

# **AN EMPLOYEE'S GUIDE TO VIRTUAL RESOURCE SOLUTION**

"Each executive agency shall establish a policy under which eligible employees of the agency may participate in telecommuting to the maximum extent possible without diminished employee performance. "

Public Law 106-346, 359:  
106th Congress

## **INTRODUCTION**

Workplace trends are triggered by social movements and political ideology, as well as by technical advances or changes. One such trend that has been enthusiastically accepted by private industry and many municipal organizations is the movement of workers out of the traditional office environment and into an alternate work setting or Telework environment. TIGTA calls our Telework program the Virtual Resource Solution (VRS), primarily because we believe there is a need to have the employee in the best location to complete the work; whether it is the home or the customer location, or other location chosen by the employee that is conducive to an optimal work environment.

VRS is an initiative to create a cutting edge organization that leverages technology and forward looking management practices toward achieving a goal of having a world of knowledge at our fingertips while providing a more productive, efficient and flexible work environment for our employees. As a first step in this evolutionary process, eligible TIGTA employees have the ability to work from anyplace, and at any time, while still meeting the business needs of the organization.

VRS or Telecommuting offers benefits to organizations such as the opportunity to reduce costs, increase productivity, attract and retain employees, and lower environmental pressures. It provides the venue for attracting and retaining a skilled workforce and accommodating an increasingly diverse workplace. However, we must also be aware that there are some concerns, issues, problems and costs to VRS, such as alienation of workers, performance evaluation, legal implications, and span of control and responsibility.

This handbook strives to provide guidance on those issues that have an impact on an employee's success while telecommuting. The Guide is meant to be used in conjunction with input from the manager rather than a stand alone "how to" book. Once telecommuting, the employee should contact his/her manager with any questions or concerns.

## **POINTS OF CONTACT**

The following individuals are designated as points of contact for questions you may have as you prepare to implement VRS.

For Personnel questions please contact:

Your Servicing Personnel Specialist

For Performance Management questions please contact:

Ray Bimbo - 914-304-1604

For Budget questions please contact:

Gordon Burns - 202-622-8072

Carolyn Smith - 202-622-6002

For IT questions please contact:

Richard Westfield - 202-927-7162

For General Program questions please contact:

Donna Leach - 202-927-5925

# EMPLOYEE'S GUIDE TO VRS

## Table of Contents

Introduction	page i
Points of Contact	page ii
Table of Contents	page iii

### *Section I*

#### **Guidance**

The Benefits of VRS	page 1
The Impact of VRS	page 2
Security	page 6
Equipment	page 8
Issues for the Telecommuter	page 9
VRS Self Assessment Instructions	page 11
VRS Self Assessment	page 12
From Office Worker to Teleworker	page 13
The Appeals Process	page 14
Training for VRS	page 15
Getting Connected at High Speed	page 16
Reimbursement for Telecommunication Expenses	page 25
Purchasing Approved Incidentals	page 27
Telecommuter's Work Products	page 29
Leave and Attendance	page 30
How to Work with Your Manager to Ensure Success	page 32
Myths and Misperceptions	page 33

### *Section II*

#### **Policy**

VRS Program Policy	page 35
IT Use Policy	page 42
IT Computer Password Policy	page 49

*Section III*

**Forms**

Application for Participation	page 54
VRS Work Agreement	page 55
Safety/Security Checklist	page 60
Attachments	page 62
Sample Public Voucher for Purchases & Services	
Blank Public Voucher for Purchases & Services	
Information Systems User Registration/Change Request	

## THE BENEFITS of VRS

The number of Teleworkers in the Washington, DC area has increased 65% between 1996 and 1998, from 151,999 employees to 250,000. Teleworking, also known as telecommuting, is defined as working from an alternate worksite one or more days during the workweek. Teleworking extends the workplace and enables productive work outside the traditional office workplace. An increasing number of people are going to work by simply turning on their computer or picking up the telephone. For the teleworker, the benefits are many. Most workers report they get more work done and are more satisfied with their jobs as a result of telecommuting. The shortened commute decreases employee travel time, decreases employee expenses and decreases employee stress while enhancing the quality of work life and increasing the time for personal enjoyment. Teleworkers also enjoy a greater degree of work-related autonomy and responsibility.

VRS does not appear to be an isolated fad, but rather a transformation of the workplace. This transformation is shaped by digital technology, software based tools, and changes in the workforce. For best results, Teleworking must be beneficial for the teleworker employee, co-workers and manager, and the organization and its client. Listed below are some of the benefits to businesses and their employees.

### Business Benefits:

- ◆ Flexibility in location and time or work
- ◆ Increased productivity and work quality
- ◆ Increased collaboration
- ◆ Encouraged management for results
- ◆ Reduced real estate costs over the long term
- ◆ Improved ability to recruit and retain valued employees

### Employee Benefits:

- ◆ Increased productivity and work quality
- ◆ Increased flexibility at work
- ◆ Reduced commuting stress and possibly cost
- ◆ Distraction-free environment
- ◆ Improved morale
- ◆ Accommodation of work and family considerations.

However, there are many things that VRS is not.

- VRS is not usually a full-time arrangement.
- VRS is not sending people home and never seeing or hearing from them.
- VRS is not a substitute for child or dependent care.
- VRS is not a right, but a privilege.

While managers and supervisors have the final say in determining eligibility, not everyone wants to participate or is suitable to participate in VRS. Employees should assess their own suitability and develop their own business plan for how they will accomplish their work outside the traditional office environment. They need to look at how they will communicate with co-workers, clients and managers. They also need to look at the frequency of these communications. Remember the goals are to increase productivity, increase customer satisfaction and by attaining those first two goals, increase employee satisfaction.

## THE IMPACT OF VRS

### It Sounds Good, But Is VRS For Me?

Telecommuting is not for everyone. Before signing up for VRS, employees and their managers need to consider the impact on each participant: the employee, the manager, the co-worker and the customer. In addition the employee participating in VRS needs to assess the impact and effect of telecommuting on his/her family.

### Employee Impact

As previously mentioned, telecommuting offers numerous benefits to the employee, including reduced stress and enhanced quality of work life. It also raises certain concerns such as the isolation from co-workers. Many telecommuters will not know the extent of their social needs until they have been in the program for a short period of time. Some telecommuters report initial feelings of loss of professional identity as well as self-esteem, possibly because they missed the spontaneous supervision and the reduced level of performance feedback by their managers. Finally, some telecommuters perceive (either accurately or inaccurately) that telecommuting will lead to reduced visibility with their managers and, consequently, reduced opportunities for promotion and/or more desirable job assignments. For these reasons, we suggest each participant and manager undertake a trial period first, before officially starting VRS.

There are likely to be changes in the frequency, spontaneity, mode (telephone or e-mail as opposed to face-to-face conversations) and length of typical work-related communications for new VRS participants. Because of these changes, the effectiveness of communications becomes much more important. Telecommuters may find that they have fewer but more productive meetings than before teleworking. This makes meetings more valuable and requires planning and preparation for participation in necessary meetings.

To effectively resolve the "out of sight, out of mind" concerns, and to achieve the quality of communications necessary for successful telecommuting, open dialogue about these issues and joint planning between the telecommuter and his/her manager must take place. Also, VRS participant's schedules should be individually tailored to provide a balance between work at the alternative work-site and work at the official work-site. Generally, this arrangement should address the participant's need for being informed about related projects, advancement opportunities, and events that may occur in the office on days that the employee spends telecommuting.

Telecommuting is a flexible program. The telecommuter should remain flexible especially during the initial adjustment period. This flexibility during the adjustment period will allow the telecommuter to find the optimal arrangement for his/her personality and job requirements. This will also enable the telecommuter to be responsive to unexpected contingencies, which may require a change of schedule.

One other factor for the telecommuter to be wary of is overworking. Because of the increased productivity experienced by the telecommuter, some individuals may fall into the trap of working inordinately long hours. Sometimes this is to prove to their managers and co-workers that they are working hard on days they are telecommuting, or sometimes as a sense of guilt about not being in the office. Being aware of this possibility, reminding themselves of the full support for this program by Senior TIGTA management, and ensuring regular breaks helps telecommuters avoid the tendency to work long hours.

### **Impact on Co-Workers:**

Not only are the manager and telecommuter affected by a telecommuting arrangement, but co-workers may be impacted as well. Co-workers may have work assignments which involve the telecommuter or which may result in workload changes due to the telecommuter's new location. Some co-workers may feel resentment at not having been allowed to participate and/or harbor preconceived misconceptions about telecommuting in general. For example, some co-workers may believe that telecommuters do not actually work on days they are telecommuting.

Preventing or overcoming co-worker concerns, misperceptions and/or resentment is an important challenge for both the telecommuter and the manager. To the extent possible, the telecommuter and the manager need to include co-workers in the planning process, provide for open communication between all parties, and keep co-workers informed of the telecommuter's schedule and any changes that may occur in the telecommuter's arrangements. The telecommuting arrangement should provide for convenient means of communication between the telecommuter and his/her co-workers. Telecommuters and their managers should also be extremely careful not to over burden other employees in the office with additional responsibilities such as faxing, copying or attending meetings.

As part of their adjustment, it is common for co-workers to compensate for telecommuters' absence by increasing the frequency of communications. This increase usually levels off after new routines and patterns are established. Eventually, co-workers are likely to save their messages and contact the telecommuter on a single occasion instead of several times throughout the day. When a co-worker is nearby, a problem or question may seem urgent enough to cross the hall to discuss the issue immediately. When the employee is telecommuting and must be reached by telephone or e-mail, some people begin to realize the issue is not as important or the information is not needed immediately. The physical separation caused by telecommuting can be enough to encourage employees to reconsider the need to interrupt another co-worker and recognize that issues initially deemed urgent can be resolved at a more convenient time.

## **Impact on the Manager**

Perhaps the most significant impact of telecommuting is on the part of the manager. Expectations and definitions of the role of manager are undergoing scrutiny and change. We are moving out of the era dominated by industrial and manufacturing philosophies. New roles, which are more consistent with an information-based workforce, with flatter management structures (fewer management layers) and markedly changed values and attitudes toward working, are being espoused for today's managers. Managers are expected to:

- ◆ Act as facilitators as opposed to supervisors or bosses;
- ◆ Push responsibility to the lowest practical level;
- ◆ Manage by results as opposed to observations; and
- ◆ Support worker efforts to achieve a more fulfilling balance between their work and family and/or other personal life needs.

While this new role is important in general for today's manager, it is specifically recommended for managers of telecommuters. This type of management is an essential component for a successful telecommuting arrangement.

Some managers already embrace some or all aspects of this facilitative management style. For such managers adjustment to telecommuting arrangements should be simple. Other managers are receptive to adopting this style of management; for them, the adjustment will be challenging but not difficult.

The major challenge, however, will be for those managers who view these new expectations with skepticism and disdain, and/or who think that adoption of the new management role will hinder their ability to accomplish their organizational missions and subject their organizations to abuses. In most cases, these concerns are unnecessary and unfounded.

## **Impact on the Organization**

There are several significant ways in which telecommuting benefits organizations. These include improved employee morale, improved ability to recruit and retain employees, more effective management, improved job performance, and reduced operating costs (in areas such as facilities, facility maintenance, health and sick leave costs). To some extent, however, the impact of telecommuting on organizations depends on the culture of the organization, and especially on its receptivity to change. Some organizations will implement telecommuting with minimal effort, while others may experience difficulty. For those organizations, proponents of telecommuting should be prepared to devote the time, effort and understanding needed while the organization adjusts to the new arrangements. As is true with individuals, organizations may need time to adjust to these changes.

### **Impact on the Customers**

In addition to organizational, job and staff considerations, managers and telecommuters need to consider the impact of telecommuting on their customers. Internal and external customers have needs and requirements that must be addressed in any telecommuting plans. Adjusting the telecommuting arrangement so that it has a zero impact, or even a positive impact on customer service is an important objective. The ideal situation should allow the customer to continue receiving goods and/or services while being totally unaware of the telecommuter's work arrangement or site location.

### **Impact on Personal Life/Families**

A majority of telecommuters report that telecommuting has had a positive impact on the quality of their personal life. The benefits of decreased stress, more personal time and greater job satisfaction can carry over to the telecommuter's home life. Telecommuting may make it easier to manage and schedule child and elder care arrangements. Experienced telecommuters warn however, that telecommuting cannot become a substitute for dependent care.

Finally, for the home-based telecommuters it is important that a comfortable boundary, both physical and social, be maintained between job activity and personal/family activity. The telecommuter must establish a specific workspace that should not intrude into the rest of the household and likewise, the rest of the household should not intrude upon the workspace of the telecommuter. Since the telecommuter is closer to home, family members may see this as an opportunity for the telecommuter to assist with errands or other personal responsibilities. The telecommuter must avoid allowing personal activity to intrude into the work time and activity.

## SECURITY

Security is an important aspect of telecommuting. Typically, alternative worksites are not as secure as the main worksite or office. A high degree of attention and/or adherence to security procedures, precautions and issues at the alternative worksites is, therefore, required.

There are three main areas of security in which telecommuters should focus attention. These areas are:

- ◆ Personal - specifically safeguarding the telecommuter;
- ◆ Information - specifically safeguarding confidential, private or classified information; and
- ◆ Property - specifically safeguarding government and telecommuter property used in the course of doing business.

The objective of this section is to sensitize the telecommuter to various security considerations. Adequate security is more than hardware, software and passwords; it is also a mindset that leads to common sense precautions. Everyone involved with the program should be familiar with the array of security precautions and also who is responsible for each. Telecommuters should know what actions must be taken and take them when there is a breach in security. TIGTA's policies and procedures should be readily available for all participants before they begin telecommuting.

The telecommuter should use good judgement regarding personal security at the alternative work site. For example, if the alternative worksite is not the home, then the telecommuter should be aware of and comfortable with the security at the alternative site.

### **Sensitive Information**

By following these rules, telecommuters can ensure protection for sensitive information.

- ◆ Telecommuters must use authorized storage facilities for storing sensitive materials.
- ◆ Telecommuters should be careful not to walk off and leave sensitive material out in the open for anyone to view (including family members not authorized to view sensitive information).
- ◆ Telecommuters should be conscientious about covering up sensitive information when approached by visitors.
- ◆ Managers and telecommuters alike should ensure that sensitive information is removed from computer equipment before the equipment is sent for service.
- ◆ Telecommuters should follow specified procedures for disposal, transfer or distribution of storage media, that contain or have contained sensitive materials.

- ◆ Telecommuters should not rely upon software deletion commands such as remove, delete or erase, to fully remove files from the computer. Even though information may appear to be deleted, there is a possibility that it may be retrieved with the correct software.
- ◆ Telecommuters should use passwords in conformance with the OIT policy on passwords contained in the policy section of this document.

### **Other Security Precautions**

The following are some general security precautions that telecommuters should be aware of:

- ◆ Program officials and/or telecommuters should ensure that anyone servicing the alternative work site is authorized to do so.
- ◆ Managers must ensure that the designated workspace has adequate physical or environmental security measures in place to prevent unauthorized access. This can be accomplished by completing the Security/Safety Checklist.
- ◆ Modem access to government computers presents special security concerns. Strict adherence to TIGTA IT security guidelines and policies is essential in all telecommuting environments.

## EQUIPMENT

Make sure you understand TIGTA's policy on equipment. A copy of the policy document is included under Section II of this document. You and your supervisor will need to determine what equipment is necessary. TIGTA will supply the telecommuter with a laptop and the necessary software. Additional equipment will be supplied based on the level of participation. Below are some points for the employee's information:

- ◆ The employee is responsible for supplying all other equipment such as desk, chair, lighting, etc. The employee may want to check GSA surplus for any office equipment.
- ◆ The Help Desk can provide support for government owned equipment by telephone; otherwise the employee will need to return the equipment to the office for repairs. The Help Desk is not equipped nor staffed to make house calls.

Before you receive your equipment, you need to understand one more point regarding liability:

- ◆ If TIGTA equipment breaks down, the help desk will fix it, just as they would in the office. If, however, TIGTA equipment is damaged through the employee's negligence, the employee is responsible for the repair.

To protect against transporting software viruses to your computer, consider the following measures:

- ◆ Do not use borrowed software, nor non-TIGTA issued software.
- ◆ Do not log onto private bulletin boards.
- ◆ Scan disks and/or hard drives before or after each telecommuting session (if episodic) if not automatic when you log on.

## ISSUES FOR THE TELECOMMUTER

The telecommuter needs to become aware of many issues. Some of them, while applicable to the traditional office worker are sometimes taken for granted. The following are items the teleworker needs to pay special attention to when working at home or an alternative worksite.

### ◆ Maintaining Interaction and Relationships with Co-Workers

Staying in contact with co-workers can be very important. Regularly scheduled days in the office each week may help maintain communication between telecommuters and co-workers. Telecommuters should encourage co-worker communication on telecommuting days; there should be no attempt to hide or downplay participation in the telecommuting program. Hiding the program can only serve to increase a co-workers feelings of resentment. Finally, telecommuters should not become rigid and entrenched in their telecommuting arrangements. Remaining flexible will facilitate telecommuter accessibility and maintain a relationship with the organization.

### ◆ Identifying Workload

Telecommuters often wonder how much of a workload they should take home with them on telecommuting days. The answer is: more than you think you can do. Most telecommuters are surprised by how much they can accomplish when they don't have the interruptions, distractions and stress associated with getting to and being in their office.

### ◆ Responding to Emergency Meetings and Crises on Telecommuting Days

To the extent possible go into the office for meetings, or arrange to attend through teleconferencing. With a telecommuting program, managers know where employees are and can usually reach them by telephone. Many managers say that the planning that goes with telecommuting eliminates some crises entirely.

### ◆ Employee Injury at the Alternative Worksite

Workers' compensation rights apply to alternate worksites in the same way they apply at the traditional office site. If you are injured on the job, notify your manager immediately. As soon as possible complete the CA-1 form and forward it to the IRS Workers' Compensation Office in Richmond VA. You may call 1-800-234-8323, for additional information.

### ◆ Emergency Closures on Telecommuting Days

A telecommuting employee may be affected by an emergency and may be excused from work.

If the work is disrupted at the alternative worksite due to loss of electricity, for example, the supervisor must be notified immediately. After discussion with the employee, the supervisor will make the determination as to whether: (1) any work can still be performed at the alternate site; (2) administrative leave would be appropriate under the circumstances; (3) the employee should proceed to the official worksite. Another option is for the employee to request to use annual leave for the remaining portion of the workday.

If the official duty station is closed after the workday begins, the manager may excuse telecommuters if he/she cannot perform their work because employees or systems at the official duty station are not available. Remember the key factor is the telecommuter's ability to perform the work, not whether the office is open or closed.

If, before the workday begins, there is an OPM announcement closing Federal agencies, telecommuting employees are excused from duty without loss of pay or charge to leave.

## VRS PARTICIPANT SELF-ASSESSMENT QUESTIONNAIRE

### **Instructions:**

The following questionnaire is to be used by employees to determine their ability to be a successful teleworker. Employees should honestly assess their potential for successful participation in TIGTA's Virtual Resource Solution Program. Upon completion of the questionnaire, and if the employee believes he or she can be a successful teleworker, he/she should ask his/her manager for the application materials.

The manager will be completing a questionnaire on the employee's likelihood of success in a virtual environment, and sharing his/her observations with the employee. It would be a good idea for the employee and the manager also to discuss the employee's self-assessment questionnaire to ensure agreement. For those items where the employee ranks himself/herself low, the employee should develop a development plan to improve his/her rating before he/she meets with the manager. An employee coming to a meeting prepared to discuss his/her needs is, in itself, a way of demonstrating to the manager a certain level of organizational ability. Again, this self-assessment is intended to provide the employee insight into his/her potential for successfully working at an alternative site. Completion of the Self-Assessment Questionnaire is not mandatory for participation in VRS.

## VRS PARTICIPANT SELF-ASSESSMENT QUESTIONNAIRE

**Name:**

**Position:**

**Grade:**

**Date Completed:**

**INSTRUCTIONS:**

Place a check mark on the appropriate line. A rating of 5 means the skill is at a high or excellent level, while a rating of 1 indicates a low or poor level.

<b>Teleworker Profile</b>	<b>5</b>	<b>4</b>	<b>3</b>	<b>2</b>	<b>1</b>
◆ Self-disciplined - requires minimal supervision	—	—	—	—	—
◆ Experience/skills - require minimal supervisory assistance	—	—	—	—	—
◆ Past and current performance/productivity levels	—	—	—	—	—
◆ Organizational skills	—	—	—	—	—
◆ Communication skills	—	—	—	—	—
◆ Relationship with peers	—	—	—	—	—
◆ Relationship with customers	—	—	—	—	—
◆ Ability to be flexible	—	—	—	—	—

## **FROM OFFICE WORKER TO TELEWORKER**

Once you have determined you would like to telecommute, there are several steps that you need to follow. The most important step is to open a dialogue between you and your manager to iron out all the issues surrounding teleworking.

After gaining your manager's approval to begin telecommuting there are several steps you should complete before beginning to telework.

1. Complete the Self-Assessment Questionnaire.
2. Complete the application form and submit it to your manager.
3. Encourage your manager to complete the Employee Assessment Questionnaire.
4. Discuss the results of the Employee Assessment Questionnaire with your manager.
5. Determine the parameters you will follow when you telecommute during the meeting with your manager.
6. Reach agreement on hours of work, days out of the office, days in the office, etc.
7. Complete the Program Work Agreement (Agreement) and the Safety/Security Checklist and submit them to your manager.
8. If applicable, make arrangements for your high-speed telecommunication service to be installed.
9. If applicable, complete the training course designed for the program.
10. While waiting for high-speed telecommunication service, begin a trial period under the parameters set forth in the Agreement.
11. Assess the outcome of the trial period and determine if any changes to the Agreement are necessary.
12. Once your telecommunications service is installed, you are on your way.
13. Enjoy your new stress-free work environment.

## THE APPEALS PROCESS

You have submitted an application for participation in VRS and your manager has determined you are not suited for working from a remote environment. You have completed the assessment sheet and discussed it with your manager, but the two of you cannot come to agreement. Now what happens?

The manager has the final word on whether an employee can work from an alternate worksite. The employee, however, does have appeal rights. The following is the appeal process:

- ◆ Meet a second time with your manager to try to reach agreement on the matter.
- ◆ If agreement cannot be reached, you have the right to appeal your managers decision to the next level manager.
- ◆ If you decide to appeal, submit the appeal in writing (e-mail is acceptable) to your manager within five (5) workdays from your initial meeting with him/her.
- ◆ Your manager will schedule a meeting to be attended by you, your manager, and your second level manager.
- ◆ Sufficient time will be allowed for the second level manager to listen to both points of view.
- ◆ Bring to the meeting any documentation you have to support your position. Your manager will do the same.
- ◆ Present your "case" to your second level manager. You will be given sufficient time to do so.
- ◆ Answer any questions posed by your first and second level managers.
- ◆ The second level manager has a reasonable amount of time to make his/her decision.
- ◆ The second level manager's decision is final.

## TRAINING FOR VRS

Before embarking on a new initiative, it is important that participants receive proper training. TIGTA has decided that all participants at the expanded or full level of participation must avail themselves of the stated training before entering a telework environment. The training will be provided by a contractor, Management Services Inc., in a virtual classroom environment.

Management Services Inc., a California based firm, was founded in 1995 to provide consulting and training services to technology companies working with geographically dispersed project teams. Their research into the area of distance communication led to the design and development of revolutionary tools and techniques in the distance learning arena.

### Course Content

- ◆ *Overview of Telecommuting* - explaining the most common forms; key benefits, business objectives and elements of a successful telework arrangement.
- ◆ *The Individual Telecommuter* - sets the expectations for a successful program; dealing with the fears of the telecommuter; understanding the myths and realities; and setting up a home office.
- ◆ *Effective Distance Communication* - identification of the four key principles of effective distance communication.
- ◆ *Managing Telecommuting* - explaining the role of the manager in a telecommuting environment and the importance of managing by objectives; measuring overall performance and useful techniques for team building.

### Availability and Delivery

- ◆ Employees telecommuting on an expanded and/or full-time basis and their managers are expected to complete the course.
- ◆ The training will be offered on-line in a virtual classroom environment.
- ◆ Students have the flexibility to take the lesson anytime during the day.
- ◆ The vendor will contact you several days before class begins to provide instructions for accessing the course.
- ◆ Sessions will be limited to groups of 16 per session and will be coordinated through each functional training coordinator.
- ◆ Training classes will take place beginning August 20 and run through September 28, 2001.
- ◆ Training will consist of approximately a 1-hour lesson per day over one workweek.
- ◆ A Certificate of Completion will be provided to each participant upon successful completion of the training. This Certificate should be filed in the employee's Drop File.

## GETTING CONNECTED AT HIGH SPEED

Broadband connection services provide high-speed data connections to the Internet over telephone or cable. The TIGTA Virtual Private Network (VPN) is accessed by users from home using, predominantly, a broadband connection. There are three types of broadband connections approved for use by TIGTA. All three have been tested and work. We recommend them in the following order.

**DSL** - Digital Subscriber Line (DSL) high-speed Internet connection that provides speed at varying levels. DSL service can be purchased from your local telephone company or from several Internet Service Providers.

**Cable Modem** – High-speed connection using your local cable company's cable network.

**IDSL** – Variation of DSL using slower speeds. It has been tested, is reliable, but is more expensive than DSL because it requires the use of a digital telephone line.

No other broadband services are approved for use by TIGTA employees participating in VRS.

### Preferred Solutions and Research Tips

Each employee needs to research in his or her area to determine which of these broadband solutions is available. We recommend a bandwidth capacity of 256Kbps up and 768Kbps down for an optimal VRS experience. The bare minimum bandwidth capacity that should ever be installed is 128Kbps up and 144Kbps down.

You should ask each vendor the following questions when you are looking for broadband services:

1. **Can I get your service at my residence?**
2. **What upstream and downstream speeds can I get, and what are the associated costs?** (Remember we are looking for 256Kbps up and 768Kbps down)
3. **Can you provide me with a broadband modem with an Ethernet (RJ-45) interface?** (The answer must be yes) Universal Serial Bus (USB) interface modems will not work.
4. **Does your network support the IPSEC protocol?** (The answer must be yes) You will not be able to connect to the TIGTA network unless your broadband service vendor supports the IPSEC protocol.
5. **Do you have a self-installation kit for your service?** (Choose the self-installation kit, if it is available) Many providers now offer a self-installation kit for their broadband service. This means that all of the equipment and software necessary to install your broadband service will be shipped directly to your

house. OIT personnel will assist you with the installation. This installation method can get your broadband service installed much quicker than waiting on a technician from your broadband service provider to perform the installation.

When you are finished researching and are ready to purchase broadband services from a particular vendor, call the vendor and schedule the installation. The installation scheduling will be dependent on the vendor. Please schedule the installation between the hours of 8:00 AM to 5 PM, Eastern, on a normal workday, so that OIT can assist with the installation. On the day of installation, the applicable checklist for DSL, IDSL, or cable modem will be used to collect detailed information necessary to perform your service installation.

TIGTA will reimburse the installation cost of the service and up to half of the recurring charges if you are in expanded or full VRS modes. **You must get approval from Dan Devlin, Director, Strategic Development, for recurring charges that will exceed \$100 per month.**

Good places to start your research are with your local telephone company for DSL and IDSL and with your local cable company for cable modem service. You can also do research online at the DSL Reports web site at [www.dslreports.com](http://www.dslreports.com). The DSL Reports web site also has lots of information on the different broadband services that are available. Click on the "Find Service" link to see what kind of DSL service is available in your area.

Your vendor will provide the hardware and software for the broadband connection; however, the TIGTA IT staff will install software and make any changes required on your government laptop computer.

**DO NOT allow vendors to install software or change the settings on these computers.**

**DO NOT attempt to use a self-installation kit to install software or change the settings on these computers without OIT assistance.**

## **TIMEFRAMES:**

It can take several weeks from the time you order your broadband services to the time the vendor will actually arrive at your home for the installation. This varies from vendor to vendor and by technology type (DSL, cable modem, etc.) and geographical area.

After you have **scheduled the vendor installation**, please notify the IT staff by completing a HELPDESK TICKET and include –

- Name of vendor(s) and type of service
- Date of scheduled installation at your home (and approximate time)
- Telephone number of service provider technical support

The Helpdesk will determine if the VPN software is installed on your desktop. If not, you will be asked to bring the unit into the office for software installation.

NOTE: With the new laptops scheduled for deployment in late summer, the VPN software will be pre-installed on everyone's desktop.

Request a digital certificate from the TIGTA IT Security Staff by completing an electronic Form 5081 (attached). A digital certificate is the electronic equivalent of a drivers license or government credentials. The digital certificate is used by the VPN software as a form of electronic identification on the TIGTA network. The VPN software will not work without a valid, TIGTA-issue, digital certificate. Once issued it is good for only 15 days.

To request your digital certificate, complete the following steps.

- Complete the form and have immediate supervisor approve it
- Transmit the form via email to Gino Talbot, IT Security Staff

The TIGTA Security staff will not issue your certificate until on or after your actual installation date. **One exception** - If you are going to use the VPN for remote dial up access prior to the installation of your broadband service, Form 5081 is required.

On the **day of vendor installation**:

- Call the Helpdesk Hotline (1-877-570-5094) when the technician arrives
- An OIT employee will help answer questions and fill out the appropriate checklist with the service provider technician.
- You will be established as a Local Administrator on your laptop computer to assist in this installation over the telephone with an IT Staff administrator.

Attached are two information sheets, one for DSL and IDSL type installations and one for cable modem. Please keep these information sheets handy, as they need to be filled out on the day of installation. Also note, that you will be assigned a TIGTA OIT POC to help you through the installation process. That name will be provided prior to your installation date.

Any questions, please contact the TIGTA Helpdesk.

**CABLE MODEM INFORMATION SHEET  
FOR VPN BROADBAND USERS**

**NAME:** \_\_\_\_\_

**VENDOR:** \_\_\_\_\_

**IP ADDRESSING: STATIC** \_\_\_\_\_ **DHCP** \_\_\_\_\_

**IF STATIC ADDRESSING:**

**IP ADDRESS:** \_\_\_\_\_

**SUBNET MASK:** \_\_\_\_\_

**DEFAULT GATEWAY:** \_\_\_\_\_

**DNS SERVERS:** \_\_\_\_\_

**MAKE & MODEL OF CABLE MODEM:** \_\_\_\_\_

**TECHNICAL SUPPORT PHONE NUMBER(S):** \_\_\_\_\_

**CLIENT NAME:** \_\_\_\_\_

**DOMAIN NAME:** \_\_\_\_\_

---

**DSL/IDSL INFORMATION SHEET  
FOR VPN BROADBAND USERS**

**NAME:** \_\_\_\_\_

**TYPE OF SERVICE:** \_\_\_\_\_

**VENDOR:** \_\_\_\_\_

**IP ADDRESSING: STATIC** \_\_\_\_\_ **DHCP** \_\_\_\_\_

**IF STATIC ADDRESSING:**

**IP ADDRESS:** \_\_\_\_\_

**SUBNET MASK:** \_\_\_\_\_

**DEFAULT GATEWAY:** \_\_\_\_\_

**DNS SERVERS:** \_\_\_\_\_

**ISP:** \_\_\_\_\_

**USERNAME:** \_\_\_\_\_

**PASSWORD:** \_\_\_\_\_

**PROTOCOL REQUIRED (other than TCP/IP):** \_\_\_\_\_

**TYPE & MODEL OF DSL/IDSL**

**MODEM:** \_\_\_\_\_

**TECHNICAL SUPPORT PHONE NUMBER(S):** \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

## **GLOSSARY OF TERMS**

### **Bandwidth**

- A general measurement that refers to the amount of information that can pass through a network circuit at any given time.

### **Cable Modem**

- A high-speed connection using your local cable company's network.

### **DHCP**

- Dynamic Host Control Protocol – This technology automatically assigns Internet Protocol (IP) addresses to computers that are connected to a network. Computers use Internet Protocol addresses to send data between each other.

### **Domain Name Server (DNS) Addresses**

- Domain Name Servers translate numeric IP addresses to easily remembered names. For example, the IP address 123.345.123.95 could be mapped on a DNS server to the web site named “MyWebSite.Com”. It is obviously much easier to remember the name of a web site, rather than the numeric address.

### **Downstream speed (download)**

- The bandwidth capacity that is available to download something into your local computer.

### **DSL**

- Digital Subscriber Line (DSL) high-speed Internet connection that provides speed at varying levels. DSL service can be purchased from your local telephone company or from several Internet Service Providers. This technology uses telephone lines to transmit your data. The distance between your house and your telephone company's central office determines the speed of your connection. DSL is not available if your home is more than 18,000 feet from the telephone company central office. It has been tested and is reliable for the TIGTA VPN architecture.

### **Ethernet Interface**

- A type of computer connection that is used to create a network of computers. This is the standard that TIGTA uses on our entire network. An Ethernet interface is also referred to as an RJ-45 interface.

## **IDSL**

- A variation of DSL using lesser speeds (128Kbps up and 128Kbps down). This is the only kind of DSL service that is available once you start getting close to the 18,000 feet distance threshold. It has been tested and is reliable for the TIGTA VPN architecture.

## **IPSEC Protocol**

- A data transmission technology that allows data to pass securely between public and private networks, i.e., Internet and TIGTA VPN

## **ISDN**

- A digital telephone line connection that provides 128Kbps speed up and down. ISDN is an older technology that is being phased-out.

## **Linksys Device**

- A device that connects your computer to your DSL or cable modem. OIT personnel will configure this device using information that is collected from your broadband services vendor.

## **Microwave Satellite**

- A wireless Internet connection that uses satellite-broadcasting equipment to transmit data.

## **Point-to-Point Protocol over Ethernet (PPPoE)**

- PPPoE (Point-to-Point Protocol over Ethernet) is a method that DSL providers use to limit access to their network to bona fide customers. Each customer is assigned a login and password to access the DSL network. In order for VRS personnel to activate their DSL service, the PPPoE protocol must be configured on the Linksys device.

## **Private Network**

- A network of private leased lines and computers that are dedicated for a particular organization's use. The general public does not have access to the network. The TIGTA network is a private network.

## **Public Network**

- A network that is open to the general public. Examples of public networks are the Internet, long distance telephone, local telephone, etc.

## **Remote Access VPN**

- The VPN system that TIGTA uses which permits secure, encrypted connections between mobile or remote users and the corporate network via a third-party network, such as an Internet service provider.

## **Static IP Addressing**

- Some vendors elect to assign permanent, or static, IP addresses to the machines on their network, rather than administer these using DHCP. In this case, the vendor will provide 4 items, including the IP address assigned to your machine, a subnet mask for their network, default gateway for their network, and domain name server addresses.

## **Universal Serial Bus (USB)**

- A type of computer connection that is used to attach different kinds of peripheral devices, such as printers, modems, cd-writers, etc. USB interfaces are not supported on the TIGTA network.

## **Upstream speed (upload)**

- The bandwidth capacity available when you are sending information from your computer to the server.

## **Virtual Private Network**

- Virtual Private Networks (VPN's) use advanced encryption technology to establish secure, end-to-end, private network connections over third-party networks, such as the Internet or extranets. VPN's provide the highest level of security using advanced encryption and authentication protocols that protect data from unauthorized access. A VPN allows mobile workers, telecommuters and day extenders to take advantage of high-speed, broadband connectivity, such as DSL and Cable, when gaining access to their corporate networks, providing workers significant flexibility and efficiency. VPN connections can also be established over dial up modem lines.

## **REIMBURSEMENT FOR TELECOMMUNICATION EXPENSES**

The reimbursement procedures below are the same for everyone regardless of the level of participation (Expanded or Full) in TIGTA's VRS Program. Employees will be reimbursed at the conclusion of every six-month period. The employee is responsible for immediately discontinuing all services if he/she stops participating in the program.

Effective October 1, 2001, employees who were in the pilot program, who plan to continue participating in the program (at the expanded or full level) and are currently receiving DSL service will need to contact their vendor and make arrangements to have the service charged to their residence. Credit card holders, who are currently paying for the DSL service with their small purchase card, should contact the vendor to cancel the service. To avoid interruption of service, the credit card holder and employee should coordinate their efforts.

### **Obtaining High Speed Data Installation / Service**

- ◆ Contingent upon your home location, contact your local Cable Company or DSL provider to obtain high-speed data service.
- ◆ If you plan to obtain cable modem service, ask your cable company if they can provide you with a separate monthly statement just for the cable modem service. Not all companies will provide a separate billing.

### **Reimbursement for High Speed Data Installation / Service (50% Reimbursement- Expanded or Full Participation)**

- ◆ If your cable company has provided separate monthly billing or you chose to obtain DSL service, simply make copies of the bills and forward them as a package to the address shown on the next page every six months.
- ◆ If, however, your cable company has not provided separate monthly billings, you need to place a check mark next to the expense line item(s) on your bills that directly relate to the cable modem service. Make copies of the marked bills and forward them as a package to the address shown on the next page every six months.
- ◆ Complete SF 1034, "Public Voucher for Purchases and Services," and include it with copies of the billing statements for reimbursement. The SF 1034 should be for reimbursement for the prior six months of service. A sample completed form for your reference, and a blank form from which additional copies can be made are found under the Forms section of this guide.

Mail Form 1034, with copies of the monthly billings, to the following address:

Treasury Inspector General for Tax Administration  
Attention: Carolyn Smith IG:MS:PI:F, Rm 700A  
1125 15<sup>th</sup> Street NW  
Washington, DC 20005

**Second Phone Line Installation / Monthly Service / Reimbursement  
(100% Reimbursement- Full Participation Only)**

- ◆ Follow the same procedures as described above for obtaining cable modem service and receiving billing reimbursement.
- ◆ The bills for the prior six months are to be included on the same SF 1034 as the DSL/Modem reimbursement requests and should cover the same period of time.

## PURCHASING APPROVED INCIDENTALS

TIGTA will not provide an office suite of furniture for your home or alternate work location. There are, however, a couple of items that will be required, dependent upon the employee's level of participation. Those items, with instructions for their purchase, are listed below.

### **Printer (Expanded or Full Participation Only)**

- ◆ OIT will be responsible for the purchase of all printers for the VRS program. The printers will be delivered to the appropriate office location for employees to arrange transportation to their homes.
- ◆ Should assistance be needed in hooking up the printer to your laptop, contact an OIT representative by placing a Help Desk request for assistance.

### **Locking File Cabinet (Full Participation Only)**

- ◆ For the purchase of a file cabinet, the maximum dollar allowance that TIGTA will provide is \$200.00.
- ◆ The cabinet specifications are as follows:
  - Metal on all sides;
  - Locks for all drawers;
  - Stationary; (i.e. not on rollers or casters); and
  - Black or neutral in color.
- ◆ The cabinets may be purchased at any local store or by supply catalog. Cabinets in the Corporate Express and Office Depot catalogs meet the above criteria.
- ◆ Once a file cabinet is selected, the employee should contact his/her small purchase credit card holder and provide him/her with the information needed to make the purchase (catalog name, item number, page number, etc.).
- ◆ When placing the order, the cardholder should provide the clerk with the name of the person that will be picking up the cabinet.
- ◆ For **local purchases** (Staples, Wal-Mart, etc.) the employee is responsible for picking up the cabinet and any assembly, if required.
- ◆ For **catalogs** or stores that deliver, the cardholder should provide the employee's name and home address. There may be a small delivery fee.

Note: Corporate Express will only deliver to the order points currently in place and will not deliver to an employee's home address. If using Corporate Express, therefore, the employee will need to make the necessary arrangements for picking up the cabinet.

- ◆ Should the employee leave TIGTA or stop participating in the VRS program, for whatever reason, the employee must return the file cabinet to the nearest TIGTA office. These cabinets remain TIGTA property. They will be made available to other VRS participants as they enter the program.
- ◆ The accounting string on which to charge the cabinets is as follows:  
01-0119-0390-8005-8005-18-3192

## **TELECOMMUTER'S WORK PRODUCTS**

Telecommuters often worry that managers and co-workers will think they are not working as hard or being as productive as employees in the office. Because of this perception, telecommuters will need to:

- ◆ Be diligent in identifying measurable tasks and deadlines with their supervisors and meeting those deadlines.
- ◆ Ensure that their work is discussed in staff meetings or other forums.
- ◆ Communicate regularly with managers and co-workers.
- ◆ Exercise diligence in progress reporting.

In some cases, telecommuters will need to refine their skills and methods of progress reporting. Telecommuters' work products and/or detailed progress notes (either written or verbal) should be the indicators that they are working according to agreed upon expectations. Telecommuters will need to begin marketing their work.

Remember telecommuters and their managers should focus on the quality, quantity and timeliness of the work products.

## LEAVE AND ATTENDANCE

Employees should understand the procedures for requesting leave and reporting their time and attendance. The information contained below is to be used as a guide, and is in no way a substitute for the guidelines developed in the TIGTA Operations Manual and applicable personnel policy guidelines.

### **Definitions:**

*Core Hours* - The hours during the workday that are within the tour of duty during which the employee covered by a flexible work schedule must be present for work or on approved leave. For TIGTA employees core hours are 9:30 a.m. through 2:30 p.m.

*Compressed Work Schedule (CWS)* - An alternative work schedule available to TIGTA employees. CWS available to TIGTA employees are 5/4/9 or 4/10.

*Full Time Tour of Duty* - The basic workweek for employees in a pay status, to include holidays and/or leave.

*Part Time Work Schedule* - A scheduled tour of duty of 16 to 32 hours per week.

*Sick Leave* - Leave used for when the employee is physically incapacitated or unable to work in accordance with applicable TIGTA policies, practices, laws and regulations.

*Tour of Duty* - The hours of a day (a daily tour of duty) and the days of an administrative workweek (a weekly tour of duty) scheduled in advance and during which an employee must perform work on a regular recurring basis.

### **Establishment of the Workweek:**

- ◆ The administrative workweek for TIGTA is Sunday through Saturday, with the basic workweek being Monday through Friday.
- ◆ An employee's workweek need not be changed due to participation in VRS.

### **Establishment of Work Schedules:**

- ◆ The daily standard tour of duty for a full-time employee shall consist of 8 working hours, worked continuously except for an unpaid lunch period.
- ◆ Participant work schedules must adhere to office work schedules (business hours) and core hours.
- ◆ Adjustment of work schedules for educational purposes is authorized per regulations contained in the TIGTA Policy Manual on Leave and Attendance.
- ◆ Assignments to standard tours of duty are to be recorded on the time sheet.
- ◆ Adjustment to work schedules for religious observances will be in accordance with applicable TIGTA guidelines and policies.

- ◆ Compressed work schedules, at management's discretion, are available to participating employees.

### **Leave:**

- ◆ Leave should be requested and approved in accordance with existing policies, practices, laws and regulations.
- ◆ Employee will use either a SF-71 or other approved document (for example e-mail message) to request leave.
- ◆ Managers decide when annual leave may be taken, consistent with applicable rules, regulations and TIGTA policy. This decision is made considering the needs of TIGTA and the employee.
- ◆ An employee requesting sick leave shall notify the manager as early as practicable, but no later than 9:30 a.m. on the day for which leave is requested.
- ◆ Employees participating in VRS may be advanced sick leave in accordance with applicable regulations and TIGTA policy.
- ◆ The granting of Leave Without Pay (LWOP) is a matter of management discretion.
- ◆ Employees who are absent from duty without authorization are considered to be Absent Without Leave (AWOL) until leave is requested and a decision is made by the manager in accordance with applicable regulations and policies.

### **Attendance:**

- ◆ All employees, regardless of participation in VRS, shall use the standard Time and Attendance form (or what is currently being used in their function).
- ◆ The Time and Attendance form shall be routed electronically to the manager with the employee's signature affixed in the appropriate area, or sent via facsimile to the manager for submission to the timekeeper.
- ◆ For purposes of certifying time and attendance, the employee may use an electronic signature.
- ◆ In lieu of an electronic signature for certification purposes, the transmission e-mail from the employee documenting the date, time and originator may be attached to the timesheet.

## **HOW TO WORK WITH YOUR MANAGER TO ENSURE SUCCESS**

Telecommuting arrangements must include a written agreement between the manager and the telecommuter, which outlines organizational policies and logistics for telecommuting. This agreement will address, among other matters, the time period for participating in the program, the official and alternate duty stations, the hours of work, timekeeping procedures, the work assignments and reporting requirements.

In addition to a work agreement, managers and telecommuters should establish performance goals and objectives or progress reporting procedures and associated expectations with specific timetables and deadlines clearly spelled out before starting the telecommuting arrangement. Any additional work procedures specific to the telecommuter's office should also be spelled out. The level of detail in these procedures and expectations depends on factors such as the manager's style of supervision, the telecommuter's style of communication, the job requirements and organizational needs.

Remember, telecommuting is not a right, but a privilege. It may be terminated by either the employee or the manager at any time.

## MYTHS AND MISPERCEPTIONS

Even after considering all the previously addressed issues, questions and misperceptions about telecommuting may linger. The following are some of the most commonly shared myths about telecommuting and the responses to these misperceptions.

***MYTH # 1 There is no way to judge if telecommuters are really working. They could be taking the day off.***

The employee's completed work products or progress reports are the indicators that he/she is working. Managers of telecommuters should focus on the quality, quantity and timeliness of work products. Managers should manage by results, rather than by observation. For those whose results are difficult to define using traditional performance measurements, performance expectations may be developed and refined through systematic progress reporting by the telecommuter. The manager and the employee should establish goals and objectives together.

***MYTH # 2 Employees work less if they work unsupervised.***

Survey results show marked improvements in productivity, often because employees have fewer distractions and interruptions and are less stressed due to the absence of a commute to work. Employees who have demonstrated their commitment to work at the traditional office typically exhibit the same or a greater level of commitment at the alternate work site. In fact, as opposed to working less, the reported tendency is for telecommuters to work much more, sometimes to the point of becoming a workaholic.

***MYTH # 3 Social interaction cannot be maintained between telecommuters and their colleagues.***

There are many techniques for overcoming feelings of isolation, including telecommuting for only a portion of the workweek, core days in the office and regular communication by telephone, voice mail or other communications media. Telecommuters should be included in all scheduled meetings and events and should receive all office correspondence.

***MYTH # 4 I won't be able to reach my employees when I need them. What if a crisis comes up?***

Managers can set the hours that employees are available by telephone or require telecommuters to call in at specified times. As for crisis situations, ask yourself: When a crisis happens now, is everyone available? Some people are out sick, some are on travel and some are off-site in meetings. With a successful telecommuting program, managers know where employees are and can usually reach them by telephone. Many managers say the planning that goes into telecommuting eliminates some of the crisis management entirely.

***MYTH # 5 Our office requires a relatively formal structure. Telecommuting is too unstructured for such an environment.***

Telecommuting is flexible, but that does not equate to unstructured. Managers often use a Telecommuter Agreement to spell out what is expected of an employee, and supervisors and telecommuters agree on tasks and due dates.

***MYTH # 6 Telecommuting is a nice, simple solution for the issues my organization faces.***

Any successful telecommuting program recognizes that telecommuting is just one tool organizations and managers can use to help solve the complex problems facing today's government organizations. Telecommuting should not be seen as a panacea for social difficulties or as a dumping ground for non-performers.

***MYTH # 7 Supervisors should feel grateful to be able to participate in a telecommuting program.***

Supervisors and managers often view telecommuting as a favor they can do for their employees, without any consideration for the tremendous benefits they gain from a telecommuting arrangement. In terms of productivity, flexible work arrangements allow participants and their organizations to take greater advantage of employee productivity peaks.

In fact, telecommuting should not be seen as a benefit or a reward, but rather as one human resources work option. Making it appear as a benefit or reward may have the effect of creating unnecessary resentment in the office.

**TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION**  
**VIRTUAL RESOURCE SOLUTION**  
**PROGRAM POLICY**

**POLICY**

It is the policy of the Treasury Inspector General for Tax Administration (TIGTA) to offer teleworking, also known as Virtual Resource Solution (VRS), at an alternative worksite as an effective way to meet TIGTA and employee needs.

**APPLICABILITY**

This policy applies to all TIGTA employees whose annual performance appraisal rate is "Pass," are not in a temporary, trainee or probationary period, and have executed a telework agreement.

**DEFINITIONS**

*Alternative worksite* - The location where the employee may conduct business, whether it be a home office or customer location.

*Designated office* - The employee's usual and customary work address, also known as official post of duty or regular office.

*Episodic Participation* - Participation in VRS is dependent upon the needs of the worker and the demands of the work. This is a task-based arrangement. The employee works on a particular task from an alternate worksite.

*Expanded Participation* - Employee participation in VRS for a majority of the workweek, either 2 or 3 days per week under a set schedule.

*Full Participation* - The employee works full time (4 - 5 days per week) at an alternative worksite, only coming into the office at the request of his or her manager and for a specific purpose.

*Limited Participation* - The employee works 1 day per week at an alternative worksite under a set schedule.

*Teleworking* - also called *Telecommuting* - The practice of working from a remote workplace, such as the home, instead of commuting to a designated office.

*Teleworking Schedule* - Teleworking is a flexible deployment of staff to meet TIGTA and employee needs. Telework may occur on a regular schedule (one or more set days each week) or on an episodic or intermittent basis.

*Virtual Office* - Employees working in the field work from their vehicle or various non-fixed locations. Communication with the designated office is generally by telephone, laptop computer, fax machine and/or other communication device.

## **EVALUATION CONSIDERATION**

The employee and his/her supervisor will work together to determine whether it is appropriate for the employee to participate in a telework arrangement. In making this determination, they shall consider the following:

- ◆ The employee's desire to telework;
- ◆ The employee's characteristics, job knowledge, skills and work history;
- ◆ The work to be performed;
- ◆ The availability of tools necessary to successfully perform the work;
- ◆ The security of Government information and equipment;
- ◆ The ability to manage work hours and employee expenses; and
- ◆ Scheduling issues.

## **TELEWORK AGREEMENT**

Teleworking is a management option, not an employee right. It is a privilege extended to employees as a voluntary option with the clear understanding that every job may not be appropriate for remote work. This is a voluntary program for both TIGTA and the employee and may be unilaterally terminated by either party.

A formal agreement must be signed by both parties prior to participation. A copy of the agreement must be filed in the employee's EPF, with a copy offered to the employee. The telework agreement covers such items as the voluntary nature of the arrangement; if episodic participation, the length of telework assignment; hours and days of duty for each worksite; responsibilities for timekeeping, leave approval, and requests for overtime and/or compensatory time; performance requirements; and proper use and safeguard of Government property and records. The manager should discuss requirements and expectations with the employee prior to the approval of the agreement.

## **TRAINING**

Participants in VRS, their managers, and other involved staff must participate in a specialized telework training program before the participants can begin to work from alternate worksites. A Certificate of Completion will be issued to the employee upon successfully completing the class; a copy should be provided to the manager.

The training will be provided by a vendor who specializes in delivering on-line or virtual classroom training and has subject expertise. The basic training course will be approximately five (5) hours in duration, including a 1-hour introductory lesson. The remaining four hours can be taken at the student's discretion during a pre-scheduled

timeframe. Participants should expect to spend one hour per lesson and will have the flexibility to take the lesson any time during the day. Instructors will be available to monitor student discussions and assignments daily.

**AUTHORIZED EXPENSES**

Executives or their designees are authorized to approve, following established TIGTA procedures and guidelines, expenditures for communication devices (to include charges for high speed telecommunications or second phone line/phone), computer peripherals, and office supplies needed by teleworkers at their alternate worksite based on need and available funding. Specifically, the following equipment and service expenditures are authorized based on the employee's level of participation:

Episodic or limited	No expenditure is authorized for equipment, phone or high-speed Internet service.
Expanded	Printer 50% of installation and monthly cost of high-speed Internet service
Full	Locking File Cabinet Second phone line (no cell phone) 100% of installation and monthly phone service cost Printer 50% of the installation and monthly cost of high-speed Internet service.

**COMPUTER EQUIPMENT AND SOFTWARE**

Government-owned property may be used by employees in their private residence consistent with the TIGTA Limited Personal Use Policy (TIGTA #01-17). The Government retains ownership and control of equipment provided the employee for use at the alternate worksite, and is responsible for its maintenance, repair and replacement. However, the employee may be held financially liable if the equipment is lost, stolen or damaged because of the employee's (or the employee's family member's) negligence, misuse or abuse. Transfer of the equipment and software between the official duty station and the alternative worksite is the responsibility of the employee.

## **TIME AND ATTENDANCE**

### **General:**

Work time away from the office will vary depending upon individual arrangements between employees and their supervisors. Supervisors and employees should mutually agree on days the employee will be in the designated office or official duty station. The frequency with which the employee will check and respond to e-mail and voice mail messages should be discussed and agreed upon prior to the employee's participation in VRS.

Fixed work schedules should identify the days and times employees will work in each work setting. Work schedules should be in compliance with TIGTA policy to ensure that employees are available during core hours. (Use of compressed work schedules is available consistent with TIGTA policy and supervisory approval).

Employees and managers should ensure that work-at-home situations do not adversely affect customers, clients and TIGTA mission goals. This policy document does not void other TIGTA policies that set availability standards.

### **Leave:**

Annual leave, sick leave, leave without pay, or other leave options must be requested and approved in accordance with existing TIGTA policy and practices and applicable laws and regulations.

### **Certification of Time and Attendance:**

Proper monitoring and certification of employee work time is essential for the successful implementation of the VRS program. Supervisors shall report time and attendance to ensure that employees are paid only for work performed, and that absences from scheduled tours of duty are accounted for correctly. Federal policies and procedures governing certification of time and attendance require principle offices with employees working at remote locations to provide reasonable assurance that they are working when scheduled.

### **Administrative Leave, Dismissals, Emergency Closings:**

Although a variety of circumstances may affect individual situations, the principles governing administrative leave, dismissals and closings remain the same for VRS participants and non-participants. The ability to conduct work (and the nature of any impediments) whether at home or at the office determines when an employee may be administratively excused from duty. For example, if the employee is working at home and the official duty station closes, the employee is expected to continue working. However, if for any reason beyond the control of the employee he/she cannot perform the work at home (such as a power failure or natural disaster), the supervisor has the option of granting administrative leave, consistent with TIGTA policy. When the

employee knows in advance of a situation that would preclude working at home, the employee should schedule an alternate site, time in the office or leave.

### **FAIR LABOR STANDARDS ACT (FLSA)**

The existing rules in 5 U.S.C section 5542 and FLSA governing overtime apply to VRS participants.

### **Injuries, Continuation of Pay and Workers' Compensation:**

VRS participants are covered by the Federal Employees Compensation Act if injured in the course of actually performing official duties at the regular office or alternative duty station.

### **Pay:**

*Duty Station* - for pay purposes, the official duty station is the employee's regular office and will not change with participation in VRS.

*Special Salary Rates* - The employee's official duty station serves as the basis for determining special salary rates and travel originations.

*Premium Pay* - The normal rules apply for night differential, Sunday and holiday pay whether work is accomplished at the official duty station or the alternative worksite. Official work schedules determine employees' entitlement to premium pay.

### **FACILITIES**

#### **Home Office Space:**

VRS participants working at home must have a designated workspace or workstation for performance of work. Requirements will vary depending on the nature of the work and equipment provided. Failure to maintain a safe work environment is grounds for terminating participation in the program. Participants will be required to complete a home safety/security checklist.

Unless otherwise agreed to, a minimum of 48 hours advance notice shall be given before management may inspect the employee's home worksite. Such inspections may be conducted at periodic intervals during the employee's normal working hours to ensure proper maintenance and operation of Government-owned property, to ensure compliance with the Safety/Security Checklist and/or for other legitimate purposes.

#### **Home Utility Expenses:**

TIGTA will not pay home utility costs associated with working from home. Combined savings to the employee resulting from reduced commuting, meals, clothing, etc., expenses should offset any incidental increases in home utility expenses. Exceptions

apply only where the personal expense directly benefits the Government, such as business-related long distance telephone calls from the employee's personal telephone.

### **Telephone Service:**

TIGTA will use appropriated funds to pay for all or part of the telecommunication service charges depending upon the level of the employee's participation in the program. Costs associated with the installation of a second telephone line or high-speed telecommunications service will be reimbursed according to the specifications cited earlier under the section entitled "Authorized Expenses."

### **COMPUTER SECURITY REQUIREMENTS**

Only hardware/software configurations provided by TIGTA's Office of Information Technology (OIT) or approved by OIT (as in the case of high-speed telecommunications) for the alternate worksite shall be installed. Under no circumstances shall the employee be allowed to add non-agency owned or unauthorized hardware or software to the workstation. No personally owned computers or software shall be used for processing classified or sensitive but unclassified information without the approval of the OIT staff.

Additionally, employees shall comply with organizational security procedures described in TIGTA's Information Technology Systems Security Policy (ITSSP), and ensure adequate security measures are in place to protect equipment from being accessed by unauthorized individuals. OIT staff will ensure that all TIGTA equipment being used for this program meets the security requirements for sensitive TIGTA IT systems described in the ITSSP.

### **PRIVACY ACT AND SENSITIVE DATA**

Access to sensitive materials must be consistent with regulations on Production or Disclosure of Information or Materials (34 CFR Parts 5 and 5b and FOIA and the Privacy Act 5 U.S.C sections 552 and 552a and 26 U.S.C section 6103). Employees participating in VRS agree to secure all sensitive but unclassified material in a locked container (e.g., file cabinet, brief case, etc.). Classified and highly sensitive material (e.g., grand jury material) shall not be taken to an alternative worksite.

### **DEPENDENT CARE COSTS**

This program is not intended to reduce dependent care costs or serve as a substitute for child care, day care, elder care, or any other type of dependent care. Employees are to treat work hours as if they were at their official duty station giving full attention to their work duties.

## **TAX BENEFITS**

An employee who uses a portion of his or her home for the benefit of the Government will be subject to current tax regulations and benefits. However, employees should consult their tax advisors or the Internal Revenue Service for information on Federal tax laws and interpretations that address their specific circumstances.

## **EVALUATION**

Evaluation of this program is critical to determining the best means of conducting an alternative work arrangement. To make this determination, an evaluation of the program will be completed after six-months. This evaluation will be comprised of the employees' and supervisors' overall perceptions on the impact and benefits of the Telework arrangement.

The success of the Telework program will be determined by assessing whether goals are being met, levels of production and service to customers remain stable or improve, and whether costs and other benefits remain stable or decrease for the employee and TIGTA.

TIGTA # 01-17

MEMORANDUM FOR ALL TIGTA EMPLOYEES

*David C. Williams*

FROM: David C. Williams  
Inspector General

SUBJECT: Personal Use of Government Office Equipment Including  
Information Technology

1. PURPOSE. This memorandum defines acceptable personal use of government office equipment, including information technology (IT) by TIGTA employees.
2. SCOPE. This memorandum applies to all functions within TIGTA. This policy applies to all TIGTA employees, including detailees, temporary employees, and interns performing work for TIGTA (hereafter called employees), whether the employee is working in a government-designated office, traveling, or working from home or other remote site on behalf of TIGTA.
3. POLICY. It is the policy of TIGTA to:
  - a. allow employees the privilege to use government office equipment, including IT, for non-government purposes when such use involves minimal additional expense to the government and does not overburden any of TIGTA's information resources;
  - b. permit limited personal use to employees during non-work time for reasonable duration and frequency of use;
  - c. grant use that does not adversely affect the performance of official duties or interfere with the mission or operation of the Agency; and
  - d. authorize use that does not violate the Office of Government Ethics (OGE) Standards of Ethical Conduct for Employees of the Executive Branch found at 5 Code of Federal Regulations (CFR) Part 2635, the Supplemental Standards of Ethical Conduct for Employees of the Treasury Department found at 5 CFR Part 3101, the Department of the Treasury Employee Rules of Conduct found at 31 CFR Part 0, and the TIGTA Operations Manual, chapter (700)-30, Ethics.

The personal use of government office equipment including IT resources requires responsible judgment, supervisory discretion and compliance with applicable laws and regulations. See Appendix A for specific guidance applicable to this policy. Employees

must be aware of IT security issues which are addressed in the Department of the Treasury Security Manual, TD P 71-10 (<http://intranet.cio.treas.gov/sites/cio/mag3/securityfs.htm>), TIGTA Operations Manual, chapter (500)-70, and other privacy concerns.

#### 4. DEFINITIONS.

- a. “Employee non-work time” means times when the employee is not otherwise expected to be addressing official business. Employees may, for example, use government office equipment during their own off-duty hours such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, or weekends or holidays (if their duty station is normally available at such times).
- b. “Government office equipment including IT” includes but is not limited to: personal computers and related peripheral equipment and software, library resources, telephone services, facsimile machines, photocopiers, office supplies, Internet connectivity and access to Internet services, and e-mail, but does not include the use of franked or official envelopes, mailing labels, or endorsements authorized by law.
- c. “IT” means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement control, display, switching, interchange, transmission, or reception of data or information.
- d. “Minimal additional expense” means that an employee’s limited personal use of government office equipment is limited to those situations where the government is already providing equipment or services and the employee’s use of such equipment or services will not result in any additional expense to the government or the use will result in only normal wear and tear, or the use of small amounts of electricity, ink, toner or paper. Examples of minimal additional expenses include making a few photocopies, using a computer printer to print out a few pages of material, making occasional brief personal phone calls (consistent with Department of Treasury policy and 41 CFR § 101-35.201), infrequently sending personal e-mail messages, or limited use of the Internet for personal reasons.
- e. Limited personal use by employees during personal time is considered an “authorized use” of government property as the term is used in the Standards of Conduct for Employees of the Executive Branch (5 CFR § 2635.704(a)). Employees are specifically prohibited from the pursuit of private commercial business activities or profit-making ventures using the government’s office equipment. The ban also includes employees’ using the government’s office equipment to assist relatives, friends, or other persons in such activities (e.g., employees may not operate or participate in the operation of a business with the use of TIGTA computers and Internet resources).

f. "Privilege," in the context of this policy, means that TIGTA is extending the opportunity to its employees to use government property for limited personal use in an effort to create a more supportive work environment. However, this policy does not create the right to use government office equipment for non-government purposes. Nor does the privilege extend to modifying the equipment used, including loading personal software, copying existing software, or making configuration changes. Specific exceptions may be necessary to accommodate staff members with a valid need. Requests for such exceptions should be directed to the employee's first level supervisor.

## 5. RESPONSIBILITIES.

a. The Assistant Inspector General for Information Technology (AIG-IT) has TIGTA-wide responsibilities to manage IT, including IT security, and to formulate TIGTA policies on IT. AIG-IT will disseminate additional policy appropriate to this subject and provide, as necessary, assistance to TIGTA functions in its implementation.

b. Managers should ensure that employees are informed of appropriate uses of government office equipment and information technology as a part of their introductory training, orientation or the initial implementation of this policy (See Appendix A – Specific Guidance).

c. Employees are accountable to follow rules and regulations and to be responsible for their own personal and professional conduct. The OGE Standards of Ethical Conduct states, "Employees shall put forth honest effort in the performance of their duties." 5 CFR § 2635.101(b)(5). In addition, the Office of Personnel Management (OPM), Employee Responsibilities and Conduct, states, "An employee shall not engage in criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, or other conduct prejudicial to the Government." 5 CFR § 735.203.

## 6. AUTHORITY.

a. 5 CFR Part 2635, Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch

b. 5 CFR Part 3101, Supplemental Standards of Ethical Conduct for Employees of the Department of the Treasury

c. 31 CFR Part 0, Department of the Treasury Employee Rules of Conduct

d. 5 CFR Part 735, Office of Personnel Management, Employee Responsibilities and Conduct

e. Treasury Directive 87-04, Personal Use of Government Office Equipment Including Information Technology, May 17, 2001

- f. TIGTA Operations Manual (700)-30, Ethics
7. REFERENCES.
- a. 5 CFR § 2635.101 (b)(5) and (9), Basic Obligation of Public Service
  - b. 5 CFR § 2635.702 (b), Appearance of Governmental Sanction
  - c. 5 CFR § 2635.704 (a) and (b)(1), Use of Government Property
  - d. 5 CFR § 2635.705, Use of Official Time
  - e. 5 CFR § 735.203, Conduct Prejudicial to the Government
  - f. 31 CFR § 0.213, General Conduct
  - g. Federal CIO Council, Recommended Executive Branch Model Policy/Guidance on “Limited Personal Use” of Government Office Equipment including Information Technology, May 19, 1999, <http://www.cio.gov/files/peruse.pdf>
  - h. 41 CFR § 101-35.201 (FPMR)
  - i. Office of Management and Budget (OMB) Circular A-130, Appendix III, “Security of Federal Automated Information Resources”
  - j. TD P 71-10, Department of the Treasury Security Manual (<http://Intranet.cio.treas.gov/sites/cio/maq3/securityfs.htm>)
  - k. TD P 81-01, Department of the Treasury Information Technology (IT) Manual
  - l. TIGTA Operations Manual, chapter (500)-70, Information Systems Security.

## Specific Guidance

### 1. Specific Provisions on the Limited Personal Use of Government Equipment and Information Technology

Under this policy, employees are authorized limited personal use of government office equipment. This personal use must not result in loss of employee productivity or interference with official duties. Moreover, such use should incur only minimal additional expense to the government in areas such as:

- a. communications infrastructure costs; e.g., telephone charges, telecommunications traffic, etc.;
- b. use of consumable products in limited amounts; e.g., paper, ink, toners, etc.;
- c. general wear and tear on equipment;
- d. minimal data storage on storage devices; and
- e. minimal transmission impacts with moderate e-mail message sizes with small attachments.

### 2. Inappropriate Personal Uses

Employees are expected to conduct themselves professionally in the workplace and to refrain from using government office equipment for activities that are inappropriate. Misuse or inappropriate personal use of government office equipment includes but is not limited to:

- a. the creation, copying, transmission, or retransmission of greeting cards, video, sound or other large file attachments that can degrade the performance of the entire network. "Push" technology on the Internet and other continuous data streams would also degrade the performance of the entire network and be an inappropriate use;
- b. access to pornography or hacker sites opens TIGTA to unacceptable security risk and is considered an inappropriate use;
- c. using the government systems as a staging ground or platform to gain unauthorized access to other systems;

- d. the creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter;
- e. using government office equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation;
- f. the creation, download, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials;
- g. the creation, download, viewing, storage, copying, or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited;
- h. downloading, copying, and/or playing of computer video games;
- i. use for commercial purposes or in support of “for-profit” activities or in support of other outside employment or business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services);
- j. engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity;
- k. use for posting government information to external news groups, bulletin boards or other public forums without authority. This includes any use that could create the perception that the communication was made in one’s official capacity as a Federal Government employee, unless appropriate agency approval has been obtained;
- l. any use that could generate more than minimal additional expense to the government (e.g., subscribing to unofficial LISTSERV or other services which create a high volume of e-mail traffic); and
- m. the unauthorized acquisition, use, reproduction, transmission, or distributions of any controlled information including computer software and data, that includes privacy information, copyrighted, trademarked, or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.

### **3. Malicious Software**

All employees should remain alert to malicious software or messaging often transmitted under the guise of a friendly greeting or joke in the subject field of e-mail transmissions. Loading and/or executing any foreign files or software on an individual workstation may result in damage to personal computers or compromise the security of sensitive government records. It is therefore imperative that employees exercise appropriate caution in their electronic communications.

#### **4. Proper Representation**

It is the responsibility of employees to ensure that they are not giving the false impression that they are acting in an official capacity when they are using government office equipment for non-government purposes. If there is a reasonable expectation that such a personal use could be interpreted to represent an official position, then an adequate disclaimer must be used. One acceptable disclaimer is – *“The content of this message is mine personally and does not reflect the position of the U.S. Government, the Department of the Treasury, or the Treasury Inspector General for Tax Administration.”*

The OGE Standards of Ethical Conduct states that “...an employee shall not use or permit the use of his Government position or title or any authority associated with his public office in a manner that could reasonably be construed to imply that his agency or the Government sanctions or endorses his personal activities.” 5 CFR § 2635.702(b). In addition, 5 CFR § 2635.704 concerning the use of government property, 5 CFR § 2635.705, Use of Official Time, and 31 CFR § 0.213 concerning general conduct should be reviewed.

#### **5. Privacy Expectations**

Employees do not have a right, nor should they have any reasonable expectation, of privacy while using any government office equipment at any time, including accessing the Internet or using e-mail. To the extent that employees wish that their private activities remain private, they should avoid using government office equipment such as their computer, the Internet, or e-mail for such activities. By using government office equipment, employees give their consent to disclosing the contents of any files or information maintained using government office equipment. In addition to access by TIGTA officials, data maintained on government office equipment may be subject to discovery and Freedom of Information Act requests.

By using government office equipment, consent to monitoring and recording is implied with or without cause, including (but not limited to) accessing the Internet or using e-mail. Any use of government communications resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

## **6. Sanctions for Misuse**

Unauthorized or improper use may result in loss of use or limitations on the use of the information technology resources, disciplinary or adverse actions, termination, criminal penalties and/or the employee being held financially liable for the cost of improper use.

## TIGTA-IT INFORMATION SECURITY PASSWORD POLICY

Treasury Directive 71-10 (TDP 71-10) requires Treasury Bureau systems utilize some form of user authentication (i.e., TIGTA currently uses passwords for user authentication to all TIGTA systems). Your password is your personal key to the TIGTA systems. This document specifies the password policies set forth by TIGTA for implementation and compliance by all TIGTA personnel. A LOGIN, in conjunction with a password, assists in determining accountability for all transactions. Therefore, creating and maintaining an effective password methodology is crucial in protecting TIGTA information assets.

The following is TIGTA password policy.

**P1: All TIGTA users' passwords must have at least eight (8) characters in length.**

*A Strong password helps to ensure that only authorized individuals access your TIGTA computer systems. For more information in creating a strong password, please see Password Guidelines [http://web.tigta.treas.gov/AISS\\_WEB/guidelines/policyindex.htm](http://web.tigta.treas.gov/AISS_WEB/guidelines/policyindex.htm)*

***P2: All TIGTA passwords shall be changed every 90 days. Notification for change shall start 10 days prior to required changed date. Users must not employ the same password more than once in a twelve-month period.***

The fixed password change interval must be synchronized across all computer and network platforms TIGTA wide.

***P3: Users with privileged user-IDs (Administrators) must never use the same password twice in a twelve-month period and must change passwords every 90 days.***

***P4: Users with privileged user-IDs (Administrators) must use their unique administration password to perform only administrative duties such as configuring systems, loading applications, etc.***

**P5: System administrators must have at least two user-IDs. One of these user-IDs must provide privileged access and be logged; the other must be a normal user-ID for the day-to-day work of an ordinary user.**

This policy is intended to separate the work of systems administrators into two distinct categories, each of which has different access control privilege needs. By segmenting the work of systems administrators, this policy supports the notion of the need-to-know.

**P6: All user-chosen passwords for computers and networks must be difficult to guess.**

*Words in a dictionary, derivatives of user-IDs, and common character sequence such as "123456" must not be employed. Likewise, personal details such as spouse's name, automobile license plate, social security number, and birthday must not be used unless accompanied by*

*additional unrelated characters. User-chosen passwords must also not be any part of speech. For example, proper names, geographical locations, common acronyms, and slang must not be employed. For more information see Password Guidelines [http://web.tigta.treas.gov/AISS WEB/guidelines/policyindex.htm](http://web.tigta.treas.gov/AISS_WEB/guidelines/policyindex.htm)*

**P7: Users are prohibited from constructing fixed passwords by combining a set of characters that do not change, with a set of characters that predictably change. Users must not construct passwords, which are identical or substantially similar to passwords that they had previously employed.**

*In these prohibited passwords, characters that change are typically based on the month, a department, a project, or some other easily guessed factor. For example, users must not employ passwords like "X34JAN" in January, "X34FEB" in February, etc.*

**P8: All user-chosen passwords must contain at least 3 of the following character types: UPPERCASE LETTER (A...Z), lowercase letter (a...z), numerical (0-9), and/or non-alphanumeric characters (,%&!).**

*The use of control characters and other non-printing characters is discouraged because they may inadvertently cause network transmission problems or unintentionally invoke certain system utilities.*

**P9: The display and printing of passwords must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.**

*The intention behind this policy is to prevent passwords from falling into the hands of unauthorized parties. This policy supports two secure systems design principles: (1) each user should have a unique password and user-ID, and (2) each user should have a password known only to that user. Even the security administrator/system administrator should not know user passwords (with the temporary exception of a newly issued or reissued password).*

**P10: The initial passwords issued by an administrator must be valid only for the involved user's first on-line session. At that time, the user must be forced to choose another password before any other work can be done.**

*The intent of this policy is to make sure that only an involved end-user knows his/her own password. This will in turn allow system activity logged with a corresponding personal user-ID to be uniquely attributable to a certain user.*

**P11: The user shall be allowed only five (5) unsuccessful attempts to enter a password. After 5 attempts the user-ID must be either: (a) suspended until reset by a system administrator, (b) temporarily disabled for no less than three minutes, or (c) disconnected, if dial-up or other external network connections are involved.**

One of the most frequently successful attack methods for gaining system access is simple password guessing. Besides simple context-sensitive guessing (knowing a bit about the user and the circumstances), attackers can use password cracker programs to exhaustively go through words in the dictionary.

**P12: When logging into any TIGTA network or data communications system, if any part of the log-in sequence is incorrect, the user must not be given specific feedback indicating the source of the problem. Instead, the user must simply be informed that the entire log-in process was incorrect.**

*Persons attempting to break into systems can use specific feedback messages to determine what they are doing right, thereby narrowing the number of different combinations they need to try.*

**P13: TIGTA wide, all workstations including laptops, must be using some type of screen-savers with fixed-password-based boot protection along with a time-out- after-no-activity feature.**

The intention is to prevent unauthorized persons from gaining access to sensitive information stored within in the TIGTA systems using the unattended workstation as the access vehicle.

**P14: When the system is idle longer than ten (10) minutes, an automatic blanking of the screen (with a password screen saver evoked) and a suspension of the session shall occur. Re-establishment of the session may take place only after the user has provided the proper password.**

*The intention of this policy is to prevent unauthorized disclosure of information and unauthorized system usage resulting from authorized workers walking away from their desks without locking their workstation.*

**P15: Passwords must not be stored in readable form in: automatic log-in scripts, hardcopy, software macros, terminal function keys, computers without access control, or other locations where unauthorized persons might discover or use them.**

*The intention of this policy is to prevent readable passwords from falling into the hands of unauthorized persons.*

**P16: Passwords or password files must always be encrypted when held in storage for any significant period of time or when transmitted over networks.**

This will prevent them from being disclosed to wiretappers, technical staff who are reading systems logs, and other unauthorized parties.

**P17: Passwords must never be hard-coded (i.e., incorporated) into any software developed in-house or outsource.**

To hardcode or incorporate a password into developed software requires intervention by the developer to change the password. This leads to inflexible security policy implementation that the user password be known to only that user.

**P18: Computer and communication systems must be designed, tested, and controlled so as to prevent both the retrieval of and unauthorized use of stored passwords, whether the passwords appear in encrypted or unencrypted form.**

The intention of this policy is to prevent unauthorized persons from obtaining access to passwords that might then be used to gain unauthorized system access.

**P19: TIGTA application systems developers must consistently rely on the password access controls provided by the TIGTA approved operating system or a TIGTA approved access control package that enhances the operating system. Developers must not construct separate mechanisms to collect passwords or user-IDs. Similarly, developers must not construct or install other mechanisms to identify or authenticate the identity of users without the advance permission of the TIGTA PRINCIPAL ACCREDITING AUTHORITY or his/her designee.**

*This policy is useful to achieve consistent access controls across application systems. Generally speaking, operating systems and related access control packages (e.g., IBM's RACF) have the strongest access control mechanisms of any type of software.*

**P20: TIGTA computer and communication systems access control must be achieved via passwords, which are unique to each individual user. Access control to files, databases, computers, and other system resources via shared passwords (also called lockwords) is prohibited. Should a shared password become necessary, a waiver request, accompanied a business need justification, must be submitted to the TIGTA PRINCIPAL ACCREDITING AUTHORITY for approval to waive this policy.**

*The intention of this policy is to prevent systems administrators from establishing access control privileges with a scheme that leads to problems (specifically with lockwords rather than passwords).*

**P21: All TIGTA internal network devices (e.g., routers, firewalls, access control servers, etc.) must have unique passwords or other access control mechanisms. Therefore, a compromise in the security of one device will not automatically lead to a compromise in other devices.**

*This policy is intended to prevent the discovery or unauthorized disclosure of a network device fixed password from leading to catastrophic damage. If unique, fixed passwords are used for each device, then the damage could be restricted to that compromised device only and what that device can do (perhaps capture other fixed passwords flowing through it).*

**P22: All vendor-supplied default passwords must be changed before any computer or communications system is connected to the TIGTA Enterprise Architecture.**

One of the oldest, yet still most successful ways to break into systems is to employ default vendor passwords. These default passwords are typically strings such as "sysadm," "sysmanager," or "guest."

**P23: To prevent the compromise of multiple systems, TIGTA system users must use different passwords on each of the systems to which they have been granted access (i.e. NT pswd., AIX pswd., IDRS pswd., etc.).**

This policy prevents the users from putting "all of their eggs in one basket," thereby allowing unauthorized persons to gain access to a variety of systems (LAN/WAN) rather than just the particular compromised system.

**P24: All system passwords must be promptly changed if they are suspected of being disclosed, or known to have been disclosed, to unauthorized parties.**

**P25: All multi-user computer systems with a fixed password as its primary access control mechanism, must utilize a unique, strong password for each system. The fixed password on all those systems must be changed immediately after evidence of system compromise.**

*This policy assumes that all users have their own unique user-IDs. If the password in question has been disclosed to some other party, or if this is only suspected, then the password must be immediately changed. It is also assumed that the system technically allows users to change their passwords, otherwise the system administrator must provide a temporary password and the user must change the provided password immediately. An example of a multi-user system is the application servers that audit uses.*

**P26: Passwords must not be written down and left in a place where unauthorized persons might discover them.**

Many users don't think about these risks unless management alerts them to the problems.

**P27: Regardless of the circumstances, system passwords must never be shared or revealed to anyone other than the authorized user.**

*To do so makes the authorized user responsible for actions taken by the unauthorized user. If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other approved mechanisms.*

**P28: All users must have their identity verified with a user-ID and password--or by other means which provide equal or greater security--prior to being permitted to remotely connect to TIGTA's network.**

*The intent of this policy is to make sure that only authorized people gain access to organizational networks.*

**Application for Participation in the Virtual Resource Solution  
Program  
And  
Privacy Act Authorization**

I \_\_\_\_\_, wish to participate in the Telecommuting program, Mobile Office Concept, offered by the Treasury Inspector General for Tax Administration (TIGTA). The specific telework arrangement I am requesting is set forth below. I understand that when I work from home or any other telecommuting location, that TIGTA must be able to contact me during my normal hours of work. I further understand that a requirement of my participation in this program is that information relative to contacting me must be provided to the Bureau designee on a voluntary basis. I understand that my personal (home) electronic mail address and my personal (home or portable) telephone number (s) is generally protected from public disclosure under the Privacy Act of 1974, 5 U.S.C Section 552a (1994 & Supp. II 1996), amended 1997, 5 U.S.C. Section 552a (West Supp. 1998).

To satisfy the requirements for participation in the telecommuting program, I hereby authorize TIGTA to disclose my personal e-mail address and personal telephone number(s) to my supervisors (immediate and hierarchical), other TIGTA employees (as determined necessary by my immediate supervisor) and to outside (non-TIGTA) persons (to be determined by me before disclosure in conjunction with my supervisor) which I have voluntarily provided to TIGTA for the sole and limited purpose of telecommuting to conduct official business.

Telework Arrangement Requested: \_\_\_\_\_

\_\_\_\_\_  
Name

\_\_\_\_\_  
Position/Office

\_\_\_\_\_  
Date

**TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION  
(TIGTA)**

**VIRTUAL RESOURCE SOLUTION (VRS)**

**PROGRAM WORK AGREEMENT**

The following constitutes an agreement between: \_\_\_\_\_ and  
(Name of Employee)

\_\_\_\_\_ of \_\_\_\_\_  
(Supervisor) (Function)

on the terms and conditions of the VRS Program. The supervisor and employee agree as follows:

**A. Alternative Work Place Option:**

Episodic \_\_\_\_\_ Limited \_\_\_\_\_ Expanded \_\_\_\_\_ Full \_\_\_\_\_

**B. Voluntary Participation**

Employee voluntarily agrees to work at the TIGTA-approved alternate workplace indicated below and to follow all applicable policies and procedures. Employee recognizes that telecommuting is not an employee benefit but an alternative method approved by TIGTA to accomplish the agency's mission and work objectives.

**C. Trial Period**

Employee and supervisor agree to try the arrangement for a period of 30 days unless otherwise changed by either party. The Trial period will begin \_\_\_\_\_ and end \_\_\_\_\_. This agreement may be renewed or extended at the end of the trial period.

**D. Salary and Benefits**

TIGTA agrees that this arrangement is not a basis for changing the employee's salary or benefits.

**E. Duty Station and Alternate Workplace**

Supervisor and employee agree that the employee remains at his/her current official duty station. The employee's approved alternate workplace is

\_\_\_\_\_ All pay, leave, and travel entitlements are based on the official duty station.

**F. Official Duties**

Unless otherwise instructed, employee agrees to perform official duties only at the regular office/official duty station or TIGTA approved alternative workplace. No business meetings will be conducted at the employee's home worksite. Employee agrees not to conduct personal business while in official duty status at the alternative workplace, for example, caring for dependents or making home repairs.

**G. Work Schedule and Tour of Duty**

Supervisor and employee agree the employee's tour of duty will be as follows:

Days \_\_\_\_\_ Hours \_\_\_\_\_ Location \_\_\_\_\_

If the employee's work hours at the alternate worksite differ from those at the official duty station, please explain:

**H. Time and Attendance**

Supervisor agrees to make sure the employee's timekeeper has a copy of the employee's work schedule. The supervisor agrees to certify biweekly the time and attendance for hours worked at the regular office and the alternative worksite.

**I. Leave**

Employee agrees to follow established office procedures for requesting and obtaining approval of leave.

**J. Overtime**

Employee agrees to work overtime only when approved by supervisor in accordance with established office policies.

**K. Equipment and Supplies**

Employee agrees to protect any Government-owned equipment and to use the equipment for Government purposes. Personal use of Government-owned equipment will be consistent with TIGTA's Personnel Use Policy (TIGTA # 01-17). TIGTA agrees to service and maintain any Government equipment issued to the employee. The Employee agrees to install, service, and maintain any personal equipment used. TIGTA agrees to provide the employee with all

necessary office supplies, which can be obtained through established office policies and procedures.

#### **L. Security**

Employee agrees to follow all TIGTA security provisions described in TIGTA's Information Technology Systems Security Policy (Section 4.4.7 addresses work-at-home). TIGTA will ensure that information technology equipment used to process sensitive but unclassified information meets the security requirements for sensitive TIGTA IT systems as presented in the Information Technology Systems Security Policy.

**Employee agrees to secure all sensitive but unclassified material in a locked container (e.g., file cabinet, brief case, etc.). Classified and highly sensitive material (e.g., grand jury material) will not be taken to an alternative workplace.**

**Employee's initials \_\_\_\_\_**

#### **M. Liability**

The employee understands that TIGTA will not be liable for damages to the employee's real or personal property while the employee is working at the alternative work site, except to the extent the agency is held liable by the Federal Tort Claims or the Military Personnel and Civilian Employees Claims Act.

#### **N. Work Area**

The employee agrees to provide a work area adequate for performance of official duties.

#### **O. Worksite Inspection**

The employee agrees to permit the manager, with a minimum of 48 hours notice, to inspect the alternative workplace during the employee's normal working hours to ensure proper maintenance of Government-owned property and conformance with safety and security standards. Employees working at home must complete a self-certification safety/security checklist to ensure the safety/security of the employee and Government-owned property at the alternate worksite.

#### **P. Alternative Workplace Cost**

The employee understands that TIGTA will not be responsible for any operating costs that are associated with the use of his/her home as an alternative worksite.

### **Q. Injury Compensation**

Employee understands that he/she is covered under the Federal Employee's Compensation Act if injured in the course of actually performing official duties at the regular office or the alternative duty station. The employee agrees to notify the supervisor immediately of any accident or injury that occurs at the alternative workplace and to complete any required forms. The supervisor agrees to investigate such a report immediately.

### **R. Work Assignments/Performance**

Employee agrees to complete all assigned work according to procedures mutually agreed to by the employee and the supervisor. The employee agrees to provide regular reports, if required by the supervisor, to help judge performance. The employee understands that a decline in performance may be grounds for terminating the alternative workplace arrangement.

### **S. Disclosure**

Employees agree to protect TIGTA records from unauthorized disclosure or damage and will comply with requirements of the Privacy Act of 1974, 5 U.S.C. section 552a, and I.R.C. section 6103, (confidentiality and disclosure of return and return information).

### **T. Standards of Conduct**

Employee agrees to be bound by TIGTA standards of conduct while working at the alternative worksite.

### **U. Cancellation**

TIGTA agrees to let the employee resume a regular schedule at the official duty station after notice to the supervisor to terminate the arrangement. Employee understands that TIGTA may unilaterally cancel the VRS arrangement and instruct the employee to resume working at the official duty station. TIGTA agrees to follow any applicable administrative procedures.

## **V. Policy**

The TIGTA VRS Program Policy supplements this agreement. Employee and supervisor agree to become familiar with and adhere to the policy, a copy of which is attached.

---

**Employee's signature and date**

---

**Supervisor's signature and date**

**Self-certification Safety and Security Checklist  
for  
Home-based Telecommuters**

**EMPLOYEE NAME:** \_\_\_\_\_

**ORGANIZATION:** Treasury Inspector General for Tax Administration (TIGTA)

**FUNCTION:** \_\_\_\_\_

**ADDRESS:** \_\_\_\_\_

**CITY/STATE:** \_\_\_\_\_

**HOME TELEPHONE:** \_\_\_\_\_

**BUSINESS TELEPHONE:** \_\_\_\_\_

The following checklist is designed to assess the overall safety and security of the employee's alternative workplace. The employee should complete the self-certification checklist. Upon completion the employee and his/her manager should both sign and date the checklist in the applicable spaces provided. A copy of the checklist should be provided to the employee, with the original maintained in the employee's Drop File.

**Describe the designated work area in the alternate duty station:**

**A. WORKPLACE ENVIRONMENT**

1. Are temperature, noise, ventilation, and lighting levels adequate for maintaining your normal level of job performance? Yes \_\_\_ No \_\_\_
2. Are all stairs with 4 or more steps equipped with handrails? Yes \_\_\_ No \_\_\_
3. Are all circuit breakers and/or fuses in the electrical panel labeled as to intended service? Yes \_\_\_ No \_\_\_
4. Do circuit breakers clearly indicate if they are in the open or closed position? Yes \_\_\_ No \_\_\_
5. Are fire/smoke detectors installed and in proper working order? Yes \_\_\_ No \_\_\_
6. Do doors have security locks? Yes \_\_\_ No \_\_\_
7. Is there an alarm/security system installed and in working order? Yes \_\_\_ No \_\_\_
8. Do windows (especially ground level) have positive locking devices? Yes \_\_\_ No \_\_\_
9. Do you have adequate security in your home to protect others from sensitive equipment (e.g., firearms, radios, pagers, telephones or other Government issued items)? Yes \_\_\_ No \_\_\_
10. Is all electrical equipment free of recognized hazards that would cause physical harm (e.g., frayed wires, bare conductors, loose wires, flexible wires running through walls, exposed wires to the ceiling)? Yes \_\_\_ No \_\_\_
11. Will the building's electrical system permit the grounding of electrical Yes \_\_\_ No \_\_\_

equipment?

- 12. Are aisles, doorways, and corners free of obstructions to permit visibility and movement? Yes \_\_\_ No \_\_\_
- 13. Are file cabinets and storage closets arranged so drawers and doors do not open into walkways? Yes \_\_\_ No \_\_\_
- 14. Do chairs have any loose casters (wheels) and are the rungs and legs of the chairs sturdy? Yes \_\_\_ No \_\_\_
- 15. Are the phone lines, electrical cords, and extension wires secured under a desk or alongside a baseboard? Yes \_\_\_ No \_\_\_
- 16. Is the office space neat, clean, and free of excessive amounts of combustibles? Yes \_\_\_ No \_\_\_
- 17. Are floor surfaces clean, dry, level, and free of worn or frayed seams? Yes \_\_\_ No \_\_\_
- 18. Are carpets well secured to the floor and free of frayed or worn seams? Yes \_\_\_ No \_\_\_
- 19. Is there enough light for reading? Yes \_\_\_ No \_\_\_

**B. COMPUTER WORKSTATION (IF APPLICABLE)**

- 1. Is your chair adjustable? Yes \_\_\_ No \_\_\_
- 2. Do you know how to adjust your chair? Yes \_\_\_ No \_\_\_
- 3. Is your back adequately supported by a backrest? Yes \_\_\_ No \_\_\_
- 4. Are your feet on the floor or fully supported by a footrest? Yes \_\_\_ No \_\_\_
- 5. Are you satisfied with the placement of your VDT and keyboard? Yes \_\_\_ No \_\_\_
- 6. Is it easy to read the text on your screen? Yes \_\_\_ No \_\_\_
- 7. Do you need a document holder? Yes \_\_\_ No \_\_\_
- 8. Do you have enough leg room at your desk? Yes \_\_\_ No \_\_\_
- 9. Is the VDT screen free from noticeable glare? Yes \_\_\_ No \_\_\_
- 10. Is the top of the VDT screen at eye level? Yes \_\_\_ No \_\_\_
- 11. Is there space to rest the arms while not keying? Yes \_\_\_ No \_\_\_
- 12. When keying, are your forearms close to parallel with the floor? Yes \_\_\_ No \_\_\_
- 13. Are your wrists fairly straight when keying? Yes \_\_\_ No \_\_\_
- 14. Are files containing sensitive information or data able to be secured when not in use or in your possession? Yes \_\_\_ No \_\_\_
- 15. Will equipment, software, and magnetic media be protected from magnets, liquids and other obvious hazards? Yes \_\_\_ NO \_\_\_

Note: Not all the questions need to be answered yes; however, a preponderance of the answers should be affirmative before an employee can work at home. For those questions that have a negative response, the manager will need to determine if a "no" for a particular question is critical to the employee's performance of his/her job.

**Employee  
Signature:**  
**Manager  
Signature:**

**Date:**

**Date:**

**Approved:  
Disapproved:**

The following forms are included for your information and use. The first SF-1034, Public Voucher for Purchases and Services is a sample of what should be contained in your submission for reimbursement for high-speed telecommunication services. The subsequent SF-1034 is blank and may be used for submitting your claim for reimbursement. The SF-5081, Information Systems User Registration/Change Request should be completed as specified in "Getting Connected At High Speed", page XX in this document.



SF1034.doc



SF1034.doc



tigta5081.doc