



U.S. Fish & Wildlife Service

USFWS Telework Pilot Project Computing Standards

Version 1.7

April 26, 2007

Document prepared by:
Kevin Dunham – (703) 358-2344
Kevin_Dunham@fws.gov



USFWS Telework Pilot Project 1

Section 1.0 Introduction 3

 1.1 Purpose..... 3

 1.2 Technical Requirements..... 3

 1.3 Plan Benefits 3

 1.4 Scope..... 3

Section 2.0 Requirements 4

 2.1 Hardware..... 4

 2.2 Software 4

 2.3 Security Requirements 5

 2.4 Telecommunication Standards..... 5

 2.5 Remote Access Configuration 5

Section 3.0 Appendix 7

 3.1 Telecommunication Descriptions 7

 3.2 References..... 13

DRAFT



Section 1.0 Introduction

1.1 Purpose

The purpose of this document is to outline the standards that will be used to acquire Government Furnished Equipment (GFE) including both hardware and software to be used in the telework pilot project. This document is targeted to those individuals that are involved in the acquisition process of all equipment and services related to the telework pilot project. An installation checklist is being developed to assist technical personnel in the specific configuration and setup of this equipment based on the individual needs of the employee and to meet the requirements set forth in the Official Telework Policy that is being developed by the Human Resources Department.

1.2 Technical Requirements

As required by DOI, the computers used in the telework project must be GFE and meet all security requirements and be STIG compliant. Once GFE can be insured thru proposed security measures at ESN, access to FWS Resources (ie Shared directories and home directories) will be enabled. This access will need to be configured on the laptop by technical personnel before the teleworker is sent off-site.

1.3 Plan Benefits

- Standardized hardware (better vendor support)
- Standard software package (Telework Standard Image)
- Technical support staff from R4, R5, and the WO can provide improved support to the users

1.4 Scope

1.41 Inclusions

1. Laptop Computer to be used for teleworking.



Section 2.0 Requirements

2.1 Hardware

All equipment, (new purchase or currently in use) must be purchased from the BPA and meet the following minimum standards:

ITEM	MINIMUM	RECOMMENDED
Processor	1.0 GHZ	2.0 GHZ
RAM	1.0 GB	2.0 GB
Hard Drive	60 GB	80 GB
Drive Bay	DVD-ROM	DVD +/-RW

2.2 Software

The following software is required to be installed on the equipment to insure optimum productivity can be maintained:

- Microsoft Office 2003
- Lotus Notes 6.51
- Adobe Acrobat Reader v.7.0 or above
- Blue Zone (Internal and external connection options)
- Symantec Anti-Virus / Anti-Spyware v.10
- Firewall Software (Windows Firewall)
- See ITB 2005-003 for more information
- Connection Software if required (i.e. DSL communications software)
- Remote Administration Software (SMS Client)
- Encryption Software
IRTM recommends Microsoft EFS for disk and file encryption and Kanguru for USB devices, as interim solutions with the full knowledge that they may be temporary and may have to be replaced when DOI establishes the standard



2.3 Security Requirements

- Operating system (Currently Windows XP SP2) configuration options must be selected to increase security. The default configuration of the operating system is generally inadequate from a security standpoint. File and printer sharing must be disabled. The operating system and major applications must be updated to the latest and most secure version or patch level. All computers must have an anti virus program installed and configured to scan all incoming files and e-mails. The anti virus program must have its virus database updated on a regular basis.

2.4 Telecommunication Standards

- Cable Modem
- DSL Connection
- Satellite Connection
- Please see [Appendix 3.1](#) below for standards involving telecommunication

2.5 Remote Access Configuration

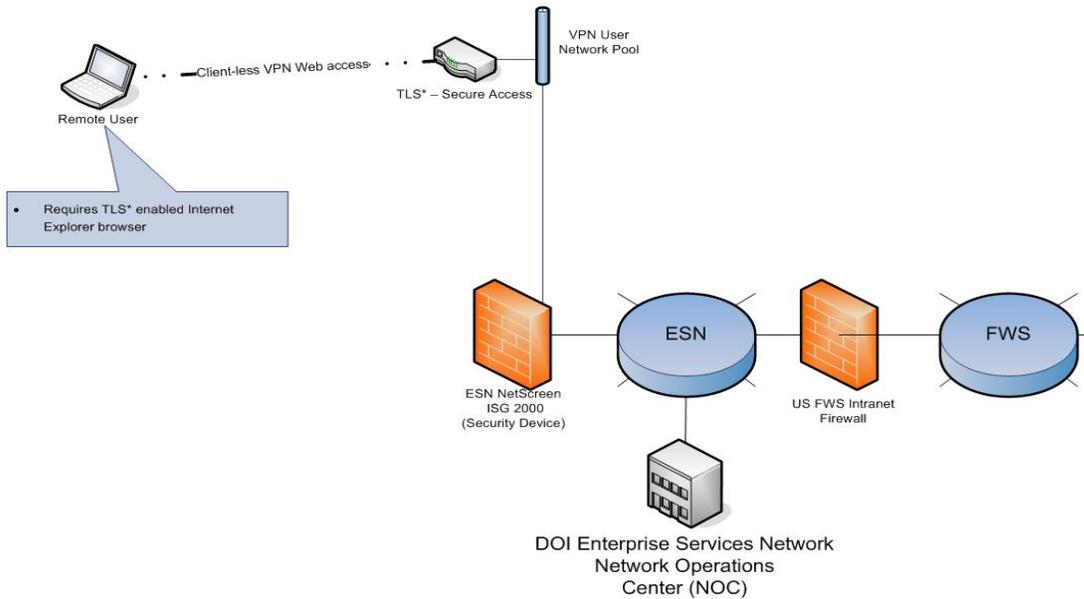
Any user who wishes to connect to the FWS network to access internal applications (e.g. BAS, CARES, SPITS, etc.) or network resources (e.g. shared drives and home directories) must connect to the DOI network using a secure VPN connection. The following is the standard configuration for establishing such a connection

- **Web-TLS Net Connect Method**
The Net Connect configuration establishes a traditional encrypted VPN tunnel using transport layer security (TLS.) The tunnel provides a generic virtual network connection to the ESN Intranet using the Internet as transport. Any form of traffic can be sent over the tunnel. The user connects to the Web-TLS appliance with a web browser, authenticates and establishes the tunnel. See figure 2.51 for a graphical explanation



Figure 2.51

Telework Client Connection to ESN and FWS



*TLS = "Transport Layer Security," a method to secure communications

The GFE connection process:

Authorized users of Government Furnished Equipment (GFE) may access network file servers on the FWS network using the Juniper NetConnect VPN client. After entering a username and password at vpn.doi.gov, the Juniper NetConnect Host Checker will scan the connecting machine to ensure that:

- The computer is running a recent version of Symantec Antivirus with current antivirus definitions
- The computer contains a special, periodically rotated file in %SYSTEMROOT% designating it as FWS GFE.

If these checks pass and the logged in user is a member of the ifwU-GFEVPN group, the user's machine will obtain an IP address within a range designated for FWS government furnished computers and access to network file servers is granted.



Section 3.0 Appendix

3.1 Telecommunication Descriptions

3.11 Introduction

At the teleworker's residence or other work location, a large variety of network configurations are likely to be encountered. This document provides a summary description of the most common configurations and discusses some of the technical issues involved in the installation and support of each remote configuration.

3.12 Configuration Type I

The simplest remote configuration consists of the government furnished laptop PC connected directly to a DSL, Cable, or Satellite connection (see Figure I, below).

The network configuration of the laptop in the case of a cable modem (Type Ia) normally does not need to be very different from the network configuration that would be used in the Washington Office. (i.e., the laptop is a standard DHCP client) However, many cable modem ISPs require that that Computer Name (found in Control Panel > System) be assigned by the ISP and takes the form of an alphanumeric string of characters. Often the ISP technician will enter the assigned Computer Name when the cable modem service is activated. Since the user will not normally have administrative privileges to the laptop, a mechanism needs to be developed by which the ISP's assigned Computer Name can be configured into the laptop.

Whereas the broadband Internet service provided by most cable-based ISPs provides a constantly active connection to the WAN, DSL connectivity (Type Ib) is typically based upon PPOE protocol, which requires the user to log into the service provider's network. The ISP will normally provide and/or install onto the PC the appropriate software that enables the user to log into the service provider's network. Consideration needs to be given to how this software will be installed



U.S. Fish & Wildlife Service

onto the laptop, given that the user will not normally be provided administrative privileges to install the software himself/herself.

Where a teleworker lives in an area not serviced by either cable or DSL lines, satellite connectivity (Type Ic) would be needed if the teleworker is going to have broadband Internet connectivity. In most cases, this satellite system would be one-way, which provides a high speed downlink from the Internet, but the uplink operates via modem on a standard telephone line. Depending upon the particular satellite provider, some of the same laptop configuration issues may arise, in which the laptop requires some element to be configured in a particular way, but the laptop user does not have the administrative privileges necessary to make the change himself.

Another problem that might arise is that VPN client software often has difficulties working over high latency satellite links. The use of satellite connectivity by a teleworker needs to be tested and verified. It is worth noting that a teleworker who lives so far away from an urban area that neither cable nor DSL Internet access is possible is probably someone who could greatly benefit from teleworking.



FIGURE I Telework Configurations - Type I

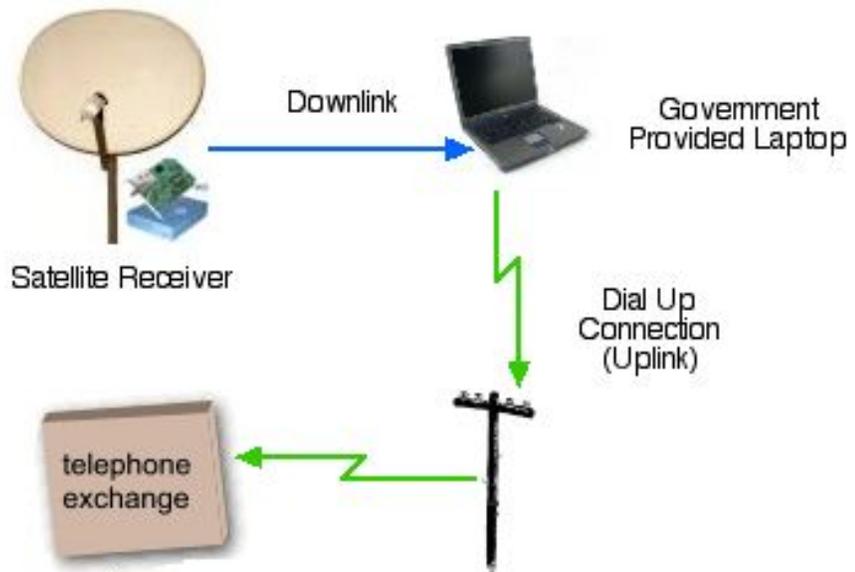
Type Ia



Type Ib



Type Ic





3.13 Configuration Type II

When the teleworker already has a residential network, some aspects of the technical support equation become easier, but some other elements can be more difficult. (See Figures II and III, below).

In most cases the network configuration of the laptop will not need to be different at all from the network configuration that would be used in the Washington Office, i.e., the laptop is a standard DHCP client. If the cable modem ISP requires a particular Computer Name, this is normally configured into the Router. Similarly, in the case of a DSL line, the Router is normally configured to support PPOE and has the ability to log into the ISP's network, either upon detection of data activity or maintains a constant connection. Therefore, such configuration parameters do not need to be incorporated into the government furnished laptop.

However, issues may arise with respect to physical connectivity between the laptop and the router, for example, if the router is not located near the workspace that the teleworker intends to use. Although the hardware "package" that is currently planned for teleworking does not include a printer, the teleworker may desire and truly benefit from using a networked printer available on his/her home network. The technical support issues when a teleworker already has a home network in place can become quite numerous and complex. The technical support staff will need to have on hand documentation for the teleworker reflecting the topology and key configuration parameters of the residential network, so that any connectivity problems experienced by the teleworker in the use of the government provided laptop can be efficiently and accurately diagnosed.



FIGURE II

Telework Configurations - Types IIa, IIb

Type IIa



Type IIb

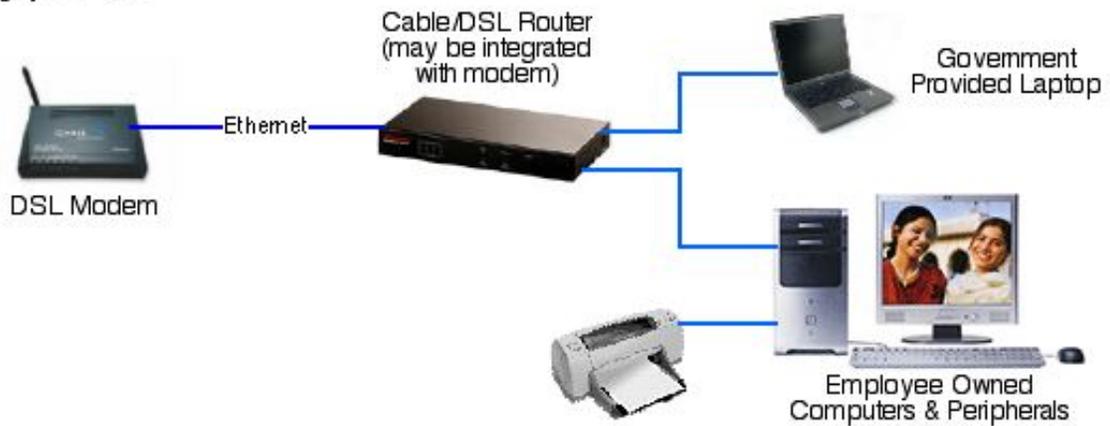




FIGURE III

Telework Configurations - Type IIc

Type IIc





3.2 References

- OMB M-06-16 - *Protection of Sensitive Agency Data* 06-23-2006
- OMB M-06-15 - *Safeguarding Personally Identifiable Information (PII)* 05-22-2006
- NIST SP 800-46 *Security for Telecommuting and Broadband Communications*
- All Employee Message from Secretary Kempthorne - *Important Notice on Safeguarding Personally Identifiable Information* 06-20-2006
- OCIO Memorandum 2006-016, *OMB Requirements for Safeguarding Personally Identifiable Information.*, 06-15-2006
- OCIO Memorandum, *Protection of Personally Identifiable Information and Department Sensitive Information*, 09-08-2006
- OCIO Directive 2006-XXX *Restrictions on Transmission, Transportation and Use of, and Access to, DOI Data Outside DOI Facilities* (draft)
- ITB 2005-003 – *Personal Firewalls on Remote Computing Devices* 06-21-05
- Whitepaper - *Information Technology for Telework* 09-21-06