Privacy Impact Assessment
for the

Biodefense Knowledge Management System v. 2.0

(Supporting IC and LE users)

May 4, 2011

Contact Point
David Shepherd
Chemical-Biological Division
Science and Technology Directorate
(202) 254-5897

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

Abstract

The Department of Homeland Security Science and Technology Directorate's (DHS S&T) Biodefense Knowledge Center (BKC) developed and operates the Biodefense Knowledge Management System (BKMS). The current generation of the BKMS, version 1.0, enables approved users to access and analyze biological sciences topics and related biodefense information to assist with their efforts to better understand or characterize biological threats, by offering an integrated suite of tools for managing and indexing scientific documents and information. In BKMS 2.0, S&T intends to add a component to the system to include data derived from the intelligence community (IC) and law enforcement (LE)-sensitive data. S&T is conducting this Privacy Impact Assessment (PIA) because such an addition will allow for a new function of the system for selected BKMS users, who are authorized to explore IC/LE data (which may contain personally identifiable information (PII)).

Overview

The BKC is funded and managed by DHS S&T and operated by Lawrence Livermore National Laboratory (LLNL), a Department of Energy federally funded Research and Development Center. One component of the BKC is the BKMS, a database of biodefense-related information available 24/7 via secure websites at two (soon three – see below) classification levels to users approved by DHS S&T. Data in the BKMS include scientific reports, research databases, and news-related articles. DHS S&T funded LLNL to develop, maintain, and operate the software and hardware that makes up the BKMS architecture, as well as perform the basic scientific analysis underpinning some of the data and information stored in the BKMS. Using the existing BKMS 1.0 system and infrastructure, S&T and LLNL will include an additional classified/law enforcement component to the system, thus creating the BKMS 2.0, to be used specifically by law enforcement or intelligence analysts.

BKMS 2.0 is a user-based indexing tool that enables law enforcement or intelligence users to upload their own data onto the system and conduct topic-based searches against the scientific and bio-defense related data found in the existing BKMS 1.0 system. BKMS 2.0 integrates and indexes the data to show intersections between the data that may not have otherwise been apparent. This data integration could provide rapid context about a given topic to the users, enabling quicker analysis of the information. Rather than spending hours and hours manually analyzing the data, the system simply indexes and integrates the data in a more efficient manner; it does not collect or use any additional information. Furthermore, BKMS 2.0 is not a fully automated system and is not capable of finding meaning in the data sources on its own. BKMS 2.0 does not identify individuals to investigate or provide value to the content beyond the keyword and indexing search results. The system is a user-based tool and relies on the users to apply their knowledge and expertise to make any judgments or conclusions based on the data; all decision-making authority lies with the users, not the system.

DHS S&T does not own or access any of the data provided by the law enforcement or intelligence users. DHS S&T does provide a user agreement to all LE/IC users prior to operational deployment of the system. By acknowledging the user notice, BKMS 2.0 users agree that:

- No operational decisions will be made based solely on the output of BKMS 2.0. Rather, users may use the BKMS 2.0 analysis to support ongoing investigations by reinforcing data available

through other methods such as traditional law enforcement techniques;

- All data use and data sharing must be done in accordance to the data owner's legal authority and standard procedures;
- The user must conduct their own legal and privacy compliance review. These reviews will ensure that any PII uploaded into the system is used according to existing legal authorities and that all appropriate documentation (SORN, PIA, etc.) are completed; and
- S&T and/or LLNL will conduct periodic audits with the users to check that the system is being used and accessed appropriately.

This PIA provides some background information on the BKMS 1.0 for context; however, it focuses primarily on the privacy risks and mitigations associated with the BKMS 2.0, given that the BKMS 1.0 is already covered by the Portals PIA. The Portals PIA documents online portals for authorized users to obtain, post and exchange information, access common resources, and generally communicate with similarly situated and interested individuals. BKMS 1.0 is a portal for scientists to share information regarding biodefense issues.

BKMS 1.0

BKMS 1.0 manages and indexes (i.e., to tag and categorize, according to categories and priorities predefined by DHS and LLNL scientists) information in the database to allow for efficient access and searches by registered users. DHS S&T works with scientists at LLNL to determine the content that is included in BKMS, according to suggestions from users of the BKMS and the appreciated need by S&T, such as scientific relevance and relevance to users' mission spaces. Users of BKMS 1.0 do not load data into the system by themselves, although they can request that certain scientific data sources be loaded. Users of BKMS 1.0 include U.S. government biodefense community members and Australian government biodefense community members. The BKMS provides access to publicly available scientific databases (maintained by both government and non-government agencies); For Official Use Only (FOUO) scientific reports generated by analysts at the BKC and other U.S. government-affliated organizations (such as the National Biodefense Analysis and Countermeasures Center); reports generated by the government of Australia; and related scientific research information.

The BKMS currently contains three components, that have been reviewed and approved by the DHS Privacy Office, and are covered under the Portals PIA. The previously approved portions of the BKMS include:

1. BioEncyclopedia Pilot: The pilot provided data obtained by accessing 12 open-source scientific data bases (e.g., PubMed) and BKC-generated reports and information to highlight how the BKMS BioE Pilot may be useful for DHS users to analyze, characterize, and understand biological threats.
2. Directory of Cleared Life Scientists (DCLS), formerly called the Subject Matter Expert Directory, (SME Directory): The DCLS exists to provide a listing of scientific experts who can provide peer review of classified scientific research programs, and to help identify scientific specialties for which there is a shortage of SMEs with appropriate security clearances.
3. Global Knowledge Center (GKC): The GKC is a mechanism for international users (at this early stage of GKC development, international users are only from Australia) to use a subset

of the existing components of the BKMS, in accordance with DHS privacy, security, and document release rules and regulations.

The main focus of the scientific data contained in the current BKMS software release is biodefense topics. Limited PII related to the authors of biodefense articles and publications may be included in BKMS. However this is limited to: the name of author(s) and researcher(s) and related information, such as names of coauthors; the article's institutional affiliation; the author's subject matter expertise or credentials (as mentioned in the article); the article's country affiliation (i.e., country where the article was published); and names of individuals' biodefense-related funding grants, technologies developed, or descriptions of patents. BKMS organizes the data to facilitate search functions by system users. For example, if a BKMS user is interested in learning about anthrax research, he/she can search the system using keywords and find scientists conducting research in that area; from those search results, he/she can find other relevant information on the topic (i.e., scientific techniques used in anthrax research, conferences that may cover anthrax research, etc.). Standard bibliographic materials (information maintained in a conventional reference library) are not considered to be systems of records, and are therefore exempt from the System of Records Notice (SORN) requirement set forth by the Privacy Act of 1974.

BKMS 2.0 Overview

DHS S&T is developing the next generation of the BKMS (BKMS 2.0), a research tool that integrates, or indexes, the existing biodefense-related data in the current version of the system with new IC/LE-sensitive data derived from the intelligence and law enforcement communities. The overall mechanics for BKMS 2.0 will be the same as BKMS 1.0, but rather than indexing only scientific data sources, version 2.0 indexes and enables searches of both scientific data and IC and LE data. A unique aspect of the indexing process is that BKC analysts and other subject matter experts pre-identify lists of biodefense-related keywords of interest to the biodefense community (categories of lists include pathogens, diseases, antimicrobials, etc.). As the BKMS processes these otherwise disjointed and unaffiliated data sources, it extracts the keywords of interest as potential linkage points across documents and to rapidly highlight sections of the documents of potential interest to a biodefense analyst. The system displays the results across all categories according to user queries, so that users can readily see all the documents that match their query, as well as related terms that are found within the broad keyword categories. The system does not apply any logic beyond the keyword hits, entity extraction, and entity ranking algorithms (which computes and ranks correlations between pre-defined entities of interest and user-specified themes); the user entering the search terms and topic searches drives the results.

Objective

The objective of the data integration is to enable the end users, i.e., analysts from the IC/LE communities, to easily conduct topic-based searches against otherwise disparate data types – the existing biodefense data and the IC/LE community-derived data. This is intended to allow IC/LE analysts to find intersections contained within biodefense data and IC/LE data that might not otherwise have been apparent if these data sets were not integrated, thus providing analytical value. This may include conducting searches based on names; however, these names belong to individuals of interest or subjects of ongoing law enforcement investigation. Once the user finishes the search on BKMS 2.0, the IC/LE users can choose to save their query on BKMS 2.0 to facilitate analysis and enable continuing

investigation of people of interest. The data and resulting output by default are not saved by the system. This decision is made by the end user; S&T does not make this decision. The users also determine whether to share the resulting indexing output and analysis with additional users or groups, based on mission and legal authority.

Data

In all cases for BKMS 2.0, the user provides the IC/LE data to be loaded into the system, either manually via a data storage device or electronically over a secure network. S&T does not own nor will it provide any IC/LE-sensitive data. The BKC Program Managers will continue populating the system with biodefense related articles and publications. This information is periodically updated, as needed. The existing biodefense data in BKMS 1.0 already contains limited PII of the authors of the scientific articles and publications. As mentioned above, standard bibliographic materials, such as basic author information, is exempt from the SORN requirement.

The additional data sources provided by the IC/LE analyst may also contain PII. However, this information typically refers to a suspect or person of interest, and is provided by an approved IC/LE analyst, who has the appropriate legal authority and need to know to view this information. IC/LE users will consult with their legal counsel and privacy office prior to uploading any data, including PII, into BKMS 2.0 for operational use to ensure that all information is maintained, used, and shared in accordance to their own legal authorities. The users' privacy office will also ensure that all appropriate privacy compliance documentation is completed.

There are three categories of IC/LE data in BKMS 2.0:

1) Broadly available IC/LE reports. These could include IC/LE sources that are widely available to IC/LE community members with a common need to know, and are available to everyone who has access to the network on which the data reside (e.g., classified networks). These data have low risk and no retention policy, as they are openly and easily accessible to all users of the data. The BKMS will adopt the same criteria and restrictions as the original source for those data. LLNL will upload this data into BKMS 2.0.

2) Data owned, uploaded, and accessed by a single user. These data include content loaded by the user of the BKMS using a special upload interface. These data are owned by the user who uploads the data into the BKMS; access is exclusively restricted to that user and no one else. The BKMS policy regarding retention of these data is to place the burden of responsibility on the user to audit and maintain her data according to her agency's retention policies and authorities. Risks associated with these data are increased as data could contain PII or other privacy sensitive components unknown and unregulated by the BKMS and staff. To mitigate that risk, sets of documents uploaded by a user for personal use within the BKMS will be tracked by the date of last update. If the archive has not changed within six months the user (owner) is prompted upon login to review her data for privacy-related concerns. It is the responsibility of the user to address privacy issues of data they upload by updating the data, removing the data, or obtaining proper authorization to collect, use, and retain the data in the BKMS.

3) Data owned by one user and shared with a group of users. In this scenario, the user provides the BKC with a dataset and asks that it be shared with a group of other BKMS users named by the data provider. BKMS administrators will then load the data onto the

BKMS and assign security permissions to ensure that only specified users can access the data. Users cannot add, edit, or delete this archive; those functions are handled by BKMS administrators. With respect to risks and data retention, these data are managed in the same manner as the user loaded/owned data described in Category 2. Users who have access to a data archive that has not been updated in six months are notified upon login that the archive has potentially dated material.

System

The BKMS is not connected with other systems. BKMS 2.0 users only have access to their own information that they themselves load into the system unless it is an IC/LE source that is commonly available to the community (common need to know) or explicitly shared by another data owner. IC/LE users can determine with whom to share their data, based on common need to know and legal authority, as described above. Furthermore, BKMS 2.0 is not a fully automated system and is not capable of finding meaning in the data sources on its own. BKMS 2.0 does not identify individuals to investigate or provide value to the content beyond the keyword and indexing search results. It is up to the analysts to apply their knowledge and expertise to make any judgments or conclusions based on the data; all decision-making authority lies with the analyst, not the system. Throughout the BKMS 2.0 lifecycle, S&T and LLNL will continue to develop, test, and evaluate the system for improvements based on end user feedback. Current plans are to host BKMS 2.0 at LLNL for both the unclassified and the Joint Worldwide Intelligence Communication System (JWICS) deployments, but at the DHS Homeland Secure Data Network (HSDN) data center for secret level Secret Internet Protocol Router Network (SIPRNet) and HSDN deployments. The analyst can access any of the deployments from his own computer on the appropriate networks.

Use Case

An example use case would be that an analyst from the IC/LE community, perhaps through an ongoing investigation, obtains data sources, like a thumb drive, from a suspected bio-terrorist or person of interest. An analyst uploads the data from the thumb-drive into BKMS 2.0. The BKMS 2.0 software indexes the data with the existing biodefense data. The resulting indexed data is categorized and listed together (fused) in a single, easily searched repository. This single repository would be useful in showing data intersections, relevance, patterns and trending between the two data sources not easily demonstrated if the data were not integrated and indexed. The intersections between the data could potentially provide rapid context about a given topic to the IC/LE analysts, such as how the biotechnology is commonly used for legitimate purposes, where is it found globally, and what level of expertise is required to employ it. This provides the analysts with an added layer of background information to support or direct additional investigative efforts, and could save the analyst a lot of time that would have otherwise been spent on manual analysis of the information.

Users and Participants

BKMS is configurable to enable access only to restricted sets of approved users (IC and LE analysts) with an authorized need-to-know, as determined by the user groups. DHS S&T vets all users prior to permitting them to access the BKMS, based upon a clearly stated mission need for official duties. BKMS administrators at LLNL control all data contained in the BKMS as well as user access to all documents and datasets. BKMS administrators assign permissions to each user account, to ensure that users cannot access data they have not been authorized to view.

All IC/LE end users acquire, provide, and use the information in the BKMS 2.0 in accordance with their own legal authorities. Individuals that use BKMS solely for scientific research do not have access to the IC/LE-sensitive data in BKMS 2.0. By virtue of the fact that the BKMS is an S&T-funded system, S&T BKC Program Managers determine which organizations have access to the components of the BKMS 2.0, depending upon mission or operational need. S&T will provide user agreements to these LE/IC organizations prior to permitting access to BKMS 2.0. The user notice is provided to users and states that IC/LE users will not make any operational decisions based solely on the output of BKMS 2.0, and that all user data and sharing will be done in accordance to the users' own legal authority and operating procedures. Upon acknowledging this notice, the responsibility is on the users to appropriately use and share the data; S&T will not be responsible for how the tool is used by IC/LE analysts or what results the IC/LE analysts derive from the use of the data. The user agreement also requires that all acquiring conduct their own legal and privacy compliance reviews with the respective counsel and privacy office, prior to deploying the system for operational use. These reviews will ensure that any PII uploaded into the BKMS 2.0 is used according to existing legal authorities, and that all the appropriate documentation (SORNs, PIAs, etc,) are completed. The user agreement also allows for S&T and/or LLNL administrators to conduct periodic audits on the deployed systems to ensure that information is being used and accessed appropriately.

Participants in the BKMS 2.0 effort include:

- S&T Chemical-Biological Defense Division's BKC, which provides programmatic direction and funding to operate the BKMS, and approves access for authorized users. S&T BKC's role is limited to providing the BKMS tool to the IC/LE users and performing periodic audits of the systems.
- IC/LE user community, which provides data sets in accordance with information-sharing agreements between DHS and members of those communities. Access is limited to IC/LE community users with a specified need to know. Persons outside of this community are not permitted to access data stored in BKMS 2.0. IC/LE users control user access and sharing privileges to the data they upload onto BKMS 2.0. IC/LE users conduct their own legal and privacy reviews prior to deploying the system.
- LLNL employees, who develop, operate, maintain, and load data into the BKMS at LLNL, and maintain access controls to the system. LLNL employees do not act upon or undertake investigations or analyses based on any results produced by BKMS 2.0. They only provide computerized results, in the form of compiled data and supporting evidence, to data owners for follow-up and action by the data owners. LLNL also develops, tests, and evaluates new BKMS 2.0 capabilities to ensure that the system adequately meets the needs and supports the IC/LE community users.

Section 1.0 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 as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

For BKMS 2.0, the system integrates the biodefense and/or scientific data currently in BKMS 1.0 with IC/LE data related to current law enforcement investigations or analyses, as determined by search terms entered by the IC/LE analyst. The IC/LE data may contain non-PII data such as information relating to scientific topics. The IC/LE data could also contain PII, such as names of individuals of interest or suspected bio-terrorist or other information associated to that individual that is collected or obtained during ongoing investigation. This information could pertain to both U.S. and non-U.S. citizens. It is collected by the IC/LE entities, in accordance to their own legal authorities. The BKMS indexing capabilities enables IC/LE users to perform searches across both the biodefense/scientific data and the IC/LE data to determine if the topics intersect. This helps provide scientific background and context to and supports IC/LE investigations and decision making. No operational decisions will made based solely on the information from BKMS 2.0. IC/LE users may use the BKMS 2.0 analysis to support ongoing investigations by reinforcing data available through other methods such as traditional law enforcement techniques. The IC/LE users may share their analyses with other entities; any information sharing will be conducted in accordance to their legal authorities and receiving party's authorized need to know.

Users decide how long the data resides on BKMS 2.0. Data are not automatically archived. Nor does S&T decide when to retire the data.

1.2 What are the sources of the information in the system?

Currently, BKMS 1.0 contains the BKMS Reference Library (the collection of biomedical documents, articles, and journals, as well as reports authored by the BKC and other DHS-funded research groups) and data from open source databases, such as PubMed. With additions in BKMS 2.0, approved users from the IC/LE communities are able to upload IC/LE data by themselves to conduct their searchers and analyses against existing BKMS 1.0 data and new scientific data. The IC/LE data may include reports or media (e.g., a thumb drive from a suspected bioterrorist) that is obtained through ongoing investigations.

BKMS 2.0 will contain law enforcement sensitive data and reports that are widely available to the IC/LE community, through unclassified and classified networks. These data and reports are published by members of the IC/LE community and are shared with those in the community with a common need to know. All other IC/LE data included in the BKMS 2.0 are owned by the users. Neither S&T nor LLNL own these data. The publicly-available biodefense and scientific data and law enforcement sensitive reports continue to be uploaded by S&T and LLNL.

1.3 Why is the information being collected, used, disseminated, or maintained?

BKMS 2.0 allows authorized IC/LE users to conduct searches across existing biodefense/scientific information and user provided IC/LE data to make informed analyses based upon the integration of information. The goal of data integration is to highlight to the analysts in the IC/LE community intersections contained within biodefense data and law enforcement data that

might not otherwise have been apparent if these disparate data sets were not integrated. This integration enables queries, searches, and comparisons to be made across several data sets simultaneously, which has the value of showing overlaps (i.e., similar keywords) not readily apparent. The data integration also saves time by eliminating tedious manual comparisons of the data sets. All approved end users will use the information in accordance to their own legal authorities.

1.4 How is the information collected?

In addition to the publicly available data sources uploaded into BKMS 1.0, BKMS 2.0 contains IC/LE data sources provided by the user of the system, from agencies of the law enforcement and intelligence communities. Data are uploaded through secure channels such as a classified computer network or secure FOUO channel. IC/LE users collect their data during their normal operations (e.g., investigations), in accordance with their own legal authorities and operating procedures.

1.5 How will the information be checked for accuracy?

The user community providing or uploading the data will conduct checks for accuracy, as appropriate and applicable, prior to providing the information to BKMS 2.0. No additional accuracy checks are conducted on the biodefense or scientific data.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The Homeland Security Act of 2002 [Public Law 1007-296, §302(4)] authorizes the Science and Technology Directorate to conduct "basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs." In exercising its responsibility under the Homeland Security Act, S&T is authorized to collect information, as appropriate, to support R&D related to improving the security of the homeland.

The IC/LE end users collect and use information uploaded to BKMS 2.0 in accordance to their own legal authorities. Prior to deploying the system into operational use, all acquiring LE/IC users are required to go through their own legal and privacy compliance review. If LE/IC user plan to upload data containing PII into the BKMS 2.0, these reviews ensure that the users have the appropriate SORN, PIA, or other documentation in place.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Privacy Risk: The system may inaccurately link an individual to bioterrorism or illegal activities.

Mitigation: Data cannot be altered or manipulated once it is entered into BKMS. An additional mitigation strategy employed is that the BKC will require users to agree to user notices. The user notice requires that IC/LE users not make any operational decisions based solely on the output of BKMS 2.0.

Rather, IC/LE users may use the BKMS 2.0 analysis to support ongoing investigations by reinforcing data available through other methods such as traditional law enforcement techniques. LE/IC users must agree to comply with user notices each time the user logs into BKMS 2.0.

In addition, S&T and LLNL will not make any operational decisions based on the information in BKMS 2.0; S&T and LLNL only provide the BKMS 2.0 capabilities to the IC/LE users. S&T and LLNL also provide analysis on the effectiveness of the system and continue to make improvements to the system.

Privacy Risk: Authors of scientific articles, known or suspected bioterrorists and other incidental PII found in the existing BKMS 1.0 data, may be implicated or inaccurately linked to bioterrorism or illegal activities.

Mitigation: User notices require that no operational decisions are made based solely on the output of the BKMS 2.0. All IC/LE users apply their own analysis and expertise to come to their own conclusions about the BKMS 2.0 data. Typically, the IC/LE users already have a person of interest under investigation and the BKMS 2.0 data will only support ongoing investigations. A known or suspected bioterrorist may be implicated or linked to bioterrorist or illegal activities, but IC/LE users will only come to this conclusion through their own analysis and investigations; the BKMS tool itself does not assign any value to the data. The IC/LE users must use their professional judgment and analysis regarding the worth and value of the output to determine the accuracy of the linkages, and will not base any operational decisions solely on the output of BKMS 2.0.

Privacy Risk: Unauthorized users will gain access to the IC/LE data sources.

Mitigation: Access is restricted to those approved by the external organization providing the data (e.g., FBI or other law enforcement entities or agencies within the IC), and approved users of classified networks (e.g., JWICS or HSDN), as appropriate and approved by data owners. The BKMS can do this because it was built to allow role-based access; the system does not automatically share data with other users. Each and every user is assigned access privileges according to his or her permissions granted by data owners. For example, the FBI can determine who should have access to its IC/LE data that is uploaded onto the BKMS 2.0. The FBI's data is not automatically shared with all BKMS 2.0 users. All IC/LE users may share their data in accordance with their own legal authorities and sharing agreements.

Furthermore, the BKMS is transmitted over networks of different classification levels (FOUO and Top Secret (TS) levels, with Secret (S) level planned to be available in 2011, as appropriate to the level of classification of the data and user. Within each of these networks, the BKMS has the capability to segregate and present data by user, data type and data originator, further mitigating risks.

Section 2.0 Uses of the System and the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

BKMS 1.0 was created to facilitate researchers studying biodefense related topics. The addition of the IC/LE data sets in BKMS 2.0 enables the IC/LE analysts to learn more and provide more context

and scientific background to support investigations of persons of interest (i.e., suspected bioterrorist). The additional data sets also help identify potential topics of interest for further investigation through topic-based indexing (using predetermined keywords and topics) and searches. The searches may be based on names; however, these names belong to individuals of interest or subjects of ongoing law enforcement investigation. The BKMS 2.0 system itself is not capable of making any judgment or determinations on any individuals, and users agree as a precondition of use that no operational decisions will be made based solely on the BKMS 2.0 results or output. The IC/LE users conduct their own analyses on the results and draw any conclusions based on experience and training.

The S&T BKC Program Managers only provide the users with the BKMS 2.0 system capabilities; users provide their own IC/LE data to have loaded into the system. S&T and LLNL will continue to upload the biodefense and scientific data into the system. Users have to acknowledge the user agreement, including conducting their own privacy compliance review, before being able to use BKMS 2.0. Based on the system's output, the IC/LE users decide whether to pursue a data point further. S&T and LLNL will also conduct periodic audits to ensure that the system is being used appropriately and that there is no unauthorized access to the system. S&T BKC Program Managers may also use IC/LE user feedback to continue to test and evaluate the system and make improvements.

2.2 What types of tools are used to analyze data and what type of data may be produced?

BKMS 2.0 utilizes the same tools as the current BKMS, and will continue to facilitate similar types of keyword searches and indexing capabilities to present otherwise disjointed and unaffiliated data of potential interest to an analyst. However, rather than aggregating and organizing scientific information solely from open source data, such as scientific articles, BKMS 2.0 allows users to analyze, aggregate and organize information from scientific articles as well as IC/LE-sensitive data (provided by the user community). It is intended to enable users who search for topics found in scientific and IC/LE data to produce data illustrating the cross-references or intersections between multiple data sources. The results may contain PII of individuals of interest, as the user provided IC/LE data may contain PII.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

BKMS 2.0 utilizes the existing scientific and biodefense-related information, along with the IC/LE data provided by the IC/LE user community. The IC/LE data will not be commercial or publicly available data.

The BKMS 2.0 allows users to search for topics found in both the existing biodefense/scientific data and the IC/LE data to produce data illustrating the cross-references or intersections between the multiple data sources. This ultimately provides IC/LE users with scientific context to their own data and supports their research and analyses.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Privacy Risk: Unauthorized access to the system.

Mitigation: Through the use of its role-based access capability, the BKC ensures that only approved users with an authorized need-to-know are allowed access to IC/LE data records. Only users with access to the BKMS 2.0 system can conduct the analyses and each user must acknowledge the user agreement before using the BKMS 2.0 system. Access to data from the IC and LE is restricted to personnel from the agencies providing the data. Additionally, end users can control and determine which other agencies get access to their data. For example, FBI users can determine which other IC/LE agencies can access their information; BKMS 2.0 does not automatically grant users access to all IC/LE data that is uploaded onto BKMS 2.0. Contributing IC/LE agencies provide privacy and security training to BKMS 2.0 users within their agencies.

Privacy Risk: Unauthorized use of IC/LE data.

Mitigation: All IC/LE users agree to user notices prior to receiving access to BKMS 2.0 stating that no operational decisions will be made based solely on the output of BKMS 2.0. All users must apply their own analyses and expertise to come to their own conclusions. Additionally, the BKMS 2.0 is used to support ongoing investigations; not to initiate investigations on any individuals.

S&T and LLNL may also conduct periodic audits of LE/IC users to ensure that the system is being used appropriately and in compliance with the user agreement. Audits will be conducted also to ensure that only authorized parties have access to the system.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

The IC/LE sensitive data is owned by the IC/LE end user community, and is being included in the BKMS 2.0 for indexing and search purposes. Data and the resulting analyses are retained in the system according to users' needs and legal authorities. Using the BKMS 2.0 capabilities, IC/LE users determine how long data is retained. Information available for retention includes IC/LE data related to current federal/international investigations or analyses, such as IC/LE reports and analyses or information obtained during routine investigations, scientific data, and PII, such as names of subjects of interest or other information associated to that individual. This information may pertain to both U.S. and non-U.S. citizens.

3.2 What is the retention period for the data in the system?

IC/LE data is retained in accordance to the organization from which the data originates.

3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

The IC/LE user will work with the organization and NARA to obtain an approved retention schedule from NARA.

3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Privacy Risk: Data may be outdated, superseded, or incorrect leading to increased likelihood of inaccurate linkages.

Mitigation: Sets of documents uploaded by a user for her personal use within the BKMS are tracked by the date of last update. If the personal archive has not been updated in six months, upon login to the site, the user is presented with a notification that her data could be out-of-date and the user should consider updating or deleting it. This notification is presented at each login until the user updates her document archive or deletes it from the system.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared?

Potential DHS component users of BKMS include personnel from S&T, Office of Intelligence and Analysis (I&A), Customs and Border Protection (CBP), Office of Health Affairs (OHA), and Immigration and Customs Enforcement (ICE). Additional users with an authorized need-to-know may also be included.

S&T determines which DHS components receive access to the BKMS 2.0 based on mission needs and operations. The components determine how and with whom their information is shared. All BKMS 2.0 users must agree to user notices prior to gaining access to BKMS 2.0.

4.2 For each organization, what information is shared and for what purpose?

DHS component users provide their own data to upload into BKMS 2.0. The DHS component user also controls how to share their IC/LE data and analyses. This determination may depend on existing information sharing agreements between agencies as well as legal authority and authorized need to know.

4.3 How is the information transmitted or disclosed?

Unclassified information is transmitted or disclosed via secure Internet-based technology using a web-based interface. Classified information is transmitted using either the HSDN or the JWICS network. This interface is available only to authorized users who log in to the BKMS with user names and passwords provided by BKMS administrators at LLNL after receiving authorization from the BKC Program Manager at DHS S&T. For users of the Top Secret JWICS and Secret HSDN networks, data is further protected by utilizing an IC standard public key infrastructure (PKI) authentication system.

4.4 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy Risk: The IC/LE data and analyses may be used by unauthorized users.

Mitigation: The S&T BKC Program Manager determines which organizations have access to BKMS 2.0 itself. In addition, all users must acknowledge a user notice and agree to the terms prior to gaining access to BKMS 2.0. S&T and LLNL will conduct periodic audits of LE/IC users to ensure that only authorized users with security clearances and a need-to-know are granted access and assigned user account names and passwords to BKMS 2.0. All DHS employees and contractors who are granted access are required to comply with DHS privacy and security requirements.

IC/LE users of BKMS 2.0 determine which agencies and users get access to their own data. This determination is based on user operating legal authorities and authorized need to know for the information.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Potential external users of the BKMS 2.0 may include approved analysts from the U.S. Department of Agriculture (USDA), and Department of Justice (DOJ), and federal agencies that are part of the IC (i.e., CIA). State and local law enforcement and intelligence agencies, and international partners may be potential users and gain access to the BKMS 2.0.

Approved external users have access to all open source and FOUO data contained in the BKMS in performance of official duties. Access BKMS 2.0 is restricted only to users approved by the S&T BKC Program Manager. The external organization providing the data (e.g., FBI or agencies within the IC) determines which organizations can access their own IC/LE data. S&T and LLNL will conduct periodic audits to ensure that the system is being used in compliance with the user agreement and that only authorized users have access to the systems.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The S&T BKC Program Managers only provide the users with the BKMS 2.0 system capabilities; S&T itself does not share this information with any external entities, and does not use this information for any operational purposes. The sharing of information by external organizations is dependent on the user decision and existing data sharing agreements. The user notice requires that all LE/IC organizations acquiring the BKMS 2.0 will go through their own legal and privacy compliance reviews prior to deploying the system for operational use. During this review, the users determine the type of data, including PII, will be uploaded into BKMS 2.0 and ensure all the appropriate documentation, such as the SORN, PIA, and other documentation are completed. IC/LE users of the system will use and share information in accordance with their own SORNs and legal authorities.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

The information in both BKMS 1.0 and 2.0 is transmitted or disclosed via secure Internet-based technology using a web-based interface. This interface is available only to authorized users who log in to the BKMS with assigned user names and passwords. Authorization for user accounts is provided by federal employees of S&T.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Privacy Risk: Unauthorized use by analysts at the external organization.

Mitigation: Only authorized users with security clearances and a need-to-know are granted access and assigned user account names and passwords to BKMS 2.0. All users are required to agree to a user notice and agree to the terms prior to gaining access to BKMS 2.0 for operational use. All users will use and share the IC/LE data in accordance to their own legal authorities and privacy documentation.

Furthermore, IC/LE users upload and access their own data, and it is up to the contributing agency (data owner) to determine how to use and share their information with others IC/LE entities in the community (with a common need to know).

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Individual subjects of the IC/LE-sensitive data may or may not be provided notice at the time of data collection, depending upon the nature of the investigation. The determination of whether to provide notice is made by the data owner, the IC/LE users (not BKC managers) when the IC/LE data is provided to the BKC for inclusion in the BKMS, based on respective legal authority and standard operating procedures.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

The original data owner is responsible for determining whether the individual subjects have the right to decline information.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No. For all instances of the BKMS, including BKMS 2.0, individuals do not have the right to particular uses of the data other than as agreed to when the data is provided or integrated.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Privacy Risk: Individual subjects of the IC/LE-sensitive data are not provided notification that their information is being collected because this could alert bioterrorism suspects to ongoing investigations.

Mitigation: BKMS 2.0 only includes IC/LE information provided by IC/LE analysts, who collect, share, and use this information in accordance with their respective legal authorities. To mitigate risks, IC/LE analysts are instructed to only use the information from BKMS 2.0 solely to support investigations and analysis, and not to use the information as determinative and final. BKMS 2.0 information is one of a number of tools to be used to assist the IC/LE community in the investigative process.

Section 7.0 Individual Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

In the case of the IC/LE data in BKMS 2.0, individuals do not have access to their information because IC/LE data is used for law enforcement or intelligence purposes and therefore exempt from Privacy Act disclosure requirements. Further, BKMS 2.0 does not directly affect an individual's right to benefits. For example, if a known or suspected bioterrorist is placed on a watch list, then it is due to a compilation of intelligence and law enforcement information, and not solely based on BKMS 2.0 data.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Individuals can submit Privacy Act requests to the component owning the inaccurate or erroneous data to correct the information. However, data used for law enforcement or intelligence purposes are exempt from Privacy Act disclosure and correction requirements.

7.3 How are individuals notified of the procedures for correcting their information?

In cases of the IC/LE data in BKMS 2.0, individuals will not be notified of methods of correcting their information because IC/LE data is used for law enforcement purposes and therefore exempt from Privacy Act correction and disclosure requirements.

7.4 If no formal redress is provided, what are alternatives are available to the individual?

For BKMS 1.0 (approved under the Portals PIA), formal redress is available via the FOIA mechanism described in the published PIA found at www.dhs.gov/privacy. No additional redress mechanism is provided for the IC/LE data.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Privacy Risk: Given the IC/LE nature of the information included in BKMS 2.0, individuals do not have access to their data.

Mitigation: The data owners are responsible for updating and maintaining accurate information pertaining to individuals listed in BKMS 2.0.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

All user accounts are approved as follows:

- Accounts of LLNL personnel may be created only after approval by management of the BKC, the LLNL entity, based on requirements of the users' official duties.
- Accounts of non-LLNL personnel (e.g., personnel from DHS or other agencies, including all IC/LE personnel) must be approved by DHS S&T Program Managers of the BKC program, and also are based on requirements of official duties.

After approval, BKC IT staff creates the accounts with the approved roles. The names, identities and roles of the account holders are maintained by the BKC network administrator.

There is no public access to the BKMS. All users must be registered users with appropriate usernames and passwords. Within the BKMS, the username will be assigned the appropriate approval for specific information access. DHS management of the BKC, with BKC administrators will assign roles and responsibilities to approved users. The classified systems have restrictions to ensure that only approved users' access the networks.

For the IC/LE data contained in the BKMS 2.0, roles are used to limit access to authorized users with the proper need to know of the data in order to perform their official duties, within their legal authorities. The IC/LE data owner controls how she shares her information, and with whom she shares it.

8.2 Will Department contractors have access to the system?

Yes. DHS contractors may provide support to U.S. Department of Energy (DOE) National Laboratories (Livermore, Los Alamos, Sandia); the Battelle National Biodefense Institute (BNBI) and the Homeland Security Institute (HSI), which both operate federally funded research and development centers (FFRDCs); the National Biosurveillance Integration System (NBIS); and the Office of Intelligence and Analysis (I&A).

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

IC/LE personnel that have access to the BKMS 2.0 are required to complete privacy and security training prior to obtaining access to the system. The agencies providing the IC/LE-sensitive data are responsible for conducting such training programs.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes, under LLNL's Master Security Plan for unclassified computing, LLNL-MSP-GSS-01. Certification & Accreditation was last completed in 2010, and is valid until 2013. Addition of IC/LE data does not change the C&A requirements for the BKMS, as the BKMS was built from the ground up to incorporate multiple levels of data from multiple organizations.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

The BKMS maintains logs of approved users who have accessed the system and performed queries. BKMS administrators at LLNL review logs to ensure no unauthorized users have accessed the system as well as to ensure proper system operation and code surety. BKMS administrators also perform periodic (every six months) password resets. If a user does not reset his password, the account is locked. On the classified networks, there is a yearly account audit as well. The audit ensures that only active users with appropriate and continued need have access to the system.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy Risk: A privacy risk could be the loss of information due to breaches in security.

Mitigation: To mitigate this risk, the BKC implements access control procedures and policies. The BKC has also implemented policies to control access to the facility housing the BKMS, as well as to the network on which it resides. These include:

- Providing limited, secure access from a public Internet entry point through the use of an encrypted channel to the BKMS application server. A firewall restricts network access, and a user directory system authenticates user account access.
- Upon access to the BKMS URL (https://bkms.llnl.gov), the user is immediately challenged for his or her account and password. User access membership is provided only upon authorization by appropriate management, i.e. LLNL management for LLNL personnel or DHS S&T management for other users. The list of cleared personnel for the restricted IC/LE information is maintained by DHS managers of the BKC and the BKC network administrator, who also have a need to know and appropriate clearance.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

The BKMS was built from the ground up by the BKC at LLNL for DHS S&T as a web-based initiative that integrates a variety of biodefense-related information and presents it to web-based users in intuitive ways. The database of biodefense-related information is available 24/7 via secure websites at three classification levels to users approved by S&T.

DHS S&T is developing the next generation of the BKMS (BKMS 2.0): the integration of the existing biodefense-related data in the current system with new IC/LE -sensitive data to be used by the IC/LE community. The goal of this integration is to highlight to analysts in the IC/LE community intersections contained within biodefense data and intelligence and law enforcement data that might not otherwise have been apparent if these disparate data sets were not integrated. These new data will extend the capabilities of the current, science-focused BKMS by providing context and information to IC/LE analysts who otherwise would not have the opportunity to correlate these data.

9.2 What stage of development is the system in and what project development lifecycle was used?

The BKMS is simultaneously an operational system (available to end-users seeking to understand the biodefense landscape) and a research platform (for new technology components incorporated to take advantage of the state of the art in database and web technology). It was developed in accordance with the DoD's 6.X lifecycle.

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

The BKMS main engine is a state of the art data indexing (i.e., categorizing) engine with the capacity for secure data transfer and viewing. Its data transmission mode is secure web-based transfer available at three classification levels. It is based on technology that permits data to be indexed according to any number of classification schemas, such as person, place, and thing; this permits potentially sensitive personal information to be easily segregated from non-PII data. It also minimizes privacy concerns by requiring users to present their credentials upon each logon, and has the ability to further segregate data for presentation to users according to the users' roles, which are maintained in a well-known, commercial user directory system. The BKMS employs these technologies specifically because they permit the levels of granularity and security required for a technology platform intended to support U.S. government users who need to understand biodefense information while retaining data integrity and security.

Responsible Officials

David Shepherd
Program Manager, Threat Vectors Analysis
Threat Characterization and Attribution
S&T Chem-Bio Division
Department of Homeland Security
202.254.5897

Approval Signature Page

Original signed copy on file with the DHS Privacy Office

_____

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security