Privacy Impact Assessment
for the

National Infrastructure Coordinating Center INSight Application

November 23, 2007

Contact Point
Chris Anderson
Deputy Director, National Preparedness and Programs Directorate, National Infrastructure Coordinating Center, Contingency Planning and Incident Management Division
Department of Homeland Security
(703) 563-3212

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The National Infrastructure Coordinating Center (here after refer to as the NICC), part of the National Operations Center (NOC) in the Operations Directorate, operates the INSight Information Management System (INSight), designed to support the identification of potentially significant changes in the operational status of the nation's Critical Infrastructures and Key Resources (CI/KR) so that trained analysts can provide timely coordination with the NOC, respective Information Sharing and Analysis Centers (ISAC), and other involved agencies in the public sector and federal sectors. INSight may collect personally identifiable information (PII) associated with infrastructure information; accordingly NICC has conducted this privacy impact assessment (PIA).

Introduction

The NICC is a component of the Department of Homeland Security's (DHS) NOC and is functionally aligned under the National Preparedness and Programs Directorate, Crisis Planning and Incident Management Division. The mission of the NICC is to maintain awareness of the operational status of the nation's CI/KR as defined by the *National Infrastructure Protection Plan*.[1] The NICC uses the information to provide status and impact reports on the nations CI/KR operational status to the DHS NOC, other federal agencies, and commercial organizations. DHS uses this information to build the operational status of CI/KR sites in the DHS Common Operational Picture (COP).[2] Maintaining operational awareness is a 24 x 7 mission, and the NICC performs this mission by serving as the communication and coordination point between DHS and all private sector owners and operators of CI/KR, sector specific agencies, state and local entities, regional partners, and individual private citizens.

The INSight system is designed to support the identification and management of potentially significant changes in the operational status of the nation's CI/KR so that trained NICC analysts can provide timely coordination with the NOC, respective ISAC's, and other involved agencies in the public sector. Significant changes in the operational status of the nation's CI/KR would be: a major power outage that effects numerous locations and in effect disrupts or causes delays in the development, manufacture or delivery of goods and or services; a large weather disturbance (e.g., hurricane or tornado) that affects the ability of a commercial organization(s) to produce goods required to support critical infrastructures. Although other possible examples are too numerous to name, a simple example would be a hurricane that disrupts the service of or capability of commercial oil and or natural gas companies to run oil or gas producing rigs in the Gulf of Mexico.

INSight supports the NICC mission and major functions of the NICC by providing automated tools that allow trained personnel to record, manage, and monitor information reported to the NICC. This collective information allows the NICC to report potentially significant changes in the operational status of the nation's CI/KR to the NOC as well as other federal agencies and the private sector. Part of the NICC's operations include the retention and use of PII associated with CI/KR, whether the PII be on individuals associated with analysis or investigation, or individuals with whom the Department may contact regarding updates or bulletins concerning CI/KR.

INSight provides the capabilities to manage, monitor, and analyze relevant data from government and commercial sources, both open and sensitive in nature. All information in the INSight

[1] http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
[2] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_hsind.pdf

system is considered sensitive but unclassified. The INSight system is designed to contain Protected Critical Infrastructure Information (PCII) that is provided by private sector owners and operators.[3] The database component of INSight uses a relational database for the retention and management of all system data elements fields and records. A basic description of how the NICC's INSight commonly operates is as follows:

As an example, INSight might receive an email alert from the National Response Coordination Center that identifies a life threatening chemical leak has been reported by a commercial organization. The NICC would then contact the required commercial and federal organizations directly to obtain an initial impact assessment as to the event's impact of critical infrastructure in the area of the incident. The NICC would then create a SPOT report within the INSight system with the required critical reporting information. The NICC would use the INSight capabilities to report this information directly to the DHS NOC Watch Staff.

An example of how PII may be used in INSight would be as follows:

The NICC might receive a suspicious activity report from one of the private sector owner and or operators, or the National Response Coordination Center, stating that certain individuals had sought unauthorized access to a chemical plant in a certain geographic location. Descriptive information about the individuals, including any available biographic information, would be distributed to other critical infrastructure sites and/or law enforcement personnel in order to prevent these individuals from attempting to access other facilities as well as to prevent the methods attempted for unauthorized access to be repeated. The sharing of PII in these circumstances increases the protection of the nation's CI/KR.

Section 1.0 Characterization of the Information

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

CI/KR information makes up the significant amount of information retained and used by INSight. The CI/KR information contained in INSight consists of:

- Infrastructure operational information such as contact information for federal and privately owned critical infrastructure owners and operators and reports and analysis of past events that affected critical infrastructures.
- Data related to events affecting the nation's CI/KR such as date and time of an incident, persons reporting the incident, how the incident affected critical infrastructure operational capabilities, and ultimately any reports generated by the NICC staff using INSight in respect to the incident or event.
- Information and reports about events and or individuals that could pose an impact to the nation's CI/KR, such as detailed description of the person or persons involved in suspicious activity (e.g., make/model of vehicle driven by individuals with certain characteristics, or suspicious individuals photographing key infrastructure sites)
- Information considered to be PCII in nature such as the proprietary processes used by private or commercial companies in the conduct of their normal business processes. This includes but is not limited to plant locations, processes of production, and delivery of goods.

[3] The PIA for the PCII Program is at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_pcii.pdf.

- Public-source data (media reports, including periodicals, newspapers, internet, broadcast transcripts and publicly available collections of data related to specific companies, industries and or individuals.)
- Law enforcement and intelligence investigation information, such as the name of an individual on a reported terrorist watch list.
- Information systems security analysis and reporting such as a reported vulnerability in the processes or methods used by an organization in producing its products.
- Historical law enforcement information such as a historical report on an event that occurred and the resolution of the investigation into the event.
- Operational and administrative records such as an organizations ability to respond to a given electrical outage that affects their ability to produce or deliver goods.
- Financial information such as an organization's reported impact to their business process or delivery of goods over the period that the business was impacted by a severe weather system.
- Other information received from agencies and components of the Federal Government, foreign governments, organizations or entities, international organizations, state and local government agencies (including law enforcement agencies), and private sector entities or individuals such as questions asked of the NICC prior to, during or in recovery of a major event that impacted a geographical area and the business.

Specifically related to the privacy of individuals, two separate types of PII may be collected or used within INSight: PII related to individuals named in reports or other analytical or investigative materials, and PII related to individuals associated with CI/KR or on contact lists related to CI/KR.

PII on individuals related to analytical or investigative materials

This information consists of descriptive information about the person or person(s) that were observed in a suspicious behavior associated with and or around a CI/KR. An example of this would be a report from a commercially owned and operated oil refinery where a security guard observed a person of white race, medium build, with dark hair, in a white ford vehicle, license plate # 99-999-999 taking pictures of the refinery itself.

The NICC records this information within INSight and ensures that this information is provided to the DHS offices and watches that provide more investigative details and or tips to other DHS offices and or the Critical Infrastructure owners and operators themselves.

The information from the original suspicious activity report is placed into INSight. The INSight system then generates a report that is forwarded to the DHS NOC where the State local Fusion Desk, and others begin to look at this information for interest. The information contained in INSight is not limited to relevant information for which there is considered to be a nexus of terrorism. Since the mission of the NICC is not purely terrorism specific, much of the information is related to man made or natural events that have the ability to impact the nation's CI/KR operational status, or relate to the recovery of national CI/KR after an event has occurred.

PII related to contacting individuals associated with CI/KR

This information consists of name, organization, phone number, country, state, county, street address, location of company, associated PCII sector, email, pager number and means of transmission of information. This information is stored in a separate database component which contains all federal, private, and corporate contact information. This information is used to support the NICC's mission of providing emergency notifications to the federal and private / commercial owners and operators of national CI/KR. This information further supports the NICC in the coordination of daily information sharing between DHS and the owners and operators of CI/KR.

Limited data concerning the providers of information, including the means of transmission, the organization's direct phone number, emails and/or other communication assets (pagers, cell phone numbers where relevant or necessary) and contact information, (such as the company's name, company operational watch centers, officers and or regulator reporting officials within the organization. An example would be the security officer of a particular commercial company, or the name and telephone number of a federal organizations operations center), and the CI/KR relationship between the sender and the data itself may also be retained where necessary. For example, where it is determined that information is related to a specific agencies' responsibility such as a Sector Specific Agency, responsible for regular reporting on a given CI/KR and that individual's name, contact information to include address, email address, phone number etc. and date of information provided will be maintained in the INSight system to provide an indicator of the reliability and validity of the data provided.[4]

This information is captured in the INSight system so as to support the awareness and reporting of potential infrastructure impacting events. This information is not collected by the NICC Watch Staff and placed into the INSight system. Rather this information is provided by voluntary reporting, reporting from other commercial or federal watch centers.

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

- Infrastructure operational information is provided by: Federal organizations Operations Watch Centers, Commercial Owners and Operators of Critical Infrastructures, Other DHS Watch and Operations Centers, as well as open source freely available news services and internet web sources. Some information is also provided by the reporting and communication portals of the DHS HSIN system and supporting DHS databases.
- Data related to events affecting the nation's CI/KR is provided by individual CI/KR system owners and operators, other federal watch centers, open source news sources, and DHS watch centers.
- Information about events and or individuals that could pose an impact to the nation's CI/KR is provided by individual CI/KR system owners and operators, other federal watch centers, State and Local Law Enforcement Watch Desks in DHS, open source news sources, and DHS Intelligence and Analysis watch centers.
- Information considered to be PCII in nature is provided by commercially owned and operated organizational watch and security centers.
- Public-source data including media reports, periodicals, newspapers, internet, broadcast transcripts and commercial databases. The NICC and INSight do not currently use or access any commercially provided owned or operated database sources. However, as the needs require in the future, the NICC may need or require access to these types of information sources.
- Suspicious activity information reported by private organizations and entities is provided by private sector owner and operators and other federal operations centers

[4] Sector Specific Agencies are : Department of Energy, Department of the Interior, Food Drug and Alcohol Administration, United Stated Department of Agriculture, Federal Emergency Management Agency, United States Army Corps of Engineers, Department of Homeland Security, Department of Transportation, Department of Health and Human Services, United States Postal Service, Department of Commerce, Department of Defense

- Intelligence analysis and reporting is provided by other DHS NOC departments and other Federal watch operations centers.
- Ongoing law enforcement investigative information is provided by state, regional, and DHS NOC intelligence fusion desks and centers.
- Information systems security analysis and reporting is provided by commercially provided information systems security watch centers, DoD and Federal information security watch centers, and the DHS CERT operation center.
- Historical law enforcement information is provided by state, regional, and DHS NOC intelligence fusion desks and centers.
- Operational and administrative records provided by DHS Watch centers, Commercial CI/KR watch Centers
- Financial information is provided by the Federal Information Security watch Center

Information is obtained by contact with private company's operations centers, individual person wishing to make reports, federal organization's watch and operations centers, other DHS reporting components, publicly available web pages that contain news, company information, and or industry related reported open source materials.

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

NICC uses the information in the INSight system to access, receive, analyze and coordinate information, and other communications to integrate such information in order to identify and assess the nature and scope of natural, terrorist or other threats to the nations CI/KR.

1.4 How is the information collected?

All information is collected from telephone calls, face to face contact and conversations, open source news services, standardized event reporting from external entities, and forwarded emails. All information entered into the system is manually reviewed prior to entry in to the database.

1.5 How will the information be checked for accuracy?

All information is verified by trained NICC personnel for relevance to the CI/KR sectors and accuracy prior to being entered into the system. Management of the data within the database is restricted to valid users based upon their roles and enforced by role based rules. Management of the data within the supporting Oracle database at the record and field levels is restricted to the development / maintenance team members who also audited for any and all access and changes to the data.

Prior to inclusion in INSight, information is reviewed by NICC personnel to ensure its relevancy to national CI/KR. During this review further quantitative information is added by NICC personnel to ensure accuracy and to determine any potential nexus to terrorism. All information is separated based on sector, event, subject matter, geography, and need to know.

The information contained in INSight is not limited to relevant information for which there is considered to be a nexus of terrorism. Since the mission of the NICC is not purely terrorism specific, much of the information is related to man made or natural events that have the ability to impact the nation's CI/KR operational status, or relate to the recovery of national CI/KR after an event has occurred.

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

The Homeland Security Act of 2002 as codified within the United States Code at 6 U.S.C. § 121(d)(1); 6 U.S.C. § 121(d)(4); 6 U.S.C. § 121(d)(11); 6 U.S.C. § 121(d)(12)(A); 6 U.S.C. § 121(d)(15); and 6 U.S.C. § 121(d)(17) provide DHS and the NICC (as part of the National Operations Center (NOC) with authority to collect the information in the INSight System.

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

For the most part, the information collected as part of the INSight system will not be personally identifiable. In instances where PII is relevant and necessary to the analysis of CI/KR information or the operational awareness of CI/KR sites, the PII will be protected with additional safeguards so that only those individuals with appropriate access and a verifiable need to know will be able to review the PII collected.

For example, INSight has been developed in order to minimize the amount of personal information incorporated. In instances where personal information is required, a mask is placed on the information so that it may only be viewed by appropriate personnel with the correct user roles and verifiable need to know. This ensures that privacy and information safeguarding requirements are met by limiting access to sensitive information, such as PII, only to those users whose operational role and mission warrants such access. This limitation is further enforced by ensuring that the data is distinctly segregated into sections based upon its sensitivity.

This masking process, along with other access controls detailed in Section 8.0, mitigate the risk that unauthorized user may view PII. Because INSight uses a large amount of information, even though not all of it is PII, INSight's controls over that information are an important guard against privacy risks.

Section 2.0 Uses of the Information

2.1 Describe all the uses of information.

As stated in the introduction, the NICC uses the information to provide status and impact reports on the nations CI/KR operational status to the DHS NOC, other federal agencies, and commercial organizations. DHS uses this information to build the operational status of CI/KR sites in the DHS Common Operational Picture (COP).[5] Specifically, this information allows INSight user's to research and analyze all captured information so as to coordinate and report upon impacts to the nation's CI/KR. This information further allows the NICC to coordinate appropriately between DHS and the private sector owner's and operators as to incidents or events (natural or terrorist) that have the ability to adversely impact the nations CI/KR. PII may, at times, be a part of this information. PII is only used in two

[5] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_hsind.pdf

instances: as part of contact information regarding specific CI/KR sites or information contained in analytical or investigatory materials associated with CI/KR.

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

INSight uses a commercially available trouble ticketing system for data access, tracking, and search capabilities to allow authorized users to see and manage the information. The system also uses the Microsoft Office Suite of capabilities to allow for the automatic generation of reports, status sheets, and graphs for reports generated by the system. The trouble-ticketing system allows for organized intake and assigning of research tasks within the NICC by specifically tasking individuals to provide information for a certain information request. Access to these tools requires the user to be an authorized user with a need to know the information potentially used in the reports. The NICC Watch standers and staff analyze all CI/KR information in a manner that attempts to clarify and validate any reported facts as to its impact on the operational effectiveness of a given (or set of) critical infrastructures. Analysis is conducted by trained analysts, not INSight itself. INSight merely presents information in an easily accessible and organized fashion.

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

INSight contains publicly available information which is obtained via internet open-source published web pages, organizational web pages, federal publicly available web pages, news broadcasts, and Real Simple Syndication (RSS) news feeds over the internet. This information is used to alert the NICC watch as to events and or incidents of a potential nature that would require further analysis to determine the eminent or potential impact to the nation's CI/KR. An example of this type of data would be access the National Oceanographic and Atmosphere's (NOAA) publicly available weather web pages.

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.

Information in this system is safeguarded in accordance with applicable rules and policies, including any applicable NPPD and DHS automated systems security and access policies. Strict controls have been imposed to minimize the risks of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals specifically authorized and granted access by DHS regulations, who hold appropriate security clearances, and who have a need to know the information in the performance of their official duties.

The system also maintains a real-time auditing function of individuals who access the system. All information is managed as Sensitive but Unclassified (SBU). All PCII information is managed in accordance with the directives of the PCII Program Management Office of the Department of Homeland Security. Access is limited to authorize personnel only. All user screens that contain PCII information are bannered in accordance with the PCII Handling Guidance provide by the PCII Program Management Office.

The following security controls are used to ensure for the appropriate access and security of all data managed by the NICC within the INSight system:

- Users Access controls
- Encryption of transmitted data
- Redaction on appropriate form entries
- User Level Information Assurance Awareness
- Labeling and appropriate handling of all external Media
- Physical Control and Access to all systems access points and system physical environments

All commercial data used by the NICC undergoes human review and verification prior to this data being entered in the INSight supporting database. All access to these commercial data sources are controlled by the standard operating processes and procedures of the NICC Watch.

Section 3.0 Retention

3.1 How long is information retained?

NICC personnel plan to request records disposition schedules and coordination of those schedules with the National Archives and Records Administration (NARA) for 10 years from the time of inclusion in INSight.

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

No, but once a final retention schedule is approved by DHS, NICC and NPPD will make a formal request to NARA for approval.

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

The major advantage to maintain this data for an extended period of time would be to allow for trending and analysis of historical events.

Given that most of the contained data is not PII, but is more focused on the nation's CI/KR operational status, contemporary knowledge of incident and recovery planning indicates long periods of historical data is required to make good decisions on current events. A 10-year retention period is deemed necessary for law enforcement investigative activities, governmental and other subject matter experts to link the information with known terrorist / non terrorist activity or to identify the activity as benign and unrelated to terrorist activity.

In order to minimize the number of individuals with access to information while maximizing the usefulness of the information provided, information in the database is protected by user level access controls at the field level. INSight then uses role-based access to enforce these rules.

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?

The information contained within INSight is currently made available to any user within the DHS construct that has a need to know and is a validated user. For the purposes of CI/KR operational analysis this need to know primarily includes divisions of the NPPD, the Federal Emergency Management Agency (FEMA, responsible for disaster response, among other duties), Intelligence and Analysis (I&A, intelligence information) and the Operations Directorate (responsible for information coordination, among other duties). The INSight system shares its information with the DHS COP (Operations Directorate, supporting the common operational picture), the Integrated Critical Asset Viewer (iCAV, geospatial tracking of DHS assets, NPPD)) and the Homeland Security Information Network Private Sector Portal (information sharing portal for private sector CI/KR members, Operations Directorate).[6] The data is shared to allow for the common view of CI/KR reported information across DHS.

Information contained within the INSight system is primarily shared within DHS to provide the NOC and other DHS departments with the details related to the operational status, or incidents affecting the operational status, of CI/KRs across the nation. This information serves to provide the other watch and reporting organizations within DHS detailed relevant information about the nation's CI/KR status. The organization within DHS that this information is shared with includes:

NOC Fusion Desk; NOC FBI Desk; NOC Homeland Security Information Network (HSIN) Desk; NOC Senior Intel Analyst (SIA); NOC Infrastructure Protection (IP) Desk; NOC Department of Transportation (DOT) Desk; NOC National BioSurveillance Group (NBSG) Desk; Bureau of Alcohol, Tobacco, Firearms and Explosives Operations Security Branch; FBI Counter Terrorism Watch; Homeland Infrastructure Threat and Risk Analysis Center (HITRAC); National Communications System (NCS); Office of Intelligence & Analysis Fusion Center liaisons; OIP Chemical and Nuclear Preparedness and Protection Division (CNPPD); OIP Infrastructure Partnerships Division (IPD) Deputy Director; OIP Information Coordination and Analysis Office (ICAO); OIP National Infrastructure Coordinating Center (NICC); OIP Protective Security Advisors; USCG Maritime Intelligence Fusion Center (MIFC) - Atlantic & Pacific; United States Computer Emergency Readiness Team (US-CERT); Office of Intelligence & Analysis Chemical,Biological, Radiological, Nuclear and Explosives Branch

4.2 How is the information transmitted or disclosed?

All information is transmitted vie Secure Socket Layers (SSL) with virtual Private networking technologies as well as applied levels of encryption. The information is not made publicly available. Reports may also be transmitted via other Information Technology (IT) systems but is secured via separate devices. All information is secured and protected by user level access controls. We must show security

[6] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ops_hsin.pdf

levels applied. All users must have an account established by the INSight Management Staff and must further present a password upon attempted access.

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.

The information provided to individual users in the systems described in Question 4.1 is mapped directly to their user's role with in the INSight application. This allows the NICC to monitor that any information coming in and out of the NICC is mapped to a certain user and a certain system. This mitigates any risk of mixing information, and mixing access to content otherwise forbidden to certain users.

All access to the INSight system is secured via encrypted internet traffic. Each user must first request an account, be registered as a user in the role based access control management system, and present a password upon logging into INSight. All transaction are secured via a point to point connection between the end user and the INSight application.

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 information contained within INSight can be made available to any state and local government user with a mission to support homeland security. This information is shared with:

State-Level Emergency Operations Centers, FEMA Joint Field Offices in response to certain events, existing Federal Organizations Operations and Watch Centers, and Private Sector Consortium Industry Organizations.

The information is shared via the DHS HSIN communication portal, via secured fax, via DHS emails mechanisms, and in the case of the private sector, thru redacted reports generated by the NICC Watch and emailed to the end user.

Upon request and in accordance with NICC operational procedures the NICC Watch will remove all personally or organizational identifying information in reports that are sent outside of DHS. This process allows the users of the information to only see elements like "A US PERSON" or "A US Company" versus the real name of the person or company in the report. The NICC uses a manual review and evaluation process to identify and redact all personally or organizational identifying information. Once this is completed by the NICC watch a quality control review is then conducted by the NICC management prior to the release of these documents.

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.

INSight users individually will have to comply with an End User Agreement that requires their strict adherence to the rules and policies associated with the use of the system and the organization as well as the laws and policies of the jurisdictions in which they operate. Additionally, all entities accessing and using the INSight system will be bound by a memorandum that details the Rules of Behavior for the INSight system and or a Memorandum of Understanding that will detail all aspects of their access, use, security, and restriction of further dissemination of the data within INSight system.

The Homeland Security Operations Center (HSOC) System of Records Notice (SORN) (April 18, 2005, 70 FR 20156) controls the information sharing in INSight. The HSOC SORN at page 20157 (routine use "B") allows for information to be shared with "to a Federal, state, local, joint, tribal, foreign, international or other public agency or organization, or to any person or entity in either the public or private sector, domestic or foreign, where such disclosure may promote assist or otherwise serve homeland or national security interests."

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

All information is transmitted vie Secure Socket Layers (SSL) with virtual Private networking technologies as well as applied levels of FIPS 140.2 compliant encryption. The information is not made publicly available.

Information in this system is safeguarded in accordance with applicable rules and policies, including any applicable NPPD and DHS automated systems security and access policies. Strict controls have been imposed to minimize the risks of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals specifically authorized and granted access by DHS regulations, who hold appropriate security clearances, and who have a need to know the information in the performance of their official duties. The system also maintains a real-time auditing function of individuals who access the system. All information is managed as SBU at the unclassified level. All PCII information is managed in accordance with the directives of the PCII Program Management Office of the Department. Access is limited to authorized personnel only.

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

DHS and external agencies, organizations requiring access to the INsight system formally request access to NICC management. If the requesting organization has a need to know for use and or access to the INSight system, the Director of the NICC approves this access. These users are required to complete all normal user account creation actions (i.e. Rules of Behavior acceptance documentation). All DHS internal shared information is properly marked as PII or PCII if necessary. Appropriate PCII cover sheets are used to notify the user of the contained data. All shared information to DHS organizations is protected by individual account access type privileges applied to the individual account types. The INSight system also enforces data level restriction to ensure that the user's profile includes the necessary read / write restrictions.

All information shared to organizations outside of DHS is first reviewed for potential redaction requirements. Access to this information is secured via encrypted SSL connections and all user account role based access control is applied. The INSight system also enforces data level restriction to ensure that the user's profile includes the necessary read / write restrictions.

The NICC uses a manual review and evaluation process to identify and redact all personally or organizational identifying information. Once this is completed by the NICC watch a quality control review is then conducted by the NICC management prior to the release of these documents. This process provides the necessary controls to ensure adequate control of risks associated with the release of sensitive PII information.

The controlled community that INSight information is shared with includes: DHS organizations in the IPD and IA directorates; members of the IPD IMC; critical infrastructure information coordination groups, and other HSIN-CS 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?

The HSOC SORN (April 18, 2005, 70 FR 20156) provides notice of the collection and sharing of information within the INSight system. Information taken from other systems would be noticed individually by those systems.

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

When an individual is submitting information to INSight, he/she has the right to decline providing personal information. As an example, an anonymous caller contacts a law enforcement agency with a report of suspicious activity. The information may be submitted to INSight without capturing the callers identifying information. For personal information that may be associated with suspicious activity reports, or when this information is received from another reporting agency, department, organization or publicly available source there is no opportunity to decline to provide information because INSight did not initially collect the information. Responsibility for notice and choice of collection remains with the agency that originally collected the data.

Upon request and in accordance with NICC operational procedures the NICC Watch removes all personally or organizational identifying information in reports that are sent outside of DHS. This process allows the users of the information to only see elements like "A US PERSON" or "A US Company" versus the real name of the person or company in the report.

The NICC uses a manual review and evaluation process to identify and redact all personally or organizational identifying information. Once this is completed by the NICC watch a quality control review is then conducted by the NICC management prior to the release of these documents.

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

Although some INSight information may have originator controls that govern particular uses of it, in general, individuals will not be able to consent to particular uses of the information. For information received in the form of suspicious activity reports or received directly from individuals, however, such individuals may be protected as confidential sources.

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.

Individuals will be provided notice through the System of Records Notice. Given that in some instances personal information will be collected without the knowledge of the individual, the INSight database protects all data at the record and field level and that data can be masked so that only those individuals with appropriate clearance and a verifiable need to know are able to see the personal information.

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.

There is currently no Redress capabilities provided by the NICC and or the INSight application

Should a request for correction be requested, the NICC Watch can access the specific record entries, and using the INsight application, make the necessary corrections to the appropriate records contained within the supporting database. The ability to conduct a thorough search across all records in the database to ensure all similar changes required can then be ran by the NICC watch to ensure 100% update of all required information. Furthermore, the supporting data audit logs will show that this information was updated, by whom and when.

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

Individual access to information in the INSight system is available through the provisions of the Freedom of Information Act and the procedures for submitting FOIA requests are available in 6 C.F.R. Part 5. Please write to "FOIA, U.S. Department of Homeland Security, National Programs and Protection Directorate, attn FOIA Officer: Alisa Turner, Washington, D.C. 20528" You may also make informal inquires to NPPD.FOIA@dhs.gov.

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

Because personal information is likely to be in the INSight system based upon a third party reported event, open source news reports, or federal / organizational reporting, or a suspicious activity report, no procedures will be established to allow for correction of this information.

If an individual believes that he or she has suffered an adverse consequence related to the INSight System, that individual will be able to provide any information that they deem relevant with a request that it be included within any record maintained in the INSight System regarding a particular incident, activity, transaction, or occurrence.

Individuals wishing to address their concerns and or potential personal impacts resultant from information maintained and or distributed from NICC's INSight system can contact the NICC Watch at any time to address their concerns.

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

If an individual feels that the information maintained in the INSight system is inaccurate, there will be three methods available to provide accurate information to the NICC Watch. The DHS FOIA process (see Question 7.1) allows access to records. The FOIA web site will contain a link permitting any individual to send information to the NICC via a designated email address reserved for that purpose. The FOIA page will also contain a fax number and a mailing address for the same purposes for those who prefer to use those means to contact to the NICC. All communications received, regardless of method, will be entered into and remain on record within the INSight system pursuant to its general record retention schedule and will be subject to audit.

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

Redress is not currently provided.

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

If an individual believes that he or she has suffered an adverse consequence related to the INsight system, that individual will be able to provide any information that they deem relevant with a request that it be included within any record maintained in the NICC INSight system regarding a particular incident, activity, transaction, or occurrence.

The development of the INSight system and the processes governing its use included detailed consideration of the impact of erroneous data on individuals as well as on the official users of the information with the component Database. Information in the INsight system is, by definition, raw information. The INSight system is simply a pool of unvetted, reported "as-is" information that is maintained in a manner making it accessible to appropriate official entities for further investigation and analysis predicated upon reasonable suspicion of a terrorism nexus.

Having verified and accurate information is the ultimate goal of the NICC, as well as any all law enforcement, intelligence community, and other governmental officials using the system. The redress indicated in 7.2, above, will help to ensure that the information is accurate.

NICC Watch-standers will ensure the integrity of the INSight information based upon information provided by individuals, as well as any updates received from law enforcement and other government authorities.

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?

The NICC's controlled registration process will verify registrant eligibility for specific access to the INSight system. The INSight system is protected by access controls that are role-based. Controls and access limitations are in place to ensure that sensitive information is protected from unauthorized access or exchange. Additional controls may be established to further define access to emergent, incident, and event-based information as required. In all cases access will be in accordance with applicable law and policy.

Role-Based Access Limitations. As an example of the role-based access, only a NICC Watch stander or authorized person with a need to know will have access to any part of the INSight system. NICC Management has access to the entire system and all of its component data. NICC Watch staff has a different level of access that only allows them to see those data elements that are required for the performance of their watch duties. NICC INSight System Administrators have access to the entire system and all component data elements so as to operate the system, conduct continuity of operations processes, and ensure for the uptime of all system and data resources on the INSight system.

System Rules of Behavior: Every User must read sign and acknowledge the INSight Rules of Behavior guidance prior to being granted access to the INSight System,

Today users of this system include the NICC Watch and Management Staffs, selected members of the IPD supporting leadership, and the IP Watch Desk Staff of the NOC and FEMA watches (NAC Location and FEMA NRCC Location). Selected IPD supporting staffs to the Joint Field Offices who respond in support of major incidents or events also have access to the INSight system. Future potential users include the IMC management staff, IPD leadership, and NOC Watch and Leadership as well.

8.2 Will Department contractors have access to the system?

Department contractors who have at minimum a Secret DHS approved clearance, require knowledge based upon a Need to Know, and are registered users of the INSight system will be able to access the system. Based upon their role the appropriate role based controls will be applied to their INSight user account to ensure they only see those records that they have a mission need for. Every user of the INSight system has previously passed the required DHS Suitability clearance verification. At a minimum all users of the system will have passed the DHS employment verification clearance process.

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

Currently, all NICC Watch personnel managing material in the INSight system must review the DHS and U.S. Person Privacy Guidelines prior to operating the system. All users must read and acknowledge by signature the System User's Guide and the Rule of Behavior covering the INSight System.

All user's must also perform mandatory PCII Users' Training which details the information handling procedures required for the user to process any PCII information contained within the INSight system. Each user's training certificate is maintained by the NICC management team.

Those guidelines as well as other information handling requirements are incorporated into all user based training modules used to train and refresh users as to the allowable function on the INSight system.

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

INSight is currently under process for Certification and Accreditation within the Department of Infrastructure Protection, Department of Homeland Security. Expected completion date is 30 November 2007. The system will be certified at a level of High Assurance.

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

Advanced Auditing: Through the audit capability an administrator can see any actions a user has performed at the server, application and database levels and undo any malicious behavior as necessary. The INSight system also uses an EAL 4 certified firewall that conducts application level packet inspection and performs antivirus and anti-spam functions on all traffic crossing the INSight network. Intrusion prevention and detection inspection is also performed at the network layer detecting any malicious behavior on the INSight system

Detailed Users Access Auditing: This feature enforces accountability for a user's actions within the application. Similarly, any submissions to update or add asset information will be validated by NICC Watch personnel prior to inclusion in the INSight System. Detailed audit records of every user's actions at the application level are collected and reviewed on a weekly basis to ensure no malicious activities take place.

Audit Controls and Sanctions. All information will also remain linked with detailed audit records of who/when that information was accessed and subjected to a periodic audit to ensure that information in the INSight Database is used in accordance with the above described policies.

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?

The INSight system employees the use of role based access control, detailed event and access control auditing to mitigate any potential risk of information being inappropriately managed or used.

Every user's action within the system is date stamped so that the action, data, and resultant outputs are logged by the system. These detailed security controls allow the administrator as well as management to ensure for the accurate use and control over the system and the managed data elements.

All NICC users are trained on the systems authorization, access control, and auditing procedures before being granted access.

Risks identified and the mitigation to these risks are:

All system hard copy print outs from INSight are mitigate by appropriate classification marking and document handling procedures. INSight data backup tapes are labeled in accordance with DHS 4300.00A Sensitive System Policy Directive and Sensitive System Handbook guidelines, and remain under physical control until stored in a fireproof waterproof safe off site.

The potential for human data entry mistakes is mitigated by user level training, user agreements, non disclosure agreements, and individual DHS as well as INSight Rules of Behavior.

PCII material risks are mitigated by each user having access undergoing the require PCCI training and having signed PCII information handling agreements in place. All INSight system user screens are clearly marked with PCII data banners when PCII data exists on the user's terminal.

The risk of inaccurate information being placed in to the system is mitigated by the NICC's Standard Operating Procedures requiring Watch management review of all record and their data prior to being committed to the database.

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, radio frequency identification device (RFID), biometrics and other technology.

9.1 What type of project is the program or system?

INSight is an operational system supporting infrastructure protection. INSight is systems development and maintenance contract managed under a Time and Material contract.

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

The INSight is an operational system. The system consists of an operational environment, a staging and testing environment as well as a development environment. The INSight system is in a live operational stage as well as undergoing further developments to enhance the user functionality required to meet the NICC mission needs. A spiral develop lifecycle is currently being used to ensure the finite development of detailed requirements, detailed testing and operational testing, and maintenance of any live application issues.

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

The system does not use or employ any technologies that may raise privacy concerns. INSight does make use of the current DHS iCav geospatial capabilities by allowing the users of INSight to connect to the iCAV system. iCAV is the DHS standard geospatial tool set. Icav is used by the NICC to obtain a geospatial reference of any items of interest and to add more details to NICC reports within DHS.

Responsible Officials

Chris Anderson
Deputy Director, National Infrastructure Coordinating Center, National Infrastructure Preparedness Directorate, Contingency Planning and Incident Management Division,
Department of Homeland Security
(703) 563-3212

Approval Signature Page

Original signed and on file with the DHS Privacy Office November 28, 2007

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security