Richard V. Purcell
Chair, DHS Data Privacy and Integrity Advisory Committee

26 March 2009
Via Hand Delivery

Hon. Janet Napolitano
Secretary, 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 Recommendations on the Privacy Impact Assessment Process for Enterprise Services Bus Development

Dear Secretary Napolitano and Ms. Callahan:

I have the honor to convey to you the enclosed Report, which sets forth recommendations on implementing the DHS Privacy Impact Assessment process for Enterprise Services Bus development. 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 build information-sharing technology infrastructure 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,

Richard V Purcell

Richard V. Purcell
Chair
DHS Data Privacy and Integrity Advisory Committee

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

Recommendations for the PIA Process for Enterprise Services Bus Development

A Report by the

Data Privacy and Integrity Advisory Committee

Report No. 2010-02

This report 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 March 18, 2010, in Washington, DC.

Summary

In planning Service Oriented Architecture (SOA) solutions to replace existing application-based services, the DHS Privacy Office should be aware of specific risks to information privacy and data protection and include lines of inquiry to the Privacy Impact Assessment focused on Enterprise Service Bus implementations. To this end, the DHS Privacy Office tasked the Data Integrity and Information Protection subcommittee to investigate these issues.

Background

The Department of Homeland Security (DHS) has embarked on an initiative to move the agency towards a Service Oriented Architecture (SOA) approach to building infrastructure and services technologies. The two primary components of this approach include the infrastructure that delivers the data (Enterprise Services Bus, or ESB), and the services that utilize the data for specific purposes. The underlying objective of developing the architecture is to develop an enterprise-wide method of delivering information that enables current and new services to be maintained and/or developed efficiently, replacing application-based implementations which may be redundant, out-of-date, or otherwise inefficient.

The DHS Privacy Office has been working with the Office of the CIO to explore the underlying challenges in implementing the Department's policy for Fair Information Practice Principles[1] as they move forward with the development of a proposed SOA.

This paper focuses on the challenges of completing the Privacy Impact Assessment (PIA) for the Enterprise Services Bus (ESB) to serve as the foundation for the agency SOA, an area upon which the Privacy Office is focusing specific effort.

In its early work addressing this issue, the Privacy Office developed a Privacy Impact Assessment for an ESB. Our subcommittee was asked to review this PIA and provide additional guidance on the topic to support further PIA's across DHS ESB development.

This document will focus on the privacy issues we believe must be addressed when architecting and implementing an ESB. The recommendations contained herein should be considered as the Privacy Office completes the development of a department-wide template for ESB planning and development.

[1] Privacy Policy Guidance Memorandum No. 2008-01 (December 29, 2008), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

Fair Information Practices in ESB Implementations

As with all DHS PIA's, the PIA for an ESB must comply with the requirements of the Department's policy on adhering to the Fair Information Practice Principles (FIPPs). Moving from individual application structures to an integrated ESB has clear advantages in complying with the FIPPs[2], which consist of the following principles:

- 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 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.

The PIA process requires an examination of each principle during the development stages for all technologies and services, applying the relevant practices requirement for the planned activity. We are careful to state here that ESB architectures are unique in comparison to application-based services, which they replace, in that the purposes for which the services

[2] ibid.

subscribing to the ESB may not be wholly anticipated or described in the ESB planning process. This advantage of ESB's, flexibility to host new services and purposes with minimal, if any, specific changes to the architecture or data, must be anticipated in the PIA process.

Privacy Risks in ESB Implementations

Services that are available on an ESB may provide a variety of capabilities, ranging from simple database query responses to detailed processing of input data from a diverse collection of services that result in some returned output.

Privacy risks in ESB implementations fall into three categories:

- Controls for access to the ESB by individuals and services
- Policy enforcement
- Auditing

ESB Access Controls

ESB's present an increased risk of connecting unauthorized individuals and/or services to the centralized data conduit. The nature of an ESB is that a broad set of individuals can have access to the ESB and services can connect easily and communicate their availability. While the ESB essentially provides a trusted bus or pipeline for the SOA environment, consideration should be given to the process for vetting or qualifying all individuals and services being connected to the ESB.

Access Controls for Individuals

In application-based systems, access controls are partly enforced by the availability of the system to the individual; these systems host limited services, so access to the system itself limits individual access to data and services. ESB architectures are different in that they provide comprehensive data delivery services from multiple sources throughout the organization. Therefore, qualifying individual access to an ESB needs to be more rigorous than for application-based systems. Access controls for individuals have to take into account the authority of the individual to access the data and the specified purposes for which the individual may use the data.

Access Controls for Services

The ESB architecture allows services to be developed and connected to the data conduit efficiently. These services may both request data for use and offer data for use by other services. Therefore, the need to qualify each subscribing service is critical to protecting the privacy, security and appropriate use of the data. Additionally, services that offer data via the ESB must be verified to be providing data appropriate to the security level of the ESB and protected by auditable service access control policies. As an example, a service providing sensitive personally identifiable information (PII) on an ESB should only connect to an ESB

providing the appropriate level of security, including authentication of any requesting individual or service.

A service that combines data from other sub-services to produce a result must be verified not only as having authorized access to those data sources, but must be analyzed to ensure that the combination of those data sources does not result in an inappropriate data leak or use. For example, one sub-service might address library book loans while another deals with international travel. The original intent might have been to correlate the use of travel-related books with actual travel. However, such a service could also explore unrelated correlations of other interests, travel histories, travel companions, and so on.

Services that access data available on the ESB must be identified and authenticated as having legitimate access not only to the ESB but to the data being requested. In the case of DHS, this becomes complicated since an employee of one DHS agency may be utilizing a service to access data maintained by a different agency. A robust and controlled cross-agency identification and authorization protocol is an important prerequisite capability for any DHS ESB implementation.

Policy Enforcement

With the ESB providing connectivity to one or more services potentially serving PII to a requesting service, all services providing PII should be able to meet organizational policy and management requirements. These policies include those ranging from implementations of FIPPs to security policies such as those ensuring data confidentiality and integrity. This protection may require encryption, for example, for certain data classes while at rest and/or while in transit. Safeguards may be invoked during specific processes within the ESB for normal operations, or may involve end-to-end processes from the data resource to the requesting service, depending on requirements set by security and privacy policies.

Auditing

Auditing the system is increasingly important due to the ability of an ESB to provide broader access to more data to more people and services. Care should be take to prevent ESB audit data from capturing actual system data, as opposed to activity meta-data, as that can create an unnecessary risk of data exposure.

Auditing the ESB enables the analysis of transaction histories when necessary (e.g., after an employee leaves, after data leaks, etc.). These audit logs may themselves contain sensitive information, as discussed earlier, so access to these auditing tools may require restrictions; indeed, auditable logs must be maintained for such accesses themselves. Similarly, access to audit logs for classified systems require a matching security clearance. In the case where audit logs are held locally to the ESB or backed-up to a secondary system, care should be taken to protect the audit log from unauthorized access or manipulation. Access control to the audit log should be at the same or higher security clearance to the users of the ESB.

Audit logs from distinct ESB's should be designed so as to be as consistent as possible to enable comparisons and cross-ESB usage and incident investigations.

Recommendations

With these observations and comments in mind, we make the following recommendations to DHS and the Privacy Office in their efforts to support the development, implementation and deployment of an Enterprise Services Bus.

1. Develop rigorous policies, procedures, technical mechanisms and controls to qualify individuals and services requesting access to the ESB including:
   - qualifying and authenticating all individuals accessing the ESB
   - qualifying and authenticating services that request data from and provide data to the ESB
   - acceptable uses of the data distributed by the ESB, including conditions necessary to protect sensitive personal information
2. Develop a mini-PIA process that is applicable whenever new purposes are planned for an existing ESB; such a process may be more targeted than the initial PIA used to plan and develop the system itself
3. Develop policies, procedures, technical mechanisms and controls under which services and sub-services may combine data for specified purposes; include procedures to qualify the authority for access to the data as well as to assure the protection of the resulting data from unauthorized use or disclosure
4. Support the development, maintenance and updating of policies, procedures, technical mechanisms and controls to encrypt sensitive data in both resting and transmission states, as appropriate to the data classification, intended uses, and potential disclosure
5. Review ESB audit capabilities, including access, data requests, data supplies, services uses and security safeguards to assure compliance with the FIPPs
6. Consider including the following requirements as part of the PIA for an ESB:
   - Describe the ways the ESB complies with the FIPPs (Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality & Integrity, Security, Accountability & Auditing)
   - Describe how the ESB improves compliance with the FIPPs over current systems it replaces
   - Describe the controls in place to qualify an individual's access to the ESB, based on the individual's need-to-know basis for access, the relevance of the data to that need and the appropriateness of the data class to the individual's access and purpose
   - Describe the information security safeguards the ESB implements to protect data from unauthorized use, disclosure, corruption or loss
   - Describe how the ESB supports data retention standards of the Department, including support for destruction of unneeded or aged data

- Describe the audit protocols supported by the ESB and how are they enforced, reported and monitored

SOA Considerations Beyond the ESB

We have examined the privacy challenges presented by implementing the infrastructure portion of SOA; the other portion, the services utilizing the data delivery system, also presents an opportunity for considering privacy and data protection effects. Though a thorough analysis of those effects is beyond the immediate scope of this paper, we believe that a preliminary list of questions in this area is relevant for the Privacy Office's consideration.

We developed these questions specifically for individuals considering a service for an existing ESB. Our first set focuses on the effects implied when a service is matched to an existing ESB; the second focuses on the use of the ESB for a particular service under consideration.

Services Considerations for Existing ESB

These are among the questions that practitioners conducting an impact assessment may wish to consider when planning the introduction of a service to an ESB.

1. What type of information is going to be carried?
2. What is the sensitivity of the information that is carried?
3. Who has access? ("who has access to what and why?")
4. How is access controlled?
5. What credential(s) govern data access?
6. How is information secured?
7. At what level is information secured?
8. Who controls security and how (unitary policy?)?
9. What information is trackable?
10. What information is audited?
11. What/how are audit reports generated?
12. Who controls audit?
13. How can transactions be recreated?
14. Separation of duties between audit responsibility and access controls?
15. How are systems and audits backed up?
16. What is the defined functional capacity of the Bus?

ESB Considerations for Planned Services

1. Have you reviewed the PIA for the ESB to be used?
2. What security access control and audit function does your service require?
3. Are there gaps between the needs of the service and the capabilities of the Bus?
4. What are the results of your Gap analysis and what is your mitigation strategy?

Conclusion

The desired future state of fully interoperable agency ESB's across DHS will require extra care in their design to ensure that the policies governing those distinct implementations are harmonized. Like all technology implementations, ESB's are subject to a comprehensive PIA process. Ensuring consistent and compatible policies and procedures for Department ESB's is key to ensuring the security, integrity, and privacy of all of the ESB's data and services, as well of Department applications that might use data obtained from an ESB.