Privacy Impact Assessment
for the

DHS SharePoint and Collaboration Sites

March 22, 2011

Robert Morningstar
Information Systems Security Manager
DHS Office of the Chief Information Officer/Enterprise Service Delivery Office
(202) 447-0467

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) is developing SharePoint as a Service (SharePoint), which will be an enterprise offering available to all organizations within the Department. This platform will serve as an enterprise collaboration and communication solution, eliminating additional investments in duplicative collaborative technologies, leveraging economies of scale, and connecting separate organizations through the use of the same platform in an integrated environment. DHS is conducting this Privacy Impact Assessment (PIA) because personally identifiable information (PII) may be collected and stored in the SharePoint environment. This PIA sets out the minimum standard for SharePoint privacy and security requirements; DHS components may build more detailed controls and technical enhancements into their respective sites.

Introduction

Throughout DHS methods of communications and collaboration strategy vary. Many tools are utilized to store, manage, and share information. For example, many DHS components use shared drives which increase storage costs, require work by external technical personnel to manage access permissions, and reduce the ability to manage different versions of the same document. Use of e-mail presents similar problems: users are storing large quantities of files, which drives up email storage and network bandwidth costs, does not allow individuals to easily share files, and increases the risk of loss of control with respect to dissemination of data. Unnecessary time, resources, and costs are being expended on resolving issues caused by using these disparate and out-dated tools.

The enterprise SharePoint service offering is being introduced to minimize these deficiencies and improve cross-organization communication and collaboration. SharePoint provides a single infrastructure for DHS components to create websites, or team sites from a template designed for team collaboration. This enterprise solution will not only provide DHS and its components with a common platform, but will also provide such capabilities as document management, version control, and ability to manage user access permissions. SharePoint provides a forum in which to coordinate team activities with document collaboration and storage.

In order to reduce dependency on the current tools of email, shared drives, and various other content and collaboration tools, the SharePoint platform will maintain various types of sensitive data, including PII. This environment will not house classified, secret, or top secret information.

This PIA covers all variances of PII including contact information as well as Sensitive PII (SPII) (e.g., Social Security number (SSN), biometric information, criminal history information, medical information, and financial data).

The main privacy risks associated with the use of SharePoint to manage assets containing PII and/or SPII are misuse of information, data spills, and unauthorized account access. DHS is building controls and visual cues into the SharePoint environment to mitigate these risks. A template will be implemented on all team sites to include a background with either “SPII ALLOWED on this site” or “No SPII” text repeated throughout the page. The template will also include corresponding text on all page headers.

Detailed notice will be provided to each site user on each SharePoint site on the policy for posting PII and how the PII can be used. General notice of the creation of SharePoint sites is also provided

through this PIA to the public. As there is no single source of data for various SharePoint sites, data will be collected in accordance with the respective, governing System of Records Notice (SORN) and/or underlying authorities for the offices using SharePoint to manage records containing PII.

All sites will have a designated site owner, or administrator, responsible for determining the user base and ensuring the site is only used for approved purposes such as internal collaboration and document and workflow management. Site owners will be required to complete the "DHS SharePoint Team Site Request Form," questionnaire as well as be required to sign an agreement acknowledging understanding of the use of PII in the DHS HQ SharePoint environment. Site owners provide general information regarding the requested site, the user base, the document library, the administrative roles, funding, and the type and sources of data to be stored. Through this process, the SORNs providing coverage for the collection of information will be identified. Site owners will be responsible for ensuring that users understand which sites are and are not allowed to contain SPII. For sites that contain SPII, site owners must ensure that only users with a verifiable need to know are granted access privileges to the information. Site owners will be responsible for regularly reviewing the information that has been posted to all team sites of which they are the owner. Site owners and users alike will be responsible to ensure SPII has not been posted on sites that do not allow posting of SPII, understanding that the purpose of this approach is to minimize the likelihood of privacy incidents. Where inappropriate posting of SPII is discovered, site owners will ensure its immediate removal from the SharePoint site and report the posting as a privacy incident.

Fair Information Practice Principles (FIPPs)

The Privacy Act of 1974 articulates concepts of how the Federal government should treat individuals and their information and imposes duties upon Federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information. The Homeland Security Act of 2002 Section 222(2) states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974.

In response to this obligation, the DHS Privacy Office developed a set of Fair Information Practice Principles (FIPPs) from the underlying concepts of the Privacy Act to encompass the full breadth and diversity of the information and interactions of DHS. The FIPPs account for the nature and purpose of the information being collected in relation to DHS's mission to preserve, protect, and secure.

DHS conducts Privacy Impact Assessments (PIAs) on both programs and information technology systems, pursuant to the E-Government Act of 2002 Section 208 and the Homeland Security Act of 2002 Section 222.

1. Principle of Transparency

Principle: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

As SharePoint is a tool for DHS components and program offices to use rather than a new collection of PII, PII will be used in accordance with the uses enumerated in the underlying privacy

documentation for each component or program office. Additional notice about SharePoint is provided to the public through this PIA. The underlying SORN for the source systems provide further notice. Site users are also provided a more detailed notice via a customized privacy policy link on every SharePoint site depending on type of data to be posted.

2. Principle of Individual Participation

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

Individuals may access information collected and maintained by DHS through the Privacy Act and Freedom of Information (FOIA) process. The process for access, amendment, and redress remain consistent with the existing privacy compliance documentation. SharePoint, similar to email, is one location where DHS may find responsive records. For additional information about this process, individuals may contact the FOIA office of the relevant component. Contact information for the component offices is available on the component website, www.dhs.gov/FOIA.

As part of the site owner training, the site owner will be required to sign an agreement acknowledging understanding of the use of PII in the DHS SharePoint environment. The site owner will be responsible for providing that additional level of control to ensure there is no inappropriate use of the site. The agreement will also include corrective actions for any breaches, processes for reporting misuse, and acknowledgement that, in the role of site owner, s/he is responsible for training the end users and ensuring that the end users agree to the terms. The DHS Office of the Chief Information Officer (OCIO) will provide a template for the site owners to use for approval by their users.

The general user will be expected to understand and agree to the Terms of Use for posting SPII data on the SharePoint sites. The user will also be expected to report any misuse.

3. Principle of Purpose Specification

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

Data will be collected according to the respective underlying authorities of the source system. SORN coverage will be identified in the questionnaire that must be submitted prior to the creation of a SharePoint site.

Further, the DHS SharePoint environment will implement visual cues on the SharePoint sites indicating that SPII is allowed and SPII is posted on the site or that SPII is prohibited and no SPII is posted on the site. An example of the visual cues will be:

- **SPII-allowed site:**
    1. A background with the text "SPII ALLOWED on this site" repeated throughout the page.
    2. Page headers throughout the SharePoint site with the text "SPII ALLOWED."

3. A non-removable privacy policy on the home page of each site regarding the posting of SPII on the SPII-allowed sites.

- **No SPII site:**
  1. A different colored background from the SPII-allowed sites with the text "No SPII on this site" repeated throughout the page.
  2. Page headers throughout the SharePoint site with the text "No SPII."
  3. A non-removable privacy policy on the home page of each site regarding the posting of SPII on the SPII-restricted sites. The policy will include specific examples of SPII and the reasons such data cannot be posted. Contact information for the site administrator or owner will be provided in the event of accidental posting of SPII.

As stated above, there may be slight variation with DHS components respective instantiations of SharePoint and the visual cues implemented. This sample language is meant to set the minimum standard required and establish a distinction for those sites containing SPII and those that do not; it does not preclude the use of other equivalent language and controls.

4. Principle of Data Minimization

Principle: 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). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration (NARA).

Only authorized users required to perform the stated mission will be granted rights to access and post data on respective SharePoint sites; this access to information will be limited to a need to know basis. For example, USCIS is seeking to use SharePoint to store Fraud Detection National Security Data System (FDNS DS) data. FDNS handles PII such as immigration inquiries, investigative referrals, law enforcement requests, background checks, and case determinations. The site owner for the FDNS SharePoint site would complete the questionnaire itemizing the categories of information collected and affirm that the collection and use will be done in accordance with the DHS/USCIS-006 FDNS DS SORN. The site owner would assume responsibility for ensuring that their use is limited to that which is needed to pursue USCIS's fraud detection and national security mission and that only those individuals who are responsible for managing this type of data are granted access to the FDNS SharePoint site.

Retention of data in the SharePoint environment is consistent with the approved retention schedule for the original data collection. SharePoint is an extension of the systems already identified in a SORN, and therefore the retention schedules applicable to the SORN apply to particular IT instantiation holding the data, in this case a particular SharePoint site. In the case of FDNS, it was determined that a 15-year retention period was adequate to provide FDNS with access to information that is critical to an investigation of fraud, criminal activity, egregious public safety, and national security concerns. Users will follow the established data retention guidelines that govern existing processes.

5. Principle of Use Limitation

Principle: 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 will be used for discrete purposes in furtherance of underlying DHS component missions. SharePoint will be designed to direct site owners to one of two platforms (i.e., SPII allowed or restricted) depending on whether they will be using the specific site to post SPII or not. Users will be trained on proper use and posting onto these respective sites and will be asked to acknowledge their understanding that data is not to be used for purposes other than those specified in the narrowly tailored notice provided on each site. SharePoint sites will not be made available to external entities.

6. Principle of Data Quality and Integrity

Principle: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

In addition to providing training on the proper use of SharePoint, components will train site administrators in the proper management of SharePoint security. Each organization with SharePoint site(s) will identify one or more site owners or administrators who will assume responsibility for the proper maintenance of the site, including granting permissions. Site administrators will utilize the Deny All-Allow by exception access to SPII and sites, in other words, no one will gain access to a site unless specifically granted access by the site administrator. The SharePoint administrators will ensure that this is the default setting across the SharePoint instance. Site administrators will be trained on the appropriate use of approval controls within SharePoint to ensure that data is properly reviewed before it is released.

Delegating responsibility to each organization puts the responsibility of securing the data into the hands of the personnel most qualified to understand the data and the appropriate audience for the data.

7. Principle of Security

Principle: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

In addition to the visual cues and training/communication outlined in Sections 1 and 3, the DHS OCIO will also be implementing a compliance tool to monitor and report the use of PII in order to automate the monitoring and reporting process.

The Information Systems Security Officer (ISSO) responsible for the SharePoint installation (including all layers, sites, and subsites) will be responsible for ensuring adherence to this policy and will conduct random audits monthly on the SharePoint sites to verify compliance.

PII leakage will be handled in accordance with DHS Spillage and Incident Response procedures. The System Security Plan will be amended to clearly define the controls in place to handle these situations. The Contingency Plan and Contingency Test Plan will specifically include a scenario involving data spillage.

The ISSO and Information Systems Security Manager (ISSM) will be involved and ultimately approving the compliance tools selected to assist in enforcing the above rules of behavior regarding PII.

Further, site administrators will utilize the Deny All-Allow by exception access to PII and sites. The SharePoint administrators will ensure that this is the default setting across the SharePoint instance.

8. Principle of Accountability and Auditing

Principle: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and should audit the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

The DHS SharePoint team will train all site owners about the use of SPII on the SharePoint sites. Site owners will be required to attend this training before they can be provisioned a SPII-allowed site. Site owners will then be required to train their end users on the processes and policies (leveraging a train the trainer model). In addition, DHS will maintain a transaction log to ensure appropriate use.

DHS OCIO and the Privacy Office will also work together to develop reference materials outlining the policy, process for protecting SPII, instructions to end users who notice violations of the process, incident management for data spillages, etc. The DHS OCIO will then work with the Office of Public Affairs (OPA) on posting this information on DHS Connect.

Responsible Official

Robert Morningstar

Information Systems Security Manager

DHS OCIO ESDO

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security