COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF HUMAN SERVICES

INFORMATION TECHNOLOGY STANDARD

Name Of Standard: **Business Partner Network Connectivity**	Number: **STD-ENSS022**
Domain: **Network**	Category: **Wide, Metro. & LAN Networks / Business Partners**
Date Issued: **04/30/2004**	Issued By Direction Of: 
Date Revised: **03/08/2016**	Clifton Van Scyoc, Chief Technology Officer

Abstract:

For years DHS has provisioned Business Partners with connections to the DHS network based on numerous business factors such as the type of connection needed, projected traffic volume, applications accessed, and overall cost. DHS management has decided that a comprehensive document is needed to summarize all of these scenarios into one standard.

General:

The purpose of this document is to provide a standardized procedure for provisioning network connectivity to DHS Business Partners. This standard has been published by staff of the Network Architecture and Telecommunication Management Unit (NATMU) of the Division of Technology Engineering, DHS Bureau of Information Systems. Questions related to these procedures or referenced documents may be addressed to the Business Partner's Program Office Coordinator.

Standard:

High-level Overview of the Connection Procedure

Definition of a "Business Partner" (BP)

A Business Partner is defined as a vendor, contractor, provider, other PA agency, or local government agency. Business Partners are *NOT located* in any Department business site and must have an agreement in place with a Department Program Office addressing the need to access Department network resources.

Assessing a Partner's Business Needs

The first step in provisioning a connection to a BP is to evaluate their business needs. This includes but is not limited to the following:

A. Type of business conducted and applications used – This is important to know in that it may give DHS staff and the telecommunications provider insight into the volume of traffic that could be generated by the BP.

B. Frequency of use – Partners who access the network only occasionally, such as a monthly file transfer, may not need a dedicated leased circuit.

C. Physical location of the BP site – This is important to know if the site is physically situated near an existing county or Business Partner already connected to the Commonwealth, so that they could possibly share their circuit (such as a JNET site).

D. Equipment already on site – It is important to know what type of equipment is already on site so that DHS can determine what the BP has to order. For example, if the BP is already running a Local Area Network (LAN) and has connectivity to another entity through a router, they may need to purchase another router depending on the number of NIC slots available.

Types of Connections Available

There are two traditional types of connectivity that can be requested for a Business Partner. These are described below:

A. ***Leased Frame Relay*** – This is the standard leased circuit through a telecommunications provider such as Verizon and can be requested using DHS form **"Business Partner Site Access Request/Approval"**.

B. ***Commonwealth Inter-Agency Routing*** – This approach should be used for state offices who constitute part of the Commonwealth Enterprise Network and are merely routing and gaining firewall access through to DHS. This option may also be selected on the above mentioned "Site Access Request/Approval" form.

Three less traditional methods that are becoming more popular are ***eGovernment*** transactions, pure ***Internet*** access, and ***Virtual Private networks (VPN).***

A. ***eGovernment*** transactions are those which involve web-based exchanges of information using some type of integration broker tool. The Pennsylvania Department of Human Services (DHS) has developed a standardized methodology for secure data exchange leveraging industry standard Internet technologies and protocols. These methods of secure data exchange have been developed to expedite data exchange, meet federal security requirements while minimizing costs, and develop specialized hardware, networking components, and operational support that would otherwise be superimposed upon business partners. Several methods have been instituted to accommodate business partners of varying size, technical infrastructures, and resources.

The types of data exchanges supported are (1) Server-to-Server (S2S) over the private Business Partner network for large file high volume transmissions, (2) Web browser-to-Server for low volume data transfer using the internet and Unified Security authentication, and (3) Secure File Transfer Protocol (SFTP) which is supported between DHS and Business Partners over the Internet. Business Partners interested in using one of these data exchange methods must submit a **separate** form **"eGovernment Exchange Registration Form"** through the appropriate Program Office.

B. ***Internet*** access is simply connecting to DHS network resources via the internet. It is used mostly by small healthcare providers and/or private individuals to apply for human services with a standard PC equipped with a web browser. All that is required is an internet-capable PC and a userid and password for the application being accessed (CIS, COMPASS, HCSIS, etc.).

C. A ***Virtual Private Network*** is a way to use a public telecommunication infrastructure, such as the internet, to provide remote users with secure access to a network. A VPN works by encapsulating data packets to create a "tunnel" following the Layer Two Tunneling Protocol (L2TP). The protocol encrypts the data at the sending end and sends it through the "tunnel" until it is decrypted at the receiving end.

Required Steps to gain DHS Connectivity

Following are the steps in connecting DHS business partners and other agencies to the DHS network:

1. The business partner request is received from a sponsoring program office in a Memorandum of Understanding (MOU) containing details of the purpose of the service as well as the equipment needed to complete the circuit, long distance services, and so on. The request is assigned to a BIS DTE person as the primary contact.
2. Upon approval of the request, the agency/business partner submits a contract of agreement to initialize the installation process.
3. The agency/business partner supplies a letter of authorization to bill them for the costs of installation and continued regular monthly service. This includes a specific address to be submitted to the service provider at the time of the service request that is initiated by the DTE representative.
4. All connectivity of this nature must be firewall protected and adherence to the DHS security policy is required, with a completed "**Firewall Change Request form**" submitted before activation of the circuit.
5. The business partner provides any devices or equipment needed to complete this circuit and adheres to the provisions of the DHS guidelines for server, switches, routers, and other devices.
6. The DTE contact initializes the Field Limited Purchase Order (FL) to have the current telecom vendor install the circuit as requested by the business partner.
7. The DTE representative contacts the Commonwealth's Office of Administration/Office of Information Technology (OA/OIT) Security Office to notify them of the new Business Partner and to request firewall access for their IP address space. This is accomplished by submitting a ticket into the Remedy Service Management System.

Templates and Forms

Additional Instructions For Filling Out Applications

A. "Business Partner Site Access Request/Approval Form"

This is the basic form that must be submitted for most Business Partner network access requests. It is supplied to the Business Partner by the Program Office Coordinator (POC). The form includes line-by-line instructions for filling out each field and is self-explanatory. However, special attention should be given to the section where Internet Protocol (IP) addresses are to be entered.

DHS highly recommends that Business Partners contract with a telecommunications vendor that will provide a complete end-to-end service; i.e., installation, management, maintenance, and troubleshooting. If they choose to contract with a provider who does not provide a complete telecommunication solution, it will be the obligation of the Partner to provide its own technical support and DHS cannot be responsible for troubleshooting the circuit.

With a complete end-to-end solution, the vendor will assign the Router WAN IP, the inside LAN IP, and the LAN segment IP's. Any Network Address Translation (NAT) that needs to take place to connect to the local LAN will be performed in the router.

If the BP elects to contract with a provider offering only a partial solution, DHS will supply the vendor with authorized address spaces for the corresponding devices and local LAN segment (s).

The completed form will then be submitted to the desired provider through the appropriate Program Office Coordinator. *It should be stressed that any unusual connection requests may be subject to special maintenance and port/collocation charges.*

B. "Business Partner User Access Request/Approval Form"

This is an access form required by all Business Partner applicants regardless of connection method requested. It is required to document end-users accessing the DHS network for security reasons. Line-by-line instructions for filling out this application are also included with this form.

While there may be some reluctance on the part of end-users to provide their Social Security Numbers, a Name, Address, and Telephone Number is absolutely essential for each individual accessing the DHS network. As with the other access forms, this application must be submitted to the Partner's corresponding Program Office Coordinator.

C. "eGovernment Exchange Registration Form"

This form is somewhat specialized and should be filled out with assistance supplied by the eGovernment Exchange staff of the Technical and Architecture Development Unit. Business Partners should contact their respective Program Office Coordinator to initiate this process.

Exemptions from this Standard:

Any request for an exemption to this standard must be made to and approved by the DHS Network Architecture and Telecommunication Management Unit supervisor.

Refresh Schedule:

All standards and referenced documentation identified in this standard will be subject to review and possible revision annually or upon request by the DHS Information Technology Standards Team.

Standard Revision Log:

Change Date	Version	Change Description	Author and Organization
04/30/2004	1.0	Initial Creation	NACMS
12/17/2004	1.0	Reviewed Content	Doug Rutter
04/05/2010	2.0	Updated and edited style	Doug Rutter, DTE
11/18/2013	2.0	Reviewed Content – No Changes	Matthew Messinger
03/30/2015	2.1	Reviewed Content – Made minor formatting changes. Updated DPW to DHS.	Bob Gordon, BIS-DTE
03/08/2016	2.1	Reviewed content – No Changes	Aamir Qureshi, BIS-DTE