Privacy Impact Assessment
for the

Integrated Common Analytical Viewer (Sensitive but Unclassified)

(iCAV SBU)

March 29, 2010

Contact Point
Michael Clements
National Protection and Programs Directorate
Infrastructure Visualization Branch
703-235-3911

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

Abstract

The Department of Homeland Security (DHS) National Protection and Programs Directorate (NPPD) implemented the Integrated Common Analytical Viewer (iCAV SBU), a sensitive but unclassified, secure, web-based, geospatial visualization tool that integrates commercial and government-owned data and imagery from multiple sources enabling homeland security partners to establish comprehensive situational and strategic awareness across the nation and around the globe to better prepare for, prevent, respond to and recover from natural and man-made disasters. This privacy impact assessment (PIA) was performed to analyze and evaluate any privacy impact resulting from the use of visualization technology.

Overview

In 2003, Homeland Security Presidential Directive-7 (HSPD-7) directed the Department of Homeland Security (DHS) to "geospatially map, image, analyze, and sort" the nation's Critical Infrastructure and Key Resources (CIKR) to assist in providing a comprehensive understanding of the national infrastructure risk environment. HSPD-7 established U.S. policy for enhancing CIKR protection by establishing a framework for national infrastructure protection partners to identify, prioritize, and protect the nation's CIKR from terrorist attacks. Within DHS, the Office of Infrastructure Protection, a sub-component of NPPD, is the office charged to fulfill this directive.

iCAV SBU responds to the requirements of HSPD-7 by providing federal, state, and local homeland security organizations with an advanced mapping tool that provides the ability to geospatially map, image, analyze, and sort information regarding CIKR. iCAV SBU utilizes commercially and publicly available maps, and allows authorized users to layer different datasets from the Homeland Security Infrastructure Program (HSIP) database and other publicly and commercially available datasets to build a more comprehensive view of CIKR sites. The HSIP database includes information about emergency services, commercial and government facilities, public venues, public utilities, telecommunications, as well as chemical, energy, transportation, and industrial sites. Incorporating iCAV SBU with HSIP creates an improved geospatial context for situational and strategic awareness across the nation and U.S. territories and holdings around the globe that allows better preparation for, prevention of, and response to natural and man-made disasters. Data hosted on and distributed from iCAV SBU does not contain personally identifiable information (PII) but it is possible for users to view PII from external data feeds and streams through iCAV SBU. Therefore, the ability to overlay multiple datasets (including external data feeds and streams with personal information) and visualize them, make iCAV SBU a privacy sensitive system.

iCAV SBU serves DHS and the broader federal, state, and local infrastructure protection community through the Homeland Security Information Network (HSIN).[1] HSIN is a comprehensive, nationally secure and trusted web-based platform able to facilitate Sensitive But Unclassified (SBU) information sharing and collaboration between federal, state, local, tribal, private sector, and international partners. The HSIN platform was created to interface with existing information sharing networks to support the diverse communities of interest engaged in preventing, protecting from, responding to, and recovering from those threats, hazards and incidents that fall under the purview of DHS. Users with access to the HSIN system also have access to iCAV SBU. Once a user is vetted and allowed access to the HSIN system, a HSIN username

[1] HSIN Communities of Interest PIA, June 22, 2007.
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_hsin.pdf.

and password allows access to the tools in iCAV SBU. iCAV SBU is the primary situational awareness tool for visualization of geospatial CIKR data during steady-state and surge events.

iCAV SBU stores only HSIP infrastructure and geospatial data (including feature maps and imagery), for which the primary source is CIKR data collected through, and associated with, the HSIP and its dataset: a unified infrastructure geospatial data inventory assembled by the National Geospatial Intelligence Agency (NGA) in partnership with DHS, Department of Defense (DoD), and United States Geological Survey (USGS). The HSIP dataset is used by DHS and other organizations that support the DHS homeland security mission to increase readiness and knowledge about potential threats and vulnerabilities to the nation, and to reduce response and recovery times in the event of a natural or terrorist-caused disaster. DHS and more than a dozen other federal agencies support the HSIP database for the purpose of identifying infrastructure in the following areas: agriculture and food, banking and finance, communications, industry, energy, information technology, national monuments and icons, transportation, water, and public safety. Due to licensing restrictions, there are two HSIP datasets provided through iCAV SBU: *HSIP Gold* for employees of the federal government, and *HSIP Freedom* for state and local officials that support homeland security missions.

DHS Earth is a data feed service of the HSIP dataset usable on two-dimensional maps and three-dimensional earth browsers and available to all users with a valid HSIN user name and password. DHS Earth is not an IT application or tool, but is a CIKR, geospatial, and situational awareness data feed that is provided as a value-added service through iCAV SBU in the KML data format that Google Earth and other similar software applications can read. DHS Earth combines all of the CIKR and geospatial data stored locally within iCAV SBU with a number of static and dynamic data feeds provided primarily by other federal agencies (including weather, wildfire, hurricane, seismic, flood gauge, and population density data) to create a comprehensive national infrastructure situational awareness data stream.

iCAV SBU tools allow authorized users to add additional data from external sources to tailor their view so upon signing onto iCAV SBU users are warned to not use any of the tools to overlay and/or visualize datasets containing PII. iCAV SBU users who access external data feeds may only access feeds through the Internet connections on local equipment (and not through iCAV SBU architecture), and any external data resulting from the access resides on local equipment for the duration of the session only, then is deleted as soon as the session ends. With DHS Earth, users can create local "mashups" on local equipment that may include DHS Earth and/or other external services but external data sources are accessible only with local equipment, and only for the duration of the individual user's session.

iCAV SBU allows authorized users to share links to other sites (except external data sources) with other authorized HSIN users. To view a link, the recipient user must enter an approved HSIN user name and password. To save the link for later viewing, the user may create a bookmark in the system. A user may also export a current map view and save it as a .jpg file. Currently, iCAV SBU does not support exportation or sharing of user-added content from external sources.

The following example illustrates how an authorized state or local user might use iCAV SBU for situational awareness by building specific views in the event that there is a train derailment near critical infrastructure, an authorized user could log into iCAV SBU with a user name and password to search for the specific area of the derailment (i.e., Wilmington, DE). Once the derailment area is located, the user may click-on and drag the map by selecting a navigational arrow. The user can then change the zoom level of the view to see more detail if necessary. iCAV SBU uses commercially available software, so the level of

granularity and detail on the map is the same as is available to the public. To view data layers related to chemical infrastructure and transportation, the user could click on the chemical data and transportation layers under the HSIP dataset to view chemical plants and rail lines in the derailment area. Additionally, once the user selects the appropriate view of the area, he/she can change the view to a 'street' view, and toggle between street-based and imagery-based views to better visualize scenarios and conduct a vulnerability analysis. From the HSIP data layers, iCAV SBU can be used to identify any critical assets that might be impacted, such as area schools, major transportation routes, and/or local emergency response services. The user might use the public health overlay along with the distance tools to visualize the proximity of the local trauma hospitals to the location of the derailment.

The primary risk presented by the iCAV SBU suite of tools is the potential to overlay multiple datasets, including those that contain PII, visualize them, and use the view for purposes unrelated to protecting the nation's CIKR. There is also a privacy risk presented by the granularity of images available to a user through iCAV SBU. To mitigate these risks, iCAV SBU contains a warning (see Appendix I), that warns users that the tool may not be used to overlay and visualize datasets containing PII and reiterates that iCAV SBU was created to serve as "a geospatial visualization tool designed for homeland security partners to assist them in protecting the nation's critical infrastructure and key resources." Since iCAV SBU uses only commercially available data to create maps, the images have the same level of granularity and detail that are available to the public so the tool does not present any additional privacy risk.

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?

iCAV SBU allows for one-way dissemination of CIKR data to authorized users who have been assigned valid HSIN user names and passwords. The primary source of data for iCAV SBU is associated with the HSIP dataset which identifies infrastructure in the following areas: agriculture and food, banking and finance, communications, industry, energy, information technology, national monuments and icons, transportation, water, and public safety. In addition, iCAV SBU makes use of commercially available maps and allows authorized users to layer different datasets from the HSIP database as well as other external datasets provided by individual users. Only the HSIP infrastructure data and geospatial data, including feature maps and imagery of most of the areas of the U.S., can be stored on iCAV SBU. Although iCAV SBU does not collect PII, and the HSIP dataset does not contain it, the capability exists for users to visualize their own external datasets including those that may contain PII.

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

The HSIP data is provided by the Homeland Infrastructure Foundation Level Data (HIFLD) Working Group, which is funded and managed jointly by DHS, NGA, DOD Defense Critical Infrastructure Program, and the USGS, and contains data encompassing over 350 unique infrastructure data layers (such as police stations, fire stations, hospitals, electric transmission lines, power plants, road and rail networks, chemical

production facilities, financial institutions, etc.). HSIP data is obtained through a number of sources via the HIFLD working group, including purchase from commercial data vendors and data sharing agreements with numerous federal, state, and local governments, as well as through a number of static and dynamic data feeds provided primarily by other federal agencies (including weather, wildfire, hurricane, seismic, flood gauge, and population density data).

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

iCAV SBU responds to the requirements of HSPD-7 by providing federal, state, and local homeland security users with an advanced mapping tool that provides the ability to geospatially map, image, analyze, and sort information regarding critical infrastructure and key resources.

1.4 How is the information collected?

iCAV SBU does not collect information, but functions as a "data viewer" for infrastructure data.

1.5 How will the information be checked for accuracy?

iCAV SBU does not have the capacity to check sources for data accuracy. However, as the primary source of iCAV SBU data, the HSIP dataset is checked for accuracy on a near daily basis by the HIFLD Working Group and at the end of each calendar year by iCAV SBU system users. Additionally, the HIFLD Working Group publishes an updated HSIP version consisting of the previous year's version plus any corrections and/or updates generated through their near-daily data checks that when published, is incorporated into iCAV SBU.

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

iCAV SBU responds to the requirements of HSPD-7 directing DHS to "geospatially map, image, analyze, and sort" the nation's CIKR to help provide a comprehensive understanding of the national infrastructure risk environment. iCAV SBU provides authorized federal, state, and local homeland security officials with a commercially available advanced mapping tool that allows viewing of infrastructure data from various sources, including the HSIP dataset, commercial data vendors, and data sharing agreements with numerous other federal, state, and local governments.

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

There is the risk that the iCAV SBU suite of tools could be used to overlay multiple datasets, including those that contain PII. To mitigate this risk, iCAV SBU contains a warning (see Appendix I), that warns users that the tool is not to be used to overlay and visualize datasets containing personally identifiable information. In addition the warning states that the system "is a geospatial visualization tool designed for homeland security partners to assist them in protecting the nation's critical infrastructure and key resources." Before authorized users gain access to the HSIN system, they agree to comply with the

policy governing acceptable use in addition to the Rules of Behavior for accessing any DHS system.

Section 2.0 Uses of 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.

iCAV SBU serves as a single portal to consolidated, authoritative and vital national-level CIKR and multiple situational awareness data for infrastructure protection planning, response, and recovery, and is critical in facilitating decision making associated with emerging events or incidents.

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

iCAV SBU architecture is designed to allow users to rapidly view infrastructure-related geospatial data, but some non-complex analytical inquires may be performed to identify some trends and/or threats.

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

iCAV SBU does not host, store, or otherwise use commercial or publicly available datasets that contains PII. iCAV SBU primarily uses the HSIP dataset, which is only available to authorized federal, state and local users. iCAV SBU also uses other publicly and commercially available maps, and a number of static and dynamic data feeds provided primarily by other federal agencies (including weather, wildfire, hurricane, seismic, flood gauge, and population density data) to create a comprehensive national infrastructure situational awareness data stream.

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.

iCAV SBU was developed to support homeland security partners to achieve their homeland security mission of protecting critical national resources and infrastructures. To ensure the use of iCAV SBU is consistent with this purpose, a warning (see Appendix I), advises users that the tool may not be used to overlay and visualize datasets containing PII and reiterates that iCAV SBU was created as "a geospatial visualization tool designed for homeland security partners to assist them in protecting the nation's critical infrastructure and key resources." Additionally, iCAV SBU does not host, store, or otherwise use government, commercial or publicly available datasets that contains PII.

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?

iCAV SBU allows users to visualize the HSIP dataset and other commercially and publicly available datasets but does not retain any visualized images. The HSIP dataset is updated on an annual basis by the HIFLD working group then uploaded to iCAV SBU. Any other commercially and publicly available datasets that may be visualized through the tool are never stored or retained.

3.2 How long is information retained?

iCAV SBU does not retain images visualized through the tool.

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

iCAV SBU does not have a retention schedule because it does not retain images.

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 risks are mitigated because iCAV SBU does not store or retain HSIP datasets indefinitely, and because HSIP datasets do not contain PII. Additionally, iCAV SBU does not store or retain images visualized by users.

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, what information is shared and for what purpose?

iCAV SBU utilizes HSIN as its credentialing mechanism so authorized DHS users who have access to the HSIN system also have access to iCAV SBU. Authorized DHS users of both systems may share visualizations between each other.

4.2 How is the information transmitted or disclosed?

iCAV SBU allows authorized users to create a view within iCAV SBU on their local computer and to share that view with other iCAV SBU users via an HTML link. The shareable link does not provide direct access to the originator's computer to see the originator's view. Rather, the link provides the recipient's web browser a set of directions describing the geographic area being viewed in the originator's web browser, as well as any iCAV SBU data layers being viewed within that geographic context. These sharable links are only viewable to other authorized iCAV SBU users, and the links are only valid for the duration of the originator's browsing session. When that session ends, the link no longer works. Additionally, if the originator's view includes a link to data from a source, such as an external data feed, other than iCAV SBU, the sharable link will not include directions for accessing that external data feed.

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

Privacy risks associated with internal sharing are minimal because iCAV SBU does not collect or disseminate any PII and any sharing of the images visualized through the tools is limited to other authorized HSIN users.

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?

The purpose of iCAV SBU is to increase information sharing for homeland security purposes, therefore, access to the system is limited to only those federal, state or local government officials serving in an organization that supports the DHS homeland security mission and requiring access to fulfill an official duty, or to private sector infrastructure owners and operators who have been granted access to the HSIN Critical Sectors portal.

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.

iCAV SBU does not collect, maintain, or disseminate PII and its use does not create a system of records covered under the Privacy Act.

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

The security measures that safeguard the sharing of links to other sites outside of DHS with other authorized HSIN users include several layers of physical access controls which include the use of a user name and password, and IT safeguards such as firewalls, intrusion detection appliances, and log file monitoring. System users utilize a secure-internet connection using a DHS-owned and operated network.

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

Privacy risks associated with external sharing are low because iCAV SBU does not collect or disseminate any PII and any sharing of the images visualized through the tools is limited to other authorized HSIN users.

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?

Notice is not required since iCAV SBU does not collect or maintain PII. However, a PIA was conducted to provide notice and transparency into the uses of iCAV SBU because the capacity exists to overlay and visualize multiple datasets (including external data feeds and streams that may contain PII).

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

iCAV SBU does not collect information from individuals.

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

As noted above, iCAV SBU does not collect information from individuals.

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.

Although iCAV SBU does not collect information from individuals, the capacity exists to overlay and visualize multiple datasets, including external data feeds and streams that may contain PII. Therefore this PIA was conducted to provide notice and transparency into the capabilities and uses of iCAV SBU.

Section 7.0 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?

iCAV SBU does not collect, use, or store information regarding individuals.

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

As the primary data source for iCAV SBU, the HSIP dataset is checked for accuracy by the HIFLD Working Group on a near daily basis, and at the end of each calendar year an updated HSIP version is incorporated into iCAV SBU so information is maintained to be as accurate and useful as possible.

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

iCAV SBU does not collect information from individuals.

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

Individuals may contact the NPPD Privacy Officer by directing correspondence to NPPD Privacy Officer, 245 Murray Lane SW, Arlington, VA 20598-0380.

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

Formal redress is not provided because iCAV SBU does not collect information from individuals, but individuals with concerns are encouraged to contact the NPPD Privacy Officer at the address above.

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?

iCAV SBU leverages the HSIN system for credentialing and verification. All iCAV SBU users require HSIN identification and need-for-access validation, which is granted by each HSIN portal owner based on the specific access criteria established for their portal. HSIN portal administrators are responsible for granting access, determining the level of information access needed, and maintaining a current comprehensive user list. Within DHS, before access is granted, users must have access to the DHS secure network, and have a signed user access agreement with supervisor certification that access is needed for official duties. User access agreements include rules of behavior regarding responsibilities for safeguarding information and the consequences and accountability for failure to do so. Before unique user accounts are assigned, all user access requests are approved by the system Information System Security Officer.

8.2 Will Department contractors have access to the system?

Contract technicians and operational managers with responsibilities for ensuring system performance and proper use are registered and given appropriate role-based access. Additionally, contractors supporting federal, state, and local government officials in the execution of their official duties can be granted access to the system as long as a government official can validate the contractor's need for access.

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

All DHS personnel must complete comprehensive privacy training prior to system access, and thereafter pass annual refresher training to retain access. Other authorized users of iCAV SBU are subject to privacy training requirements as established by their respective organizations.

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

Yes. Certification and accreditation for iCAV SBU has been completed and is valid until 2011.

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

iCAV SBU is located behind the DHS Trusted Internet Connection which incorporates robust and multi-layered physical access controls and IT safeguards such as firewalls, intrusion detection appliances, and log file monitoring to not only prevent unauthorized physical access to iCAV SBU, but also to monitor and protect the network and all the data stored within.

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?

Given that iCAV SBU does not collect, maintain, or disseminate PII privacy risks are considered minimal and are appropriately mitigated through the controls described in section 8.5.

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?

iCAV SBU is a growing legacy system/major application operating under a valid Authority to Operate.

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

iCAV SBU has been fully functional without interruption since 2004 and is currently operating in the maintenance phase of its operating life cycle.

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

Government use of visualization technology inherently raises privacy concerns related to the potential for domestic surveillance. In consideration of these concerns, safeguards were built into iCAV SBU to minimize risk. Users are warned upon signing into iCAV SBU that the tool is not to be used to overlay and visualize datasets containing PII. Also, users who access external data feeds may only access feeds through the Internet connections on local equipment (and not through iCAV SBU architecture), and any external data resulting from the access resides on local equipment for the duration of the session only, then is deleted as soon as the session ends. Lastly, iCAV SBU uses only commercially available data to create maps and images with the same level of granularity and detail that are available to the public.

Responsible Officials

Michael Clements
National Protection and Programs Directorate
Infrastructure Visualization Branch
Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security

Appendix I

iCAV SBU Log-on Notice

WARNING: FOR OFFICIAL USE ONLY

You are about to access a U.S. Government computer system. Access to this system is restricted to authorized users only. Individuals who accesses this system without authorization, or exceeds authorized access, could be subject to a fine or imprisonment, or both, under Public Law 98-473.

By accessing this system, you consent to having your activities and or accesses recorded by the system software and periodically monitored. If this record reveals suspected unauthorized use or criminal activity, the evidence may be provided to supervisory personnel and law enforcement officials.

This is a geospatial visualization tool designed for the use of homeland security partners in protecting the nation's critical infrastructure and key resources. This tool may NOT be used to overlay and/or visualize datasets that contain personally identifiable information.

THE PROCESSING OF CLASSIFIED OR PERSONALLY IDENTIFIABLE INFORMATION IS STRICTLY PROHIBITED