J. Howard Beales
Chair, DHS Data Privacy and Integrity Advisory Committee

May 21, 2009

Via Hand Delivery

Secretary Janet Napolitano
Department of Homeland Security
Washington, DC 20528

Ms. Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Washington, DC 20528

Re: DHS Data Privacy and Integrity Advisory Committee White Paper on DHS Information Sharing and Access Agreements

Dear Secretary Napolitano and Ms. Callahan:

I have the honor to convey to you the enclosed White Paper, which sets forth recommendations regarding DHS information sharing agreements with external organizations. We believe that implementation of these recommendations, which reflect the Department's Fair Information Practice Principles policy framework, would strengthen the Department's ability to share information externally in a manner that both protects privacy and furthers the DHS mission.

If I may be of any assistance to you concerning these recommendations, please do not hesitate to contact me.

Sincerely,

/Howard Beales/

J. Howard Beales III
Chair, DHS Data Privacy and Integrity
Advisory Committee

Enclosure
cc: Members, DHS Data Privacy and Integrity Advisory Committee (via e-mail)

Report No. 2009-01

A White Paper:
DHS Information Sharing and Access Agreements

This white paper reflects the consensus recommendations provided by the Data Privacy and Integrity Advisory Committee to the Secretary and the Chief Privacy Officer of the Department of Homeland Security (DHS). The Committee's charter under the Federal Advisory Committee Act is to provide advice on programmatic, policy, operational, administrative, and technological issues within the DHS that relate to personally identifiable information (PII), as well as data integrity and other privacy-related issues.

The Committee deliberated on and adopted these recommendations during a public meeting on May 14, 2009, in Washington, DC.

Summary

Information systems enable ever-increasing abilities to collect, store, copy, and move data quickly, efficiently and broadly. Given its many component parts, the Department of Homeland Security (DHS) has one of the most comprehensive data environments in the U.S. Federal system. Its mere scale, along with its mission, underscores that this information environment is not only large - it contains information that is critically important to both the government and the individuals to whom the data pertains.

As DHS continues to consolidate its operations, it is taking steps to implement the Information Sharing Environment required under the Intelligence Reform and Terrorism Prevention Act[1] (IRTPA) and the supporting One DHS policy addressing the need for improved information sharing. The One DHS policy states that "…it is critical that each DHS component gives the highest priority to the sharing of potential terrorism, homeland security, law enforcement and related information"[2] and calls for every DHS component to utilize all components as a single entity for information sharing purposes. The policy also instructs that no single component should enter into any commitment that is inconsistent with this policy without express authority from the Secretary. IRTPA and the One DHS policy could potentially lead to widespread sharing of personal data, not only within DHS, but also between DHS and other US Federal agencies, as well as between DHS and other non-Federal government agencies, including those of other countries.

---

[1] *Pub. L. No. 108-458, § 1016 Stat. at 3664-70, amended by Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act), Pub. L. No. 110-53, § 504, 121 Stat. 266, 313-17*

[2] *DHS Policy for Internal Information Exchange and Sharing, Secretary Michael Chertoff, 01 February 2007*

For these reasons, the Information Sharing Environment (ISE) and the One DHS policy raise information protection and privacy concerns. It is critical that DHS establish specific policies and practices to govern broad information sharing to ensure that personal data is respected and protected for sharing between DHS and organizations external to DHS. The Committee also recommends DHS review the content of this paper to determine which controls would be appropriate to apply to information sharing within DHS. Governments have recognized that there are two key elements to implementing any process for sharing personal data between agencies. Initially, it is important to decide whether it is appropriate to share the data for a specified purpose. Then, a determination has to be made as to how the data should be shared, particularly the type and volume of data as well as the means for sharing.[3]

The Committee agrees that these two key steps should be considered in all decisions about sharing information; in addition, the Committee believes that a third step must be added, which is a process to review whether the personal data will be shared and protected appropriately.

In order to implement the ISE and One DHS policies, the Committee recommends the Department establish a policy requiring Information Sharing and Access Agreements (ISAAs) for all personal data information sharing with entities external to DHS. The ISAAs must be a critical element of the Department's data governance model and must include central controls for managing the risks of unauthorized use, uncontrolled sharing, and non-compliant information processes.

Herein, we address information sharing policies and practices, including: oversight of the ISAAs, information sharing threshold analysis, ISAA preparation and review, communications supporting agreements, and audit procedures related to the information sharing process and ISAA terms. These policies and practices are framed within the Fair Information Practices Principles (FIPPs) policy framework outlined by the DHS Privacy Office in its Privacy Policy Guidance Memorandum, dated 29 December 2008.

Recommendations

The Committee recommends that:

I. Oversight

- The Secretary direct all components to utilize ISAAs when sharing personal information between DHS and other Federal agencies, as well as other external parties.
- The Secretary establish an Information Sharing Review Board (ISRB) to develop, manage, and oversee a Department-wide information sharing process, including guidance for threshold analysis, agreement requirements, communications, and audit

[3] *Data Sharing Review Report, Richard Thomas and Mark Walport, 11 July 2008.*

procedures.

II. Threshold Analysis

- The Secretary require all component CPO's, or responsible parties in components lacking a CPO, to complete an information sharing threshold analysis (ISTA) whenever they receive an inquiry for information sharing to organizations external to DHS. Also, the DHS Privacy Office should include a question in the template Privacy Impact Assessment to trigger the determination of whether an ISTA is necessary.

III. Sharing Agreements

- DHS prepare and document components of the ISAA itself, including a template, with robust information privacy and security provisions based on the FIPPs policy framework.

IV. Communications

- DHS Privacy Office develop and implement a comprehensive information sharing training program for component CPO's and other parties responsible for sharing agreements.
- DHS Privacy Office develop and implement a communications protocol designed to support CPO's and other responsible parties in communicating the terms and compliance requirements of ISAAs to affected individuals.

V. Audit Procedures

- DHS prepare, document, and apply auditing standards and protocols to measure compliance with the information sharing process and ISAA terms.

The Committee desires expedient creation of ISAAs, a coordinated ISAA approach by all DHS components, and removal of unwarranted information barriers between components. At the same time, we support the Privacy Office's efforts to assure that all personal data handled by DHS components has the protections outlined in FIPPs.

Fair Information Practice Principles Policy Framework

The Fair Information Practice Principles (FIPPs) are the foundational principles for privacy policy and implementation at DHS.[4] When personal information sharing agreements are designed for "… potential terrorism, homeland security, law enforcement and related information", as stated by Secretary Chertoff in the One DHS memo, special procedures should be employed to avoid the inevitable 'scope creep' of the specified purpose. The Committee supports the DHS mission of protecting the United States and its citizens from all manner of terrorist and criminal activities while committing to the Fair Information Practices Principles Policy Framework to protect our citizens' liberties, civil rights and due process through comprehensive and meaningful protection of personal data. The FIPPs support ISSAs by providing controls that ensure accountability and maintain discipline in the ISE.

These eight principles are embedded in the US Privacy Act of 1974 and form the basis of the authority of the DHS CPO, under Sections 222 (a)(1) and (a)(2) of the Homeland Security Act of 2002. The FIPPs, and therefore DHS privacy policy, include:

*"**Transparency**: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).*

***Individual Participation**: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.*

***Purpose Specification**: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.*

***Data Minimization**: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).*

***Use Limitation**: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.*

***Data Quality and Integrity**: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.*

***Security:** DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or*

[4] *Privacy Policy Guidance Memorandum #2008-01, Hugo Teufel III, 29 December 2008*

unintended or inappropriate disclosure.

***Accountability and Auditing**: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements."*[5]

The Committee believes that DHS information sharing must be implemented within the context of the FIPPs policy framework. DHS components should only share personal data under their control within the constraints of the FIPPs policy framework, and the five part structure described herein.

Information Sharing and Access Agreements

I. Oversight – Information Sharing Review Board

The Committee recommends that the Department create an Information Sharing Review Board (ISRB) tasked with responsibility for all phases of the information sharing process, from initial threshold analysis to oversight of compliance with agreement terms. The ISRB should include representatives responsible for information management compliance with legal, security, and privacy policies and practices. The DHS Privacy Office should be a member of the ISRB.

The ISRB should be responsible for evaluating information sharing requests, with the authority to approve or refuse requests, require more information, grant final approval for ISAAs and monitor compliance with the terms of the resulting agreements.

II. Review – Information Sharing Threshold Analysis

Upon receiving an inquiry to share data that includes PII, a component CPO should immediately conduct a comprehensive and accurate Information Sharing Threshold Analysis (ISTA) for review and approval by the ISRB. Component CPO's should be aware of all sharing requests. One important mechanism for this is to include a question in the Privacy Impact Assessment to trigger the need for an ISTA. The ISTA process should be based on documented procedures and administered consistently throughout DHS.

The ISTA must contain thorough and complete entries detailing all aspects of the intended sharing relationship, including a legal analysis addressing the authority under which the sharing is permitted and why the request is necessary and not redundant to pre-existing information sharing arrangements. Each ISTA must include a thorough description of the data source(s) and types, a detailed description of the intended purpose, the security safeguards protecting the data from unauthorized access, use, or loss and the controls in place to monitor compliance with department policies.

---

[5] *Ibid*

When the source of the requested data is a Federal entity, the request must include a detailed analysis of the associated System of Records Notice (SORN), showing that the SORN allows the requested information sharing and use.

Applying the FIPPs Framework to ISTAs

ISTAs help integrate the Transparency principle into the ISE. Additional FIPPs compliance includes:

- Purpose specification – the intended use of the data should be unambiguously stated;
- Data Minimization – precise descriptions of the data sources, types, and fields required with justification for each according to the intended purpose;
- Data Integrity – clear statements concerning the processes used to maintain data accuracy through edit/change/delete practices, including how data changes will be communicated to the data source;
- Individual Participation – detailed description of the manner by which affected individuals may review, challenge, and correct their PII; and
- Information Security – detailed description of the safeguards and controls in place to protect the data from non-compliance with department policies, ISAA terms and with the FIPPs.

To embed the FIPPs into the information sharing analysis, we recommend the following integration into the ISTA.

Information Security Management Controls

A basic tenet of data protection and privacy is that personal information be secured from unauthorized access, use, distribution, modification, and loss. To this end, the ISTA needs to address the information management context in which the requester intends to use the data. These queries include:

- Does the receiving party have a chief information security officer or other named individual with the experience, training, and authority to protect the data appropriately?
- Does the receiving party have a documented information security policy and supporting procedures, and are the individuals who will handle the data trained accordingly?
- What enforcement mechanisms are employed to assure policy compliance and how are violations handled?
- Who monitors compliance with the security policies and procedures, and do they have appropriate resources and authority?
- The information sharing request must include a security analysis, demonstrating that controls and safeguards are adequate to protect personal information both in storage and in transit; additional controls must be implemented to protect the data in all forms, including digital, print, visual, and conversational.

Privacy Management Controls

Integrating privacy into information sharing requires behavioral controls and oversight to ensure personal information is disclosed and used appropriately. In any information sharing request, the Committee recommends that the ISTA must, at a minimum, answer the following questions:

- Does the receiving party have a chief privacy officer or other individual who has the experience, knowledge, and authority to oversee the privacy requirements of the agreement?
- Does the receiving party have a documented privacy policy and supporting procedures, and are the individuals handling the information appropriately trained to comply?
- What enforcement mechanisms are implemented to protect the privacy of the data, and how are violations handled?
- Who is responsible for monitoring compliance, and what audit procedures measure the efficacy of and compliance with the privacy controls?

FIPPs Compliance

In addition to understanding the information security and privacy management controls, the ISTA must evaluate how the data will be processed, stored, and used. To that end, the ISTA must, at a minimum, answer the following questions:

- Is the purpose stated for receiving the data complete and specific?
- Is there a detailed analysis of how the quality and type of data requested meets the specified purpose?
- Does the requested data include any sensitive personal information as defined by the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information[6] ? If so, does the specified purpose require such data? Are there additional controls to assure the information security and privacy of this data?
- How will the data requester provide individual data subjects reasonable access to the personal information held about them? Are the policies and procedures in place adequate to allow the correction, or even expungement, of verifiably inaccurate personal information?
- Do the sharing request and the specified purpose comply with the notifications provided at the time the data was collected about how the data would be processed?
- Does the sharing request include procedures for individual redress should the data be processed in a manner that does not comply with existing law, regulation, or the terms of the agreement pertaining to the original stated purpose for the data collection?

[6] *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, 31 October 2008*

- What safeguards does the recipient have in place to prevent significant adverse consequences to individuals based solely on automated processing without human intervention?
- Should the recipient have to ask for specific approval prior to disseminating the data to additional and/or third parties?
- Should the recipient have to ask for specific approval to process the data outside the United States? If the recipient has approval to disseminate to third parties or to process outside the United States, what controls are in place to assure that the obligations of the agreement flow with the data?

III. Documentation – Information Sharing and Access Agreements

If the ISRB approves an ISTA, then the component privacy officer should ensure an Information Sharing and Access Agreement is completed. These agreements for sharing information must be robust, as they potentially allow for the sharing of large amounts of personal information, some of which may have substantial adverse impact on the given individual. When these agreements are requested from sources external to DHS, this need for robust agreement language increases because responsibility for the accountability and security principles shift to a new party – one that may not have been anticipated under the purpose specification of the original collection.

The Use Limitation principle specifies that all uses of personal information must be compatible with the uses stated at the collection of that data. This concept means that purposes, use limits, security safeguards and other policy considerations must be accounted for in all ISAA requests. When information is obtained from non-public and/or commercial sources, the Department becomes responsible for an array of obligations that must 'travel with the data.

IV. Communications

The role of the DHS Privacy Office is essential in the success of communicating the requirements and process for ISAAs through designated individuals in each DHS component. Also, privacy officers in each of the components should play a critical role in making certain the appropriate analysis is done on information sharing proposals. A component privacy officer is best situated to understand the mission needs of the department component, and to determine how to accomplish such needs without impacting privacy. DHS has made considerable progress in naming component privacy officers, and the Committee looks forward to the continuation of this progress.

ISAAs need to be embedded and integrated throughout DHS. Senior leadership, along with those managing and operating systems, should be fully informed about new and existing ISAAs, as should the Chief Information Officer, Chief Information Security Officer, the DHS Privacy Office, and the Information Sharing Coordinating Council. An individual who reports to senior management should be designated as the accountable person responsible not only for

overseeing compliance with the terms of the agreement, but also for communicating those terms to those individuals within the component group with operational responsibility for the execution of the terms of the ISAA.

We recommend that the component privacy officer or an individual designated by and accountable to senior leadership be tasked with responsibility for communicating the contents of ISAAs in which the component is a participant. The communications program should include, at a minimum, a description of the following elements of the agreement:

- The purpose of the agreement, including the intended use of the data;
- Any specific use limitations included in the agreement or dictated by other agreements or policy directives;
- The type of data governed by the agreement, including whether any of the data is sensitive [7];
- The safeguards required to protect the data from unauthorized access, distribution, or revision;
- The controls required to limit access to those with a legitimate interest in the data; and
- Provisions included in the agreement, or through standard component or department requirements, for auditing compliance with the agreement's terms.

The communications program should include specific instructions about the responsibilities of each involved party and designate the individuals to be held accountable for compliance with the terms of the ISAA and Department policies for information security and privacy.

All relevant and appropriate channels should be utilized to assure that the terms of the agreement(s), the parties responsible for complying with those terms, and the procedures for auditing that compliance are clearly communicated. These channels include, for example, email, written instructions, and in-person presentations.

When ISAAs have expiration dates, the accountable individual should communicate with all participants, assuring that activities involving that agreement cease and the subject data be removed, deleted, and/or destroyed according to established Department policies and procedures.

V. Audit Procedures

Copies of ISTAs and ISAAs, along with all supporting documents of the request for sharing, must be maintained in a secure archive, accessible to those responsible for enforcing compliance with the terms of the agreements. This archival process, including data retention and destruction policies, access controls, and records management protocols should be a

[7] *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, 31 October 2008*

mandatory aspect of the overall ISAA process.

Reasonable and appropriate compliance monitoring and audit procedures must be implemented in a rigorous and regular manner to assure compliance with the terms of the agreements. Non-compliance must have meaningful consequences, including termination of access and escalating to the appropriate level of management.

Accountability and Auditing

All ISAA requests and review processes must include detailed descriptions of the controls in place to assure compliance with all applicable laws, department policy, and terms of the agreement. These controls must be fully documented, thoroughly examined, and diligently implemented.

Conclusion

Implementation of this information sharing process has the potential to substantially mitigate risk to individuals. The ISTAs and ISAAs can be important tools to use toward this end.

The Committee looks forward to continuing its efforts to identify ways to bring the DHS Privacy Office expertise in privacy law, the FIPP's, and the Freedom of Information Act to bear on ISAAs within DHS.