Privacy Impact Assessment
for the

Critical Infrastructure Warning Information Network

January 7, 2006

Contact Point
Kevin Piekarski
CWIN Program Manager
Information Assurance and Infrastructure Protection
703-235-5335

Reviewing Official
Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Introduction

This Privacy Impact Assessment (PIA) examines the privacy implications for the Critical infrastructure Warning Information Network (CWIN). The Department of Homeland Security (DHS) is responsible for protecting the national infrastructures. DHS is also responsible for ensuring that in the event cyber or physical infrastructures are compromised, there is a means to collaborate and coordinate the necessary resources to restore impacted infrastructures. The mission of CWIN is to facilitate immediate alert, notification, sharing and collaboration of critical infrastructure and cyber information within and between Government and industry partners. CWIN provides a technologically advanced, secure network for communication and collaboration, and alert and notification.

CWIN is DHS' only survivable, critical communications tool not dependent on the Public Switch Network (PSN) or the public internet that can communicate both data and voice information in a collaborative environment in support of infrastructure restoration. CWIN provides a survivable, dependable method of communication allowing DHS to communicate with other federal agencies, state and local government, the private sector, and international organizations in the event that primary methods of communication are unavailable.

CWIN Members belong to one of the vital sectors of the national infrastructure as named in the National Response Plan, appear in the Interim National Infrastructure Protection Plan, or are a state Homeland Security Advisor. Only CWIN members have access to CWIN. CWIN membership is by invitation only, with invitations issued from the Infrastructure Coordination Division (ICD) Director through a contractor. The CWIN operation consists of the collection of point of contact information for administrative purposes, and the placement of a CWIN terminal at member locations. Should an event occur where traditional communication methods are not operable, CWIN provides a communication method between key infrastructure sites across the country.

SECTION 1 QUESTIONS ABOUT THE DATA AND ITS PURPOSES

1.1 What information is to be collected?

Two sets of information are collected from member organizations.

First, the CWIN Program Office requests Point-of-Contact information (referred to as Administrative POC information) from CWIN Members consist of name, title, company name, business telephone number, and business email address. A contractor (Arrowhead Global Solutions, Inc) stores and maintains this information off-site from the CWIN Program Office. Member organizations designate who, within their organization, will be the CWIN Administrative POC of record. This collection of personal information is covered by the DHS System of Records Notice 002 published December 6, 2004 69 Fed Reg 70460 DHS/ALL 002.

Second, and more central to the CWIN mission, the CWIN Program Office maintains the CWIN Membership Directory which contains the member organizations' corporate or government agency name, CWIN email address associated with the member organization, and designated installation site location. The contractor assigns the CWIN email address subject to approval by the CWIN Program Manager.

CWIN accounts are assigned to the organization as a whole; no individual user can be identified in the Membership Directory. The Directory is necessary in order for members to contact each other. The directory is updated monthly.

1.2 Why the information is collected?

The Administrative POC information is collected in order to manage CWIN membership, including invitations and resignations, and to involve CWIN members in CWIN activities.

The Member Directory information is collected in order to execute CWIN's critical communication mission. In the event of either a threat to or an attack on one of our Nation's critical infrastructures or key resources, CWIN will allow government agencies and industry to be able to communicate and coordinate efforts in real time without having to depend upon the PSN, which can be subject to disruptions.

1.3 Is it relevant and necessary to the purpose for which the system is designed?

The CWIN Program Office requests administrative POC information from potential CWIN members in order to complete CWIN installations, maintain accountability of CWIN equipment, and communicate policy changes and routine information regarding CWIN. Administrative POC information is also used to invite members to the annual CWIN Membership Forum; no other use of this information is permitted. Administrative POC information is maintained in a database that is available only to designated individuals, including the DHS CWIN Program Manager, as well as members of the contractor staff that support the program.

The CWIN Membership Directory provides organizational contact information for the CWIN community to utilize only on CWIN. Since CWIN does not connect to the internet or the PSN, the information in the Membership Directory is only accessible to previously vetted CWIN members. The Membership Directory identifies information by organization only and lists only CWIN Voice Over Internet Protocol (VoIP) phone extensions and CWIN email addresses for each organization; no external phone numbers or email addresses are included. The information in the Directory makes it possible for members to communicate and share critical infrastructure information, which is the purpose of CWIN.

1.4 What is the intended use of the information?

The POC information is used to manage CWIN membership.

The CWIN Membership Directory, available on CWIN, allows for CWIN member organizations to communicate with each other. In the event of an attack or major infrastructure disruption, CWIN would provide direct, real-time connectivity between all sectors of critical infrastructure and key government entities. Industry and government will be able to make proactive decisions to minimize damage and reduce recovery time. During the recovery process, CWIN partners will be able to share information, assign duties and cooperate to repair damages to critical infrastructures.

1.5 What are the sources of the information?

Administrative POC information and Membership Directory information is provided directly by the organization. Membership Directory information (including CWIN email address and VoIP extension) are assigned by the contractor and approved by the CWIN Program Office. The name of the organization as it appears in the Membership Directory is suggested by the member.

1.6 Where and how are you acquiring the information?

Once the Department of Homeland Security identifies a CWIN member, the contractor is instructed to begin the invitation process through phone conversations and emails via the public communications network. Upon acceptance, the contractor sends an official welcome letter and site survey via the public network. Once the CWIN installation is complete, POC information for the CWIN site is requested through a verifying email (again, via the public network).

1.7 How the information is checked for accuracy?

Administrative POC information can be updated and corrected at any time by the member organization. The accuracy of this information is ensured by the members themselves through the CWIN Program Office and the contractor housing the Administrative POC information.

Email via CWIN is sent to the member organizations to verify members' information contained in the Membership Directory on a monthly basis. The CWIN Directory is reviewed monthly by the members and updated accordingly. Members report changes or corrections to the CWIN program manager via CWIN. Periodic audits of the Member Directory are performed to ensure the accuracy of CWIN email addresses, CWIN VoIP phone extensions, and site locations.

1.8 Will the system derive new data or create previously unavailable data about an individual through aggregation for the information collected?

No new data is created or interpolated by CWIN. Since the administrative POC information is collected from the CWIN member and no other information is collected, there is no aggregation of data. The information collected on participant organizations and their infrastructure is not utilized in any capacity other than for the purpose of communication between users.

1.9 Will the newly derived data be placed on the individual's record?

No new data is created.

1.10 Can the system make new determinations about an individual that would not be possible without the new data?

No.

1.11 How will the newly derived data be verified for relevance and accuracy?

Not applicable. No new data is created.

1.12 Are the data elements described in detail and documented?

Yes. CWIN data elements, membership parameters, and a description of the CWIN mission and operation are described in the CWIN *Report* issued by the CWIN Program Office issued through the Infrastructure Partnerships Division of the Information Analysis and Infrastructure Protection Directorate.

SECTION 2 QUESTIONS ABOUT REDRESS:

2.1 What opportunities do individuals have to decline to provide information?

Regarding Administrative POC information, at a minimum CWIN operations requires the name of a contact person as well as a way to contact the individual (phone or email). In order to be a CWIN Member an invitee must furnish a minimum of contact information in order to participate in CWIN.

It is possible for a CWIN member organization to request that its information be excluded from the CWIN Membership Directory, but such determinations are made by the CWIN Program Manager and are not common.

2.2 What opportunities do individuals have to consent to particular uses of the information?

Administrative POC information for individual CWIN members is used by the CWIN Program Office in order to send membership forum invitations. If an individual no longer wishes to be the administrative POC, the information may be updated by the CWIN member organization.

CWIN member organization and member POC information is used for official CWIN business only. Member organizations may request their information be withdrawn from the CWIN Membership Directory at any time by sending an email, via CWIN, to the CWIN Program Manager. As stated in Question 2.1, such determinations are made by the CWIN Program Manager and are not common.

2.3 How do individuals grant consent concerning how their information will be used or shared?

By engaging in the DHS membership vetting process, and by accepting an invitation to join CWIN, members grant consent concerning how Administrative POC and organizational information contained in the CWIN Membership Directory is used.

2.4 What are the procedures for individuals to gain access to their own information?

Individual CWIN members may request access to their own administrative POC information from the CWIN Program Manager at any time. The CWIN Project Manager will then contact the contractor and arrange any change of information that may be needed.

The CWIN Membership Directory is stored in the library on the CWIN active desktop. All CWIN members have access to the directory. Should information in the Directory need to be changed or updated the member would submit information to the CWIN Project Manager through the CWIN network.

2.5 What are the procedures for correcting erroneous information?

Member organizations should contact the CWIN Program Manager to report erroneous information found in the Administrative POC information or in the CWIN Membership Directory. The CWIN Program Manager notifies the contractor to correct the error.

SECTION 3 QUESTIONS ABOUT ACCESS TO THE DATA

3.1 Who will have access to the data in the system (users, managers, system administrators, developers and others) and is it documented?

The CWIN Program Manager, CWIN members, CWIN Administrators, and the CWIN Program Office have access to the CWIN Membership Directory. Only the CWIN Program Manager and the contractor have access to the administrative POC information.

Membership criteria are documented in the CWIN Concept of Operations and Standard Operating Procedures. CWIN Members come from three categories of users: member of vital infrastructure sectors (electric, information technology, and telecommunications), are considered Sector Specific Agencies or Resources as outlined in the Interim National Infrastructure Protection Plan, or are Homeland Security Advisor for each state. Homeland Security Advisors for the territories of the United States will be added once funding is secured.

3.2 How will access to the data by a user be determined?

Participation in CWIN is by invitation only (see answer to question 1.6). Only those who have access vetted by DHS and who have joined the network will have access to information in the CWIN Membership Directory.

3.3 Are criteria, procedures, controls, and responsibilities regarding access documented?

First, policies dictating information security and special access are available in the form of CWIN Acceptable Use and Behavior Policies. Members are expected to abide by those policies and violation of CWIN policy would result in termination of membership. Second, membership criteria are documented in the CWIN Concept of Operations and Standard Operating Procedure. Lastly, Memoranda of Understanding between each CWIN Member, DHS leadership, and the CWIN Program Manager are in the process of being completed and signed.

3.4 Will users have role-based access to data on the system limiting them to some but not all of the data?

Yes. Certain groups of individuals are provided access to Administrative POC INFORMATION in order to conduct their duties. The CWIN Program Office and the contractors used to administer the system are provided access to the Membership Directory in order to conduct CWIN activities.

3.5 What controls are in place to prevent the misuse of data by those having access?

Access to system files and folders is closely monitored with automated verification system and system-generated audit trail logging. Activities of the CWIN engineering staff are included in the monitoring process to ensure global oversight is maintained.

Information in the Membership Directory is accessible to all members, unless a member requests to withdraw from the Membership Directory.

No individual administrative POC information is available over CWIN.

Information on system usage is collected for audit purposes as mandated by Defense Information Systems Agency (DISA) security profile regulations. The data stored in the system audit logs pertains to organizational user accounts and cannot be tied to a specific individual.

3.6 Do other systems share data or have access to data in this system?

CWIN is a closed network that is not interoperable with other networks.

3.7 Will other agencies share data or have access to data in this system?

CWIN members include international, Federal, state and private sector organizations.

3.8 How will the data be used by these other agencies?

Only appropriate individuals employed by the contractor maintaining the information and the CWIN Program Office have access to the administrative POC information.

The Membership Directory is not shared with anyone outside of CWIN.

3.9 Who is responsible for assuring proper use of the data by other agencies?

The CWIN Program Manager is responsible for proper use of data and overall CWIN operations. Policies dictating the handling and usage responsibilities of data stored on CWIN are available in the CWIN Acceptable Use and Behavior Policies. CWIN Members are expected to abide by such policies as a condition of membership. Additionally, Memoranda of Understanding between each CWIN Member, DHS leadership, and the CWIN Program Manager are in the process of being completed and signed.

3.10 How will the system ensure that other agencies only get the information they are entitled to?

Information contained within the CWIN Membership Directory is necessary for members to carry out the mission of CWIN. CWIN members are entitled to this information by virtue of the CWIN Concept of Operations.

SECTION 4 QUESTIONS ABOUT MAINTANCE AND ADMINISTRATIVE CONTROLS

4.1 How will the information be secured and is it consistent with agency requirements under the Federal Information Security Act? Specifically:

4.1.a Affirm that the agency is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured;

In May 2004, the National Communications System (NCS) Designated Approving Authority issued to CWIN an Authority to Operate (ATO) for three years, expiring April 15, 2007. The accreditation is based on the comprehensive Security Test and Evaluation (ST&E) performed in December 2003 by the Defense Information Systems Agency. It signifies completion of the Department of Defense Information Technology Security Certification and Accreditation (DITSCAP). NCS was the lead organization for this effort; in March 2003 NCS transitioned to DHS. On May 11, 2004, CWIN received its Authority To Operate (ATO) from the National Communications System.

CWIN is FISMA and OMB Circular A-130 compliant.

CWIN has a System Security Authorization Agreement (SSAA)(June 2005). The SSAA addresses issues relevant to the requirements of NIST SP 800-18 and 800-37 in the areas of security controls, auditing, password management, risk management, data sensitivity management as well as security life-cycle management and review of security controls and methodologies.

4.1.b Acknowledge that the agency has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls;

The CWIN Program Office approved a final Risk Assessment and Management Plan in December 2004. The document outlines risks and mitigations taken to address those risks.

CWIN is a Federal IT system with a high degree of sensitivity with the following operational mandates: a high degree of confidentiality, a high degree of information integrity and high degree of availability (as prescribed by the National Institute of Standards and Technology (NIST) Special Publication 800-26, providing information concerning an IT system's sensitivity assessment. Physical assets, equipment, software, and documentation are stored in locked facilities. Modifications to software including extracting functionality to prevent unwanted consequences to limit the possibility of compromise and user privileges were tailored to the client. Hardware was modified to limit remote access and to restrict the storage of residual data on user platforms. The local operating system was customized to enhance security.

Management and operational security controls are incorporated into the Standard Operating Procedures, which have been distributed to all CWIN users.

4.1.c Describe the monitoring/testing/evaluating on a regular basis to ensure that controls continue to work properly, safeguarding the information.

CWIN administrators test the network each month to ensure continued compliance with its DITSCAP certification. On a daily basis, the network administrator performs checks on the significant components of the network, i.e. servers, routers, exchanges, antivirus software and power supplies. Monthly, CWIN participants servers are subjected to a rigorous security profile audit that reviews security and configuration settings spanning every aspect of the operating system.

Consistent with continuity of operations best practices, CWIN administrators back up the network once every 24 hours. The tapes contain only the data resident on the system at that time. Data is archived to tape and stored at an off-site location.

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

CWIN consists of data centers and multiple end user locations. CWIN uses a Commercial Off the Shelf (COTS) operating system with terminals for each user. Applications and data are deployed and executed from the data centers. The terminal technology offers data and desktop security. However, it is important to note that no data resides on the desktop. The CWIN Concept of Operations and Standard Operating Procedure govern use of the CWIN pathway. Both documents are accessible to members through the library of the CWIN and are provided at sign up. The CWIN Membership Directory is available to all members and is stored at the datacenter.

4.3 What are the retention periods of data in the system?

Contact information is maintained in the Membership Directory for as long as the organization is a CWIN member or until a member requests the CWIN Program Manager remove the information.

DHS is working with National Archives and Records Administration to obtain approval of a records retention and disposal schedule. Until an approved records retention and disposal schedule is established, records are retained indefinitely.

4.4 What are the procedures for expunging the data at the end of the retention period and are these procedures documented?

When member information must be changed or deleted to reflect a change in membership name, address, or contact information, the data is removed from the network. The contractor administrator maintains historical information in a password-protected database accessible only to approved personnel.

4.5 Will the system provide the capability to monitor individuals or groups of individuals?

No.

4.6 What controls are in place to prevent unauthorized monitoring of individuals or groups of individuals?

Not applicable. This system is not capable of monitoring individuals.

4.7 Under which Systems of Record Notice (SORN) does the system operate?

Not applicable. A System of Records Notice is not required for CWIN.

SECTION 5 DECISION ANALYSIS

5.1 Did you evaluate competing technologies on their privacy handling capabilities?

CWIN was developed as DHS' critical, survivable network during incidents of national significance when the internet or PSN are inoperable. While other DHS systems utilize internet-based technologies for information sharing, CWIN does not. Internet access presents opportunities for invasion of privacy and vulnerabilities affecting reliability. CWIN mitigates both issues because it is a closed network, independent of the internet or the PSN.

5.2 Were any choice changes made to system architectures, hardware, software, or implementation plans as a result of doing a PIA?

The nature of the system architecture for CWIN is such that communications do not contain personally identifiable information. CWIN has a user policy that prohibits passing information of a personal nature while using a Government network. CWIN Project Management Office stores all information related to infrastructure and communication amongst CWIN members, and administrative POC information is collected and stored by a contractor on the contractor site.

It was determined that the information collected by CWIN, including administrative POC information and infrastructure information, was the least amount necessary to carry out CWIN's operation mission. Should more information be required in the future, or information be shared with other entities not mentioned herein, this Privacy Impact Assessment will be amended to reflect such changes.

Conclusion

CWIN provides essential infrastructure institutions with a survivable communication network not dependent on public means of communication. The use of personally identifying information has been limited to one area: Administrative Point of Contact information. Administrative Point of Contact information is used in a very limited fashion and is securely stored by the contractor. The CWIN Membership Directory uses no personally identifying information. These two sets of information are not commingled. Administrative POC information is available only to the contractor and the CWIN Program Manager, and the CWIN Membership Directory is available only to CWIN Member and the CWIN Program Manager.

Responsible Officials

Kevin C. Piekarski, CWIN Program Manager

Department of Homeland Security

Approval Signature Page

_____ January 7, 2006

Maureen Cooney
Acting Chief Privacy Officer
Department of Homeland Security