

DHS Policy for Internal Information Exchange and Sharing

February 1, 2007

MEMORANDUM TO: All Department of Homeland Security Components
FROM: Secretary Michael Chertoff
SUBJECT: DHS Policy for Internal Information Exchange and Sharing

In order to promote a united, Department-wide information-sharing environment, it is critical that each DHS component gives the highest priority to the sharing of potential terrorism, homeland security, law enforcement, and related information(1). DHS personnel must have timely access to all relevant information they need to successfully perform their duties. Therefore, absent any legal prohibitions as set forth by the Department's General Counsel, information shall be shared within DHS whenever the requesting officer or employee has an authorized purpose for accessing the information in the performance of his or her duties(2), possesses the requisite security clearance, and assures adequate safeguarding and protection of the information. Furthermore, all DHS components are considered part of one "agency" for purposes of the Privacy Act 5 U.S.C. § 552a(a)(1), (b)(1). No DHS component should consider another DHS component to be a separate agency for information-sharing purposes.

The Assistant Secretary for Intelligence and Analysis is the DHS official responsible for assessing and analyzing all terrorism, homeland security, and related law enforcement and intelligence information received by the Department. As such, I direct that each component conduct an immediate review of its existing information-handling procedures and ensure that appropriate mechanisms are in place to provide the Office of Intelligence and Analysis (I&A) with access to all potential terrorism, homeland security, law enforcement, and related information, including foreign intelligence information(3). Like all DHS components, I&A likewise is under an obligation to share information in its possession appropriately across the Department. To facilitate this and other homeland-security-related information-sharing activities, each component's information sharing action officer should be prepared to work with I&A and the coordinating principals of the Offices of Policy and Operations, as well as the Chief Information Officer, which shall constitute the DHS Information Sharing Governance Board.

Additionally, I direct all DHS components, with the Chief Information Officer, to ensure that each DHS employee has access to all information pertinent to his or her responsibilities. DHS must move to standardize the technology used to describe, access, exchange, and manage information in our automated systems, so that we and our partners can easily locate and effectively use the most current and complete data available in support of our vital missions.

No component of DHS shall promulgate information-handling guidelines or enter into agreements that are inconsistent with any aspect of this policy, unless otherwise and expressly authorized by the Secretary. The presumption is that information will be shared, not hoarded. Furthermore, each internal or external information-sharing agreement to which any DHS

component already may be a party, even if entered into prior to the Department's creation, shall be interpreted consistent with this policy, to the extent the terms of the agreement permit such an interpretation. As such, I direct all components, in coordination with the Office of the General Counsel, to take immediate steps to amend any existing agreement, procedure, or guideline that is not capable of being interpreted consistent with this policy, or that otherwise does not facilitate the sharing of information with other components. From this point forward, information-access and -sharing agreements with outside entities will be negotiated and entered into on behalf of the Department as a whole, not on behalf of an individual DHS component.

In order to establish a central repository of all such agreements, each DHS component is directed to provide copies of all information-access and -sharing agreements, including and indicating those referenced in the previous paragraph, to the DHS Executive Secretariat by February 15, 2007. With each submission, the component shall clearly indicate whether it believes the agreement is compliant or non-compliant with this policy and, if compliant, with which other components the information is shared.

It is critical to the security of our Nation that we share information in an environment that is free of unnecessary limitations or constraints. But while doing so, we must ensure the integrity of ongoing law enforcement and intelligence investigations. We must also ensure that DHS's information-sharing practices are conducted in a manner consistent with the law, including Federal privacy and civil rights laws. To that end, the Office of General Counsel, the Privacy Office, the Office for Civil Rights and Civil Liberties, and the Information Sharing Governance Board will continue to work closely with DHS components and monitor their information-management processes to ensure that privacy, civil rights and civil liberties, and other legal protections are fully respected.

Finally, if any components experience data-access denials or delays which they are unable to resolve, they are to bring the matter to the attention of the Information Sharing Governance Board, Deborah Draxler (I&A) at 202-282-8516, or Jonathan Frenkel (Policy) at 202-282-8478. Further direction will be forthcoming on the implementation of the policies, programs, and procedures described herein, including those relating to the Information Sharing Governance Board.

Distribution: All DHS Components

(1) "Terrorism information" means all information relating to the existence, organization, capabilities, plans intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, domestic groups or individuals involved in terrorism, to threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations, or to communications between such groups or individuals, and to information relating to groups or individuals reasonably believed to be assisting or associating with them.

(2) In some circumstances, DHS personnel will have "an authorized purpose for accessing the information in the performance of [their] duties" if their responsibilities necessitate access to an individual piece of information. In other circumstances, DHS personnel will have the requisite authorized purpose if their responsibilities necessitate access to an entire class or category of information.

(3) "Terrorism information" is defined in footnote 1. "Homeland-security information" has the same meaning as in Section 892(f)(1) of the Homeland Security Act of 2002. As used in this directive, "law enforcement information" refers to law enforcement information relating to terrorism or the security of our homeland. "Foreign-intelligence information" means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

This page was last modified on February 9, 2007