

Department of the Interior
Privacy Impact Assessment

September 3, 2013

Name of Project: BisonConnect – Google Apps for Government

Bureau: Office of the Secretary

Project's Unique ID: 010-000000330

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- Bureau/office IT Security Manager
- Bureau/office Privacy Act Officer
- DOI OCIO IT Portfolio Division
- DOI Privacy Act Officer

Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division. Also refer to the signature approval page at the end of this document.

A. CONTACT INFORMATION:

Teri Barnett
Departmental Privacy Officer
U.S. Department of the Interior
1849 C Street, NW, Mail Stop 5547 MIB
Washington, DC 20240
202-208-1605

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes. BisonConnect - Google Apps for Government (GAfG) includes multiple applications, many of which contain information about individuals. The applications are Mail, Calendar, Contacts, Drive, Sites, Department Browser and Chat. Although many of the applications open and run in independent windows in BisonConnect, there is a high degree of integration and data sharing between the applications. As a result, personally identifiable information (PII) collected and primarily used in one BisonConnect application may be easily accessible or used in other BisonConnect applications. Contact information, for example, is available through the Contacts application, but is also available across most of BisonConnect by clicking on links

near an individual's name. Information about individuals typically found in each of BisonConnect's applications includes:

Mail: BisonConnect will serve as the email system for the entire Department of the Interior (DOI). The Mail application (Mail) will include the names and email addresses of email senders and recipients, as well as personal information typically found in email correspondence signature lines, such as office address, organization name, fax number, professional title, and professional licensing or certification designations. In addition, the system may contain personal information concerning individuals in the body, subject, name of attachment, and attachment of email messages. BisonConnect users also may voluntarily include a profile photo that will be displayed as a part of email correspondence within BisonConnect.

Contacts: Each BisonConnect user has a contacts database, accessible from the contacts tab in BisonConnect, which provides access to the entire directory of DOI BisonConnect users. The contacts interface includes five links that break down contacts into sets: groups, local domain server, full directory, my contacts, and most contacted. Users can set up their own contact groups, add additional information to existing contacts, and add contact information for individuals outside of DOI. By default, the contacts database will also retain the email address and display name (usually the addressees' first and last name) of individuals who are not BisonConnect users who are sent a message by a BisonConnect user.

Each contact in the BisonConnect database contains basic information such as the name and email address for each BisonConnect user. In addition, directory information (where available) is automatically populated for each user. This includes name, work telephone, work address and office location. There are additional data fields which users can voluntarily add to their profile, which becomes viewable by all other BisonConnect users. These additional fields include birthday, profile photo, phonetic name, nickname, title and company, relationship, instant messaging address, URL, notes and custom fields.

Users can also insert additional contact information for other BisonConnect users. When a user adds additional data for another BisonConnect user, the additional information is only visible to the user who added the information; it is not viewable to all BisonConnect users.

Calendar: The Calendar stores information about meetings, appointments, milestone dates, reminders and deadlines of all types. Individual information typically found in Calendar items includes first and last name. By default, each user's schedule is visible to other users, with time blocks marked as "busy". Users have the option to make all calendar details public or to set specific appointments to "public" or "private" status. Private events are not viewable by other users.

Drive: Drive is a cloud based storage repository that facilitates creation, storage, sharing and collaborative work for all types of electronic files including text, graphical, audio, or video files, which may include documents, forms, reports, correspondence, briefing papers, committee and meeting minutes, contracts, grants, leases, permits, audits, manuals, studies, promotional materials, compliance information, and more. By default, Drive files are private; private files can be viewed only by the file creator and do not appear to users performing Drive searches. Users can alter permissions for their Drive files to allow either all BisonConnect users or select BisonConnect users rights to view files. File rights can further be delineated to view only, view and comment, or view comment and edit.

Due to the ability of individual users to upload files of all types, there is a potential for large amounts of PII to be added to Drive and it is not possible to predict all of the types of PII that may be included. Information about individuals may include, but is not limited to, names, email addresses, telephone numbers, Social Security numbers, dates of birth, employment history, educational background, and correspondence or comments from members of the public.

Sites: BisonConnect users have the option to create their own web sites that will be visible on the DOI domain. Users have virtually unlimited options with respect to the types of pages created and the information included; web pages may include text, PDFs, images, audio, or video files. Information about individuals may include, but is not limited to, names, profile photos or other images of individuals contained in photographs or videos, email addresses, telephone numbers and more.

Department Browser: The Department Browser provides directory listings for all users of the BisonConnect system, with tabs breaking down users by bureau or agency. The information source is the same database as the Contacts application described above, and directory information is populated for each user, which includes name, work telephone, work address and office location. There are additional data fields that users can populate for their own profile, allowing the information to be viewable by all other BisonConnect users. These additional fields include birthday, profile photo, phonetic name, nickname, title and company, relationship, instant messaging address, URL, notes and custom fields.

Chat – Chat enables BisonConnect users, to engage in live text messaging sessions with other BisonConnect users. The content of the chats are retained in an encrypted database. Individual information includes the names of the individual parties involved in the Chat session, as well as any individual information shared by the users during the course of the Chat.

a. Is this information identifiable to the individual¹? *(If there is NO information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).*

Yes. Much of the personal information in the BisonConnect system, including many of the items listed above, are identifiable to the individual including, but not limited to, name, email address, telephone numbers, social security numbers, employee IDs, and profile photos. Certain data items such as date of birth, zip code and other personal information may allow individuals to be identified in certain combinations.

b. Is the information about individual members of the public? *(If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security documentation).*

Yes. Information about members of the public can be added to the system in a number of ways, including:

- Senders or recipients of email messages may be members of the public.
- Email messages may, in the subject, body or any attachments, include information about members of the public.
- BisonConnect users may add contact information about members of the public to their contact databases.
- Electronic files added to Drive may include information about members of the public.
- Information added to Sites may include information about members of the public.

c. Is the information about employees? *(If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).*

Yes. The system will contain extensive amounts of PII about employees in the Mail, Calendar, Contacts, Department Browser, and Drive applications. The Sites and Chat applications may also include PII. This information will include, but is not limited to, name, email address, telephone contact information, employee IDs, and more.

2) What is the purpose of the system/application?

BisonConnect is a cloud-based “Software as a Service” (SaaS) information management tool that contains a suite of Google applications and tools including email, calendar, instant messaging, document development, collaboration and production and cloud storage applications. The integration of all of the above tools into a single package is designed to increase communication and collaboration, in part by improving access to information through the implementation of a single centralized system.

BisonConnect is accessible through web browsers with secured (https) connections, and can also be accessed using mobile devices. As a result, users will be able to access BisonConnect from most internet-connected devices. BisonConnect will be used Department-wide by all employees, contractors, volunteers, and others who have an official email account with DOI or any of DOI's bureaus, agencies, and offices.

BisonConnect contains multiple applications, which are Mail, Calendar, Contacts, Drive, Sites, Department Browser and Chat.

Mail: The Mail application will provide email to all of the Department's employees, contractors, and volunteers. In addition to being available through a secured web browser connection, Mail will be accessible through any web browser with a secured (https) connection, as well as through email applications that support Internet Message Access Protocol (IMAP) or Post Office Protocol (POP), including mobile device applications that permit the use of IMAP and POP enabled accounts. For archival and discovery purposes, BisonConnect mail will be captured and stored by DOI's email archiving and e-Discovery systems.

Calendar: Calendar is a web based calendar and time management system. Among other features, users can share and edit calendar items and schedule and manage meetings, appointments, milestone dates, reminders and deadlines of all types.

Drive: Drive is a cloud based storage repository that facilitates creation, storage and sharing of electronic files while permitting collaborative work by users on text, graphical, audio, or video files. This may include documents, forms, reports, correspondence, briefing papers, committee and meeting files, contracts, grants, leases, permits, audits, manuals, studies and more. By default, Drive files are private; private files can be viewed only by the file creator and do not appear to users performing Drive searches. Users can alter permissions for their Drive files to allow either all BisonConnect users or select BisonConnect users' rights to view the file. File rights can further be defined to view only, view and comment, or view comment and edit. Due to the ability of individual users to upload files of all types, there is a potential for large amounts of information to be added to Drive and it is not possible to predict all of the types of personal information that may be included.

Sites: BisonConnect users have the option to create their own web sites that will be visible on the DOI domain. Users have virtually unlimited options with respect to the types of pages created and the information included; web pages may include text, PDFs, images, audio, or video files.

Department Browser: The Department Browser provides directory listings for all users of BisonConnect system, with tabs breaking down users by bureau or agency.

Chat – Chat enables DOI BisonConnect users to engage in live text messaging sessions between two or more individuals, providing users with an additional communication tool.

3) What legal authority authorizes the purchase or development of this system/application?

Departmental Regulations, 5 U.S.C. 301; The Paperwork Reduction Act, 44 U.S.C. Chapter 35; the Clinger-Cohen Act, 40 U.S.C. 1401; OMB Circular A-130, Management of Federal Information Resources; Executive Order 13571, “Streamlining Service Delivery and Improving Customer Service,” April 11, 2011; Presidential Memorandum, “Security Authorization of Information Systems in Cloud Computing Environments,” December 8, 2011; and Presidential Memorandum, “Building a 21st Century Digital Government,” May 23, 2012.

C. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

1. All DOI employees, contractors, partners, and volunteers who have BisonConnect accounts with DOI.
2. Senders of email from outside of DOI, including employees and contractors of other Federal, Tribal, state, or local agencies, officials from international or other third-party entities, private organizations, and members of the general public.
3. Individuals whose contact information is added to the BisonConnect system by BisonConnect users.
4. Individuals identified in the body, subject, name of attachment, and attachment of email messages, documents stored in BisonConnect Drive, and individuals whose personal information may be provided in communications in applications such as Google Chat.

2) What are the sources of the information in the system?

Information enters BisonConnect in one of five ways:

1. ***Data transferred from existing systems into BisonConnect.*** BisonConnect data was initially populated by transitioning email and calendar data from existing Microsoft Office and Lotus Notes accounts held by DOI users.
2. ***Set up of new BisonConnect accounts.*** Users will be added to BisonConnect as new employees, contractors and volunteers come on board with DOI. Basic information, such as name, office address, and work telephone will be provided by new users via a paper or PDF form. The form data will be entered in the

Department's employee Active Directory; Active Directory data is then used to create a new BisonConnect user account.

3. ***Information added by BisonConnect users about themselves.*** BisonConnect users have a number of opportunities to voluntarily enter their own personal information, such as enhanced profile information, or personal information included in files added to Drive, personal images included in uploaded videos, or personal information included in blog posts or web sites created by the user.
 4. ***Information added by BisonConnect users about other individuals.*** Users can also enter other users' PII into BisonConnect in several ways, including entering enhanced contact information in the Contact database, uploading electronic files or videos that include other individual's personal information, or including personal information in documents, chats, or web pages in BisonConnect.
 5. ***Information sent to BisonConnect users from external email accounts.***
BisonConnect users will receive email from external email senders that includes PII, including information contained in the body and accompanying attachments.
- a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?**

Sources of information are BisonConnect administrators, BisonConnect users, DOI records and data migrated from other email systems, DOI's employee Active Directory system, external sources, such as other Federal, Tribal, state, or local agencies, private third-party entities and members of the public who correspond with DOI bureaus, offices, programs or officials via the email system or otherwise provide data that is transmitted via the email system or entered into BisonConnect applications.

- b. What Federal agencies are providing data for use in the system?**

BisonConnect may receive data from other Federal agencies in the form of email messages from employees of other agencies to BisonConnect users or electronic files created by other agencies that are entered into BisonConnect applications.

- c. What Tribal, state and local agencies are providing data for use in the system?**

BisonConnect may receive data from other Tribal, state and local agencies in the form of email messages to BisonConnect users or electronic files created by other agencies that are entered into BisonConnect applications.

- d. From what other third party sources will data be collected?**

BisonConnect may receive data from other third party sources in the form of email messages from third parties to BisonConnect users or electronic files created by third parties that are entered into BisonConnect applications.

e. What information will be collected from the employee and the public?

Contact information and other personal information is entered into BisonConnect for BisonConnect administrators, BisonConnect users, and external Federal, Tribal, state, or local agencies, private third-party entities and members of the public who correspond with DOI bureaus, offices, programs or officials via the email system, and can typically include, but is not limited to, name, email address, work addresses, telephone numbers, and profile photos.

Personal information for BisonConnect users and employees of external Federal, Tribal, state, and local agencies, or private third-party entities or members of the public may be included in email contents or file attachments or files uploaded to Drive. This may include contact information or other types of personal information including, but not limited, to social security number, date of birth, personal financial data, employment data, disability data, and security clearance and background investigation material.

Due to the purpose of the system and its broad range of functions, a significant amount of personal information is collected and maintained in BisonConnect.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOI records be verified for accuracy?

Due to the nature of the BisonConnect system and the volume of data being entered, data collected from sources other than DOI records will not be verified by system administrators for accuracy; it will be the responsibility of the BisonConnect user entering the data to ensure the accuracy of the information received from external sources.

As discussed above in section C(2)(2), information is obtained from the Department's employee Active Directory during the BisonConnect account setup process, including name, office address and phone number. Since this data is obtained from existing DOI records, it is not independently verified before being entered into BisonConnect.

Each time a user logs into BisonConnect, the employee's credentials are verified with the Department's Active Directory system. An employee's status is immediately changed in Active Directory as soon as a termination of employment

of any type occurs. Only active employees are able to access BisonConnect accounts.

When a user's employment status is changed in Active Directory, BisonConnect administrators will remove the user's account from BisonConnect and the user's contact information will be purged from the Contacts database. These controls are outlined in the standard operating procedures for the BisonConnect System.

b. How will data be checked for completeness?

Due to the nature of the system and the volume of data being entered, data collected from sources other than DOI records will not be verified by system administrators for completeness; it will be the responsibility of the BisonConnect user entering the data to ensure the completeness of the information provided.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

BisonConnect is an information management tool that contains a suite of applications designed to increase communication and collaboration, and improve access to information on a single centralized DOI network, and generally does not contain steps or procedures to ensure the currency of data entered by users. Individual BisonConnect users may take steps to ensure their own data or data entered into the system is current in accordance with bureau, office or program procedures for the purpose of the data collected and entered, or the specific application used.

Each time a user logs into BisonConnect, the employee's credentials are verified with the Department's Active Directory system. An employee's status is immediately changed in Active Directory as soon as a termination of employment of any type occurs. Only active employees are able to access BisonConnect accounts.

When a user's employment status is changed in Active Directory, BisonConnect administrators will remove the user's account from BisonConnect and the user's contact information will be purged from the Contacts database. These controls are outlined in the standard operating procedures for the BisonConnect System.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

The data elements are described in detail in BisonConnect System Security Plan (SSP). However, due to the nature of BisonConnect, including but not limited to the ability for users to add custom information fields, or create internal web sites

or forms, it is not possible to identify all data elements that may be included in BisonConnect applications.

D. ATTRIBUTES OF THE DATA:

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes. The BisonConnect system is the unified messaging system for DOI and will contain all official DOI email communications. BisonConnect will also include other applications that facilitate information sharing and collaborative work.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

BisonConnect is intended to be an open, flexible, and full featured system for comprehensive messaging, information sharing and collaborative work. The system is not intended to derive new data or create previously unavailable data about an individual through aggregation from the information collected or communications exchanged. However, due to the integrated nature of BisonConnect applications and the flexibility for BisonConnect users to enter a wide variety of data, it is possible that new data could be created through aggregation of information about individuals.

3) Will the new data be placed in the individual's record?

BisonConnect is not intended to derive new data or create previously unavailable data about an individual through data aggregation. However, due to the integrated nature of BisonConnect applications and the flexibility for BisonConnect users to enter a wide variety of data, it is possible that new data could be created that will be contained in one or more of BisonConnect applications, such as Mail, Drive, and Calendar. In some instances new data concerning an individual may be created as a result of an investigation or notification from a DOI network security system. While this new data will not be retained in BisonConnect, it may be added to an individual's record in another DOI system.

4) Can the system make determinations about employees/public that would not be possible without the new data?

BisonConnect is not intended to derive new data or create previously unavailable data about individuals through aggregation from the information collected. Due to the integrated nature of BisonConnect applications and the flexibility for BisonConnect users to enter a wide variety of data, it may be possible for determinations to be made about individuals using any new data; however, the system is a communications and collaboration tool and is not intended to make determinations regarding individuals.

5) How will the new data be verified for relevance and accuracy?

As discussed above, BisonConnect is not expected to derive or create new data. However, any new data that may be created or derived within the BisonConnect system will be verified for relevance and accuracy at the time it is collected and used by DOI officials and only for authorized purposes.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

BisonConnect is an integrated system that consolidates data from a number of existing systems, including Departmental email accounts previously held in multiple databases, as well as other applications in the suite of tools. In addition, data that is currently held in a variety of different locations, including Microsoft SharePoint and DOI file servers, may be transitioned by users to BisonConnect. BisonConnect applications have settings that restrict access to data created or entered by users. For example, users can use private settings for Sites and Drive files so content can be viewed only by users granted specific access.

BisonConnect uses a variety of operational and technical controls to restrict unauthorized access and use. While BisonConnect is a cloud-based system, it utilizes a private cloud community, as opposed to a public cloud service delivery model. Use of a private cloud significantly decreases penetration threats and associated risks. In addition, BisonConnect employs a variety of management, operational and technical security controls.

Administrative access to BisonConnect is granted only to authorized personnel on an official need-to-know basis. Unique administrator identification and authentication, passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels. In addition, all administrative personnel, including contractors, must consent to rules of behavior and take annual end-user security awareness training, computer security role-based training, and privacy and records training in order to obtain and maintain BisonConnect administrator access.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

BisonConnect consolidates processes from a number of existing systems, including existing Departmental email systems, as well as Microsoft SharePoint and DOI file servers.

BisonConnect uses a variety of operational and technical controls to restrict unauthorized access and use. While BisonConnect is a cloud-based system, it utilizes a private cloud community, as opposed to a public cloud service delivery model. Use of a private cloud significantly decreases penetration threats and associated risks. In addition, BisonConnect employs a variety of management, operational and technical security controls.

Administrative access to BisonConnect is granted only to authorized personnel on an official need-to-know basis. Unique administrator identification and authentication, passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels. In addition, all administrative personnel, including contractors, must consent to rules of behavior and take annual end-user security awareness training, computer security role-based training, and privacy and records training in order to obtain and maintain BisonConnect administrator access.

8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

There are numerous ways to retrieve data in BisonConnect, as described below for each module.

Mail: By default, messages are sent to each user's inbox, and sorted by date and time of receipt. All replies are grouped with their original message, creating a single conversation or thread. Users have the option to create and sort inboxes using different folders, specific rules governing email handling, sorting and retrieval.

Users can search for messages using one or more search criteria, including sender (partial or full name or email address of sender), email subject, full message text search, inclusion of an attachment, and date parameters.

Contacts: There are a number of pre-set lists built into BisonConnect, which are accessed using links included on the contact page. These include user added contacts ("My Contacts"), LocalDomainServers, OtherDomainServers, Most Contacted, Other Contacts and Directory. Users can also set up group contact lists. The Contacts module also has a search field that permits users to search for contacts by name, email address, or keywords.

Calendar: By default, calendar data is organized in chronological form using a traditional calendar view. The calendar can be adjusted to view day, week, month, four days, or agenda (which lists scheduled events in chronological order). Users can also perform a full text search of their calendar, including searching by name.

Drive: Documents stored in Drive can be accessed using the default “MyDrive” directory tree that lists the documents and folders in each user’s drive, as well as documents and folders owned by other users to which the user has been granted access. In addition, documents can be accessed through a keyword search feature that permits searches by name in the author field or throughout the text of the document

Sites: Users can access BisonConnect sites by performing keyword searches of BisonConnect sites, including searching by personal identifiers such as name.

Department Browser: The Department Browser has a search field that permits users to search for contacts by name, email address, or other keywords.

Chat: Chat sessions are archived in the system under the Mail and may be retrieved using any search term contained in the Chat session.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

The system will not generate reports on individual Bison Connect users. Bison Connect’s auditing system allows reports to be generated on various aspects of the system’s operating controls, including system functions and user actions; however, these reports provide only aggregated information and not information specific to individuals.

BisonConnect maintains an administrator dashboard that logs administrator access. The log contains administrator name and a list of administrative actions taken, such as records changes or activation or deactivation of system features.

10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)

Each BisonConnect user voluntarily provides personal information and consents to rules of behavior before their BisonConnect account is established. Individuals outside of DOI may decline the collection of information by not corresponding with DOI officials via email or providing information requested by DOI employees. Individuals who are the subject of email communications or data within the BisonConnect applications do not have the opportunity to consent to uses of information within the system, but may have that opportunity at the time the data is

collected or requested by a DOI bureau, office or employee. BisonConnect users may be able to reduce the collection of information by reducing their use of BisonConnect, including limiting email communication and file uploads. Users can also exercise discretion with respect to the PII they provide in BisonConnect, including limiting PII in emails and email signature blocks.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

BisonConnect is being operated by Google under a private cloud model and Google is responsible for ensuring the consistent use of the system and all data across all sites; however, Google is contractually bound to numerous information assurance guidelines and requirements, including National Institute of Standards and Technology (NIST) Special Publication 800-146, Cloud Computing Synopsis and Recommendations, NIST Special Publication 800-144, Guidelines on Security and Privacy in Public Cloud Computing, and a requirement for 99.95% system uptime. In addition, Google is contractually required to cooperate with external audits, evaluations, assessments and security certifications performed by DOI or DOI-appointed third parties.

Google is required to implement at least two data centers located within the continental United States with adequate geographical separation of at least 250 miles with one serving as the primary site and the other as an alternate backup disaster recovery site capable of restoration and resumption of BisonConnect services within 24 hours of failure of the services normally provided by the primary site.

DOI has retained rights to examine Google's capabilities with respect to data backup, data archiving and data recovery.

2) What are the retention periods of data in this system?

Retention periods for BisonConnect vary as records in BisonConnect are maintained by subject matter in accordance with the applicable bureau or office records schedule, or General Records Schedule, approved by the National Archives and Records Administration (NARA) for each specific type of record maintained by the Department.

System administrator logs are covered by DOI's IT Management and Maintenance of IT systems records schedule, which calls for retention for two years after the close of the calendar year in which the records were created.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Records are disposed of in accordance with the applicable records retention schedules for each bureau or office, Departmental policy and NARA guidelines. Paper records are shredded and records contained on electronic media are degaussed or erased in accordance with 384 Department Manual 1.

4) Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

BisonConnect is DOI's first use of a Federal Information Security Management Act (FISMA) compliant cloud services model for messaging and communications services.

5) How does the use of this technology affect public/employee privacy?

BisonConnect is a cloud-based enterprise-level application that contains large amounts of PII. Though the impact to individual privacy resulting from cloud utilization is mitigated by several factors, there are risks. BisonConnect will be hosted by a FISMA compliant cloud services vendor, with applicable security controls employed. Security concerns related to Federal government cloud systems have been evaluated and protocols and procedures for Federal cloud applications have been promulgated by NIST. Google has been approved to provide Federal cloud services by the General Services Administration; GSA approval requires a demonstration of compliance with all NIST standards.

BisonConnect is designated as a FISMA moderate system pursuant to the criteria outlined in Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems". The FIPS 199 classification is based upon the type of data held by a system and the need to maintain the confidentiality, integrity and availability of the system's data.

Pursuant to FISMA guidelines, the moderate risk profile requires the implementation of best practices for managing sensitive data and personally identifiable information. In addition, systems with the moderate designation must address over three hundred specified controls, which cover information handling, physical media management and threat assessments. With the implementation of these mandated practices and controls, PII held in BisonConnect will be adequately secured.

There are specific concerns related to users' ability to access BisonConnect from virtually any internet access point, including through non-government furnished equipment (non-GFE) such as employees' personal computers, personal mobile

devices such as smartphones and tablets, and shared computer terminals in libraries or hotels. These risks include:

- A lack of standardized security configuration and management for non-GFE that creates increased risk due to variation in web browser settings, physical access to devices, antivirus configuration and encryption.
- Local unencrypted storage on non-GFE can be used to download and store BisonConnect files in an unprotected environment. There are no technical mechanisms available to prevent users from performing such downloads.
- Technologies, including cookies, are used by BisonConnect to preserve the continuity of user sessions that could present the opportunity for unauthorized users to access BisonConnect on shared or public access devices.
- Enabling GFE mobile devices involves setting up a mobile device authentication password for each user that is not device specific. Therefore, users have the ability to set up non-GFE mobile devices to access BisonConnect email using Internet Message Access Protocol (IMAP). IMAP automatically stores all email messages in a local device drive, which is problematic if a non-GFE device is not properly secured.
- BisonConnect passwords saved on browsers installed on non-GFE may permit access by unauthorized parties who obtain access to non-GFE that has accessed BisonConnect.

Non-GFE is inherently difficult to secure, and deploying solutions to mitigate risks, including the use of preventative technical controls, is often not possible. There are, however, a number of steps that DOI will or may take to limit the risks arising from user access through non-GFE, including:

- DOI will provide non-GFE configuration guidance to all BisonConnect users.
- BisonConnect includes a “Sign Out” button that terminates user sessions. DOI is investigating implementing a form-based authentication mechanism to supplement BisonConnect’s single-sign on functionality when a login occurs from a non-DOI network address. Time-out settings for the form-based authentication can be adjusted to permit much shorter windows before application shut-down is initiated. In addition, Google is working on a separate timeout management function which will allow DOI to decrease the expiration time for session cookies (which preserve user sessions) to a timeframe shorter than the two-week default in place now. Estimated completion is mid-2013.
- DOI is investigating the possibility of restricting access to BisonConnect to specific web browsers in order to reduce the number of browser-specific risks.
- DOI will provide additional user education to further mitigate risks on non-GFE, including advising users on techniques such as manual clearing of cookies and browser history and the implementation of browser settings to automatically clear cookies and history at the end of each session. Instructions describing these techniques are being prepared.
- DOI will prohibit the use of IMAP on non-GFE and will advise users accordingly.

- DOI will implement policies relating to the storage of DOI files obtained from BisonConnect on non-GFE.
- Users will be directed to avoid browser storage of passwords on browsers installed on non-GFE.
- Users will be provided with education concerning best practices for avoiding viruses and malware on non-GFE used to access BisonConnect.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

The purpose of BisonConnect is to serve as a tool for communications and collaboration, and does not have the capability to identify, locate and monitor individuals.

BisonConnect is integrated with the Symantec Vontu Data Loss Prevention (Symantec DLP) software. Symantec DLP monitors internet email and chat traffic to protect against the external transmission of sensitive data, including information concerning individuals such as social security numbers. Symantec DLP monitors data only; it cannot be set up to monitor individuals.

BisonConnect maintains a minimal ability to monitor administrator access and actions through administrator audit logs. The logs contain administrator name and a list of administrative actions taken, such as records changes or activation or deactivation of system features.

7) What kinds of information are collected as a function of the monitoring of individuals?

BisonConnect's administrator audit logs contain administrator names and a list of administrative actions taken, such as records changes or activation or deactivation of system features.

8) What controls will be used to prevent unauthorized monitoring?

Access to audit logs will be granted to system administrators on a limited basis, and only authorized administrators who have been given a username and password will be able to access the system. The principal of least privileges (granting no more than the minimal access rights needed by each employee to perform their job duties) will be applied. In addition, all users must complete Federal Information System Security Awareness (FISSA), Privacy and Records Management training before being granted access to any DOI IT resource, and annually thereafter. All BisonConnect administrative staff must also complete role based security training.

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

A Privacy Act system of records notice is being developed for BisonConnect - Google Apps for Government and will be published in the Federal Register.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

A system of records notice is being developed for the BisonConnect – Google Apps for Government system.

F. ACCESS TO DATA:

1) Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)

Users: Each DOI employee, contractor and volunteer will have a BisonConnect account. Users will be able to access their own data contained in Mail, Calendar, Drive, and other BisonConnect applications. Users will also be able to access other users' BisonConnect data if rights are granted, as described below in Section F(3).

System Administrators and Contractors: System Administrators, including contractors, will be granted access to system data and system audit logs in order to provide support and to monitor proper system use, including performing system usage audits. Access procedures are described in the BisonConnect system assessment and authorization (A&A) documentation, including the system security plan.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Users: Each DOI employee, contractor and volunteer will have a BisonConnect account and will be granted access to their own data contained in Mail, Calendar, Drive and other applications, as well as access specifically granted to data or files created by other BisonConnect users.

System Administrators: System Administrators, including contractors, will be granted access rights on a least privileges basis, which will permit minimal access needed in order to perform necessary job functions. Access procedures are described in the BisonConnect system A&A documentation, including the system security plan.

3) Will users have access to all data in the system or will the user's access be restricted? Explain.

Users: In general, users will have access to their own BisonConnect data. However, BisonConnect provides for significant amounts of information sharing. Information sharing can be performed as follows:

Mail: All users have access to their own email accounts. In addition, BisonConnect permits users to delegate access to other users, such as administrative staff. Delegation only occurs if a user affirmatively grants another user delegate permission through the “Grant access to your account” section of BisonConnect’s settings. Authorization permits the delegate to sign in to the delegated account to read, delete and send email.

Contacts: All users have their own contacts database. Email account access rights can be delegated to other BisonConnect users, as described above. Authorized email account delegates will have access to contacts database for the delegated account.

Calendar: All users have their own calendar and there are several tiers of calendar options that users can employ by adjusting calendar settings. Calendar sharing options are:

- **Private.** Users can choose to not share any calendar information by unchecking the “Share this calendar with others” box under calendar settings.
- **Shared with other BisonConnect users.** All calendar data is available to all BisonConnect users. The calendar can be shared with specific calendar information displayed, or the calendar can be displayed with “free” or busy” notations instead of specific calendar information.
- **Shared with specific users.** A user can grant calendar access and editing rights to other BisonConnect users. The calendar can be shared with specific calendar information displayed, or the calendar can be displayed with “free” or busy” notations instead of specific calendar information. In addition, rights to edit calendar entries and authorize other users can be delegated.

Drive: All users have their own files stored in Drive. By default, files uploaded to Drive are viewable only by the file owner. Access rights to files and folder in Drive can be granted to other users with rights to view or edit.

Sites: Users have access to the sites they create. In addition, site creators have the option to make their sites available to all BisonConnect users or to grant access to specific BisonConnect users.

Department Browser: Department Browser data is available to all BisonConnect users.

Chat: Chat sessions are archived in the system under the Mail and may be viewed only by chat participants or their email account delegates.

System Administrators: System Administrators, including contractors, will be granted access rights on a least privileges basis, which will permit minimal access needed by in order to perform necessary job functions. Access to audit logs will be granted to system administrators on a limited basis, and only authorized administrators who have been given a username and password will be able to access the system.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)

Users: As described above, most data is private by default; users must affirmatively grant or delegate rights to other users. A number of training modules are offered to BisonConnect users, one of which addresses account access delegation. Users must complete Federal Information System Security Awareness (FISSA), Privacy and Records Management training before being granted access to any DOI IT resource, and annually thereafter.

System Administrators: Access to audit logs will be granted to system administrators on a limited basis, and only authorized administrators who have been given a username and password will be able to access the system. In addition, all users must complete Federal Information System Security Awareness (FISSA), Privacy and Records Management training before being granted access to any DOI IT resource, and annually thereafter.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Yes, contractors were involved with the design and development of the system and will be involved with the maintenance and operation of the system. Federal Acquisition Regulation (FAR) contract Clause 52.224-1, Privacy Act Notification (April 1984), FAR contract Clause 52.224-2, Privacy Act (April 1984), FAR contract Clause 52.239-1, Privacy or Security Safeguards (Aug 1996) and 5 U.S.C. 552a are included by reference in the agreement with the contractor.

6) Do other systems share data or have access to the data in the system? If yes, explain.

For archival and discovery purposes, BisonConnect email messages will be captured and stored by DOI's email archiving and e-Discovery system, the Enterprise eArchive System.

BisonConnect is integrated with the Symantec Vontu Data Loss Prevention (Symantec DLP) software. Symantec DLP monitors internet email and chat traffic to protect against the external transmission of sensitive data, including information concerning individuals such as social security numbers. All BisonConnect email and chat traffic crosses the Symantec DLP, but data is only retained when a security violation is detected. The data retained includes IP address, time of transmission and the transmitted data.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

Google and DOI system administrators will be responsible for protecting the privacy rights of the public and employee affected by the interface. DOI system administrators also are responsible for granting access to individuals to use the system and properly securing access to login credentials.

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?

No other agency will have direct access to or share data in this system. Other Federal, State, Tribal, or local agencies may receive data from BisonConnect in the course of conducting official business with DOI employees through email correspondence or the transfer of electronic files.

9) How will the data be used by the other agency?

Other Federal, State, Tribal, or local agencies will not have direct access to data within BisonConnect, but may receive data in the course of conducting official business with DOI employees through email correspondence or transfer of electronic files. Such correspondence will be conducted for official government purposes, which will vary depending on the mission and needs of the agency.

10) Who is responsible for assuring proper use of the data?

Google and DOI System Administrators for BisonConnect will have the ultimate responsibility for protecting the privacy rights of the public and employees affected by the system.