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.

Privacy Impact Assessment
for the

Immigration and Customs Enforcement Forensic Analysis of Electronic Media

DHS/ICE/PIA-042

May 11, 2015

Contact Point
Peter T. Edge
Executive Assistant Director
Homeland Security Investigations
U.S. Immigration and Customs Enforcement
(202) 732-5100

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 243-1717

Abstract

Digital evidence examination is the forensic acquisition and analysis of computer hard drives, thumb drives, cell phones, and any other data storage device obtained in the course of an investigation. The Office of Homeland Security Investigations within Immigration and Customs Enforcement (ICE) uses a variety of electronic tools to conduct criminal investigations that encompass analyzing digital media. ICE uses these tools and technologies to analyze the volume of stored digital evidence data given its rate of growth and ubiquity. ICE is conducting this Privacy Impact Assessment (PIA) because these electronic tools may be used to collect and maintain personally identifiable information (PII).

Overview

Digital evidence examination is the forensic acquisition and analysis of computer hard drives, thumb drives, cell phones, and any other data storage device obtained in the course of an investigation. Because of the increasing ubiquity of electronic media and the corresponding prevalence of digital evidence in the cases that Immigration and Customs Enforcement (ICE) investigates, specially-trained Computer Forensics Agents and Analysts (CFA) need tools to ingest and search through large volumes of electronic media and prepare the data for use throughout all stages of an investigation, including prosecution. Within the ICE Office of Homeland Security Investigations (HSI), the Cyber Crimes Center's (C3) Computer Forensics Unit helps to meet this need by making available to CFAs a variety of both free and proprietary data analysis and knowledge discovery tools. These tools can ingest and search through electronic media and extract relevant evidentiary material for use in investigations and other law enforcement activities. This information is then made available to HSI personnel who are working on the investigation, in accordance with established policies and procedures.

Electronic information is different from paper records because of its intangible form, volume, transience, and global presence. No one tool is currently available to comprehensively extract and present all relevant information from electronic data in order to meet ICE's law enforcement needs; consequently, HSI uses a number of different tools to ensure that it can fully analyze the media it has obtained.

The tools that HSI uses generally can create digital images of electronic media confiscated pursuant to a search warrant, subpoena, or summons; provided pursuant to voluntary production; or seized under border search authority.[1] HSI then employs the tools to image the media, creating a mirror copy to use as a working copy, which is critical to ensure the integrity of the underlying data on the media and its availability for verification. Once HSI images the media, it employs different tools to index the information and extract files and other data points

[1] See Section 1.1 for a list of ICE authorities to conduct forensic analysis of electronic media.

so that CFAs can easily search and analyze the extracted information. Extraction can be physical or logical. Physical extraction identifies and recovers data across the entire physical drive of a computer, without regard to the file system in which the data may appear. Logical extraction identifies and recovers files and data based on the operating system of the hardware, file systems, and applications residing on the hardware.

Once data is extracted, it must be analyzed to determine its pertinence to an open investigation or a suspected violation of law. HSI conducts searches to identify contraband or evidence within the scope of the search authority. If other contraband is located during the search that indicates a separate violation of law (e.g., a search conducted during a fraud case identifies child pornography images), HSI would seek a search warrant to expand the search authority. When ICE obtains electronic media, it is possible, and more than likely, that some of the information on the media will not be pertinent to the investigation or other law enforcement activity that prompted the acquisition in the first place. In order to determine what is pertinent, CFAs who are specially trained to conduct electronic searches and analyses must review all the information on the media to focus on what is most relevant and within the scope of ICE legal authority.

There are a number of types of analysis that can be conducted on electronic media:

1) timeframe, which can help determine when events occurred on a computer system or other device;
2) data hiding, which is used to detect and recover concealed data;
3) application and file, which may be used to correlate files to installed applications, examine the file structure of a drive, or review metadata; and
4) ownership and possession reviews, which help to identify individuals who created, modified, or accessed a file.

HSI uses a variety of tools for these types of analysis. The tools may be commercial or government off-the-shelf applications that are available to any user or that are specifically developed for and purchased by ICE. Some of the electronic tools require ICE agents to create index terms for search purposes and others have predetermined terms based on the common types of data found in electronic media. Some of the tools are useful for indexing the electronic media, although other tools extract and organize the data. All the tools are used primarily for developing evidence in connection with HSI investigations. The electronic media that ICE acquires may contain such categories of PII as names and addresses, email addresses, photographic images (in digital format), credit card information, and telephone numbers. The types of records vary from case to case, but may include sensitive personal information such as medical or financial data, records containing communications such as text messages and emails, and records of Internet activity.

ICE maintains the digital evidence that is analyzed until the investigation to which it pertains has been concluded, including any prosecution by the U.S. Attorney's Office. The original media is considered evidence and ICE keeps it in accordance with ICE chain of custody requirements. ICE retains the records associated with the analysis of forensic evidence in accordance with the DHS enterprise-wide schedule for investigative records.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

ICE possesses statutory authority for its investigations based on over 400 federal laws and regulations. Some of the pertinent statutes under which HSI may obtain digital evidence include:

- 8 U.S.C. § 1225(d), Authority relating to inspections;
- 8 U.S.C., § 1357, Powers of immigration officers and employees;
- 19 U.S.C. § 482, Search of vehicles and persons;
- 19 U.S.C. § 507, Assistance for customs officers;
- 19 U.S.C. § 1461, Inspection of merchandise and baggage;
- 19 U.S.C. § 1462, Forfeiture;
- 19 U.S.C. § 1496, Examination of baggage;
- 19 U.S.C. § 1582, Search of persons and baggage; regulations;
- 19 U.S.C. § 1589a, Enforcement authority of customs officers;
- 19 U.S.C. § 1595a, Forfeiture and other penalties; and
- 22 U.S.C. § 2778, Control of arms exports and imports.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The ICE Search, Arrest, and Seizure SORN[2] and the ICE External Investigations SORN[3] cover law enforcement investigatory records obtained and maintained by HSI. These records include, names, addresses, alien numbers, aliases, biographical information, electronic data, and reports prepared by investigators during the course of an investigation, or received from other

[2] DHS/ICE-008 Search, Arrest, and Seizure, 73 FR 74732 (Dec. 9, 2008).
[3] DHS/ICE-009 External Investigations, 75 FR 404 (Jan. 5, 2010).

agencies participating in or having information relevant to an investigation. Both SORNs apply to various types of records collected, retained, and analyzed by HSI during the course of a criminal investigation.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. The ICE Cyber Crime Center, where much of the work is conducted that involves the use of electronic tools, also participates in ICE's Continuous Monitoring Program, which provides ongoing security assessments for networks and systems.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

DHS has developed an enterprise-wide schedule for investigative records that covers those associated with the forensic examination of electronic media and provides for retention according to Federal Rules of Evidence and applicable forensic standards. NARA approval of this retention schedule is pending.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Not applicable.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

HSI agents collect electronic media in the course of their investigations, which may include computer hard drives, thumb drives, cell phones, and any other data storage devices. The media may contain a variety of categories of PII. HSI uses electronic tools to access, extract, and organize this information so that it may be searched and used for investigatory purposes. The search may look for names, addresses, cellphone or landline numbers, credit card information, specific record types, or a specific string of words or numbers. The search will be customized depending on what is needed to support an investigation. The specific PII that is accessed will

vary based on the type of electronic media imaged and the information that is stored within the media.

Some of the tools allow the data to be accessed and viewed without retaining the data, but with the possibility that query criteria be retained (e.g., the file path and access dates to a specific child pornography file encountered on the media). If legal justification is warranted, the use of different tools, which would allow for the data to be copied to government owned media, would be used.

2.2 What are the sources of the information and how is the information collected for the project?

ICE gathers information from electronic media obtained during the course of an ICE investigation or other law enforcement activity, or finds information publicly available on websites or other open and commercial sources. Electronic media identified for imaging is obtained from the execution of search warrants, subpoenas, or summons; by voluntary production; or is seized under border search authority. The individuals from whom this information is obtained varies depending on the investigation; however, it includes individuals who are the subjects of investigations, witnesses, informants, and members of the public. The data itself may contain information on a wide variety of individuals, including those listed above as well as victims of crimes. The legal process used to obtain the media determines the scope of information that may be extracted and analyzed.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

ICE uses the information collected as evidence relevant to an investigation or prosecution of a U.S. immigration or customs law violation or other law enforcement activity. Results are generated for the case agent to review, analyze, and record. Publicly available data or information from commercial sources may be collected as part of this process if an agent determines that it is pertinent to an investigation or enforcement activity.

2.4 Discuss how accuracy of the data is ensured.

The original digital media is evidence, but is imaged so that the original is always available for comparisons. The mirror image becomes the working copy against which electronic tools are applied. The original media is maintained as evidence for further use if necessary. For example, in cases in which the working copy may become corrupted, a new clone can be created by re-imaging the original electronic media. ICE uses hashing to guarantee the authenticity of an original data set. Forensic evidence can be verified through the use of hashing. A hash value is a unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file,

based on a standard mathematical algorithm applied to the characteristics of the data set.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that more data may be collected than is necessary to further an investigation.

Mitigation: It is often not possible to know in advance what information may turn out to be relevant and necessary to an investigation or other law enforcement activity and with electronic media extraneous information may be included with data that is of investigative interest. This risk is mitigated by the fact that any electronic media that is collected is acquired using a legal process, which establishes the parameters for a search and entails judicial or administrative oversight; is voluntarily shared; or is available publicly.[4] It is also mitigated by the fact that the electronic tools that are used to search copies of the media are intended to extract only that information that appears pertinent to an investigation.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

ICE uses electronic tools to examine digital media in connection with ICE law enforcement investigations and activities. Agents and analysts develop search strings and other queries to apply to the digital media in order to produce a relevant result. Different tools can be used to produce different results: one tool might display an index where the relevant search terms are found in the media and another tool might extract data from deleted files or hidden partitions. The application of different tools to the same media may also lead to further relevant inquiries or facilitate the examination of hidden files.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

The purpose of the electronic tools used by ICE is to sift through large amounts of information in response to user inquiry or programmed functions in order to produce results that may be

[4] An exception to this rule is for ICE Special Agents acting under border search authority who may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion, consistent with the ICE guidelines and applicable laws.

analytically useful in connection with an investigation or other law enforcement activity. The tools can be used to highlight anomalies in the data, but are not used for "data mining" as that term is defined by law. Starting with a predicate that a violation of law may have occurred, ICE agents obtain electronic media pursuant to legal processes and review it using these tools to either confirm or refute the underlying suspicion of a violation. Analytical results are added to case files for further investigative use, including, as appropriate, prosecution of any violations.

3.3 Are there other components with assigned roles and responsibilities within the system?

No.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a privacy risk that the data may be used or processed in ways that are inconsistent what is described in this PIA.

Mitigation: CFAs are responsible for the identification, use, preservation, acquisition, analysis, and presentation of electronic evidence and media. Their actions are governed by requirements specified in the ICE Computer Forensics Handbook and by federal laws, regulations, and policies that govern the acquisition, handling, and preservation of electronic evidence, including personally identifiable information. CFAs undergo extensive training on these requirements that mitigate the risk that the data will be used outside of the scope of these guidelines or in a manner that is inconsistent with this PIA.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

Individual notice is provided to the individual that holds the electronic media or files in question (e.g., the owner of a computer or smartphone, a web hosting service such as Google). In some cases, moreover, acquisition may be voluntary, i.e., with consent of the owner of the media. ICE's Search, Arrest, and Seizure SORN[5] provides general notice that ICE seizes property in connection with its law enforcement investigations and activities. The External Investigations SORN[6] also provides general notice that ICE may seize electronic data.

[5] DHS/ICE-008 Search, Arrest, and Seizure, 73 FR 74732 (Dec. 9, 2008).
[6] DHS/ICE-009 External Investigations, 75 FR 404 (Jan. 5, 2010).

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

If seizures of electronic media are effected through a legal process, the opportunities for consent may be limited to challenging the process by which the seizure is to be carried out during a court proceeding by defense counsel. In voluntary situations, an individual has consented, but is free to withdraw that consent. In the event information is downloaded from public websites, consent is not required because the information is available to anyone who accesses the site.

4.3 Privacy Impact Analysis: Related to Notice

Because digital media is collected either through legal process, through consent, or from publicly available sources, there is no privacy risk related to notice.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

Information that is associated with the forensic examination of electronic media is covered by a DHS enterprise-wide retention schedule that is consistent with the Federal Rules of Evidence and applicable forensic laboratory standards. Retention also depends on whether the matter was prosecuted and whether there is an applicable statute of limitations for the underlying crime.

The retention schedule is pending approval by the National Archives and Records Administration (NARA). Under this proposed schedule, the retention period for forensic images and evidence varies depending on the nature of the investigation and its outcome. For cases that result in a prosecution, the original digital evidence would be retained for five years after expiration of all appeals. For cases that do not result in prosecution, the original digital evidence would be retained until the case is closed, unless the original digital evidence is required for follow up investigation, in which case it will be retained for 16 years. For open cases where there is no statute of limitations for the crime, the original digital evidence is considered a permanent record and would be preserved indefinitely according to Federal Rules of Evidence and applicable forensic standards.

5.2 Privacy Impact Analysis: Related to Retention

The DHS enterprise-wide retention schedule for investigative records establishes retention consistent with federal law and policy and with forensic standards. Accordingly, it mitigates any privacy risk.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Because the digital media that is examined using electronic tools is typically acquired in connection with a law enforcement activity, information that is accessed may be shared with other federal agencies, such as the Department of Justice in instances in which prosecutions are involved, or other state or local law enforcement agencies if joint investigations are involved. These law enforcement agencies could also include foreign law enforcement counterparts. The information shared is used to combat violations of the law, some of which may be global in scope.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Routine use G in ICE's Search, Arrest, and Seizure Records SORN allows for broad sharing of information for law enforcement purposes. It permits disclosure to an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, including criminal, civil, or regulatory violations. The same routine use G is included in ICE's External Investigations SORN. Other routine uses in these two SORNs also provide authority for sharing with courts, third parties, and international or foreign governmental authorities. These onward law enforcement uses and disclosures are consistent with the law enforcement purpose for which the data was collected.

6.3 Does the project place limitations on re-dissemination?

The information may be further disseminated by recipients on a need-to-know basis in

order to ensure proper investigation and prosecution of criminal violations. If evidence of a potential law violation is extracted from digital media, it may be used as necessary by the recipient to carry out its law enforcement functions, including prosecution of the violation. This could involve re-dissemination to others whose input is needed.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Disclosures that are made outside of ICE are typically made as a result of an ongoing investigation or other law enforcement activity, and the record of the disclosure is made in the pertinent case file. The electronic tools at issue in this PIA can record particulars about the data that is extracted, including time and date, but typically would only record information about the user of the tool, who is an ICE employee.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a potential privacy risk that too much information will be shared externally with the Department of Justice or law enforcement partners.

Mitigation: ICE conducts investigations of the matters within its jurisdiction and bolsters its case with evidence that is gleaned through the application of electronic tools to digital media. In the event that a prosecuting attorney from the Department of Justice or a law enforcement partner believes that some of the evidence is not needed for trial or further investigation, he or she will purge the information. The use of electronic tools, however, is intended to facilitate the extraction of appropriate evidentiary information from vast quantities of electronic media. By the time that CFAs have analyzed the resultant information and determined its relevance to a particular matter, it is likely that any extraneous information that might pose a privacy risk has been eliminated from consideration. In other words, the privacy risk from information sharing is likely to be minimal because at the stage that sharing occurs, a trained agent or analyst has made a determination that the information is relevant to the case and sharing it is warranted.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

The information that is extracted using electronic tools typically is added to a case file. Individuals seeking notification of, and access to any record about themselves that may be contained in ICE case files, including data extracted using electronic tools, may submit a request

in writing to ICE Freedom of Information Act Officer, by mail or facsimile at the following address:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009
Washington, D.C. 20536-5009
(202) 732-0660
http://www.ice.gov/foia/

This right to access records is conditioned on the fact that all or some of the requested information may be exempt from access or disclosure to prevent harm to law enforcement investigations or interests. Each request for access will be considered individually.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may dispute the accuracy or integrity of any data used for prosecution purposes, during the judicial process. ICE may release non-exempt portions of investigative records to requesters pursuant to the FOIA, but investigative records are exempt from the access and amendment provisions of the Privacy Act. Providing individual access to investigative records or allowing them to alter the records could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede an investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

7.3 How does the project notify individuals about the procedures for correcting their information?

ICE provides general notice on its public-facing website about the procedures for submitting Freedom of Information and Privacy Act requests. Individuals whose digital media is obtained pursuant to a legal process have notice because of that process and also may have the opportunity to challenge the seizure in an appropriate forum. In instances in which ICE has not acknowledged an investigative interest, an individual may have no opportunity to dispute the information until (and if) the matter is set for prosecution.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that some individuals whose data resides in electronic media or devices used by multiple persons will be unaware that their information has been obtained, and therefore unaware of the opportunity for redress.

Mitigation: This risk cannot be mitigated because even in cases in which several individuals have access to the same computer, the law only requires that one individual who has authority over the computer to consent to a search of its contents. The other individuals may not be aware of or share the desire to consent to such a search.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Only trained CFAs and analysts are permitted to use the electronic tools covered by this PIA, and their examination of digital media is logged and audited. If external challenges are raised to the use of information gleaned from the analysis performed by electronic tools, these challenges are typically resolved in connection with the underlying investigation. Audit logs are reviewed routinely to identify suspected internal misuse of these electronic tools. Any violation is handled through the disciplinary process, which includes referral to the Office of Professional Responsibility in appropriate cases.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All ICE personnel, including CFAs, are required to take yearly privacy and information security training. Additionally, the agents and analysts who use electronic tools are trained on the various tools before they are provided access to use them.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

As noted previously, only trained CFAs are permitted to use electronic tools to extract information from digital media.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Any new agreements to share the results of analysis derived from use of electronic tools must be approved by the Office of the Principal Legal Advisor, with review by the ICE Privacy Officer.

Responsible Officials

Lyn Rahilly
Privacy Officer
Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

Privacy Impact Assessment
for the

SharePoint Matter Tracking Systems

DHS/ICE/PIA-043

July 9, 2015

Contact Point
Lyn Rahilly
Privacy Officer
Immigration and Customs Enforcement
(202) 732-3300

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

U.S. Immigration and Customs Enforcement (ICE) uses SharePoint as a matter tracking solution, allowing ICE program offices that do not have other matter tracking systems to more effectively manage the receipt, creation, assignment, tracking, and archiving of agency matters. The ICE SharePoint environment provides offices the ability to quickly and electronically meet their matter tracking business needs through the use of document, workflow, form, and records management as well as reporting, auditing, and organizational capabilities. In the interest of transparency to the public, ICE is conducting this Privacy Impact Assessment (PIA) to assess the privacy risk of SharePoint as a matter tracking tool. In order to ensure that this method of matter tracking does not erode privacy protections, ICE has developed and implemented processes that give effect to the Fair Information Practice Principles (FIPPs) while improving office efficiency, records management, and exchange of information. Lastly, the appendices to this PIA delineate ICE SharePoint systems used for matter tracking, which will be updated as new systems are deployed or changes to current systems take place.

Introduction

As the principal investigative arm of the Department of Homeland Security (DHS), ICE engages in criminal, civil, and administrative law enforcement as well as non-law enforcement activities. In support of the ICE mission, program offices must be able to effectively manage information and workflows, including the receipt, creation, distribution, tracking, and archiving of tasks, assignments, inquiries, and other correspondence or data (hereinafter referred to as "matter tracking") in a manner that is tailored to specific needs and requirements. ICE's agency-wide need for a more functional and secure matter tracking tool has recently increased amid a transition away from alternative methods, such as email or shared drive-based solutions or other more rudimentary database management systems. As a result, ICE will use Microsoft SharePoint as a tool available when program offices do not have other existing matter tracking or case management systems (*e.g.*, Enforcement Integrated Database (EID), Alien Criminal Response Information Management System (ACRIMe)).[1]

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 matter tracking 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 matter tracking tool, the SharePoint platform enables secure data entry, standardizes the display of information, and supports data management and analysis by ICE personnel.

[1] *See* DHS/ICE/PIA-015 Enforcement Integrated Database and DHS/ICE/PIA-020 Alien Criminal Response Information Management System (ACRIMe) PIAs, *available at* www.dhs.gov/privacy.

ICE is conducting this PIA to provide information on the agency's use of SharePoint as a matter tracking tool, addressing SharePoint capabilities, broad categories of information that may be maintained in ICE's SharePoint matter tracking systems, sources from which information is collected or derived, and safeguards implemented in the SharePoint environment to mitigate privacy risks. In addition, this PIA uses FIPPs to evaluate SharePoint's privacy risks. Lastly, the appendices to this PIA list ICE matter tracking systems that use the SharePoint platform and describe the specific types of data maintained, purpose and use, access, individuals affected, sources of information, records retention, and System of Records Notice (SORN) coverage for each system. The appendices will be updated as new matter tracking systems are deployed or as changes to current systems take place.

SharePoint Capabilities

Although SharePoint is often used for document repository and team collaboration sites, ICE business owners have expanded their use of the product to include broader capabilities and enhanced functionality. The following provides a general description of ICE's use of SharePoint capabilities for matter tracking 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 multiple sources and provide interactive features 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: SharePoint's 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 the 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 real time.

Categories of Information

ICE uses SharePoint to serve law enforcement and non-law enforcement purposes related to the agency's mission. Therefore, any ICE matter tracking system built on the SharePoint platform may include a variety of information about ICE or DHS employees, contractors, and members of the public. The specific information collected will depend on the nature and business process of the particular activity, project, or program that the matter tracking system is being used to support.

SharePoint matter tracking systems may be used to support the tracking of law enforcement activities within the scope of ICE enforcement authorities (*e.g.*, national security, customs violations, immigration benefits fraud, human smuggling, human rights violations, and gang investigations). The types of individuals on whom information is collected in these contexts varies on a case-by-case basis, but may include subjects of investigations, witnesses, victims, business associates, customers, relatives, or others whose information is collected during the course of a law enforcement investigation or activity.

SharePoint matter tracking systems used in support of non-law enforcement, administrative, or programmatic activities reduce ICE's reliance on paper records or other more rudimentary electronic systems and to make agency records accessible and searchable through electronic means. These systems may contain information that pertains solely to ICE or DHS personnel or may include information about members of the public.

This PIA covers different types personally identifiable information (PII), including employee and contractor contact information, as well as Sensitive PII, such as Social Security numbers, Alien Registration Numbers (A-Number), immigration information, criminal history information, medical information, and financial data. The SharePoint environment is not authorized to house classified, secret, or top secret information.

Sources of Information

Information contained within matter tracking systems is obtained from various sources by ICE personnel. Similar to the variances in categories of information, sources of information depend on the nature and business process of the particular activity, project, or program for which the system is used. Information may be collected directly from the individual or third

parties, or derived from other sources (*i.e.*, other paper-based or electronic systems).

Other sources of information include other ICE offices, DHS Headquarters and Components, other government agencies, Congress, the White House, nongovernmental organizations, and members of the public. The sources of information may or may not be reflected in the program office's matter tracking system. However, at a minimum, the sources are documented in the SORN[2] relative to the matter tracking system.

Privacy Safeguards

ICE has built safeguards into the SharePoint environment to help mitigate privacy risks (e.g., data spills, misuse of information, and unauthorized access). Each matter tracking system is equipped with visual cues, oversight mechanisms, and access controls:

- Visual cues: Templates are implemented on all systems that include visual cues as to whether Sensitive PII is authorized for posting in the system. Visual cues are described in additional detail in section 3 below.
- Oversight: All matter tracking systems have a designated point-of-contact (POC) who is responsible for determining the system's user base and ensuring that the system is used only for approved purposes. POCs are required to attend training and sign an agreement acknowledging understanding of the use of Sensitive PII in the ICE SharePoint environment. POCs are responsible for ensuring that users understand whether their system is authorized to contain Sensitive PII. When an inappropriate posting of Sensitive PII is found, POCs will ensure its immediate removal from the matter tracking system and report the posting as a privacy incident.
- Access controls: Role-based permissions are applied to all ICE matter tracking systems – from the system as a whole, down to individual files or items contained in the system. For systems that are authorized to contain Sensitive PII, POCs must ensure that only users with a verifiable need-to-know are granted access privileges to the information. Additional information about access controls is included in sections 4 and 7 below.

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. Section 222 of the Homeland Security Act of 2002 states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices as set out in

[2] All ICE SORNs are published in the *Federal Register* and on the DHS Privacy Office website at http://www.dhs.gov/system-records-notices-sorns.

the Privacy Act of 1974 and shall assure that technology sustains and does not erode privacy (*see* 6 U.S.C. § 142(a)(2)).

In response to this obligation, the DHS Privacy Office developed a set of FIPPs from the underlying concepts of the Privacy Act, which 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. Given the particular technology and the scope and nature of its use, ICE conducted this PIA 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.

Information maintained in ICE SharePoint matter tracking systems will depend on the particular business processes for which the systems are established. Matter tracking systems serve law enforcement and non-law enforcement purposes related to ICE's mission; therefore, systems may include a variety of information from or about the public.

When possible and appropriate, ICE provides notice to individuals about the collection and use of their information. For example, individuals who call the Enforcement and Removal Operations (ERO) Detention Reporting and Information Line (DRIL) hear a brief message alerting them that their personal information may be collected in order for ICE to handle the matter about which they are calling. ERO DRIL enters information they collect directly into its SharePoint matter tracking system. Other ICE offices that do not collect information directly from an individual (*i.e.*, a third party) or use data derived from other sources (*i.e.*, other paper-based or electronic systems) or information collections are unable to provide notice. In these instances, the program office relies on the entity that engaged in the initial information collection to provide notice.

Matter tracking systems that contain PII are governed by the SORN and 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 ICE's collection, use, and dissemination of their information. For each matter tracking system identified in the appendices, the relevant SORN is listed.

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 ICE through the Privacy Act and the Freedom of Information Act (FOIA)[3] processes. Individuals seeking notification of, access to, or correction of any record contained in a matter tracking system covered under this PIA, may submit a request in writing to ICE FOIA Officer, by mail or facsimile:

U.S. Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street SW, Stop 5009
Washington, D.C. 20536-5009
(866) 633-1182
http://www.ice.gov/foia/

Depending on the purpose and information contained in the matter tracking system, all or some of the requested information may be exempt from access pursuant to the Privacy Act in order to prevent harm to law enforcement investigations or interests. Providing individual access to records could inform the subject of an actual or potential criminal, civil, or regulatory violation investigation or reveal investigative interest on the part of DHS or another agency. Access to the records could also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension.

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.

Generally, ICE uses SharePoint matter tracking systems to track, manage, review, and report on matters related to its law enforcement and non-law enforcement activities. The specific purpose of the system and the use of the information maintained within depend on the nature of the program office and the business process for which the system is established.

Systems that contain PII are used in accordance with the purpose(s) enumerated in their relevant SORN. SORN coverage for the collection, use, and dissemination of the information is determined through the completion of a Privacy Threshold Analysis (PTA) and/or a SharePoint Matter Tracking System Template listed in Appendix A of this PIA.

All SharePoint matter tracking systems display visual cues indicating whether Sensitive PII is authorized to be posted on the system. There is slight variation with the visual cues implemented on different ICE program office systems.

For program offices in ICE ERO, Management & Administration (M&A), and the Office of the Director (OD), the visual cues are as follows:

- Sensitive PII-authorized system:

[3] See 5 U.S.C. § 552.

- Header on each page of the system that states "Notice: Sensitive PII is allowed on this site!" in green.
- Green banner fixed on the bottom of each page of the system that states "Notice: Sensitive PII is allowed on this site!" and includes a link to a privacy statement, explaining that the posting of Sensitive PII is authorized in the system.

- Sensitive PII not-authorized system:
  - Header on each page of the system that states "Warning: Sensitive PII NOT allowed on this site!" in red.
  - Red banner fixed on the bottom of each page of the system that states "Warning: Sensitive PII NOT allowed on this site!" and includes a link to a privacy statement, explaining that the posting of Sensitive PII is not authorized on the system. This link also explains the proper steps to take in the event that Sensitive PII is posted in the system.

For program offices in ICE Homeland Security Investigations (HSI), the visual cues are as follows:

- Sensitive PII-authorized system:
  - Green banner fixed on the bottom of each page of the system that states "Notice: Sensitive PII is AUTHORIZED on this site!"
  - Banner also includes a link to a privacy statement, explaining that the posting of Sensitive PII is authorized in the system.
- Sensitive PII not-authorized system:
  - Red banner fixed on the bottom of each page of the system that states "Notice: Sensitive PII is NOT ALLOWED on this site!"
  - Banner also includes a link to a privacy statement, explaining that the posting of Sensitive PII is not authorized in the system. This link also explains the proper steps to take in the event that Sensitive PII is posted in the system.

All SharePoint matter tracking systems also clearly display the name of the POC so users may contact the POC in the event that Sensitive PII is posted in systems that are not authorized to host Sensitive PII or Sensitive PII is improperly restricted on sites that are authorized to host Sensitive PII and is accessible to those without a need-to-know.

For each matter tracking system identified in the appendices, the purpose and use are described.

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).

Using SharePoint for matter tracking provides a more secure platform for and more sophisticated access controls to the data contained within the systems. SharePoint supports access controls specific to each matter tracking system, depending on the business process for which the system is created and the sensitivity of the information stored within it. These controls are placed on 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 or shared drive-based solutions or other more rudimentary database management systems, do not typically provide such controls.

Records retention and disposition in matter tracking systems varies by the type of record collected. SharePoint provides a method for systems to automatically archive or expire content based on criteria set forth by the business owner. Any time a business owner requests this type of functionality, the criteria for retaining the respective information housed in the system is documented and maintained by the ICE SharePoint development teams.

For each matter tracking system identified in the appendices, the information collected is assessed against the purpose of the system prior to inclusion in this PIA. System purpose and use, data elements, access controls, and records retention are described in the appendices.

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.

ICE uses data for purposes related to matter tracking in furtherance of the ICE mission. The specific purpose of each matter tracking system is defined prior to the creation of the system. ICE POCs are responsible for determining the system requirements and user base and, once the system is created, ensuring that it is used only for approved purposes.

Through the use of SharePoint, the proliferation of data is limited. The SharePoint environment allows for data consolidation and eliminates or reduces the need for ICE program offices to retain both paper and electronic copies of documents or multiple electronic copies in more rudimentary database management systems.

Matter tracking systems are not made available to external entities, and data stored in the systems is not directly accessible by users or computer systems outside the ICE network. Any external sharing of information contained within a SharePoint application is made

pursuant to the Privacy Act.[4] For each matter tracking system identified in the appendices, the purpose and use are described and the relevant SORN is listed.

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.

Information that is collected and stored in matter tracking systems will generally not be systematically checked for accuracy and timeliness. However, information that ICE uses as part of its law enforcement and non-law enforcement activities will be reviewed for accuracy as required by the particular activity and the laws and authorities, if any, applicable at the time the agency collects the records.

In some cases, information contained within matter tracking systems for law enforcement purposes may be known to be inaccurate. For example, records related to a fraud investigation may contain false or fictitious information. Nonetheless, maintenance of these records in a matter tracking system is necessary to support the investigation. Records pertaining to law enforcement activities may contain knowingly inaccurate information in addition to accurate PII, and must be maintained for the purposes of the particular activity.

The ICE employee or contractor entering the information into the matter tracking system is initially responsible for the accuracy of information. In general, the POC 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.

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 ICE matter tracking systems are internal-facing. Users must have access to the ICE network to gain access to systems. Only authorized users required to perform the stated purpose of the system will be granted rights to access and post data in the system; this access will be limited to a need-to-know basis. ICE establishes access controls for each matter tracking system created based the business process for which it is created and the sensitivity of the information stored within it. POCs are trained on how to use SharePoint's access controls, on a group or user-level, to systems, document libraries, and specific documents and items.

ICE personnel can gain access to a SharePoint system only after a business owner, POC, or site manager approves a particular user's access. The site manager program allows members of ICE organizational entities to gain a higher level of permissions to the ICE

[4] *See* 5 U.S.C. § 552a(b).

SharePoint environment upon successful completion of an exam and adherence to posted guidelines and rules of conduct. Site managers have additional permissions that allow them to make data and user-based modifications to a specific site they have been granted permission to manage. The ICE SharePoint development teams keep records of all site manager nominations as well as where these individuals have increased levels of permissions within the environment. For each matter tracking system identified in the appendices, the access controls are described.

In the event of a data incident – including misuse of data, unauthorized access to a SharePoint application, unauthorized posting of Sensitive PII, and inappropriate disclosure of Sensitive PII from the application – the incident will be reported and handled as a privacy incident. For cases in which misconduct is suspected, the incident will be reported to the ICE Office of Professional Responsibility for further investigation.

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.

SharePoint automatically stores information on the identity of system users and logs 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 ICE SharePoint teams can reference the detailed audit logs to determine when and who performed actions within SharePoint.

The ICE Privacy and Records Office, in coordination with the ICE SharePoint development teams, trains all POCs on the privacy protocols associated with the use of SharePoint. POCs are also made aware of their responsibility to train users and that they are accountable for the actions of their users. Attendance at this training is mandatory before a program is provisioned a system that is authorized to contain Sensitive PII.

In addition, all ICE personnel are required to complete a SharePoint privacy training that discusses Sensitive PII, posting documents and information, and SharePoint auditing. Users are informed that their POCs will provide more detailed training on their specific SharePoint system and the information it can and cannot contain. Personnel are also required to complete annual security and privacy training, which emphasizes SharePoint best practices along with the DHS Rules of Behavior and other legal and policy restrictions on user behavior.

Responsible Officials

Lyn Rahilly, Privacy Officer

U.S. Immigration and Customs Enforcement
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

APPENDICES

Appendix A – SharePoint Matter Tracking System Template

Program/System:

List the name of the agency, program office, and SharePoint matter tracking system.

Purpose and Use:

Provide a general description of the program/system and its purpose, including how the purpose of the program/system relates to ICE's mission and how the system operates/business process.

System Access:

Provide a general description of who has access to the system.

Individuals Impacted:

Provide a list of individuals (i.e., members of the public) whose information will be contained in the system.

Sources of Information:

Provide the sources from which information maintained in the system is derived.

Data Elements:

Provide a specific description of information that may be collected, maintained, and/or generated by the system. Highlight any collection and maintenance of PII and Sensitive PII.

SORN Coverage:

List the SORN(s) under which this data collection and maintenance is covered.

Records Retention Period:

List the retention period(s) for records maintained in the system.

Appendix B

Program/System:

ICE Enforcement and Removal Operations (ERO) Custody Programs Division (CP) Detention Reporting and Information Line (DRIL) Custody Assistance and Inquiry Resolution System (CAIRS)

Purpose and Use:

ERO CP operates the Detention Reporting and Information Line (DRIL) in an effort to resolve community-identified problems or concerns with ICE immigration and detention policies and operations. DRIL operators are responsible for answering inquiries (questions, requests, and complaints) sent to ICE via phone calls to the DRIL and emails to ERO CP's public email box. The majority of calls to the DRIL come from ICE detainees and involve immigration case information inquires, medical or mental health complaints, and parental or family-separation issues. After receiving an inquiry, DRIL operators may also coordinate any necessary follow-up with ERO CP's liaisons in ERO field offices and other select ICE program offices.

To manage information received during a DRIL call or in an email, CP uses the SharePoint-based Custody Assistance and Inquiry Resolution System (CAIRS). DRIL operators enter information received during the inquiry into forms built within CAIRS. After a supervisor reviews this information, operators can generate emails within the system that are sent to the appropriate ERO field office or other ICE office for real-time and priority-based actions. Once the office reviews and resolves the CAIRS referral, the designated CP liaison adds the referral disposition and closes the CAIRS entry.

CAIRS also provides a robust archival process, enabling DRIL operators to review historical notes related to previous inquiries associated with a particular Alien Registration Number (A-Number). DRIL operators can search for archived entries using an A-Number or a CAIRS-generated tracking number.

Finally, CAIRS is used to track calls pertaining to the ICE Victims of Immigration Crime Engagement (VOICE) Office. VOICE, established in 2017, supports victims of crimes committed by removable aliens through access to information and resources.[5] As part of that support, DRIL operators perform the following functions:

- Provide general information about the VOICE Office;
- Provide information about the Department of Homeland Security Victim Information Notification Exchange (DHS-VINE);[6]
- Disclose alien custody status updates to individuals eligible to receive such information; and
- Refer callers to victim service organizations.

When DRIL operators receive calls from victims or their agents (including family members,

[5] The VOICE Office was established pursuant to Executive Order 13768, *Enhancing Public Safety in the Interior of the United States*, available at https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.

[6] *See* DHS/ICE/PIA-047 DHS Victim Information and Notification Exchange, *available at*: www.dhs.gov/privacy.

friends, legal representatives, or others acting at the victim's request), they record the caller's information in CAIRS. The information collected may include the caller's name, organization name (if applicable), address, phone number, and email address. The caller may also provide information pertaining to aliens, such as the alien's name, A-Number, date of birth, country of birth, and date of entry. Finally, any information the caller provides that would assist in identifying the alien or in resolving the inquiry may be recorded. All of this information is entered in CAIRS.

Depending on the inquiry, ICE may have to follow up with the caller at a later time via phone or email. In that case, DRIL operators will send an email to ERO Community Relations Officers (CROs) for follow-up action. CROs will also have access to the CAIRS database to update information from calls, and to indicate any actions taken to resolve the inquiry.

System Access:

Access to CAIRS is granted to DRIL operators, the CP chain of command, and CP liaisons in ERO field offices and other select ICE program offices.

Individuals Impacted:

Individuals who submit inquiries to the DRIL; individuals victims of crimes committed by removable aliens and agents of the victim (e.g., family members, friends, legal representatives); individuals who are the subjects of inquiries, including individuals arrested, encountered, or detained by ICE or held in ICE custody pending removal or removal proceedings under the Immigration and Nationality Act (INA).

Sources of Information:

Information within CAIRS may be collected directly from the individuals submitting inquiries through the DRIL. Additional information about a specific individual who has been arrested, encountered, or detained by ICE or held in ICE custody pending removal or removal proceedings under the INA may be inputted into CAIRS from ICE's EARM. Finally, information may also be collected by CROs who use CAIRS to update information on inquiries pertaining to the VOICE office.

Data Elements:

CAIRS will automatically assign all incoming calls, voicemails, and emails a unique tracking number, consisting of the date and a running call-count number. In addition, CAIRS will collect information on:

- The category of the inquirer (e.g., detainee, attorney of detainee, family member of detainee, advocate, member of the general public) and identifying information, including full name, organization name (if any), email, and phone number;
- Identifying information pertaining to the detainee, if the detainee is not the inquirer, specifically: full name, date of birth, country of birth, A-Number (if any), full mailing address, whether the person is in a detention facility and where, email address, and phone number; and

- The nature and description of the inquiry (e.g., general outreach inquiry, detention concern, enforcement issue, facilitation of return, national policy concern, VOICE,[7] or general information request).

SORN Coverage:

DHS/ALL-016 Department of Homeland Security Correspondence Records[8]

Records Retention Period:

ICE has submitted a proposed records retention schedule to the National Archives and Records Administration (NARA) for approval to retain CAIRS records for seven years after the record was entered into the system.

[7] There is a dropdown menu within CAIRS where DRIL operators can select the type of call received. VOICE is one of those options.
[8] DHS/ALL-016 Department of Homeland Security Correspondence Records, 73 FR 66657 (Nov. 10, 2008).

Appendix C

Program/System:

ICE Enforcement and Removal Operations (ERO) Segregation Review Management System (SRMS)

Purpose and Use:

ERO uses the Segregation Review Management System (SRMS), to track, review, and oversee ICE detainee segregation cases. Segregation – whether administrative or disciplinary – is the process of removing a detainee from the general detainee population into a separate, individual unit.

ERO field office personnel input information pertaining to a detainee's segregation case directly into the SharePoint based-SRMS. This input, and any subsequent inputs pertaining to the same detainee, comprise the detainee's segregation case within the system. The field office can update the case at any time to reflect changes in the segregation status, including removal from segregation. Within SRMS, ERO can sort and manage cases by priority, facilitate subject matter expert (SME) review of cases, and notify field office leadership and detention facility staff of actions affecting the segregation status of a detainee.

SRMS also provides an archival process, enabling ERO to determine and report on trends related to segregation practices and inquire into specific segregation cases. ERO users search for archived entries by A-Number or SRMS-generated case tracking number.

System Access:

Access to SRMS is granted to ERO field office leadership and their staff assigned to segregation management, the Segregation Review Coordinator and administrative support staff, SMEs subject matter experts from select ICE program offices, and select ICE Headquarters staff involved in segregation review. SRMS displays data in user-specific views, so the user has most immediate access to case information most relevant to him or her.

Individuals Impacted:

Individuals in ICE detention who are placed into administrative or disciplinary segregation.

Sources of Information:

SRMS receives information from ERO detention facility staff and from ICE's ENFORCE Alien Removal Module (EARM). Case notes from field office personnel or medical personnel may also be included in SRMS.

Data Elements:

SRMS automatically assigns a unique case reference number for all segregation cases submitted by field offices. In addition, information collected and stored within SRMS includes:

- Identifying information pertaining to the detainee, including full name, A-Number, language and language proficiency, and detention facility housed in at the time.

- Information determined to be relevant to the segregation decision, including type of segregation (i.e., administrative or disciplinary); reasons for the placement in segregation (i.e., conduct/behavior, heightened concern for a detainee's risk of victimization, or other special vulnerabilities); existing medical and mental conditions; and criminal, disciplinary, and immigration history.
- Information pertaining to ICE oversight and review of individual segregation cases, including data on dates of initial segregation and release from segregation, interviews with facility or medical staff, case review dates, analyses by SMEs, and decisions for field action (e.g., limit isolation, transfer to different facility, return to general population).

SORN Coverage:

DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE)[9]

Records Retention Period:

ICE intends to request NARA approval to retain SRMS records for seven years after the record was entered into the system.

[9] DHS/ICE-011 Immigration and Enforcement Operational Records System (ENFORCE), 80 FR 24269 (Apr. 30, 2015).

Appendix D

Program/System:

ICE Office of the Director AWARDS System

Purpose and Use:

The ICE Office of the Director uses the AWARDS system to accept and manage nominations for the annual ICE Director's Awards Ceremony in Washington, D.C. The nomination process, previously captured on electronic and paper-based spreadsheets, is automated and streamlined through AWARDS.

Select staff from the Director's Office, the ICE Office of Professional Responsibility, and the ICE Human Capital Office review nominations submitted through the AWARDS system. Some nominees are ultimately selected to receive an award from the ICE Director. ICE also conducts the review and selection process using the AWARDS system.

System Access:

AWARDS coordinators in each ICE program office and select Director's Office staff can access AWARDS.

Individuals Impacted:

Individuals who are nominated for an ICE Director's Award as well as officials, guests, and attendees of the annual Awards Ceremony.

Sources of Information:

Information within AWARDS may be collected directly from the individuals who are nominated for ICE Director's Awards as well as from individuals who submit nominations on behalf of others.

Data Elements:

The information maintained in the AWARDS system includes:

- Full names of nominees, officials, guests, and attendees of the Awards Ceremony.
- Contact information, including email addresses, phone numbers, and work addresses.
- Job-related information, including job title, program office name, and ICE network login username.

SORN Coverage:

DHS/ALL-002 Department of Homeland Security Mailing and Other Lists System;[10] DHS/ALL-004 General Information Technology Access Account Records System[11]

Records Retention Period:

[10] DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659 (Nov. 25, 2008).
[11] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (Nov. 27, 2012).

Nomination records in AWARDS are retained for two years pursuant to NARA General Records Schedule 1, Item 12. Lists of nominees, officials, guests, and attendees at awards ceremonies will be destroyed when superseded by the following year's list.

U.S. Immigration and Customs Enforcement

For Official Use Only

FALCON Training & Support Multiple Award Blanket Purchase Agreement (MA BPA) Statement of Objectives

April 14, 2016

Homeland Security Investigations (HSI)

Joint Task Force-Investigations

Homeland Security

1.0 PROJECT TITLE

Statement of Objectives (SOO) for FALCON Training & Support Multiple Award Blanket Purchase Agreement (MA BPA)

2.0 BACKGROUND

United States Immigration and Customs Enforcement (ICE) is the largest investigative branch of the Department of Homeland Security (DHS). As part of ICE, Homeland Security Investigations (HSI) is a critical asset in accomplishing the ICE mission and is responsible for investigating a wide range of domestic and international activities arising from the illegal movement of people and goods into, within and out of the United States. For this acquisition, the Contractor(s) shall be responsible for providing training and employee support services for Special Agents, Intelligence Analysts, and Task Force Officers assigned to HSI supervision, regarding their utilization one of HSI Information Sharing and Infrastructure Management's (ISIM) technology platforms and software assets, FALCON.

FALCON provides HSI's agents, analysts, and Task Force Officers with a key investigative resource: a wholly integrated, consolidated platform performing federated search, analytics, geospatial referencing, reporting and situational awareness capabilities across a broadly diverse universe of structured and unstructured law enforcement data residing in numerous, disparate source environments.

The FALCON system is comprised of several sub-components. The largest of these is FALCON-SA (Search and Analysis)/Workspace, utilized by the entire community of FALCON users. Users of FALCON-SA/Workspace have access to the following data sets:

- (b)(7)(E)

3.0 SCOPE

FALCON is based upon commercial software sold by Palantir Technologies, Inc., called Palantir Gotham, configured for ICE. FALCON has been utilized by HSI since 2012.

Vendor(s), per instructions provided in each BPA call/Task Order, will provide one or more full-time training and desk-side support personnel to assist HSI Special Agents, Criminal Investigators, Intelligence Analysts, Task Force Officers assigned to HSI supervisors, and support personnel in achieving a high level of proficiency in utilizing FALCON Workspace and/or FALCON Mobile to fulfill the missions and objectives of HSI.

4.0 TASKS

Vendor will provide a mix of structured (classroom-type) and desk-side assistance training to Special Agents, Criminal Investigators, Intelligence Analysts, and Task Force Officers assigned to HSI supervisors, regarding FALCON Workspace and/or FALCON Mobile.

The Vendor employee will be responsible for the following tasks:

- Providing a training plan to the FALCON PMO no later than fifteen working days following the beginning of a task order's period of performance, following consultations with the government employees to be trained/supported, and updating that training plan whenever the operational goals of the HSI unit(s) to which he/she is assigned substantially change;
- Providing initial, introductory training in FALCON Workspace and/or FALCON Mobile to new employees;
- Providing advanced training in the functions and features of FALCON Workspace and/or FALCON Mobile to veteran employees;
- Ensuring that HSI employees and/or Task Force Officers, by the end of the period of performance, achieve independent proficiency in the features and functions of FALCON Workspace and/or FALCON Mobile;
- Acquiring sufficient knowledge of HSI missions, objectives, policies, and procedures to work iteratively with HSI personnel to create innovative and effective workflows utilizing FALCON Workspace and/or FALCON Mobile to achieve HSI goals;
- Gather feedback from government employees on their level of satisfaction with training and support activities, and report results of this feedback to the FALCON PMO on a quarterly basis;
- Coordinate with Palantir Technologies Forward Deployed Engineers and other Palantir system support staff to ensure that HSI employees are familiarized with and trained in the operations of new versions of FALCON Workspace and/or FALCON Mobile which are deployed by Palantir Technologies;
- Coordinate all training and operational support activities with the Field Support

Representatives (FSR) staff employed by Palantir Technologies, Inc., or any successor vendor which serves as lead contractor on the FALCON Operations and Support and System Enhancement contract, in order to ensure uniformity of FALCON training outcomes across HSI, to promote sharing of FALCON training best practices across HSI, and to maximize unity of effort and mutual support among HSI units and offices which utilize FALCON;

- Pre-clear any new training initiatives or meetings with HSI personnel at or above the level of Group Supervisor with the FALCON PMO (Program Management Office); and
- Report weekly on training and employee support activities to the FALCON PMO.

5.0 VENDOR'S AND VENDOR EMPLOYEE'S QUALIFICATIONS

Vendor's status as a Palantir Technologies "Preferred Vendor" is highly preferred but not required. Possession of this qualification will be one of several selection factors in the government's choice of vendors for a BPA call/Task Order. "Preferred Vendor" status provides a vendor access to Palantir's internal resources, including a Palantir vendor email account, internal Palantir distribution lists, internal Palantir project management boards, and internal engineering resources. These are only made available to Authorized Palantir Service Providers. Non-preferred vendors acting on behalf of the Government may only access the same support resources provided the Government under Palantir's standard license agreement (Support Portal access, DevZone access, Product Documentation), but non-preferred vendors do not have access to internal Palantir resources.

Vendor employee(s) shall have a minimum of two years' prior experience providing training and employee support services for the Palantir Gotham software platform, at least one year of which shall have been in the context of a federal law enforcement organization. Prior experience providing training and employee support services for the FALCON implementation of the Palantir Gotham software platform at ICE is highly preferred but not required. Possession of this qualification will be one of several selection factors in the government's choice of vendors for a BPA call/Task Order. Vendor employee(s) shall have a Secret clearance, due to required access to ICE Facilities, in order to perform on this BPA.

6.0 PLACE OF PERFORMANCE

Place of performance will be described as part of each task order and will vary between task orders. Frequent or occasional travel within the ICE Operational Area of Responsibility identified in the task order may be required to support field operations. Work hours shall be Mondays through Fridays, for eight-hour work periods between 8:00 AM and 5:00 PM.

7.0 PERIOD OF PERFORMANCE

The period of performance of the FALCON Training & Support Multiple Award Blanket Purchase Agreement will consist of a base period of twelve (12) months plus up to four (4) twelve (12) month option periods. The actual dates for periods of

performance shall be indicated at the time of the Call Order task award.

8.0 BLANKET PURCHASE AGREEMENT (BPA) TERMS AND CONDITIONS

This section presents the general requirements applicable to the Blanket Purchase Agreement (BPA) Contractor.

8.1 Description of Agreement

The vendor(s), per instructions provided in each BPA call/Task Order, will provide one or more full-time training and desk-side support personnel to assist HSI Special Agents, Criminal Investigators, Intelligence Analysts, Task Force Officers assigned to HSI supervisors, and support personnel in achieving a high level of proficiency in utilizing FALCON Workspace and/or FALCON Mobile to fulfill the missions and objectives of HSI. Vendors will ensure that the tasks described in Section 4.0 are completed in a timely fashion.

It is the responsibility of the Quoter to notify the Contracting Officer of GSA Schedule price changes affecting the services listed in this BPA prior to award of any order. Discounts shall be applied against the GSA Schedule price for the services. If discounts are conditional on a given dollar volume or other condition, this must be stated clearly. Quoter may offer further price reductions in accordance with their commercial practice. For orders issued under this BPA, the price paid shall be the GSA Schedule price in effect at the time the order is issued less applicable discounts under this BPA. The relationship between the current price in the GSA Schedule and the price offered in the contractor's quote shall not be altered to the government's detriment; i.e., the discount shall not be lessened throughout the term of the BPA, but may be increased. All orders placed against this BPA are subject to the terms and conditions of the GSA Schedule contract.

8.2 Federal Supply Schedule

All orders placed against this BPA are subject to the terms and conditions of the Quoter's Federal Supply Schedule (FSS) Contract.

8.3 Delivery

Delivery destination (place of performance) and schedule will be specified in each task order.

8.4 BPA Volume

The government estimates, but does not guarantee, that the volume of purchases through this agreement will be $5 million over a period of 5 years for this BPA. Quoters should be cognizant of the fact that task orders over the 5 year period will likely be split amongst several vendors.

8.5 Extent of Obligation

This BPA does not obligate any funds. The government is obligated only to the extent of authorized purchases made under an awarded BPA.

8.6 Individuals Authorized to Purchase Under the BPA

ICE Contracting Officers are authorized to place orders against this BPA.

8.7 Invoicing

Invoices shall be submitted at least monthly and in accordance with the instructions provided on each individual delivery/task order.

8.8 Period of Performance

The period of performance for this BPA is five (5) years from the date of the award. The period of performance for the delivery/task orders will be specified in each individual order.

8.9 Type of Contract

This is a Multiple Award Blanket Purchase Agreement (MA BPA) wherein delivery/task orders issued against it will be firm-fixed priced.

9.0 GOVERNMENT FURNISHED EQUIPMENT (GFE) AND GOVERNMENT FURNISHED INFORMATION (GFI)

9.1 GFE

The Government will provide workspace for Vendor Personnel. The Government will provide the necessary GFE, such as laptops, peripherals, etc. All work performed shall be performed on GFE. GFE will be provided to vendor personnel upon acceptable clearance/approvals. The Vendor shall manage, maintain, and control all GFE in accordance with FAR 52.245-1.

9.2 GFI

The Government will provide all current FALCON tutorials and training materials as GFI.

10.0 NON-PERSONAL SERVICES

The Government shall neither supervise Vendor employees, nor control the method by which the Vendor performs the individual tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual Vendor employees. It shall be the responsibility of the Vendor to manage its employees and to guard against any actions that are of the nature of personal services, or give the perception of personal services. If the Vendor

believes that any actions constitute, or are perceived to constitute personal services, it shall be the Vendor's responsibility to notify the Contracting Officer (CO) or COR immediately.

11.0 BUSINESS RELATIONS

The Vendor shall successfully integrate and coordinate all activities needed to execute the tasks. The Vendor shall manage the timeliness, completeness, and quality of identified issues. The Vendor shall provide corrective action plans, quote submittals, timely identification of issues, and effective management of subcontractors. The Vendor shall seek to ensure customer satisfaction and professional and ethical behavior of all Vendor personnel.

12.0 Section 508 Compliance

The DHS Office of Accessible Systems and Technology has determined that for the purposes of compliance with Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998, a National Security Exception applies. ICE received a National Security Exemption (**ICE-20120201-001**) on 2/01/2012.

13.0 SECURITY

13.1 General Clause

To ensure the security of the DHS/ICE information in their charge, ICE Contractors and Sub-contractors shall adhere to the same computer security rules and regulations as Federal Government employees unless an exception to policy is agreed to by the prime Contractors, ICE Information Systems Security Manager (ISSM) and Contracting Officer and detailed in the contract. Non-DHS Federal employees or Contractors who fail to comply with DHS/ICE security policies are subject to having their access to DHS/ICE IT systems and facilities terminated, whether or not the failure results in criminal prosecution. The DHS Rules of Behavior document applies to DHS/ICE support Contractors and Sub-contractors.

13.2 Security Policy References Clause

The following primary DHS/ICE IT Security documents are applicable to Contractor/Sub-contractor operations supporting Sensitive But Unclassified (SBU) based contracts. Additionally, ICE and its Contractors shall conform to other DHS Management Directives (MD) (Note: these additional MD documents appear on DHS-Online in the Management Directives Section. Volume 11000 "Security and Volume 4000 "IT Systems" are of particular importance in the support of computer security practices):

- DHS 4300A, Sensitive Systems Policy Directive
- DHS 4300A, IT Security Sensitive Systems Handbook
- ICE Directive, IT Security Policy for SBU Systems

13.3 Contractor Information Systems Security Officer (ISSO) Point of Contact Clause

The Contractor shall appoint and submit a name to ICE ISSM for approval, via the ICE COR, of a qualified individual to act as ISSO to interact with ICE personnel on any IT security matters.

13.4 Protection of Sensitive Information

The Contractor shall protect all DHS/ICE "sensitive information" to which the Contractor is granted physical or electronic access by adhering to the specific IT security requirements of this BPA and the DHS/ICE security policies specified in the Reference Section above. The Contractor shall ensure that their systems containing DHS/ICE information and data be protected from unauthorized access, modification and denial of service. Further, the data shall be protected in order to ensure the privacy of individual's personal information.

13.5 Information Technology Security Program

If performance of the BPA requires that DHS/ICE data be stored or processed on Contractor-owned information systems, the Contractor shall establish and maintain an IT Security Program. This program shall be consistent with the referenced DHS/ICE IT security policy documents and at a minimum contain and address the following elements:

- Handling of DHS/ICE sensitive information and IT resources to include media protection, access control, auditing, network security, and rules of behavior
- Certification and Accreditation (C&A) and FISMA compliance of Systems containing, processing or transmitting of DHS/ICE data
- Training and Awareness for Contractor personnel
- Security Incident Reporting
- Contingency Planning
- Security Reviews
- BPA Closeout Actions

13.6 Handling of Sensitive Information and IT Resources

The Contractor shall protect DHS/ICE sensitive information and all government provided and Contractor-owned IT systems used to store or process DHS/ICE sensitive information. The Contractor shall adhere to the following requirements for handling sensitive information:

- **Media Protection**. The Contractor shall ensure that all hardcopy and electronic media (including backup and removable media) that contain DHS sensitive information are appropriately marked and secured when not in use. Any sensitive information stored on media to be surplused, transferred to another individual, or returned to the manufacturer shall be purged from the media before disposal. Disposal shall be performed using DHS/ICE approved sanitization methods. The Contractor shall establish and implement procedures to ensure sensitive information cannot be accessed or stolen. These procedures shall address the handling and protection of paper and electronic outputs from systems (computers, printers, faxes, copiers) and the transportation and mailing of sensitive media.)
- **Access Control.** The Contractor shall control user access to DHS/ICE sensitive information based on positive user identification, authentication, and authorization

(Roles and Rules based) mechanisms. Access control measures employed shall provide protection from unauthorized alternation, loss, unavailability, or disclosure of information. The Contractor shall ensure its personnel are granted the most restrictive set of access privileges needed for performance of authorized tasks. The Contractor shall divide and separate duties and responsibilities of critical IT functions to different individuals so that no individual has all necessary authority or systems access privileges needed to disrupt or corrupt a critical process.

- **Auditing.** The Contractor shall ensure that it's Contractor-owned IT systems used to store or process DHS/ICE sensitive information maintain an audit trail sufficient to reconstruct security relevant events. Audit trails shall include the identity of each person and device accessing or attempting to access the system, the time and date of the access and the log-off time, activities that might modify, bypass, or negate security safeguards, and security-relevant actions associated with processing. The Contractor shall periodically review audit logs and ensure that audit trails are protected from modification, authorized access, or destruction and are retained and regularly backed up.
- **Network Security.** The Contractor shall monitor its networks for security events and employ intrusion detection systems capable of detecting inappropriate, incorrect, or malicious activity. Any interconnections between Contractor-owned IT systems that process or store DHS/ICE sensitive information and IT systems not controlled by DHS/ICE shall be established through controlled interfaces and documented through formal Interconnection Security Agreements (ISA). The Contractor shall employ boundary protection devices to enforce access control between networks, including Internet and extranet access. The Contractor shall ensure its e-mail systems are secure, properly configured, and that network protection mechanisms implemented in accordance with DHS/ICE requirements. The Contractor shall conduct periodic vulnerability assessments and tests on its IT systems containing DHS/ICE sensitive information to identify security vulnerabilities. The results, of this information, will be provided to the ICE OCIO for review and to coordinate remediation plans and actions.
- DHS employees and Contractors shall not transmit sensitive DHS/ICE information to any personal e-mail account that is not authorized to receive it.
- **Rules of Behavior.** The Contractor shall develop and enforce Rules of Behavior for Contractor-owned IT systems that process or store DHS/ICE sensitive information. These Rules of Behavior shall meet or exceed the DHS/ICE rules of behavior.
- The Contractor shall adhere to the policy and guidance contained in the DHS/ICE reference documents.

13.7 Training and Awareness

The Contractor shall ensure that all Contractor personnel (including Sub-contractor personnel) who are involved in the management, use, or operation of any IT systems that handle DHS/ICE sensitive information, receive annual training in security awareness, accepted security practices, and system rules of behavior. If the Contractor does not use the ICE-provided annual awareness training, then they shall submit to the ICE ISSM their awareness training for approval. Should Contractor Training be approved for use, the Contractor shall

provide proof of training completed to the ICE ISSM when requested.

The Contractor shall ensure that all Contractor personnel, including Sub-contractor personnel, with IT security responsibilities, receive specialized DHS/ICE annual training tailored to their specific security responsibilities. If the Contractor does not use the ICE-provided special training, then they shall submit to the ICE ISSM their awareness training for approval. Should Contractor training be approved for use, the Contractor shall provide proof of training completed to the ICE ISSM when requested.

Any Contractor personnel who are appointed as ISSO, Assistant ISSOs, or other position with IT security responsibilities, i.e., System/LAN Database administrators, system analyst and programmers may be required to attend and participate in the annual DHS Security Conference.

13.8 Certification and Accreditation (C&A) and FISMA compliance

The Contractor shall ensure that any Contractor-owned systems that process, store, transmit or access DHS/ICE information shall comply with the DHS/ICE C&A and FISMA requirements.

Any work on developing, maintaining or modifying DHS/ICE systems shall be done to ensure that DHS/ICE systems are in compliance with the C&A and FISMA requirements. The Contractor shall ensure that the necessary C&A and FISMA compliance requirements are being effectively met prior to the System or application's release into Production (this also includes pilots). The Contractor shall use the DHS provided tools for C&A and FISMA compliance and reporting requirements.

13.9 Security Incident Reporting

The Contractor shall establish and maintain a computer incident response capability that reports all incidents to the ICE Computer Security Incident Response Center (CSIRC) in accordance with the guidance and procedures contained in the referenced documents.

13.10 Contingency Planning

If performance of the BPA requires that DHS/ICE data be stored or processed on Contractor-owned information systems, the Contractor shall develop and maintain contingency plans to be implemented in the event normal operations are disrupted. All Contractor personnel involved with contingency planning efforts shall be identified and trained in the procedures and logistics needed to implement these plans. The Contractor shall conduct periodic tests to evaluate the effectiveness of these contingency plans. The plans shall at a minimum address emergency response, backup operations, and post-disaster recovery.

13.11 Security Review and Reporting

The Contractor shall include security as an integral element in the management of this contract. The Contractor shall conduct reviews and report the status of the implementation

and enforcement of the security requirements contained in this BPA and identified references.

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this BPA are being implemented and enforced. The Contractor shall afford DHS/ICE, including the Office of Inspector General, ICE ISSM, and other government oversight organizations, access to the Contractor's and Sub-contractors' facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. Access shall be provided to the extent necessary for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS/ICE data or the function of computer systems operated on behalf of DHS/ICE, and to preserve evidence of computer crime.

13.12 Use of Government Equipment

Contractors are not authorized to use Government office equipment (IT systems/computers) for personal use under any circumstances, unless limited personal use is specifically permitted by the BPA. When so authorized, Contractors shall be governed by the limited personal use policies in the referenced documents.

13.13 Contract Closeout

At the expiration of each task order, assuming no extension through option periods, the Contractor shall return all sensitive DHS/ICE information and IT resources provided during the life of this BPA. The Contractor shall certify that all DHS/ICE information has been purged from any Contractor-owned system used to store or process DHS/ICE information. Electronic media shall be sanitized (overwritten or degaussed) in accordance with the sanitation guidance and procedures contained in reference documents and with DHS/NIST/National Security Agency (NSA) approved hardware and software. Note that these procedures may be wavied by the COR, contingent upon approval of a follow-on contract with the current Contractor.

13.14 Personnel Security

DHS/ICE does not permit the use of non U.S. Citizens in the performance of this BPA or to access DHS/ICE systems or information.

All Contractor personnel (including Sub-contractor personnel) shall have favorably adjudicated background investigations commensurate with the sensitivity level of the position held before being granted access to DHS/ICE sensitive information.

The Contractor shall ensure all Contractor personnel are properly submitted for appropriate clearances.

The Contractor shall ensure appropriate controls have been implemented to prevent Contractor personnel from obtaining access to DHS/ICE sensitive information before a favorably adjudicated background investigation has been completed and appropriate clearances have

been issued. At the option of the Government, interim access may be granted pending completion of a pre-employment check. Final access may be granted only upon favorable completion of an appropriate background investigation based on the risk level assigned to this BPA by the Contracting Officer.

The Contractor shall ensure its personnel have a validated need to access DHS/ICE sensitive information and are granted the most restrictive set of access privileges needed for performance of authorized tasks.

The Contractor shall ensure that its personnel comply with applicable Rules of Behavior for all DHS/ICE and Contractor-owned IT systems to which its personnel have been granted access privileges.

The Contractor shall implement procedures to ensure that system access privileges are revoked for Contractor personnel whose employment is terminated or who are reassigned to other duties and no longer require access to DHS/ICE sensitive information.

The Contractor shall conduct exit interviews to ensure that Contractor personnel who no longer require access to DHS/ICE sensitive information understand their obligation not to discuss or disclose DHS/ICE sensitive information to which they were granted access under this contract.

13.15 Physical Security

The Contractor shall ensure that access to Contractor buildings, rooms, work areas and spaces, and structures that house DHS/ICE sensitive information or IT systems through which DHS/ICE sensitive information can be accessed, is limited to authorized personnel. The Contractor shall ensure that controls are implemented to deter, detect, monitor, restrict, and regulate access to controlled areas at all times. Controls shall be sufficient to safeguard IT assets and DHS/ICE sensitive information against loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters. Physical security controls shall be implemented in accordance with the policy and guidance contained in the referenced documents.

14.0 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

14.1 GENERAL

The United States Immigration and Customs Enforcement (ICE) has determined that performance of the task as described in HSCETC-15-F-00018 requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) may access classified National Security Information (herein known as classified information). Classified information is Government information which requires protection in accordance with Executive Order 13526, Classified National Security Information, and supplementing directives.

The Contractor will abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the contract, and the *National Industrial Security Program Operating Manual (NISPOM)* for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service. If the Contractor has access to classified information at an ICE or other Government Facility, it will abide by the requirements set by the agency.

In conjunction with acquisition HSCETC-15-F-00018 the contractor shall ensure all investigative, reinvestigate, and adjudicative requirements are met in accordance with *National Industrial Security Program Operating Manual* (DOD 5220.22-M) Chapter 2-1.

No person shall be allowed to begin work on this BPA and/or access sensitive information related to the BPA without ICE receiving clearance verification from the FSO. ICE further retains the right to deem an applicant as ineligible due to an insufficient background investigation or when derogatory information is received and evaluated under a Continuous Evaluation Program. Any action taken by ICE does not relieve the Contractor from required reporting of derogatory information as outlined under the NISPOM.

The FSO will submit a Visitors Authorization Letter (VAL) through the Contracting Officer's Representative (COR) to (b)(7)(E) for processing personnel onto the contract. The clearance verification process will be provided to the COR during Post-Award. Note: *Interim TS is not accepted by DHS for access to Top Secret information. The contract employee will only have access to SECRET level information until DoD CAF has granted a full TS.*

For processing any personnel on a classified contract who will not require access to classified information see BACKGROUND INVESTIGATIONS (Process for personnel do not require access to classified information).

14.2 PRELIMINARY DETERMINATION

ICE may, as it deems appropriate, authorize and make a favorable preliminary fitness to support decision based on preliminary security checks. The expedited pre-employment determination will allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable pre-employment determination shall not be considered as assurance that a favorable full employment determination will follow as a result thereof. The granting of a favorable pre-employment fitness determination or a full employment fitness determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary fitness determination or final fitness determination by the Office of Professional Responsibility, Personnel Security Unit (OPR-PSU). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable pre-employment fitness determination or final fitness determination by the OPR-PSU.

14.3 BACKGROUND INVESTIGATIONS (Process for personnel do not require access to classified information):

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through the OPR-PSU. Prospective Contractor employees without adequate security clearances issued by DoD CAF shall submit the following completed forms to the OPR-PSU through the Contracting Offices Representative (COR), no less than 35 days before the starting date of the task order period of performance or 35 days prior to the expected entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

1. Standard Form 85P "Questionnaire for Public Trust Positions" Form will be submitted via e-QIP (electronic Questionnaires for Investigation Processing) (Original and One Copy)

2. Three signed eQip Signature forms: Signature Page, Release of Information and Release of Medical Information (Originals and One Copy)

3. Two FD Form 258, "Fingerprint Card"

4. Foreign National Relatives or Associates Statement (Original and One Copy)

5. DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" (Original and One Copy)

6. Optional Form 306 Declaration for Federal Employment (applies to contractors as well) (Original and One Copy)

If the contract authorizes positions which do not require access to classified information: In those instances where a Prospective Contractor employee will not require access to classified information, areas or classified systems the Vendor will add to and the COR will insure the following statement is added to the eQip Worksheet prior to submitting it to OPR PSU: "Employee will not require NSI Access to Classified Information or Classified Systems at any level".

Required forms will be provided by ICE at the time of award of the contract. Only complete packages will be accepted by the OPR-PSU. Specific instructions on submission of packages will be provided upon award of the contract.

Be advised that unless an applicant requiring access to sensitive information has resided in the US for three of the past five years, the Government may not be able to complete a satisfactory background investigation. In such cases, ICE retains the right to deem an applicant as ineligible due to insufficient background information.

14.4 EMPLOYMENT ELIGIBILITY

The use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this BPA for any position that involves access to DHS /ICE IT systems and the information contained therein, to include, the development and / or maintenance of DHS/ICE IT systems; or access to information contained in and / or derived from any DHS/ICE IT system.

The contractor will agree that each employee working on this BPA will successfully pass the DHS Employment Eligibility Verification (E-Verify) program operated by USCIS to establish work authorization.

The E-Verify system, formerly known as the Basic Pilot/Employment Eligibility verification Program, is an Internet-based system operated by DHS USCIS, in partnership with the Social Security Administration (SSA) that allows participating employers to electronically verify the employment eligibility of their newly hired employees. E-Verify represent the best means currently available for employers to verify the work authorization of their employees.

The Contractor must agree that each employee working on this BPA will have a Social Security Card issued and approved by the Social Security Administration. The Contractor shall be responsible to the Government for acts and omissions of his own employees and for any Subcontractor(s) and their employees.

Subject to existing law, regulations and/ or other provisions of this contract, illegal or undocumented aliens will not be employed by the Contractor, or with this contract. The Contractor will ensure that this provision is expressly incorporated into any and all Subcontracts or subordinate agreements issued in support of this contract.

14.5 FACILITY ACCESS

ICE shall have and exercise full control over granting, denying, withholding or terminating unescorted government facility and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation.

Contract employees assigned to the BPA not needing access to sensitive ICE information, recurring access to ICE facilities or access to DHS/ICE IT systems, to include email, will not be subject to security contractor fitness screening.

14.6 CONTINUED ELIGIBILITY

If a prospective employee is found to be ineligible for access to Government facilities or information, the COR will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

The OPR-PSU may require drug screening for probable cause at any time and/ or when the contractor independently identifies, circumstances where probable cause exists.

The OPR-PSU will conduct reinvestigations every 5 years, or when derogatory information is received, to evaluate continued eligibility.

ICE reserves the right and prerogative to deny and/ or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct, 5 CFR 2635 and 5 CFR 3801, or whom ICE determines to present a risk of compromising sensitive Government information to which he or she would have access under this contract.

14.7 REQUIRED REPORTS

The contractor/COR will notify OPR-PSU of all terminations / resignations, etc., within five days of occurrence. The Contractor will return any expired ICE issued identification cards/ credentials and building passes, or those of terminated employees to the COR. If an identification card or building pass is not available to be returned, a report must be submitted to the COR, referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COR will return the identification cards and building passes to the responsible ID Unit.

The Contractor will report any adverse information coming to their attention concerning contract employees under the BPA to the OPR-PSU through the COR as soon as possible. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the employees' name and social security number, along with the adverse information being reported.

The Contractor will provide, through the COR a Quarterly Report containing the names of personnel who are active, pending hire, have departed within the quarter or have had a legal name change (Submitted with documentation) . The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for contractor payroll/voucher processing to ensure accuracy.

The contractor is required to report certain events that have an impact on the status of the facility clearance (FCL) and/ or the status of the contract employee's personnel security clearance as outlined by *National Industrial Security Program Operating Manual* (DOD 5220.22-M) Chapter1-3, Reporting Requirements. Contractors shall establish internal procedures as are necessary to ensure that cleared personnel are aware of their responsibilities for reporting pertinent information to the FSO and other federal authorities as required.

Submit reports to the email address psu-industrial-security@ice.dhs.gov

14.8 SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the OPR-PSU through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

Contractors shall provide all employees supporting any task order of this BPA proper initial and annual refresher security training and briefings commensurate with their clearance level, to include security awareness, defensive security briefings.(*National Industrial Security Program Operating Manual* (DOD 5220.22-M) Chapter 3-1. The contractor shall forward a roster of the completed training to the COR on a quarterly bases.

The following computer security requirements apply to both Department of Homeland Security (DHS) U.S. Immigration and Customs Enforcement (ICE) operations and to the former Immigration and Naturalization Service operations (FINS). These entities are hereafter referred to as the Department.

14.9 INFORMATION TECHNOLOGY

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in *DHS MD 140-01 - Information Technology Systems Security and DHS MD 4300 Sensitive Systems Policy.* Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

14.10 INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT

In accordance with Chief Information Office requirements and provisions, all contractor employees accessing Department IT systems or processing DHS sensitive data via an IT system will require an ICE issued/provisioned Personal Identity Verification (PIV) card. Additionally, Information Assurance Awareness Training (IAAT) will be required upon initial access and annually thereafter. IAAT training will be provided by the appropriate component agency of DHS.

Contractors, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. Department contractors, with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access Department information systems will be continually evaluated while performing these duties. Supervisors should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).

14.11 NON-DISCLOSURE AGREEMENT

Contractors are required to sign DHS 11000-6, Attachment 9 - Non-Disclosure Agreement, due to access to a sensitive ICE system. Non-Disclosure Agreements shall be provided to the COR and CO prior to the commencement of work on this task order.

TASK ORDER #1

1.0 SCOPE

Vendor will provide one (1) full-time training and desk-side support personnel to assist HSI Special Agents, Criminal Investigators, Intelligence Analysts, Task Force Officers assigned to HSI supervisors, and support personnel in achieving a high level of proficiency in utilizing FALCON Workspace and/or FALCON Mobile to fulfill the missions and objectives of HSI.

2.0 TASKS

Vendor will provide a mix of structured (classroom-type) and desk-side assistance training to Special Agents, Criminal Investigators, Intelligence Analysts, and Task Force Officers assigned to HSI supervisors, regarding FALCON Workspace and/or FALCON Mobile.

The Vendor employee will be responsible for the following tasks:

- Providing a training plan to the FALCON PMO no later than fifteen working days following the beginning of a task order's period of performance, following consultations with the government employees to be trained/supported, and updating that training plan whenever the operational goals of the HSI unit(s) to which he/she is assigned substantially change;
- Providing initial, introductory training in FALCON Workspace and/or FALCON Mobile to new employees;
- Providing advanced training in the functions and features of FALCON Workspace and/or FALCON Mobile to veteran employees;
- Support of the following types of operations: analysis of the transportation, storage, logistics, financial and command and control networks associated with global human smuggling criminal enterprises;
- Support approximately twenty (20) personnel at the Human Smuggling Cell located in Reston, Virginia (see Section 3.0: Place of Performance);
- Make approximately five (5) two-week (or shorter) site visits to ICE training facilities in El Paso, San Antonio, Laredo and Houston in Texas, and San Ysidro, California; five of these site visits will be completed before 9/30/2016; they will take place at a rate of 1-2 per month; shall train approximately forty to sixty (40-60) HSI Special Agents, Criminal Investigators, Intelligence Analysts, and Task Force Officers assigned to HSI supervisors per training session;
- Ensuring that HSI employees and/or Task Force Officers, by the end of the period of performance, achieve independent proficiency in the features and functions of FALCON Workspace and/or FALCON Mobile;
- Acquiring sufficient knowledge of HSI missions, objectives, policies, and procedures to

work iteratively with HSI personnel to create innovative and effective workflows utilizing FALCON Workspace and/or FALCON Mobile to achieve HSI goals;
- Gather feedback from government employees on their level of satisfaction with training and support activities, and report results of this feedback to the FALCON PMO on a quarterly basis;
- Coordinate with Palantir Technologies Forward Deployed Engineers and other Palantir system support staff to ensure that HSI employees are familiarized with and trained in the operations of new versions of FALCON Workspace and/or FALCON Mobile which are deployed by Palantir Technologies;
- Coordinate all training and operational support activities with the Field Support Representatives (FSR) staff employed by Palantir Technologies, Inc., or any successor vendor which serves as lead contractor on the FALCON Operations and Support and System Enhancement contract, in order to ensure uniformity of FALCON training outcomes across HSI, to promote sharing of FALCON training best practices across HSI, and to maximize unity of effort and mutual support among HSI units and offices which utilize FALCON;
- Pre-clear any new training initiatives or meetings with HSI personnel at or above the level of Group Supervisor with the FALCON PMO (Program Management Office); and
- Report weekly on training and employee support activities to the FALCON PMO.

3.0 PLACE OF PERFORMANCE

Primary duty location will be the DHS Human Smuggling Cell, located at 12379 Sunrise Valley Dr., Reston, VA, with a secondary local duty location at ICE HQ, located at 500 12th St NW, Washington, DC. Travel outside the National Capitol Region will consist of approximately five (5) two-week (or shorter) site visits to ICE training facilities in El Paso, San Antonio, Laredo and Houston in Texas, and San Ysidro, California. Five of these site visits will be completed before 9/30/2016; they will take place at a rate of 1-2 per month. Standard work hours shall be Mondays through Fridays, for eight-hour work periods between 8:00 AM and 5:00 PM; however, work hours will vary during travel assignments, depending upon travel arrangements and local training needs.

4.0 PERIOD OF PERFORMANCE

The period of performance will consist of a base period of twelve (12) months starting at the date of the award of this Task Order. There will be up to four (4) twelve (12) month option periods.

5.0 VENDOR'S AND VENDOR EMPLOYEE'S QUALIFICATIONS

Vendor's status as a Palantir Technologies "Preferred Vendor" is highly preferred but not required. Possession of this qualification will be one of several selection factors in the government's choice of vendors for a BPA call/Task Order. "Preferred Vendor" status

provides a vendor access to Palantir's internal resources, including a Palantir vendor email account, internal Palantir distribution lists, internal Palantir project management boards, and internal engineering resources. These are only made available to Authorized Palantir Service Providers. Non-preferred vendors acting on behalf of the Government may only access the same support resources provided the Government under Palantir's standard license agreement (Support Portal access, DevZone access, Product Documentation), but non-preferred vendors do not have access to internal Palantir resources.

Vendor employee(s) shall have a minimum of two years' prior experience providing training and employee support services for the Palantir Gotham software platform, at least one year of which shall have been in the context of a federal law enforcement organization. Prior experience providing training and employee support services for the FALCON implementation of the Palantir Gotham software platform at ICE is highly preferred but not required. Possession of this qualification will be one of several selection factors in the government's choice of vendors for a BPA call/Task Order. Vendor employee(s) shall have a Secret clearance, due to required access to ICE Facilities, in order to perform on this Task Order.

PRIVACY THRESHOLD ANALYSIS (PTA)

This form is used to determine whether a Privacy Impact Assessment is required.

Please use the attached form to determine whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

Please complete this form and send it to your component Privacy Office. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form. If a PIA is required, the DHS Privacy Office will send you a copy of the Official Privacy Impact Assessment Guide and accompanying Template to complete and return.

A copy of the Guide and Template is available on the DHS Privacy Office website, www.dhs.gov/privacy, on DHSConnect and directly from the DHS Privacy Office via email: pia@hq.dhs.gov, phone: 202-343-1717.

PRIVACY THRESHOLD ANALYSIS (PTA)

SUMMARY INFORMATION

Project or Program Name:	**ICE Cloud GSS**		
Component:	Immigration and Customs Enforcement (ICE)	**Office or Program:**	OCIO
Xacta FISMA Name (if applicable):	**ICE Cloud GSS**	**Xacta FISMA Number (if applicable):**	**ICE-07675-GSS-07675**
Type of Project or Program:	**IT System**	**Project or program status:**	**Development**
Date first developed:	**October 1, 2016**	**Pilot launch date:**	**May 1, 2017**
Date of last PTA update	**N/A**	**Pilot end date:**	**N/A**
ATO Status (if applicable)	**In progress**	**ATO expiration date (if applicable):**	**N/A**

PROJECT OR PROGRAM MANAGER

Name:	(b)(6);(b)(7)(C)		
Office:	**OCIO/OPS/ASB**	**Title:**	ICE Cloud Broker
Phone:	**202-732-**(b)(6);(b)(7)(	**Email:**	(b)(6);(b)(7)(C)

INFORMATION SYSTEM SECURITY OFFICER (ISSO) (IF APPLICABLE)

Name:	(b)(6);(b)(7)(C)		
Phone:	**202-732**(b)(6);(b)(	**Email:**	(b)(6);(b)(7)(C)

SPECIFIC PTA QUESTIONS

1. Reason for submitting the PTA: New PTA
(b)(5)

2. Does this system employ any of the following technologies: *If you are using any of these technologies and want coverage under the respective PIA for that technology please stop here and contact the DHS Privacy Office for further guidance.*	☐ Closed Circuit Television (CCTV) ☐ Social Media ☐ Web portal[1] (e.g., SharePoint) ☐ Contact Lists ☒ None of these

3. From whom does the Project or Program collect, maintain, use, or disseminate information? *Please check all that apply.*	☒ This program does not collect any personally identifiable information[2] ☐ Members of the public ☐ DHS employees/contractors (list components): ☐ Contractors working on behalf of DHS ☐ Employees of other federal agencies

[1] Informational and collaboration-based portals in operation at DHS and its components that collect, use, maintain, and share limited personally identifiable information (PII) about individuals who are "members" of the portal or "potential members" who seek to gain access to the portal.

[2] DHS defines personal information as "Personally Identifiable Information" or PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department. "Sensitive PII" is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. For the purposes of this PTA, SPII and PII are treated the same.

4. What specific information about individuals is collected, generated or retained?	
(b)(5)	
4(a) Does the project, program, or system retrieve information by personal identifier?	☒ No. Please continue to next question. ☐ Yes. If yes, please list all personal identifiers used:
4(b) Does the project, program, or system use Social Security Numbers (SSN)?	☒ No. ☐ Yes.
4(c) If yes, please provide the specific legal basis and purpose for the collection of SSNs:	Click here to enter text.
4(d) If yes, please describe the uses of the SSNs within the project, program, or system:	Click here to enter text.
4(e) If this project, program, or system is an information technology/system, does it relate solely to infrastructure? *For example, is the system a Local Area Network (LAN) or Wide Area Network (WAN)?*	☒ No. Please continue to next question. ☐ Yes. If a log kept of communication traffic, please answer the following question.
4(f) If header or payload data[3] is stored in the communication traffic log, please detail the data elements stored.	
Click here to enter text.	

5. Does this project, program, or system connect, receive, or share PII with any other DHS programs or systems[4]?	☒ No. ☐ Yes. If yes, please list:
6. Does this project, program, or system connect, receive, or share PII with any	☒ No.

[3] When data is sent over the Internet, each unit transmitted includes both header information and the actual data being sent. The header identifies the source and destination of the packet, while the actual data is referred to as the payload. Because header information, or overhead data, is only used in the transmission process, it is stripped from the packet when it reaches its destination. Therefore, the payload is the only data received by the destination system.

[4] PII may be shared, received, or connected to other DHS systems directly, automatically, or by manual processes. Often, these systems are listed as "interconnected systems" in Xacta.

external (non-DHS) partners or systems?	☐ Yes. If yes, please list: Click here to enter text.
6(a) Is this external sharing pursuant to new or existing information sharing access agreement (MOU, MOA, LOI, etc.)?	N/A
7. Does the project, program, or system provide role-based training for personnel who have access in addition to annual privacy training required of all DHS personnel?	☒ No. ☐ Yes. If yes, please list:
8. Per NIST SP 800-53 Rev. 4, Appendix J, does the project, program, or system maintain an accounting of disclosures of PII to individuals who have requested access to their PII?	☒ No. What steps will be taken to develop and maintain the accounting: N/A, does not collect PII ☐ Yes. In what format is the accounting maintained:
9. Is there a FIPS 199 determination?[4]	☐ Unknown. ☐ No. ☒ Yes. Please indicate the determinations for each of the following: Confidentiality: ☐ Low ☐ Moderate ☒ High ☐ Undefined Integrity: ☐ Low ☐ Moderate ☒ High ☐ Undefined Availability: ☐ Low ☐ Moderate ☒ High ☐ Undefined

PRIVACY THRESHOLD REVIEW

[4] FIPS 199 is the Federal Information Processing Standard Publication 199, Standards for Security Categorization of Federal Information and Information Systems and is used to establish security categories of information systems.

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	(b)(6);(b)(7)(C)
Date submitted to Component Privacy Office:	**April 14, 2017**
Date submitted to DHS Privacy Office:	April 25, 2017
Component Privacy Office Recommendation: *Please include recommendation below, including what new privacy compliance documentation is needed.*	
(b)(5)	

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	(b)(6);(b)(7)(C)
PCTS Workflow Number:	(b)(5);(b)(7)(E
Date approved by DHS Privacy Office:	April 28, 2017
PTA Expiration Date	April 28, 2020

DESIGNATION

Privacy Sensitive System:	No If "no" PTA adjudication is complete.
Category of System:	Other If "other" is selected, please describe: Click here to enter text.
Determination:	☒ PTA sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing Sensitive PII applies. ☐ Privacy Act Statement required. ☐ Privacy Impact Assessment (PIA) required. ☐ System of Records Notice (SORN) required. ☐ Paperwork Reduction Act (PRA) Clearance may be required. Contact your component PRA Officer.

	☐ A Records Schedule may be required. Contact your component Records Officer.
PIA:	Choose an item. If covered by existing PIA, please list: Click here to enter text.
SORN:	Choose an item. If covered by existing SORN, please list: Click here to enter text.

DHS Privacy Office Comments:
Please describe rationale for privacy compliance determination above.

(b)(5)