Privacy Impact Assessment
for the

DHS Employee Collaboration Tools

DHS/ALL/PIA-059

February 7, 2017

Contact Point

Jorge Reig
Portfolio Management Section Chief
Office of the Chief Information Officer
Department of Homeland Security
(202) 573-3731

Reviewing Official

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) employs various cloud-based services and employee collaboration tools to promote efficiency and improve content management and employee communication across the enterprise. DHS cloud-based services and tools are used by the Department and departmental programs that do not have other content tracking systems to more effectively and efficiently manage the receipt, creation, assignment, tracking, and storage of agency matters. DHS is conducting this Privacy Impact Assessment (PIA) because cloud-based content management solutions and employee collaboration tools collect, use, store, and disseminate personally identifiable information (PII) and sensitive PII (SPII). This PIA replaces two previous DHS PIAs: DHS/ALL/PIA-023 DHS IdeaFactory (January 21, 2010) and DHS/ALL/PIA-037 DHS SharePoint and Collaboration Sites (March 22, 2011).

Overview

On December 9, 2010, the Office for Management and Budget (OMB) released a "25 Point Implementation Plan to Reform Federal Information Technology Management,"[1] which required the Federal Government to immediately shift to a "Cloud First" policy. The three-part OMB strategy on cloud technology revolves around using commercial cloud technologies when feasible, launching private government clouds, and utilizing regional clouds with state and local governments when appropriate.

When evaluating options for new IT deployments, OMB requires that agencies default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists. Cloud computing is defined by the National Institute of Standards and Technology (NIST) as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[2] Cloud computing is defined to have several deployment models, each of which provides distinct trade-offs for agencies that are migrating applications to a cloud environment.[3]

---

[1] 25 Point Implementation Plan to Reform Federal Information Technology Management (December 9, 2010), *available at* https://cio.gov/wp-content/uploads/downloads/2012/09/25-Point-Implementation-Plan-to-Reform-Federal-IT.pdf.

[2] NIST SP-800-145 *available at* http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

[3] Cloud computing can be categorized into three types of service models (as defined by NIST):

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

This PIA is only intended to cover internal DHS uses of cloud-based services as employee collaboration tools. Departmental IT systems that migrate to the cloud are responsible for conducting a Privacy Threshold Analysis (PTA), and if needed, updating existing privacy compliance documentation, including PIA(s) and SORN(s). This PIA replaces two previous DHS PIAs: DHS/ALL/PIA-023 DHS IdeaFactory (January 21, 2010)[4] and DHS/ALL/PIA-037 DHS SharePoint and Collaboration Sites (March 22, 2011).[5]

DHS Cloud-Based Content Management Tools

Although not the only cloud-based content management tool available, many DHS organizations rely on Microsoft SharePoint for their content management needs. SharePoint is a commercial off-the-shelf (COTS) web-based application that provides a platform on which to build custom applications and features a suite of collaboration, document management, and communication tools, as well as a high degree of integration with other Microsoft Office products. SharePoint automates the content management process, eliminating or reducing the need to manually track emails and manage paper-based documents and forms, and promotes a more efficient means of sharing, storing, searching, and reporting on agency information. Used as a content management tool, the SharePoint platform enables secure data entry, standardizes the display of information, and supports data management and analysis by DHS personnel.

SharePoint Capabilities

Although SharePoint is often used for document repository and team collaboration sites, DHS business owners have expanded their use of the product to include broader capabilities and enhanced functionality. The following provides a general description of DHS's use of SharePoint capabilities for content management purposes:

- Forms management: Customized forms can be created within SharePoint so that the information gathered in the form can be stored in a SharePoint list or library for organization and analysis of data. These forms can access and display data from

Cloud Platform as a Service (PaaS). The capability provided to the consumer is the ability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

[4] DHS/ALL/PIA-023 DHS IdeaFactory (January 21, 2010), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhs_ideafactory.pdf.

[5] DHS/ALL/PIA-037 DHS SharePoint and Collaboration Sites (March 22, 2011), *available at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-all-037-sharepointcollaboration.pdf.

multiple sources and provide rich and interactive behaviors to aid in the collaboration and organization of information.

- Records management: SharePoint provides a method for systems to automatically archive or expire content based on criteria set forth by the business owner. For example, a system could delete items from a list if the items are labeled as "Status = Closed" and the items are greater than three years old. Similarly, SharePoint can move items to a separate archive list when they are better suited for long term retention.
- Reporting capabilities: A suite of reporting tools offers reporting and business intelligence solutions while eliminating the need for writing custom code. These tools can be used on specific SharePoint systems so that users can run regular or ad hoc reports that suit their business needs. For example, reporting through SharePoint can be used to manage employee workloads, manage budgets, align resources with operational needs, or perform other trend-based or statistical reporting.
- Auditing capabilities: SharePoint automatically stores information on the identity of system users and logs select actions users take while navigating throughout the environment. Tools, such as version history, can be used on SharePoint pages, lists, or libraries to determine whether any changes were made, which user made the changes, and when the user made the changes.
- Microsoft Office Integration: SharePoint ties in very closely with Office products in an effort to bring some of the native capabilities of certain Office products into SharePoint sites and pages. For example, Excel Services provides the ability to present data from an Excel spreadsheet on a SharePoint page or leverage Excel data in a SharePoint list for manipulating data. This functionality can also help to present charts and graphs from Excel in SharePoint which are automatically updated based on data changes that are made in real time.

Content Management (including SharePoint) Tools Privacy Considerations:

DHS actively deploys content management solutions throughout the enterprise. Program Managers, typically referred to as Site Collection Administrators, are responsible for managing the content of their sites. Content Management sites may include information about DHS employees and members of the public. Most content management tools are assessed for security compliance at the enterprise or Component level, but are not assessed at the tenant, or individual site owner, level.

For this reason, all collaboration site tenants must complete a PTA to:

- Document the purpose, use, and types of PII stored within the site;
- Provide visibility to their Component privacy office about the site collection;

- Inform the enterprise-wide inventory of privacy sensitive systems;
- Minimize the amount of SPII stored on the site; and
- Receive a determination from the DHS Privacy Office on whether updates to privacy compliance documentation are required.

In addition, Component privacy officers should:

- Maintain an internal inventory of all collaboration sites that store SPII;
- Ensure that visual cues are included on each site to denote which sites are authorized to maintain SPII and which are not.

DHS Employee Collaboration Tools

To ensure the timely, effective exchange of ideas and insights, DHS is facilitating anytime, anywhere collaboration for members of the Homeland Security Enterprise. DHS Components can choose from a broad range of collaboration tools available, building their own collaboration portfolios based on their particular objectives and priorities.

Collaboration Tool Functionality

"Presence" is a foundational technology for collaboration. It detects the status of participating individuals and communicates that status to authorized users. With presence awareness, people can quickly see if someone they are trying to reach is available now, temporarily busy, in "do not disturb" mode, or off the network altogether. This awareness allows employees or contractors to find others who can answer their questions immediately and avoid waiting for a response from someone who is not likely to reply in a timely manner.

Chat/instant messaging: Chat enables employees and contractors to quickly communicate with others via typed text from desktop PCs and mobile devices. DHS use of chat or instant messaging is enhanced with presence awareness and security controls. DHS employees and contractors are not required to use, and may opt-out of use of, these chat/instant messaging tools.

Internal enterprise social networking software: DHS organizations have deployed social networking software-like tools within their closed, secure networks. These tools may include:

- Blogs, which foster communication about new developments to internal teams and selected external partners within the DHS enterprise;
- Wikis, which effectively aggregate and publish the subject matter expertise of multiple authorized contributors;
- Facebook-like "walls," which allow ongoing discussions and information-sharing about specific topics; and

- Social search/tagging, which lets DHS employees and contractors add keywords, descriptors, and ratings to documents and other content so that the best information resources in the organization also become the easiest to find.

Group calendars: Collaborative calendaring has become an essential tool for scheduling meetings, coordinating travel, and otherwise ensuring that people have sufficient visibility into the activities of anyone they need to work with.

Conferencing

Audio conferencing: Key attributes for effective audio conferencing include ease of use (including a simple, intuitive way to select and invite participants), good voice quality, and complete call management functions such as muting, secure authentication, and record/archive/playback controls.

Video conferencing: This technology greatly enhances team communication and collaboration by adding the significant meaning of facial expressions, hand gestures, and other visual cues to the conversation. The types of video conferencing available today range from simple desktop tools to high-end telepresence systems that allow participants to feel as conference participants.

Web conferencing: Web conferencing allows users to share the display on their computer screens, including documents, presentations, web browsing sessions, and active software programs. This makes it useful for everything from collaborative editing to online training.

Multimedia conferencing: Multimedia conferencing is the ability to mix and match the above conferencing types, along with streaming video. For example, a multimedia conference could include a streaming video in the middle of a slideshow presentation, followed by a live, interactive question-and answer session.

Types of Tools Used at DHS

DHS organizations may subscribe to any number of employee collaboration services. Some of the most common types of cloud-based services available at DHS are:

Microsoft Office 365: This is a cloud-based version of the Microsoft productivity suite, which includes email (Outlook), Skype for Business, OneDrive, Word, Excel, PowerPoint, and OneNote, that users can access from up to five different devices. Because files are stored in the cloud, users can work with and share documents wherever they are. Microsoft Office 365 also provides features, such as secure project-specific websites, that allows for teams to collaborate on documents, coordinate schedules, and assign tasks.

Microsoft Lync Online/Skype for Business: This is a cloud-based service that provides essential capabilities such as presence, instant messaging, and multimedia conferencing through a consistent, intuitive user interface. Users can make voice calls through Lync to anyone who uses

either Lync or Skype for Business. Lync also provides capabilities such as whiteboards and screen-sharing.

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 (PII). The Homeland Security Act of 2002 Section 222(a)(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 the homeland.

DHS conducts Privacy Impact Assessments on both programs and information technology systems, pursuant to Section 208 of the E-Government Act of 2002 and Section 222 of the Homeland Security Act of 2002. Given that DHS Cloud Based Services and Employee Collaboration Tools describes multiple information collections with various purposes, uses, and authorities throughout the Department, as opposed to a particular information technology system, this PIA is conducted as it relates to the DHS construct of the FIPPs. This PIA examines the privacy impact of DHS Cloud Based Services and Employee Collaboration Tools operations as it relates to the FIPPs.

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.

Content Management Sites:

Information maintained in DHS content management sites will depend on the particular business processes for which the systems are established. Content management sites may serve law enforcement, immigration, human resources, or financial management purposes. Therefore, systems may include a variety of information from or about the public.

Privacy Risk: There is a privacy risk that individuals providing information to DHS do not have notice that explains their information is being stored on a server not owned or controlled by the U.S. Government, which may include a cloud-based service provider.

Mitigation: This risk is partially mitigated. When possible and appropriate, DHS provides notice to individuals about the collection and use of their information. However, in most cases, DHS does not provide notice that the information may be stored in a cloud-based content management system at the time of collection. Regardless of storage location, content management systems that contain PII are governed by a SORN, when applicable, specific to the record types stored within the IT system and must be used in accordance with the purpose(s) enumerated in the SORN. The relevant SORN as well as this PIA also provide notice to the public about DHS's collection, use, and dissemination of their information.

Although explicit notice is not provided at the time of collection, DHS provides system location information in all DHS SORNs. Regardless of whether the DHS data is stored on a third-party server or in a cloud vendor environment, the Privacy Act requirements are still applicable. Pursuant to 5 U.S.C. § 552a(m)(1), cloud service providers must adhere to the Privacy Act requirements whenever DHS contracts with them for the operation by or on behalf of a DHS system of records to accomplish an agency function.[6]

Privacy Risk: There is a privacy risk that cloud service providers that are Federal Risk and Authorization Management Program (FedRAMP) certified will conduct generic, independent assessments of the federal privacy requirements that do not meet the DHS privacy policy requirements. For example, FedRAMP providers may provide a generic Privacy Act Statement on their tools that do not comply with DHS privacy policy requirements.

Mitigation: All cloud service providers that contract with DHS must follow DHS privacy policy requirements. Components that employ cloud service providers should verify that the vendors meet all Department privacy policy requirements, including notice.

The DHS Privacy Office recommends that all cloud-based service providers and systems be included in the DHS Federal Information Security Modernization Act (FISMA) inventory, maintained by the Chief Information Security Office (CISO), and undergo a complete security authorization review.

Employee Collaboration Tools:

There is no privacy risk to notice for Employee Collaboration Tools. All employees are provided with a warning banner when they access government-issued hardware, software, or networks (including employee messaging or collaboration tools) that they have no expectation of

[6] See FedRAMP standard contract clauses "The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information," *available at* https://www.gsa.gov/graphics/staffoffices/FedRAMP_Standard_Contractual_Clauses_062712.pdf..

privacy when using these tools. DHS prohibits employees from archiving message text and from saving conversations into their email files. Employees do not have the option to turn on this function and DHS prohibits the use of messaging tools for official DHS business.

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.

Content Management Sites:

Individuals seeking notification of and access to any record contained in a Content Management site should consult the applicable SORN, if one exists and applies to such a site, and follow the access, correction, and amendment process noted therein.

Employee Collaboration Tools:

Generally, Employee Collaboration Tools are automatically populated with DHS user account information from Active Directory (including, email, organization, and business contact information). Employees may update or modify all of their information within Active Directory as needed (to reflect a new phone number or title). Users may opt to include additional information about themselves, including status updates and location. Users may update this information in real-time.

Privacy Risk: Because DHS data are stored on third-party servers, when an individual attempts to access his or her data, he or she may be unable to do so and may be left without proper redress.

Mitigation: As noted above, if a cloud service provider operating an internal employee collaboration tool for DHS is operating a system of records, the provider must adhere to Privacy Act access requirements. DHS employees who seek information about themselves from a newly issued system of records, or seek to contest its content, may submit a Freedom of Information Act (FOIA) or Privacy Act request in writing to:

Chief Privacy Officer/Chief Freedom of Information Act Officer
Department of Homeland Security
245 Murray Drive, S.W.
STOP-0655
Washington, D.C. 20528

FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible about the subject matter to expedite the search process. Specific FOIA contact information can be found at http://www.dhs.gov/foia under *contacts*.

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.

Content Management Sites:

Generally, DHS uses content management sites to track, manage, review, and report on any matters related to its statutory requirements. The specific purpose of the content management sites and the use of the information maintained within them depend on the nature of the program office and the business process for which the system or site is established.

Content management sites that contain PII are used in accordance with the purpose(s) enumerated in their relevant SORN if one covers that particular site. SORN coverage for the collection, use, and dissemination of the information is determined through the completion of a PTA.

All content management sites must display visual cues indicating whether SPII is authorized to be posted on the system by meeting these minimum requirements:

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.

Non-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.[7]

[7] 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

Employee Collaboration Tools:

The purpose of Employee Collaboration Tools is to facilitate internal collaboration between DHS employees and contractors throughout the enterprise.

Privacy Risk: Employee collaboration tools may be used for purposes beyond an official DHS mission.

Mitigation: DHS employees may not use chat or instant messaging tools to conduct official DHS business. However, DHS employees may use other types of employee collaboration tools that follow DHS or NARA-records retention requirements for businesses purposes consistent with their individual mission functions. Some Components have opted to use employee collaboration tools (such as SharePoint's *MySite* or *MyProfile*) to encourage employee collaboration and unity. DHS employees should have no new purposes for using these tools other than they supplement existing operational readiness and do not add any new purposes.

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).

Content Management Sites:

Records retention and disposition in content management sites vary by the type and purpose of record collected. Content management sites may provide a method for systems to automatically archive or expire content based on criteria set forth by the business owner.

Privacy Risk: There is a risk that information stored in content management systems is duplicative of data stored on Departmental shared drives or in email.

Mitigation: This risk is partially mitigated. When DHS migrates data to a cloud service provider, the original data may remain on agency shared drives pursuant to the applicable records retention schedule.

Recommendation: DHS program and system owners should verify that the archived version of their migrated data is retained in accordance with applicable record retention and disposition rules. Program and system owners should modify systems to store federal record material in specified primary and backup archives, as applicable. After migrating to the cloud, program and system owners should also audit legacy storage locations and delete any archived

those sites containing SPII and those that do not; it does not preclude the use of other equivalent language and controls.

data that is now stored in the cloud, unless retention and disposition rules require its retention in its original system of record or data format.

Employee Collaboration Tools:

Regarding instant messaging tools, DHS only retains contact information from Active Directory. DHS does not retain the contents of chats or instant messages.

DHS employees using employee collaboration tools provide the following information via Active Directory: first name, last name, work email address, username, work phone number, and office location. Some account creation pages for employee collaboration tools may include data fields for personal information, such as home phone number or home address. As a general matter, employees should not provide information beyond business contact information.

Some tools, like DHS Skype for Business rely on Active Directory to pre-populate the user's account. In other cases, DHS may send basic business contact information, such as first name, last name, and email address, to create an account. Any tools that require information beyond basic business contact information will require their own privacy compliance documentation.

Privacy Risk: There is a privacy risk that an employee will provide more information than is needed to create an account with an employee collaboration tool.

Mitigation: This risk is partially mitigated. Many employee collaboration tools are COTS products, which limit the amount of customization DHS can make to the system. DHS works with vendors or contractors to try to eliminate unnecessary data fields or add asterisks to denote required information. However, in some circumstances, DHS is unable to make edits to the data fields. DHS mitigates this risk by providing guidance to the employee about creating an account.

Recommendation: DHS employees and contractors should limit the information they include in employee collaboration tools to business contact information and professional achievements only. Program and system owners should remove any SPII data fields (such as date of birth) from the COTS products whenever possible.

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.

Content Management Sites:

DHS content management sites provide a more secure platform and more sophisticated access controls for the data contained within the sites than email or a shared drive. Content management sites

support access controls specific to each site, depending on the business process for which the system is created and the sensitivity of the information stored within it. These controls are available for the system as a whole, as well as specific files and items contained in the system so that only users with a need-to-know have access to the data. Alternative methods, such as email, shared drive-based solutions or other more rudimentary database management systems, do not typically provide such controls.

Privacy Risk: There is a risk that information, if not properly segregated, may be accessed and used by individuals within DHS without a need-to-know the information for the proper performance of their jobs.

Mitigation: DHS business owners have expanded their use to include broader capabilities and enhanced functionality to include forms management, records management, reporting capabilities, and auditing capabilities. These functions allow users to separate or partition information with more granularity than email or a shared drive.

DHS uses content management sites to manage information collected for purposes across the homeland security mission space, but employs the built-in tools to provide more granular access control than what was previously available via email and shared drives.

Privacy Risk: There is a risk that information may be accessed by the cloud services providers to analyze or search the data for its own purposes or to sell to third parties.

Mitigation: DHS cloud service providers should be FedRAMP certified;[8] however, Components will still need to verify compliance with DHS privacy policy requirements. All FedRAMP certified cloud service providers are bound by the following contract terms:

> The Government will retain unrestricted rights to government data. The ordering activity retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.
>
> The data that is processed and stored by the various applications within the network infrastructure contains financial data as well as personally identifiable information (PII). This data and PII shall be protected against unauthorized access, disclosure or modification, theft, or destruction. The contractor shall ensure that the facilities that house the network infrastructure are physically secure.
>
> The data must be available to the Government upon request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost

[8] The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. For more information, please visit www.fedramp.gov.

to the Government.

No data shall be released by the Contractor without the consent of the Government in writing. All requests for release must be submitted in writing to the Contracting Officer's Representative (COR)/Contracting Officer (CO).

Employee Collaboration Tools:

DHS uses employee collaboration tools for different purposes based on specific Component, office, or mission needs. For example, DHS uses Active Directory information to provide DHS employees with access to an instant messaging program. More information about specific instances of employee collaboration tools at the Department will be discussed in the Appendix to the PIA.

Privacy Risk: There is a privacy risk that employees may use employee collaboration tools to conduct personal business.

Mitigation: As noted in the Transparency section, all employees are provided with a warning banner when they access government-issued hardware, software, or networks (including employee messaging or collaboration tools) that they have no expectation of privacy when using these tools.

Specifically to Lync or Skype for Business, employees and contractors may not use these tools to conduct official business:

> *This U.S. Government System is subject to monitoring. Not authorized for Classified Information. Video recording restricted to authorized users. Not to be used to formally transact agency business or to document the activities of the Organization*.

Regardless of the tools provided by DHS to employees, limited personal use of DHS office equipment is a privilege, not a right. Limited personal use of the government office equipment by employees during non-work time is permissible, when such use: involves minimal additional expense to the Government, is performed on the employee's non-work time, does not reduce productivity or interfere with the mission or operations of DHS organizational elements, and does not violate the Standards of Ethical Conduct for Employees of the Executive Branch.[9]

[9] DHS Management Directive 4600.1 *Personal Use of Government Office Equipment* (April 14, 2003), *available at* http://dhsconnect.dhs.gov/policies/Instructions/4600.1%20Personal%20Use%20of%20Government%20Office%20Equipment.pdf.

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.

Content Management Sites:

Information that is collected and stored in content management systems will generally not be systematically checked for accuracy and timeliness. The DHS employee or contractor entering the information into the content management system is initially responsible for the accuracy of information. In general, the site administrator or administrative users will review incoming information, and any inconsistencies will be corrected by contacting the submitting employee or contractor. In addition, program offices may implement methods of ensuring accuracy on a system-by-system basis.

Employee Collaboration Tools:

DHS has a high degree of confidence in the accuracy of the information because DHS receives the information directly from the employees or contractors. In most cases, employees have direct control over their information and may edit it to maintain its accuracy at any time. In cases in which an individual is unable to directly modify information, he or she may contact his or her Component's IT Helpdesk to request the change.

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.

All DHS content management sites and employee collaboration tools are internal-facing. Users must have access to the DHS network to gain access to systems.

Privacy Risk: There is a risk to security because DHS data is stored on third-party servers, which may not have been assessed by DHS security compliance personnel to ensure compliance with federal IT security requirements.

Mitigation: DHS cloud service providers must be FedRAMP certified. By using FedRAMP certified providers, DHS leverages cloud services assessed and granted provisional security authorization through the FedRAMP process to increase efficiency while ensuring security compliance.

Recommendation: Even though DHS is not performing the security authorization, all FedRAMP certified cloud service providers used by DHS should be included in the DHS FISMA inventory and information assurance compliance tool. DHS may require the vendor ensure certain

data is segregated from all other third-party data as part of the cloud service. Contracts with cloud vendors must confirm DHS or a Component's ownership of the data. Cloud providers must return or destroy the data in its possession at the end of the relationship.

Additionally, the physical location of the servers in which DHS data will be stored should be specified in cloud services contracts and should restrict storage locations for DHS data to the Contiguous United States. Contracts should prohibit transmission of PII data outside of the Contiguous United States without the organization's specific consent except as explicitly specified for DHS's outside the Contiguous United States locations and users.

Privacy Risk: There is a risk to security because the FedRAMP review process does not include the NIST privacy controls. The privacy controls must be assessed by the DHS Chief Privacy Officer.

Mitigation: This risk is partially mitigated. This PIA serves as an initial assessment of some of the privacy controls for cloud service providers.

Recommendation: The DHS Senior Agency Official for Privacy should review all FedRAMP cloud service providers for privacy compliance and privacy controls assessments as part of the PTA process.

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.

Both content management sites and employee collaboration tools are hosted by third-party cloud service providers. Most content management sites automatically store information on the identity of system users and log the actions users take while navigating through the environment. Tools, such as version history, provide visibility into where, when, and by whom changes are made in SharePoint pages, lists, and libraries. If more in depth tracing is necessary, the administrators can reference the detailed audit logs to determine when and who performed actions within the content management site.

Privacy Risk: Because DHS data is stored on third-party servers, DHS may be unable to access and audit Departmental records to ensure compliance with access, use, and records retention requirements.

Mitigation: All DHS cloud service providers should be FedRAMP certified. FedRAMP certified contractors must permit DHS to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for DHS. FedRAMP vendors must provide DHS access to their facilities, installations, technical

capabilities, operations, documentation, records, and databases to safeguard against threats and hazards to the security, integrity, and confidentiality of any DHS data collected and stored by the vendor.

Recommendation: DHS should continue to use only FedRAMP certified vendors. DHS should contract directly with the cloud service providers rather than modify their terms of service agreements. In cases when cloud computing will include the transmittal and storage of PII, amending a cloud service provider's terms of service may not adequately cover all of the Privacy Act requirements. Privacy and security risks are magnified when the cloud service provider has reserved the right to change its terms and policies at will, which is a common provision in some terms of service. Appropriate contract language can help ensure that cloud service providers are transparent about other possible users such as subcontractors or that information is not transferred to other third parties without the knowledge and approval of DHS.

Responsible Officials

Jorge Reig
Portfolio Management Section Chief
Office of the Chief Information Officer
Department of Homeland Security

Approval Signature Page

Original, signed copy on file with DHS Privacy Office

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security

Appendix A

DHS Cloud-Based Services

1. Case & Relationship Management as a Service (DHS-wide)

    a. Case and Relationship Management as a Service (CRMaaS) is a strategic approach to building unified systems that connect all aspects of business relationships together. CRMaaS provides multi-level relationship management that allows users throughout the organization to make informed decisions. The platform can support several line of business requirements of various sizes and can be extended to support various types of relationships including case, task, vendor, asset management, customer service, and corresponding tracking.

    This is a full production level service offering using the Microsoft CRM Dynamics 2011 platform and integrated with Authentication as a Service (AUTHaaS), Email as a Service (EaaS) and SharePoint as a Service (SPTaaS).

2. Collaboration Software (DHS-wide)

    a. Email as a Service (EaaS): An enterprise email system service with a common address list hosted at the Enterprise Data Centers. All DHS Components have the opportunity to procure EaaS from the Enterprise Data Centers. EaaS provides Components access to a common, Sensitive-but-Unclassified email system that includes Enterprise directory services. This system establishes a DHS standard for Components to share calendars and schedule meetings across organizations, and delivers centralized access to DHS employee information (e.g., name, email address, phone number). As a result of this initiative, legacy email systems will be made obsolete, thus reducing overall email support costs, while increasing email efficiencies.

    EaaS provides standard email services via Microsoft Outlook, secure web-based access to email via Internet Explorer and Outlook Web Access (OWA), mobile support services for BlackBerry devices, and an on-line Disaster Recovery (DR) capability. EaaS is sized for daily operations and also supports surge capabilities to DHS during National Emergency events (natural or otherwise).

    b. Microsoft Lync/Skype for Business:

    Microsoft Lync can be used for instant messaging, voice and video calling, and web conferencing within DHS. Streamlined communication from within applications simplifies collaboration and boosts productivity. Microsoft Lync/Skype for Business may not be used for official Department business.

Microsoft Lync is available to the entire DHS Enterprise, which includes DHS employees working remotely.

3. Content Management (DHS-wide)

    a. SharePoint as a Service: As part of the Department's strategy to deploy on-demand, secure, convenient IT services, DHS is offering SharePoint as a Service (SPTaaS). This service provides a secure Microsoft SharePoint Server hosted environment, including tools and services to help DHS users manage information, effectively collaborate, and enhance personal productivity. This managed service offering provides users the ability to easily create and manage collaboration, intranet publishing, basic, and custom team and project focused site collections. It also provides DHS daily operational needs and supports surge capabilities during times of national emergency (natural or otherwise).

    SPTaaS is hosted using a common architecture and infrastructure with both primary and disaster recovery capabilities from the Enterprise Data Centers. Information about the SPTaaS offerings, including number of supported users, initial storage quotas, maximum size, Confidentiality/Integrity/Availability (C/I/A) security standing, and availability of each offering are provided.

    b. Web Content Management as a Service (WCMaaS): A cloud computing service offering that provides an integrated secure platform, multiple environments (test integration, staging and production), a solution stack for content management and hosting, and both tools and processes supporting application lifecycle management for public-facing websites. WCMaaS is considered to be in the Platform as a Service (PaaS) family that along with Infrastructure as a Service (IaaS) and Software as a Service (SaaS) is a cloud computing service model. In a PaaS environment, the customer creates the software application(s) leveraging tools and code from the PaaS provider. The PaaS provider serves up the networks, servers storage, and hosting platform. PaaS simplifies application development by offering a low cost of entry, easier maintenance, scalability, and fault tolerance, enabling customers to focus on their business objectives.