with the Environment, although they are most often used to locate people rather than information. To build an electronic directory service for all elements requiring terrorism information, however, we need to leverage what exists today, and introduce new capabilities to build upon and harmonize these systems toward our end goal. The PM and the ISC will assess current or planned investments within the Federal Government to provide these capabilities. The PM will also be advised of existing and planned capabilities and technologies through responses to a Request for Information (RFI) developed by the PM and ISC. Based on an analysis of existing capabilities and responses to that RFI, the PM will determine the appropriate development activities and/or acquisition strategy necessary to provide the extended capabilities required.

# V. Review of Current Federal Agency Capabilities for Information Sharing

As part of the FY06 budget process, the Office of Management and Budget (OMB) notified agencies of its intent to work with them to ensure that the investments supporting terrorism information sharing align with the implementation plan for the Environment and meet common standards for Information Sharing. OMB issued a Budget Data Request to departments and agencies collecting information to aggregate a list of Federal information technology investments that support terrorism information sharing. Terrorism information managed by these investments span the homeland security, intelligence, military, and law enforcement communities. Systems from multiple departments already link together, enabling users of one network to directly access information contained on, and to cross-post information to another. The current systems provide a foundation upon which the proposed Environment can be developed and expanded.

# VI. Conclusion

This Preliminary Report is the first milestone in the Environment development process by the PM. As such, it does not constitute an in-depth study of all issues and challenges that must be addressed to implement a government-wide terrorism information sharing program effectively. Subsequent reports will refine and advance the issues identified. As the PM plans for the Environment, the completed reorganization of the ISC, as well as continued coordination and cooperation among all departments and agencies participating in the Environment, will be necessary to establish an effective and successful Environment that meets the mission needs of the producers and consumers of terrorism-related information.

Over the next few months, the PM, in coordination with the ISC, will work to support the President's responsibilities under IRTPA, including section 1016(d), which requires the issuance of guidelines for acquiring, accessing, sharing, and using information, and the issuance of guidelines, in consultation with the Privacy and Civil Liberties Oversight Board, that protect information privacy rights and civil liberties in the development and use of the Environment, and section 1016(e), which requires the President to submit a report to Congress containing an implementation plan for the Environment.

# REFERENCES


1. The Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458).
2. Executive Order 13356—*Strengthening the Sharing of Terrorism Information to Protect Americans*, August 2004
3. Presidential Order dated 15 April 2005, designating the Program Manager, pursuant to section 1016(f) of the Intelligence Reform and Terrorism Prevention Act of 2004, for a term of two years.
4. Presidential Memorandum dated 2 June 2005, "Strengthening Information Sharing, Access, and Integration – Organizational, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment.
5. *Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, 2005.
6. The 9/11 Commission Report – *Final Report of the National Commission on Terrorist Attacks Upon the United States*, 2004
7. Executive Order 13353—*Establishing the President's Board on Safeguarding American's Civil Liberties*, August 2004.
8. "Creating a Trusted Information Network for Homeland Security", Second Report of the Markle Foundation Task Force, December 2003