Document Title:	**Virtual Private Network (VPN) Policy**
Document Type:	*Policy*
Document Purpose:	The purpose of this policy is to provide guidelines for Government and non-Government users remote access, via Virtual Private Network (VPN), to the Government network.
Scope of Application:	All Government employees, contractors, consultants, constitutional employees, temporaries, and volunteers, including all personnel affiliated with third parties using VPNs to access Government's network. This policy applies to implementations of VPN.

Policy Description

Approved Government employees and authorized third parties (visitors, vendors, etc.) may use the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting a Government VPN compatible Internet service provider (ISP), coordinating installation, installing any required software, and paying associated fees, etc.

The VPN capability is established to enable telecommuting for employees requiring more than three hours total connect time per day. Vendors and other infrequent users may utilize the Government's VPN capability if approved by associated agency directors or project managers.

Government users, such as a telecommuter, must be equipped with a Government issued laptop or workstation for remote access prior to being eligible for a VPN client. IT Department will provide the necessary software (VPN Client and anti-virus), licensing and installation instructions required to enable a secure connection to the Government network. The agency sponsoring the VPN user is responsible for providing Government equipment, additional software and licensing fees (such as Absolute, email/application software, etc.).

Non-government users, such as contractors or vendors, may use existing laptops or workstations but must abide by this policy, and maintain current anti-virus software and protection by a firewall. The sponsoring agency will approve a non-Government user access and provide details of access requirements (such as telnet/ftp access to a specific server). IT Department will provide VPN client for the user and allow appropriate access to Government network.

Additionally,

(1) It is the responsibility of the user with VPN privileges to ensure that unauthorized users are not allowed access to Government's internal network. This includes the physical security of the machine. If a user suspects unauthorized access or if the users machine is stolen they must immediately contact the Government's emergency hotline.
(2) VPN use is controlled by user Name and password. Each user is responsible for securing their user name and password. Any activity performed through the use of an authorized user account will be assumed to have been conducted by that user. The user assumes full responsibility for all actions performed by their account. If a user contacts the Government's emergency hotline, their account will be immediately disabled. The same rules will apply to the password system. Additionally, the user will assume the reasonability of physically securing the token. If a user suspects unauthorized access or if the users token is stolen they must immediately contact the Government emergency hotline.
(3) All activity while connected to the Government Network via the VPN will be monitored.
(4) When actively connected to the Government's network, VPN will force all traffic to and from the PC over the VPN tunnel. All other traffic will be dropped.
(5) Dual (split) tunneling is not permitted: only one network connection is allowed.
(6) VPN gateways will be set up and managed by the IT Department network operations group.
(7) All computers connected to the Government's internal network via VPN, or any other technology, must use the most up-to-date anti-virus software that is the Government standard. In addition these computers must also utilize a firewall (can be software or hardware or both). This includes employee/vendor owned computers.
(8) VPN users will be automatically disconnected from the Government's network after 30 minutes of inactivity. The user must then log in again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
(9) The VPN concentrator is limited to an absolute connection time of 24 hrs.
(10) Users of computers that are not Government owned equipment must configure the equipment to comply with Government's VPN and Network policies.
(11) Only approved VPN clients may be used.
(12) By using VPN technology, users understand that their personal computers are a de facto extension of the Government's network and as such are subject to the same rules and regulations that apply to Government-owned equipment (i.e., their PCs must be configured to comply with security policies).
(13) Users of (personal) computers that are not Government owned are responsible for maintaining the proper operation of their systems. Users who fail to adequately maintain their systems may forfeit VPN access privileges.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Contractors, consultants, temporaries, constitutional employees and other workers, including all personnel affiliated with third parties using VPNs to access Government's network will be held liable for all damage and destruction of Government information that results from intentional or negligent conduct.