Secure Data Network Standards and Procedures

Centers for Disease Control and Prevention (CDC)
Agency for Toxic Substances and Disease Registry (ATSDR)
HISSB Adopted - July 15, 1999

I. Purpose

The purpose of this document is to establish agency standards and operating procedures for the use of CDC/ATSDR Internet resources in the secure transmission and processing of sensitive or critical data and the support of sensitive or critical systems.

The CDC/ATSDR Health Information Systems and Surveillance Board (HISSB) has adopted a Policy for the Secure Internet Exchange of Information, which provides for the creation and operation of a secure Internet connection and gateway facility termed the *Secure Data Network* (SDN) to meet the agencies' legal obligations and mission-critical objectives. The SDN is a set of tools implementing the policy requirements for authentication using industry standard X.509 certificates, secure tokens, and other applicable means as identified; an encryption engine; and access control through the firewall by data routing to programs using an application server.

This document is intended to implement, support, and augment the policy through establishing specific standards and procedures governing the use and operation of the SDN by the CDC Information Resources Management Office (IRMO). This network is intended to allow field staff, researchers, and public health partners to securely exchange confidential, Privacy Act, proprietary and other sensitive or critical data with Center/Institute/Office (CIO) programs. The SDN also provides secure access to critical CDC/ATSDR Internet tools, program applications software and sensitive or critical data resources that can be conveniently implemented by CIO programs. Note that the SDN only serves as a mechanism from moving secure data from a client site to a program's application. Nothing in this standard prohibits a program's ability to operate their own Web servers, applications, and database servers inside the CDC/ATSDR firewall.

These standards and procedures governs all Internet-based secure access to CDC/ATSDR. The SDN shall be the Internet security system used by all CDC/ATSDR programs unless an explicit exemption has been granted.

II. Terminology

The terms CDC/ATSDR, "the Agency" or "the Enterprise" used in this document mean the Centers for Disease Control and Prevention (CDC) and the Agency for Toxic Substance and Disease Registry (ATSDR) and all their subordinate operating units.

The term "sensitive data or system" includes all data and data systems subject to the Privacy Act as a result of explicit personal identifiers within the data, data subject to the potential for Privacy Act violations due to "small-cell size" risks, trade secrets and other proprietary data, data shared with or provided to CDC/ATSDR by another entity and designated as sensitive by that entity or any other data designated by the Director of CDC or by a CIO within CDC/ATSDR as sensitive.

The pharse “external user” means any user of the CDC/ATSDR Internet connection who is not a legitimate user of the CDC Intranet.

The phrase “critical data or system” means any system (whether or not designated as sensitive) that is critical for the success of the CDC/ATSDR missions as defined by the Business Steward responsible for the data. Critical data and systems are those which if lost, corrupted, diverted or misused could result in unacceptable consequences to public health, individual health and safety, agency financial resources, agency continuity of operations, agency compliance with statutory and regulatory requirements, agency litigation risk, agency image and credibility, trading partner confidence, and agency collaborations with other institutions.

III. Background

The CDC/ATSDR Policy For Secure Internet Exchange of Information *states: “Growing use of the Internet by both the public and private sector is rapidly making network an important medium for information exchange. While the Internet allows for easy connectivity, such ease is counter-balanced by inherent issues concerning the ability to protect the privacy and integrity of information and to ensure that information is accessible only by those for whom it was intended.*

Information and data can be transmitted over the Internet -- and other media -- by connecting to servers through various protocols such as FTP (File Transfer Protocol) and HTTP (Hyper Text Transfer Protocol), as an E-mail message or attachment, or by connecting to a system as a remote user. ***Without adequate protection, information transmitted over the Internet does not inherently possess any assurance that the information actually originated from the indicated source (addresses may be spoofed), that it has been viewed only by intended parties (information might be intercepted either during transmission or from an intrusion on the local or remote systems), or that it has remained unchanged during transmission. [emphasis added]*** *In order to define appropriate security controls, the information must be categorized according to the potential harm associated with its loss, alteration or disclosure. The information can be protected by the appropriate use of security controls, including encryption, authentication, integrity verification, and assurance of non-repudiation applied to the transmission process.”*

The greatest threat to secure data exchange is not while the data are traversing the Internet but while the data reside on workstations and servers that are accessible from the Internet. However, user IDs and passwords are also vulnerabilities. To access host systems, hackers may listen on corporate and public networks for login and password information.

The SDN provides a CDC/ATSDR solution for programs needing to protect data while protecting our host systems and providing security for packet transmissions. It is recognized that the SDN may not meet the needs of all programs. Hence, the SDN Standard and present CDC/ATSDR policy allows for the introduction of alternative methods after formal approval.

To provide secure, manageable, and reliable Internet-based communications, it is critical that the CDC/ATSDR adopt standards-based, unified, enterprise-wide solutions for:

- User authentication;
- Access control (authorization) and communications routing; and
- Secure data storage and transfer, management of sensitive data, and encryption key management.

User Authentication requirements include the ability to:

1. assure that the parties to any sensitive electronic transaction are who they claim to be;

2. support bilateral authentication in which both users and agency programs can be certain that they are connected to or communicating with the correct uniquely identified individual or entity;

3. provide for multi-step electronic trust relations supported by industry standard Certificate Authority services; and

4. assure the agency-wide use of up-to-date, industry standard methods, procedures and policies.

Access Control (Authorization) and Communications Routing requirements include the ability to:

1. establish administrative and operational procedures that can enable and enforce decisions of CDC/ATSDR programs for access control of their data systems and data resources.

2. identify program personnel (required to be government employees) who will designate which users may establish secure connections to the program Internet resources and which agency staff may establish, maintain and operate server-level or back-end computational or routing facilities that process sensitive data. In addition, to delineate the chain-of-command within the programs and CIO's with respect to the SDN service request, approval and authorization.

3. establish an Access Control Database Management System that will allow automated routing of secure information from authorized users to the programs, provide secure proxy services for trans-firewall operations, and which will enforce program access control decisions. In addition, to establish an agency-level coding system that provides unique identifiers (address or codes) for each program and program activity that requires SDN services.

Secure Data Storage and Transfer requirements include the ability to:

1. securely move data files across the CDC/ADSDR firewall;

2. provide secure remote access to CDC/ATSDR Intranet applications and data residing on the CDC mainframe and SQL servers; and

3. assure the agency-wide use of industry standard means of data encryption, message digest and digital signature.

The SDN is designed to readily provide these features to programs. Alternative solutions proposed by programs must provide for equivalent access and security controls and provide for acceptable administrative controls.

IV. Standards

Scope

These standards and procedures shall apply to all Internet-based activities that transfer sensitive or critical data, provide Internet access to sensitive or critical systems, or that provide access to data and systems resources residing within the CDC/ATSDR firewall (unless explicit exemption has been granted). Any CDC/ATSDR data system or resource that may reasonably be expected to include sensitive data at some future time should be considered a sensitive data resource or system from the beginning.

Implementation Date

Operation of the SDN throughout CDC/ATSDR shall start only after completion of an acceptable operational pilot over several months testing all features and acceptance of a report on the pilot operation by HISSB. Until such time, CIO programs are encouraged to join the pilot study or submit alternative solutions as required by this standard.

Relationship With Other Policies

The following US Government and CDC/ATSDR policies and standards are incorporated by reference into this standard:

1. CDC/ATSDR Internet Policy: Secure Internet Exchange of Information (98.1), which authorizes CDC/ATSDR programs to use the Internet for transmission of Privacy Act and other sensitive or critical data provided that certain security requirements are satisfied. This policy also requires the establishment of the SDN under the CDC/ATSDR Information Management Resource Office (IRMO).

2. Office of Management and Budget circular A-130, which requires certain security capabilities, operational controls, and protections to be in effect. These include the requirement that all systems have an approved Security Plan. Use of the SDN shall constitute an adequate security component for the authentication and encryption components of transmission of data or for access to internal resources within the context of an overall security plan.

3. CDC/ATSDR Internet Standard: Commonality of Standards (95.2), which establishes applicability of standards for similar Internet functions even if not specially mentioned in the standard.

4. CDC/ATSDR Internet Standard: Establishing Routine and Special Internet Services (96.1), which allows point-to point IP address connections over the Internet.

5. Presidential Decision Directive 63, May 1998, which identifies increasing levels of threat to government information technology systems, stress security plans, protection of communications, and a general defensive posture which includes monitoring and response capacities.

6. CDC/ATSDR policy document on “Employee Use of CDC Information Technology Resources” dated April 24, 1999, and the older (March 15, 1989), but still active, policy document “Manual Guide – Information Resource Management (No. CDC-3): ADP Security Policy” which incorporates the Department of Health

and Human Services document entitled “Automated Information Systems Security Program (AISSP) Handbook.”

7. P.L. 103-62 (the Clinger-Cohen Act or Information Technology Management Reform Act - ITMRA) which requires federal agencies to use performance metrics to measure how well the information technology supports agency programs.

8. Public Health Service Act (42 USC 242m) Section 308(d) which provides for an “Assurance of Confidentiality” of data.

Services Provided by the Secure Data Network
The SDN shall provide at least these basic security gateway services on behalf of CDC/ATSDR programs:

- Control of external access to Internet resources and processes;
- Secure routing and communication of data files and documents to CDC/ATSDR programs;
- User authentication by X.509 Digital Certificates;
- Encryption, digital signatures, and key management; and
- HTTP and other protocol support.

X.509 Digital Certification

The X.509 certificate provides programs with definitive authentication of a user. The Authentication standards and procedures for the SDN shall be identical for all users, specifically including but not limited to CDC/ATSDR employees, contractors, and external users.

Any individual accessing the CDC/ATSDR SDN must be authenticated by providing an X.509 Digital Certificate authorized by a CDC/ATSDR program (see the Digital Certificate Administrator role) and approved by the CDC/ATSDR Digital Certificate Administrator. This Digital Certificate Authentication will allow the establishment of a secured communication session between the user workstation and the CDC/ATSDR secure Web server platform**.**

CDC/ATSDR may at any time provide for the SDN Digital Certificate procedures and capability to be extended to the Internet security needs that exist between the state health departments and their public or private reporting partners. This would mean that CDC/ATSDR would become a Certificate Authority for secure public health communications between, as well as with, its partners.

Each user may have one or more Digital Certificates authorized to access one or more agency programs. Any program may remove access to its systems or data at any time. The SDN includes a Directory Server which will contain all the Digital Certificates of authorized users of the SDN including CDC/ATSDR staff.

The Program Digital Certificate Administrator

CDC/ATSDR programs that require SDN services must designate one or more government employees to act as Program Digital Certificate Administrator (PDCA). The Business Steward of the program data system must appoint each PDCA.

The PDCA will grant access to program sensitive or critical data and activities critical to the program missions. Therefore the PDCA must have access to certain knowledge of which users should and should not be given access.

Controlled Access to Documents or Data

Users shall be given adequate notice by agency programs that only Digital Certificates issued by the SDN-specified Certificate Authority(ies) may be used. Use of Digital Certificates stored on personal computers shall be protected by passphrases/passwords. All policies for password management must be followed. Specific emphasis is placed on the prohibition of passphrase/password sharing.

SDN Data Access Limitations

The SDN will not operate in any fashion that requires it to act on or have knowledge of the content of program data passing through it. Any analytical data processing or program-specific database activities are the responsibility of the program that receives the communication.

Monitoring of SDN Operation

IRMO will be required to monitor and periodically audit all SDN activities. All computers communicating with the SDN are included. This includes both individual workstations and program-controlled hosts or servers. Information gathered may be disclosed to appropriate third parties, including law enforcement authorities or FOIA requesters. The SDN shall included a clearly worded "appropriate use" warning message that shall be visible to all users during the authentication process. The Business Steward of every program that makes use of the CDC/ATSDR Internet connection for sensitive data activities shall document that all program personnel have read this policy.

Since the SDN has no knowledge of the content of any data passing through it, the monitoring of appropriate use of the network cannot disclose the sensitive data passing through it. For these reasons, monitoring of the SDN will not constitute a violation of the sensitivity of any data being transmitted.

Server Facilities (Back-end Services)

The SDN supports full-time on-line server facilities for CDC/ATSDR programs:

1. Route incoming secure file transfers through the CDC/ATSDR firewall to the recipient program;

2. Provide protected server disk space for the provision of html pages, files for download, and forms processing subject to capacity limitations;

3. Provide redirection services supporting the back-end processes, html pages, etc.

External Connections to Internal Databases, Data Resources or Applications

Trans-firewall sessions that:

- require internal databases and systems to support on-line data entry or query; or
- remote data access methods capable of executing operating system; or
- other arbitrary processes on a server inside the firewall, which includes all provision of SQL query,

shall be by a secure host-based process (program, servlet, script, "intelligent agents," "3-tier client-server," "anonymous proxy services,", Virtual Private Networks (VPNs), etc.) the scope and effect of which are limited to the required data access activities and must not provide direct remote access to or remote operation of computers inside the firewall. Any sensitive or critical information stored on an external server before transfer to an internal process must be encrypted. All secure processes must themselves meet the authentication and access control requirements of the SDN.

Exemption For Use of an Alternative Internet Security Mechanism

Programs may use alternatives to the SDN for Internet transport of sensitive data in accordance with CDC/ATSDR Policy on Secure Internet Exchange of Information. The planning, development, or use of any alternative approach to Internet security by a CDC/ATSDR program shall require explicit approval in accordance the procedures set forth in that policy.

Annual Review

A subcommittee appointed by HISSB shall review this standard at least annually.

V. Procedures

Following are the current operational procedures of the SDN. Operational procedures are subject to change with technology and experience.

X.509 Certificates
X.509 Digital Certificates from Verisign, Inc., are now required by the SDN. Verisign, Inc., will act as the CDC/ATSDR Certificate Authority and Certificate Server provider. At any future date the CDC/ATSDR SDN may use another X.509 Digital Certificate provider(s) or alternatively IRMO may establish a CDC/ATSDR Certificate Authority and operate a Certificate Server for the Agencies.

The SDN is designed to provide access only to individuals that have been pre-authorized by a CDC/ATSDR program official and for Digital Certificates that carry an explicit CDC/ATSDR authorization prior to their use. Currently, it is neither operationally practical nor prudent to allow the use of alternate sources or means of provision of Digital Certificates.

Until further notice, SDN Digital Certificates will expire on a periodic basis not to exceed one year. Programs may choose a more frequent expiration schedule for authorization to their activities if needed.

Digital Certificate Administrator Roles and Responsibilities

There are two primary roles in the SDN: 1) the Agency Digital Certificate Administrator (ADCA) who operates the SDN for the Agencies and 2) the Program Digital Certificate Administrators who manage and authorize access to all CIO program secure activities through the SDN.

All Agency-level responsibility for SDN Digital Certificates resides in the position of the ADCA located in IRMO. The ADCA has the primary responsibility for establishment and maintenance of Digital Certificate processes in the Agency. In most cases the ADCA will provide the final approval or disapproval of requests for SDN Digital Certificates in accordance with the specific CIO program's decision. The ADCA is the only role in the SDN that can request revocation of a Digital Certificate. To allow rapid response, all suspected misuse of the SDN must be reported to the ADCA by email at DataNet@cdc.gov.

The ADCA's approval of SDN Digital Certificate requests will follow the decision made at the program level except in two cases: the individual in question has been identified as a security concern by another program or revocation for cause of the individual's Digital Certificate has been initiated The ADCA has no role in granting authorization to program-level activities to an SDN Digital Certificate user.

The CIO program-level responsibility for SDN access resides with PDCA who is a CDC/ATSDR employee designated by the Business Steward of the program data system for which secure access is required. The PDCA makes the actual determination whether a given individual should be allowed access through the SDN to the particular online activities of the CIO program. The PDCA is responsible for the entry into the SDN Access Control Database of program, program activity, and routing information. The PDCA is also responsible for using the SDN Access Control Database to authorize individual SDN users to specific program activities.

External user requests for SDN Digital Certificates must identify one or more specific program activities for which the access is requested. The first PDCA to authorize a given individual also acts to approve that individual's SDN Digital Certificate request. Subsequently, other PDCA's may authorize the individual to additional program activities under their management using the individual's pre-existing SDN Digital Certificate record.

The CIO program data system Business Steward will designate one or more PDCA's to the ADCA by email at DataNet@cdc.gov. Be advised that positioning of the PDCA at the CIO or Division level may not provide adequately detailed knowledge of appropriate access at the program level and may constitute a security risk. If a CIO wishes to centralize access control activities across programs, the PDCA at the CIO or Divisional level must have specific written approval from the program before granting access. It is important to emphasize that the request for SDN Digital Certificates by an external users requires no prior approval steps and cannot be granted without direct knowledge that the requested access is appropriate. The CIO's may impose additional approval steps or roles as seems necessary to them.

Using the SDN Access Control Database, a PDCA may remove access to any or all of his or her program activities at any time without the involvement of the ADCA or other SDN management. Other access authorities granted by other PDCA's, however, will remain in effect unless removed by those PDCA's. Therefore, if removal of access is due to misconduct by the users, the ADCA should be contacted so that the individual's certificate may be suspended or revoked (whichever is appropriate and to be determined by consultation with all PDCA's involved).

Secure Data Network Access Protection Levels

Using a combination of methods, the SDN will provide secure access to resources through the Internet at two different levels of protection.

> Standard Access Protection Level (SAPL) to resources on the network will be protected by digital signing of files, digital encryption, and secure transmission (X.509 Digital Certificates and Secure Socket Layer 3). This level of access protection will be entirely software-based and is critically dependent upon the correct use and maintenance of passwords.
>
> Maximum Access Protection Level (MAPL) adds additional security measures. In addition to the SAPL controls, hardware tokens or smart cards supported by CDC/ATSDR's firewall will restrict access to only users with valid token cards issued by CDC/ATSDR. In the near future, protection at this level may be added to the operating system of client workstations or may be added by installing firewall-supported Virtual Private Network (VPN) software. The SDN may in the future require the use of hardware token cards for access by CDC/ATSDR staff or all users. In addition, the SDN will support access control by hardware tokens or smart cards for specific CDC/ATSDR programs or other high-risk circumstances.

Program Level Passwords

The SDN neither allows nor supports any lower level of access control. Specifically, password-based access control can be instituted by CDC/ATSDR programs, but only as additional layers of security and never as a substitute for the SDN certificate-based access control. The program may institute other additional levels or layers of protection, provided that the requirements of the SDN may not be reduced or superseded and those additional agency-level support resources are not required. The SDN may choose to implement a password-based security method that would be available to programs as an additional layer of security. Programs are free to continue to use password protection, when approved, on Internet sites not requiring the use of the SDN.

Point-to-Point Trans-firewall Access

As permitted under CDC/ATSDR Internet Standard 96.1, this standard is establishing an additional security requirement that all point-to-point trans-firewall access shall require authentication and access control by the SDN in the manner described herein.

Requesting Server Facilities

The Business Steward responsible for a given data system or program will designate the specific individuals (who may be contractors) that can access the server facilities provided in the SDN. Criteria for granting access to back-end functions of the SDN should be discussed in the security plan. Sending an email to the CDC/ATSDR Certificate Administrator will do this. All such access shall be secured by the same digital certificate authentication that is required for general user access.

CDC/ATSDR programs will be provided with methods that may be used to verify that a given user is in the Directory Server. This is required for validating Digital Signatures on documents (files) that are claimed to be from the user.

Internet Browser Standards for Secure Data Network Access

Internet browser users will require a version that can load and correctly support Verisign, Inc., X.509 Digital Certificates and SSL3 transport for access to the SDN. Netscape Navigator version 4.5 (all platforms) or greater is satisfactory as is Microsoft Internet Explorer version 4.01 or greater. The SDN cannot guarantee the support of any other browsers. From time to time CDC/ATSDR may find it necessary to add or remove specific browsers from this list.

The SDN may also be used directly from user programs. Contact IRMO for information.

Support for NON-HTTP Protocols

The SDN provides priority service to HTTP-based activities. Other protocols, such as FTP, may be used if they support X.509 Certificate Authentication and SSL3 transport, but substantial program resources may be required to validate and support the use of other protocols where only a single or a few programs will benefit. The SDN will make an effort to provide test areas for this purpose.