Privacy Impact Assessment
for the

Interagency Operations Center (IOC) WatchKeeper

DHS/USCG/PIA-020

January 4, 2013

Contact Point
CAPT Robert S. Wilbur
DHS Interagency Operations Center (IOC), CG-9333
United States Coast Guard
202-475-3039

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS), U.S. Coast Guard (Coast Guard) operates the Interagency Operations Centers (IOC) WatchKeeper system. The WatchKeeper system was developed to improve tactical decision-making, situational awareness, operations monitoring and processing, and joint planning in a coordinated interagency environment. WatchKeeper provides a fully functioning and shared operational picture, shared mission tasking, and shared response information to all users within the IOC, partner federal agencies, and local port partners. This Privacy Impact Assessment (PIA) is being conducted to notify the public about the personally identifiable information used by and stored in WatchKeeper.

Overview

In compliance with the Security and Accountability for Every Port (SAFE Port) Act of 2006 (46 U.S.C. § 70107A), the Department of Homeland Security (DHS) has established Interagency Operations Centers for security in the nation's 35 most critical ports.[1] The Coast Guard began the IOC project to improve multi-agency maritime security operations and enhance cooperation among partner agencies at the nation's 35 most critical ports. IOCs help port agencies collaborate in the conduct of first response, law enforcement, and homeland security operations. IOCs also help port partners to:

- Collaborate and jointly plan operations through assignment of resources to meet the IOC's respective mission demands;
- Share targeting, intelligence, and scheduling information to improve situational awareness, uncover gaps in planned and ongoing operations, and reduce duplication of effort between agencies;
- Develop real-time awareness, evaluate threats, and deploy resources to the right places through active collection of port activity information; and
- Minimize the economic impact from any disruption, whether natural or manmade.

At the heart of the IOC is the WatchKeeper information sharing and management system software. WatchKeeper coordinates and organizes port security information to help DHS and federal, state, and local maritime partners make the best use of their resources to keep America's ports safe. The WatchKeeper system was developed to improve tactical decision-making, situational awareness, operations monitoring, rules-based processing, and joint planning in a

[1] A critical port is a port that the Coast Guard has determined as a critical or key component of the United States maritime transportation infrastructure.

coordinated interagency environment. WatchKeeper provides a shared operational picture, shared mission tasking, and shared response information sets to all users within the IOC, including partner federal agencies and local port partners.

The IOCs have three critical functions: Integrated Vessel Targeting (IVT), Interagency Operations Planning (IOP), and Operations Monitoring (OM). Watchkeeper is an integral information sharing and targeting tool for the IVT function. To implement IVT, IOCs establish an Integrated Vessel Targeting Team (IVTT) that consists of screeners from Coast Guard, U.S. Customs and Border Protection (CBP), and depending on the port, IOC members, which can include state and local law enforcement personnel. Their responsibilities include a thorough analysis of arriving vessels and coordinating joint mission execution over a 96 hour period. The period begins with the required 96 hour notice of arrival prior to vessel entry into the U.S. port. This is followed by an iterative process that requires action at 72, 48, and 24 hours before port entrance. This process ensures that each commercial vessel is vetted by the IVTT prior to arrival. The team completes all vessel targeting activities no later than 48 hours prior to a known vessel arrival which will adequately mitigate delays in commerce. This team then recommends whether vessels are cleared, conditionally cleared, or not cleared of threats for entry and operations in the nation's 35 most critical ports.

IOC members use WatchKeeper to capture the results across four targeting factors – people, vessels, cargo, and programs (compliance or regulatory). IOCs assign leads (lead agency/responsible authority) for each factor based on jurisdiction, capabilities, authorities, or access to enterprise systems and data. The Coast Guard is the lead for screening vessels and programs in most cases and CBP is the lead for screening people and cargo. Other federal, state, and local maritime partners use the tools provided by WatchKeeper to make the best use of their resources to keep America's ports safe. Vessels that are not cleared or conditionally cleared are handed over to the Interagency Operational Planning Team (IOPT) to determine and prioritize any activities required to mitigate those threats, as well as any other threats present in the port.

Sources of Information

To manage daily operations, WatchKeeper obtains data from multiple data sources and organizes this information into a useful workflow. The WatchKeeper system compares this multiple source data against preconfigured vessel behaviors within the application (this behavior data defines how a specific vessel or class of vessel should operate). Personally identifiable information collected and used by WatchKeeper is limited to crew and passenger data, which is

submitted by the USCG Ship Arrival Notification System (SANS) system and analyzed by the U.S. Customs and Border Protection (CBP) Automated Targeted System (ATS).[2]

Notification and alert visualizations are provided by the WatchKeeper system to the watchstander, who monitors the situation when abnormalities in vessel behavior are detected. The system also shares this situational picture with other IOC partners so event responses can be orchestrated in a unified and coordinated manner at that port. To the maximum extent possible and in order to obtain the most current and accurate information, WatchKeeper reaches into other DHS enterprise authoritative data sources to obtain and align core data elements used in the vessel tracking workflow process. The primary authoritative data sources used by the WatchKeeper system are the following:

- Tactical Track Data from Coast Guard's Nationwide Automatic Identification System (NAIS)
- Alert information associated with UNCLASSIFIED Notice Of Arrival (NOA) Information from Coast Guard's Maritime Awareness Global Network (MAGNet)[3]
- Vessel Characteristics from Coast Guard's Maritime Information for Safety and Law Enforcement (MISLE)[4]
- Strategic Track Data from Coast Guard's Common Operating Picture (COP) Web Services System (CWSS)
- Vessel Information from Coast Guard's Long Range Identification and Tracking (LRIT)
- Spatial data layers from Coast Guard's Enterprise Geographic Information System (E-GIS)
- UNCLASSIFIED Notice Of Arrival (NOA) Information and complete crew and passenger information from Coast Guard's Ship Arrival Notification System (SANS)[5]
- Crew and Passenger information and associated vetting data from the CBP's Automated Tracking System (ATS)[6]

[2] DHS/CBP/PIA-006(b) Automated Targeting System (ATS) PIA Update, June 1, 2012.
[3] DHS/USCG/PIA-005 United States Coast Guard Maritime Awareness Global Network (MAGNET) PIA, April 11, 2008.
[4] DHS/USCG/PIA-008 Marine Information for Safety and Law Enforcement (MISLE) PIA, September 8, 2009.
[5] DHS/USCG/PIA-006(a) Vessel Requirements for Notices of Arrival and Departure (NOAD) and Automatic Identification System to add the Notice of Arrival on the Outer Continental Shelf Update PIA, June 4, 2009.
[6] DHS/CBP/PIA-006(b) Automated Targeting System (ATS) PIA Update, June 1, 2012.

SANS collects and processes vessel, crew/passenger, and cargo information for arriving vessels.[7] It is operated by the Coast Guard National Vessel Movement Center (NVMC) and makes resulting information available for use by the Coast Guard intelligence and operational communities, U.S. law enforcement organizations, DHS agencies, U.S. Navy in their Homeland Defense mission, and other U.S. military and intelligence organizations via subscription service. Complete crew and passenger data are encrypted and transferred from SANS to WatchKeeper, where it is decrypted for use in information displays. The data exchange with CBP's ATS facilitates an enhanced, near real-time, situational awareness at the Caption of the Port (COTP) level in addition to the vetting already being done by CBP and Coast Guard Coast Watch teams.

The WatchKeeper system does not collect information directly from the public. Rather, WatchKeeper performs searches for and accesses information collected and maintained in other government-owned systems. Data includes crew, passenger, and cargo vetting details as processed by the ATS system to automate interagency workflow coordination. Personally identifiable information within WatchKeeper may be used by the Automated Targeting System-N (ATS-N)[8] and Automated Targeting System-Passenger (ATS-P).[9] ATS-N evaluates all cargo to identify high risk inbound cargo for examinations. ATS-P is a web-based enforcement and decision support tool used to collect, analyze, and disseminate information for the identification of potential terrorists, transnational criminals and, in some cases, other persons who pose a higher risk of violating U.S. law.

With a fuller picture of the risk profile that the vessel presents, the COTP can make appropriate, informed decisions well ahead of the vessel's arrival to the port. The data is not permanently stored by WatchKeeper, but rather temporarily cached for use a maximum of 32 days after arrival or departure, and then deleted. This is to provide local access to vetting information for the period of time that the COTP is responsible for clearance of a vessel at their

[7] SANS collection of PII is detailed within the DHS/USCG/PIA-006(a) Vessel Requirements for Notices of Arrival and Departure (NOAD) and Automatic Identification System to add the Notice of Arrival on the Outer Continental Shelf Update PIA, June 4, 2009.

[8] ATS-N evaluates all cargo to identify high risk inbound cargo for examinations. ATS-N uses numerous rule and weight sets to analyze information from manifest, importer security filing, and entry data, to prioritize shipments for review, and to generate recommended targets by scoring each shipment. ATS-N not only screens commodity information on manifest, importer security filing, and entry data, but also screens individuals, against lookouts and prior violations, who are identified on those data sources. For a detailed description of the privacy risks and mitigations associated with CBP's use of the Automated Targeting system, please see DHS/CBP/PIA-006(b) Automated Targeting System (ATS) PIA Update, June 1, 2012.

[9] ATS-P is a web-based enforcement and decision support tool used to collect, analyze, and disseminate information for the identification of potential terrorists, transnational criminals and, in some cases, other persons who pose a higher risk of violating U.S. law. ATS-P capabilities are used at ports of entry to augment the CBP officer's decision-making about whether a passenger or crew member should receive additional screening. For a detailed description of the privacy risks and mitigations associated with CBP's use of the Automated Targeting system, please see DHS/CBP/PIA-006(b) Automated Targeting System (ATS) PIA Update, June 1, 2012.

local port. The WatchKeeper system improves the capability to see, understand, and share tactical information critical to security and interagency coordination in ports and coastal areas.

Section 1.0 Authorities and Other Requirements

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

The Security and Accountability for Every Port (SAFE Port) Act of 2006 (46 U.S.C. § 70107A) authorizes the Coast Guard WatchKeeper system to collect the required information. The authority to collect this data is further supported by 5 U.S.C. § 301; 14 U.S.C. § 89; 14 U.S.C. § 632; 19 U.S.C. §§ 482, 1461, 1496, 1581, 1582; 14; 46 U.S.C. § 3717; 46 U.S.C. § 12501; the Maritime Transportation Act of 2002, Pub. L. 107-295; the Homeland Security Act of 2002, Pub. L. 107-296; the Enhanced Border Security and Visa Reform Act of 2002, Pub. L. 107-173; and the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458; 33 C.F.R. part 160.

Furthermore, the laws and regulations that govern the collection of Notice of Arrival information are Title 33–Navigation and Navigable Waterways Chapter 25 – Ports and Waterways Safety Program, and Title 33 C.F.R. Part 160 – Ports and Waterways Safety – General Subpart C – Notifications of Arrival, Hazardous Conditions, and Certain Dangerous Cargoes. Chapter 25, 33 U.S.C. § 1223(a)(5) gives Secretary authority to collect information "necessary for the control of the vessel" and does not preclude security concerns as the basis of that necessity; 33 U.S.C. § 1226 includes inspections, port and harbor patrols, the establishment of security and safety zones, and the development of contingency plans and procedures to prevent or respond to acts of terrorism.

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

WatchKeeper is a read-only system that does not collect data directly but reutilizes previously collected data from other systems and authoritative data sources. Notice is provided via the SORNs of the underlying source systems:

- DHS/USCG-029 Notice of Arrival and Departure, System of Records published on November 9, 2011 (http://www.gpo.gov/fdsys/pkg/FR-2008-12-11/html/E8-29279.htm) covers the collection of complete crew and passenger information.

- DHS/CBP-006 Automated Targeting System, System of Records published on May 22, 2012 (http://www.gpo.gov/fdsys/pkg/FR-2012-05-22/html/2012-12396.htm) covers crew and passenger information and vetting data, which includes position (i.e. job), name, date of birth (DOB), sex, nationality, country abbreviation (CD), ID Type, ID#, ID country, embark location, and embark date information.

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

WatchKeeper is an operational major application in the Coast Guard/DHS FISMA inventory (FISMA ID USC-03672-MAJ-03672) and has a valid ATO with an expiration date of September 30, 2014. WatchKeeper processes, transmits (amongst its system components and over the Coast Guard's network to end user workstations), and stores PII data. WatchKeeper has a FIPS 199 security categorization of Confidentiality "HIGH," Integrity "HIGH," and Availability "MODERATE." with an overall FIPS 199 categorization of "HIGH."

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

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

WatchKeeper is not the system of record for the PII being collected nor does the system have a requirement for making any long term storage or reporting of the data. All NARA records retention requirements remain the responsibility of the authoritative data sources.

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

The information contained in WatchKeeper is not covered by the Paperwork Reduction Act (PRA) because WatchKeeper does not collect any information directly from the public.

Section 2.0 Characterization of the Information

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

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

The WatchKeeper system does not collect information directly from the public. Rather, WatchKeeper performs searches for and accesses information collected and maintained in other government-owned systems.

Complete crew and passenger data from SANS and crew and passenger information and vetting data from the CBP's ATS are the only PII data elements received and used by WatchKeeper. These data elements include position (*i.e.*, job), name, Date of Birth (DOB), sex, nationality, country abbreviation (CD), ID Type, ID number, ID country, embark location, and embark date.

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

WatchKeeper does not collect information directly from individuals, but rather ingests or accesses and uses information collected, generated, and stored by and in other systems in compliance with those systems' Information Sharing Agreements. The government data sources of information used by WatchKeeper include the following:

- Tactical Track Data from Coast Guard's NAIS;

- Alert information associated with UNCLASSIFIED NOA Information from Coast Guard's MAGNet;
- Vessel Characteristics from Coast Guard's MISLE;
- Strategic Track Data from Coast Guard's COP CWSS;
- Vessel Information from Coast Guard's LRIT;
- Spatial data layers from Coast Guard's E-GIS;
- UNCLASSIFIED NOA Information and complete crew and passenger information from Coast Guard's SANS; and
- Crew and Passenger information and associated Vetting Data (*i.e.*, position (job), name, DOB, sex, nationality, CD (Country abbreviation), ID Type, ID number, ID Country, embark location, and embark date) from CBP's ATS.

WatchKeeper ingests data electronically from the primary authoritative government data sources identified above, provides a pointer to data in other systems, queries databases, and may receive data in accordance with certain cooperative arrangements with other government entities. Additionally, some of the information maintained in WatchKeeper is created by WatchKeeper users (none of this data is PII).

Information collected by WatchKeeper is used to provide a fully functioning and shared operational picture, shared mission tasking, and shared response information sets to all users within the IOC, including partner federal agencies and local port partners. In this context, WatchKeeper obtains the required information from the authoritative data sources for that information versus the sources from which those systems obtain that data. Furthermore, the majority of the information (including the PII) is temporal in nature.

All external data feeds to WatchKeeper are transmitted one-way. WatchKeeper does not write back to these IT systems (i.e., the system only ingests the information) and does not share any data with other systems. Information flow and access control mechanisms employed on system components and network interface devices limit WatchKeeper's access to only the data that is needed for its mission, as agreed upon by WatchKeeper and respective system's Authorizing Officials and System Owners.

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

WatchKeeper does not use information from commercial sources or publically available data unless that data is included in information obtained from the systems presented in Section 2.1.

2.4 Discuss how accuracy of the data is ensured.

WatchKeeper relies upon the source systems listed in Section 2.1 to ensure that data used by the system is accurate and complete. Discrepancies may be identified in the context of a watchstander's review of the data, and watchstanders are required by policy to take appropriate action to correct the data if they become aware of any inaccuracies. Although WatchKeeper is not the authoritative government data source, WatchKeeper receives updates from the source systems regarding any changes to those source system databases. Continuous source system updates occur in real-time or near real-time. When corrections are made to data in the source systems, WatchKeeper updates this information immediately and only the latest data is used. In this way, WatchKeeper integrates all updated data (including accuracy updates) in as close to real-time as possible.

To the extent information that is obtained from another government source is determined to be inaccurate; this problem is communicated to the appropriate government source by the watchstander for remedial action.

In addition, the integrity of the data obtained from the source systems is ensured through the specific transport protocols employed.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: Because WatchKeeper draws upon other government data sources to obtain data instead of collecting directly from individuals, there is a risk that the data will become outdated and inaccurate.

Mitigation: WatchKeeper relies upon the source systems listed in Section 2.1 to ensure that data used by the system is accurate and complete. WatchKeeper receives regular updates from the source systems regarding any changes to those source system databases. Continuous source system updates occur in real-time or near real-time. Discrepancies may also be identified

in the context of a watchstander's review of the data, and watchstanders are required by policy to take appropriate action to correct the data if they become aware of any inaccuracies.

Privacy Risk: WatchKeeper aggregates data from many systems, which may exceed the minimal amount necessary to achieve its missions.

Mitigation: The nature of Coast Guard's mission to provide effective port security and vessel screening requires WatchKeeper to collect any relevant information. Watchstanders rely on this information to make accurate determinations and are trained to identify inaccurate information. To portray an accurate and real-time picture of the port, Watchstanders require WatchKeeper's aggregation of multiple sources of data. WatchKeeper only aggregates or collects data that is critical to the Coast Guard mission of port security and vessel screening. WatchKeeper does not aggregate data outside of its mission scope.

Section 3.0 Uses of the Information

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

3.1 Describe how and why the project uses the information.

In support of the Coast Guard and overall DHS mission, WatchKeeper was built to enhance unity of effort among maritime stakeholders in the following areas:

- *Integrated Vessel Targeting (IVT*): Watchkeeper integrates targeting results of agency-specific screening processes. It builds a consolidated threat picture of people, vessels, and cargo operating within IOC operations area (OPAREA) (*e.g.*, a specific port) in support of the nation's 35 most critical ports:
    - *IOC Video Services:* Use of local IP-enabled web cameras (where available) will provide limited video coverage of critical port harbors and waterways. Cameras are identified and selected by the local users and access is controlled using system user role structure and defined data groups.
    - *IOC RADAR Services:* Use of local radar within an OPAREA will enable track correlation with Nationwide Automatic Identification System (NAIS) and local Automatic Identification System (AIS) tracks; range/sea clutter/rain clutter/gain control, and status. Radar covering critical infrastructure in an OPAREA will

have dedicated, high availability network connections to the system in order to provide "near real time" updates.

- *IOC Automatic Identification System AIS Services:* Use of local AIS track data will allow correlation with local radar tracks and associated status. It is anticipated that all AIS base stations will be Coast Guard-owned.

- *IOC Data Services:* Use of local port partner data will include an Internet connection for access to time-sensitive port partner information. Current scope of port partner shared data consists of people, cargo, and vessel vetting data as well as locally created mission and event records.

- *Interagency Operations Planning (IOP)*: WatchKeeper integrates federal, state, and local asset status and schedules within and across OPAREAs. Mission Requests are created from Integrated Vessel Targeting results, along with other mission demand sources, such as regattas, patrols, and escort missions. These Mission Requests are prioritized by IOC decision makers, who assign assets to missions. These assignments form the IOC Daily schedule.

- *Operations Monitoring (OM):* WatchKeeper helps manage the IOC Daily Schedule in the context of all emergent events, such as search and rescue, pollution spills, and other events typically occurring outside of the operational planning window. WatchKeeper creates and shares the tactical picture, including command and control, mission status, and status of IOC forces/Blue Force Tracks (BFT), which consist of IOC member identified mobile resources or assets (*i.e.*, vessels, people, aircraft).

These capabilities support the interagency operations process described in the DHS IOC Concept of Operations (CONOPS) and reflects best practices outlined in the DHS Maritime Port Operations Handbook. The WatchKeeper supports an interagency operational planning process at a Sensitive But Unclassified (SBU) level in an electronic collaborative environment. Interagency planning is the process that includes entities such as Coast Guard, other government agencies, and local port partners that collaborate in a shared computing environment for the purposes of establishing a proactive security environment.

In addition to the above, USCG uses the existing CBP ATS-N and ATS-P modules as tools to screen pre-arrival vessel cargo, crew, and passengers. The ATS-enhanced WatchKeeper will provide near real-time data for the Captain of the Port (COTP) to better evaluate threats and deploy resources through active collection of incoming vessel information. With a more detailed

picture of the risk profile that the vessel presents, the COTP can make appropriate, informed decisions well ahead of the vessel's arrival to the port.[10]

ATS-N evaluates all cargo to identify high risk inbound cargo for examinations. ATS-N uses numerous rule and weight sets to analyze information from manifest, importer security filing, and entry data, to prioritize shipments for review, and to generate recommended targets by scoring each shipment. ATS-N not only screens commodity information on manifest, importer security filing, and entry data, but also screens individuals, against lookouts and prior violations, who are identified on those data sources.

ATS-P is a web-based enforcement and decision support tool used to collect, analyze, and disseminate information for the identification of potential terrorists, transnational criminals and, in some cases, other persons who pose a higher risk of violating U.S. law. ATS-P capabilities are used at ports of entry to augment the CBP officer's decision-making about whether a passenger or crew member should receive additional screening.

ATS-P provides a hierarchical system that allows USCG personnel to focus efforts on potentially high-risk passengers by eliminating labor-intensive manual reviews of traveler information or interviews with every traveler. The assessment process is based on a set of uniform and user-defined rules based on specific operational, tactical, intelligence, or local enforcement efforts.

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

Yes. WatchKeeper relies on CBP's ATS rules engine for cargo and vessel targeting.[11] To manage daily operations, the system polls data from disparate sources, organizes this information into a useful workflow, creates visualizations to alert the watchstander, and shares the situation picture with IOC partners so they can act in a unified manner.

Integrated Vessel Targeting (IVT): WatchKeeper integrates targeting results of agency-specific screening processes and builds a consolidated threat picture of vessels and cargo operating within the IOC OPAREA (*e.g.*, a specific port) in support of the Ports, Waterways, and

[10] Additional information on ATS-Enhanced WatchKeeper may be provided to the Congress in a separate annex that contains Sensitive Security Information.

[11] For a detailed description and analysis of privacy risks of the Automated Targeting System, please see the DHS/CBP/PIA-006(b) Automated Targeting System (ATS) Update PIA, June 1, 2012.

Coastal Security Mission. The PII that is obtained from external systems and temporarily stored within the system consists of complete crew and passenger lists received from the Coast Guard's SANS and CBP's ATS. Although PII is contained and used in the system, WatchKeeper does not place any derived information into an individual's existing record nor does it create a new record as a result of these operations. The system is focused on vessel traffic and not specific individuals; therefore, the system's use is not for taking actions against an identified individual because of newly derived or queried data.

Interagency Operations Planning (IOP): WatchKeeper integrates federal, state, and local resource status and schedules within and across OPAREAs. Mission requests are created from Integrated Vessel Targeting results, along with other mission demand sources, such as regattas, patrols, and escort missions. These mission requests are prioritized by IOC decision makers, who assign resources to missions. These assignments form the IOC Daily Schedule.

Operations Monitoring (OM): WatchKeeper helps manage the IOC Daily Schedule in the context of all emergent events, such as search and rescue, pollution spills, and other events typically occurring outside the operational planning window. WatchKeeper creates and shares the tactical picture, including command and control, mission status, and status of IOC forces/Blue Force Tracks (BFT).

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

Yes. WatchKeeper users (*i.e.*, those individuals at the IOC) include personnel from the Coast Guard, CBP, Immigration and Customs Enforcement (ICE), the Federal Bureau of Investigation (FBI), and other federal, state, and local government personnel with a need to know the information. However, the WatchKeeper system does not share information with other DHS Component systems or with other systems outside of DHS.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that inaccurate information within WatchKeeper will be used for a law enforcement purpose.

Mitigation: IOC users are reminded through training curriculum, job aids, and embedded pop up notices that instruct users to re-validate all data displayed by WatchKeeper with the government source system responsible for providing the data. Such notifications are provided prior to any actual enforcement actions or boardings taken to mitigate the impact of data errors encountered during the transaction of the data from the information source to WatchKeeper.

Privacy Risk: Authorized users of WatchKeeper could use their access for unapproved or inappropriate purposes.

Mitigation: All WatchKeeper users must undergo privacy training and obtain approval from their supervisor, IOC WatchKeeper Sector Administrator, and the WatchKeeper Account Manager before gaining access to the system and its data. The WatchKeeper system performs extensive auditing that records the search activities of all users. These audit logs are reviewed upon request and any inappropriate use will be referred to the appropriate internal investigations for handling. The detection of inappropriate use will also result in the suspension of the user's access to WatchKeeper until the use can be investigated. Audit trails are created throughout the process and are reviewed if a problem or concern arises regarding the use or misuse of the information. During the log-in process, the account owner must acknowledge his/her consent to monitoring for inappropriate use or he/she cannot access the system. Additionally, WatchKeeper has role-based access, which is restricted based on a demonstrated need to know the information.

Section 4.0 Notice

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

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

WatchKeeper's data and records are a compilation of many sources. WatchKeeper does not collect information on individuals directly, but uses data containing PII retrieved from other systems. Additionally, WatchKeeper and IOC personnel do not interact directly with individuals to collect PII. However, through the publication of this PIA and SORNs applicable to the various source systems noted in Section 2.1, notice has been provided.

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

WatchKeeper does not collect information directly from individuals; therefore, notice is not directly provided from WatchKeeper. Any consent individuals may grant is controlled by the source systems described in earlier sections. Opportunities for individuals to consent to particular uses of information are addressed using the processes defined by the source systems.

As most information collected by these systems is mandated by law, there is effectively no consent mechanism other than the choice of whether to travel or ship items.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that the individual may not know that the information is being used by WatchKeeper in the ways described.

Mitigation: Both Coast Guard and CBP have published SORNs for the systems from which WatchKeeper obtains PII. Individuals, upon request, are referred back to the source system sponsor or owner. Furthermore, Coast Guard has published this PIA to increase transparency of its operations.

Section 5.0 Data Retention by the project

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

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

WatchKeeper ingests information from various other systems, and accesses other systems without ingesting the data. To the extent information is ingested from other systems, data are retained in WatchKeeper in accordance with the record retention requirements of those systems, or the retention period for WatchKeeper (i.e., data is cached for use a maximum of 32 days after arrival or departure, and then deleted), whichever is shortest.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: Data may be retained in WatchKeeper for too long.

Mitigation: WatchKeeper retains data according to the SORN requirements of the system from which the data was obtained, or 32 days after arrival or departure, whichever is shorter. Monthly "purges" of the database are performed to ensure that only current and relevant PII in the context of the 32 day retention period is retained.

Coast Guard will regularly review the retention period for WatchKeeper to ensure its continued relevance and usefulness. If these reviews demonstrate that certain data is no longer relevant and useful, Coast Guard will revise the retention period and delete the information.

Section 6.0 Information Sharing

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

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

No. WatchKeeper only ingests information from other systems. It does not share any information with any other systems, either internally or externally to DHS.

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

WatchKeeper only ingests information from other systems. It does not share any information with any other systems, either internally or externally to DHS.

6.3 Does the project place limitations on re-dissemination?

No. WatchKeeper only ingests information from other systems. It does not share any information with any other systems, either internally or externally to DHS.

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

WatchKeeper only ingests information from other systems. It does not share any information with any other systems, either internally or externally to DHS.

6.5 Privacy Impact Analysis: Related to Information Sharing

There is no privacy risk related to information sharing. WatchKeeper only ingests information from other systems. It does not share any information with any other systems, either internally or externally to DHS.

Section 7.0 Redress

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

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

Individuals may follow the procedures outlined in the PIAs and SORNs of the source systems to gain access to their information stored in those systems. Individuals seeking notification of and access to any record contained in this system, or seeking to contest its content, may submit a Freedom of Information Act (FOIA) or Privacy Act request in writing to:

United States Coast Guard
Commandant (CG-611)
2100 2nd St. SW, Stop 7101
Washington, DC 20593-0001
Attn: FOIA Coordinator

FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Specific FOIA contact information can be found at http://www.dhs.gov/foia under *contacts*.

When seeking records about oneself from WatchKeeper or any other Coast Guard system of records, the request must conform to the Privacy Act regulations set forth in 6 CFR part 5. An individual must first verify his or her identity, meaning that he or she must provide full name, current address, and date and place of birth. The request must include a notarized signature or be submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, forms for this purpose may be obtained from the Director, Disclosure and FOIA, http://www.dhs.gov/foia or 1-866-431-0486. In addition, the following should be provided:

- An explanation of why the individual believes DHS would have information on him or her,
- Details outlining when he or she believe the records would have been created, and
- If the request is seeking records pertaining to another living individual, it must include a statement from that individual certifying his/her agreement for access to his/her records.

Without this bulleted information, the United States Coast Guard may not be able to conduct an effective search, and the request may be denied due to lack of specificity or lack of compliance with applicable regulations.

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

Individuals may follow the procedures outlined in the PIAs and SORNs of the source systems to correct inaccurate or erroneous information stored in those systems.

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

The source system SORNs and PIAs provide information on accessing and amending information collected through those systems.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not have access to information maintained about them in WatchKeeper or be able to correct their information..

Mitigation: Individuals may request access to information about themselves through the redress procedures of the source systems' SORNs (see Section 1.2). Individuals have an opportunity to request access, amendment or correction to their records.

Section 8.0 Auditing and Accountability

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

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

There are numerous controls in place to ensure that information is handled in accordance with the above described uses.

WatchKeeper has role-based access. All user groups will have access to the system defined by the specific user's profile and limited through reference to the determined rights and

responsibilities of each user. Access by users, managers, system administrators, developers, and others to the WatchKeeper data is defined in the same manner and employs profiles to tailor access to mission or operational functions. WatchKeeper user roles are highly restricted and audited. Access is restricted in the form of role based access, which is based on a demonstrated need to know the information.

All users with access to WatchKeeper are required to complete security and privacy training on an annual basis and their usage of the system is audited through a number of overlapping system, database, and application level controls and reports to ensure compliance with all privacy and data security requirements.

This list of audited events is based upon the system's risk assessment and the applicable Coast Guard and DHS policies, and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS). WatchKeeper audit records are centrally managed. All of the system's servers have their system clocks synchronized so that the audit records are time coordinated across all of the servers. Audit data from all servers can be viewed in real-time and are stored both online and offline in compliance with DHS security requirements.

The WatchKeeper Information Assurance (IA) team and system engineers also review and update the content, which will be audited for the information system on a regular basis (at least weekly) or as certain risks to the information system are discovered.

In addition, the system undergoes both scheduled and ad hoc security audits.

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

All authorized users and contractors are required to complete the initial and refresher training provided by Coast Guard. This training provides all employees with the initial training requirements, including computer usage, information security, physical security access, privacy, and incident response initiatives. All users are required to undergo annual refresher training. In addition, appropriate support personnel, administrators, and managers receive training on updated system components, administration, and security requirements for any newly installed components as appropriate for duties. For Coast Guard civilian, active, and reserve duty military personnel, this brief is located on the e-Learning portal. The Coast Guard Information Assurance Division at the Coast Guard C4IT Service Center (C4ITSC) in Alexandria, VA, supplies contractor employees and others without an employee identification number (EMPLID) with automated training. In accordance with (IAW) COMDTINST 5500.13, U.S. Coast Guard Information Assurance (IA) for Unclassified Information Systems, user accounts and access

privileges, including access to email, are disabled for Coast Guard employees and contractors who have not received annual refresher training, unless a waiver is granted by the Coast Guard Chief Information Security Officer/Information Systems Security Manager (CISO/ISSM).

User training is also addressed in the Rules of Behavior for WatchKeeper. The users must read, acknowledge, and sign a form-agreeing to the conditions when requesting access. Access is only granted upon receipt of this form. IAW COMDTINST 5500.13, U.S. Coast Guard Information Assurance (IA) for Unclassified Information Systems, access rights will be suspended for users who do not receive annual Information Security training.

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

WatchKeeper user access is restricted in the form of role-based access assigned based on the user's role. Users cannot assign their roles to any other user, nor can they elevate their own rights within the system. Per the WatchKeeper Access Control Policy, a need-to-know and a system access requirement is validated by the IOC WatchKeeper Sector Administrator and the WatchKeeper Account Manager prior to approving WatchKeeper account requests. System administrator/engineering accounts (accounts with escalated privileges) must be reviewed and approved by the WatchKeeper Program Manager.

Access to the WatchKeeper system is based upon successful login using multi-factor authentication. There are two login methods for the system. WatchKeeper users with DoD Common Access Cards (CAC) authenticate to the Coast Guard's remote access solution (Juniper). The Juniper solution validates the user's login credentials using the Coast Guard Active Directory/Exchange Information System. Non-CAC users use a VeriSign Identify Protection (VIP) card for login. This device provides a one-time PIN number (unique PIN is generated for each login session) that is used in conjunction with their username and password to authenticate to the VeriSign Radius servers. These methods of authentication utilize a two factor approach and are FIPS 201 and NIST 800-63 level 3 Assurance System compliant.

All connections to the WatchKeeper system are encapsulated within a software VPN tunnel meeting FIPS 140-2 level encryption requirements.

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

WatchKeeper is an intake-only system and does not share any information with any other systems, either internally or externally to DHS. There are agreements/arrangements in place to govern WatchKeeper's access to information. These agreements or arrangements are drafted by the business owners with input from the program managers. Arrangements that involve PII are sent to the Coast Guard Privacy Officer for review and to DHS for final approval in accordance with procedures developed by the DHS Information Sharing and Safeguarding Governance Board (ISSGB).

Responsible Officials

Captain Robert S. Wilbur
CG-0933
United States Coast Guard
Department of Homeland Security

Approval Signature

Original signed and on file with the DHS Privacy Office.

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security