MEETING THE THREAT OF TERRORISM

Authorized Use

An Authorized Use Standard for Information Sharing Strengthens National Security and Respects Civil Liberties

A coherent and consistently applied mission-based authorized use standard is needed to improve information sharing in a way that strengthens national security and protects the privacy and civil liberties of the American people. One of the key lessons of 9/11 is that government officials must have access to the best information in a timely manner and under the appropriate conditions to enable the most informed decisions, especially to prevent terrorist attacks. Traditional rules for sharing intelligence serve neither the national security nor civil liberties in the face of the complex threats of the 21st century.

Under a mission-based authorized use standard, decisions on information sharing will be based on how the information will be used, rather than on where the information was collected or to whom it pertains. Authorized uses are mission- or threat-based permissions to access or share information for a particular, clearly identified purpose that the government—with public scrutiny—has determined beforehand to be appropriate and lawful. The authorized use concept demands clarity of authorized uses; that is, careful consideration of appropriate roles and missions of different agencies and offices. It also demands careful monitoring of the actual uses of information, through immutable audit logs and robust oversight mechanisms.

A mission-based authorized use standard provides a foundation for the trusted information sharing system. Access to the information will be based on agency mission, the role of individual officials, and a predicated purpose, and will be audited to improve accountability and enhance information security.

Pre-9/11 information sharing standards are no longer workable. At least since the late 1970s, access to and sharing of intelligence information collected by US government agencies have been controlled by rules based on the following criteria:

- whether the information was collected within US territory or overseas
- whether the information pertained to US citizens or permanent resident aliens (US Persons)

Over time, these standards were overinterpreted and misinterpreted well beyond their original scope and purpose. They are no longer workable to control access to intelligence information in the face of the borderless nature of post 9/11 threats.

RESULTS:
Improved National Security; Civil Liberties Protected

Encourage trusted information sharing to improve national security. An authorized use standard creates a consistent and clear standard to effectively mobilize information in a way that meets the challenges of borderless and emerging threats. An agency and its employees, based on authorized mission and roles, would be allowed to discover, access, or share information that might be inaccessible under current rules.

Safeguard civil liberties. An authorized use standard safeguards civil liberties and privacy more directly, efficiently, and effectively by permitting access only for authorized uses while utilizing technological and other means to monitor usage and identify abuses.

Better define and enforce role and authorities. An authorized use standard can extend to an entire program, or be more or less specific by program or activity, depending on the sensitivity of the information.

Increase trust between agencies when accessing and sharing information. The reasons for sharing information will be known and disclosed to participants through an authorized use standard backed up by a robust audit log and oversight mechanisms to ensure that actual use is consistent with authorized use.

Improve the security of information against insider compromise. Real-time audit and monitoring logs will help identify unauthorized access, both for counter-intelligence purposes and protecting civil liberties.

GENERAL PRINCIPLES:
Developing An Authorized Use Standard

Ensure Applicability Across the Government. The concept of authorized use should apply to all components of the information sharing environment, tailored to the specific missions and authorities of individual departments and agencies.

Recognize Anticipated Use. The authorized use standard generally should be lower when the information is not personally identifiable, such as when it is to be used for terrorism-related analysis, policymaking, or alerting functions. It should be higher when the anticipated authorized use is reasonably expected to include some action (such as detention, travel restrictions, or denial of a benefit) within the territory of the US or against US Persons.

Combine with the Use of Anonymization Technology. Anonymization technology can enable information analysis without disclosure of personally identifiable information. When combined with anonymization techniques, an authorized use standard could mobilize information to improve national security and protect civil liberties even more effectively.

Establish Public Process to Create Clear Guidelines: The Executive Branch should develop specific guidelines for implementation of the authorized use standard through a formal high-level process with as much transparency as possible.

Electronic Record-keeping and Audits to Monitor Compliance: Agencies would be required to keep an electronic, auditable record each time an authorized use was invoked for the dissemination of information. The sharing and subsequent use of the information would be subjected to audits and other oversight to ensure its use is consistent with the authorized use.

Minimize Transaction Costs. The system must be designed to record authorized uses electronically in the simplest possible way consistent with the sensitivity of the information requested.

Clarify Roles and Responsibilities. It is important to clarify the roles and responsibilities of all participants in the information sharing environment. Implementation of authorized uses will help ensure that departments and agencies keep to their missions, as authorized by our nation's leadership and understood by the public.

IMPLEMENTATION:
Moving To An Authorized Use Standard

Establishing a new mission-based authorized use standard means the United States must:

- **Develop and issue new guidelines and rules for information access and sharing based on how the party seeking access intends to use the information.**
    - These guidelines for authorized use should be based on the legal authorities for and specific mission of each agency. They should reflect the sensitivity of the information and how the receiving official will use it.
    - Authorized uses should be mission- or threat-based justifications to demonstrate that information was accessed or shared for a reason that the government has determined beforehand to be appropriate and allowable.
- **Build an efficient oversight and technology system that enables users to select, articulate, and electronically certify an "authorized use" as the basis for their access to information.**
    - The "transaction costs" of this authorized use standard must allow information to be used in a way that is timely enough to prevent attacks.
- **Prevent the risk-averse decision making that has hampered information sharing.**
    - Establish carefully considered "safe harbor" protections so that the people sharing information are confident that authorized uses will not subsequently result in unwarranted investigations or career damage if a rule is updated or reinterpreted.
- **Establish a government-wide dispute resolution mechanism for information sharing conflicts.**
- **Implement audit logs to monitor use and compliance with procedures and rules.**
- **Encourage open debate and action involving the Executive Branch, Congress and the general public** to achieve the widest consensus for implementation of clear and legitimate guidelines that improve information sharing and protect civil liberties.

Enhancing National Security, Protecting Civil Liberties
The Markle Task Force on National Security in the Information Age

The Markle Task Force on National Security in the Information Age is committed to discovering how best to mobilize information about major terrorism threats in a way that protects established civil liberties. Chaired by Zoë Baird and Jim Barksdale, working across partisan lines and engaging key national leaders, experts, and policymakers since 2002, the Markle Task Force offers a broad vision, specific solutions and ground-breaking ideas on the key policy and technology issues affecting the creation of a trusted information environment. Markle Task Force recommendations have been adopted by executive order and codified in two pieces of legislation.

The Markle Task Force first recommended a mission-based authorized use standard in its 2006 report, Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment. Its most recent report, Nation at Risk: Policy Makers Need Better Information to Protect the Country, expands upon the Markle Task Force's 2006 report with concrete recommendations to implement an authorized use standard.

For more information, please visit www.markle.org.