

**A MANAGER'S GUIDE
TO
VIRTUAL RESOURCE SOLUTION**

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.

The increase in the use of advanced technology in today's workplace coincides with the rise of the two wage-earner family and the concomitant need for more flexible work styles and work hours.

This document focuses on practices and procedures that managers need to be aware of as they manage in a virtual environment. The guide is designed to provide tips on assessing an employee's potential for survival in the virtual office, dealing with simple questions concerning attendance reporting and more complex situations concerning employee performance. The guide is not designed as a substitute for the interaction necessary between the manager, the Employee Relations Specialist and the Office of Chief Counsel in dealing with problem employees, whether or not they are participating in VRS.

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

MANAGER'S GUIDE TO VRS

TABLE OF CONTENTS

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

Section I

Guidance

Manager's Guide for Employee Participation	page 1
Assessing Your Management Style	page 3
Managerial Style and Expectations	page 4
Selection Criteria	page 8
Employee VRS Assessment Instructions	page 9
Employee VRS Assessment Questionnaire	page 10
From Office Worker to Teleworker	page 14
The Appeals Process	page 15
Training for VRS	page 16
Getting Connected at High Speed	page 17
Reimbursement for Telecommunication Expenses	page 26
Purchasing Approved Incidentals	page 28
Moving the Work Product Along	page 30
Leave and Attendance	page 31
Performance Management	page 33
Giving Effective Feedback	page 34
Coaching and Counseling	page 35
Performance Based Action: The Last Alternative	page 37
Dealing With A Conduct Problem	page 39
Manager's Checklist	page 42
Myths and Misperceptions	page 45

Section II

Policy

VRS Program Policy	page 47
IT Use Policy	page 54
Computer Password Policy	page 63

Section III

Forms

Application for Participation

page 68

VRS Work Agreement

page 69

Safety/Security Checklist

page 74

Attachments

page 76

Sample Public Voucher for Purchases & Services

Blank Public Voucher for Purchases & Services

Information Systems User Registration

MANAGER'S GUIDE FOR EMPLOYEE PARTICIPATION IN 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. That sounds simple enough; however, there is much more to successfully implementing a Telework program. 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 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 attached document should be used by managers as a guide to help them assess their management style before they determine if an employee would be suited for participation in VRS.

ASSESSING YOUR MANAGEMENT STYLE

This self-assessment can assist you, the manager, in identifying your potential levels of success in managing in a virtual environment. This assessment is not a test. There is no pass or fail. It is, however, designed to provide insight into the characteristics a manager should possess to be successful at managing employees in this new environment.

Rank yourself on each of the following elements by putting an "X" on the appropriate line. A rating of 5 is considered excellent or high, while a rating of 1 is considered poor or low. Remember this is not a test so be honest with yourself.

<u>MANAGEMENT CHARACTERISTICS</u>	5	4	3	2	1
◆ Manages by objectives and results	—	—	—	—	—
◆ Comfortable with remote supervision	—	—	—	—	—
◆ Ability to be flexible with work schedules	—	—	—	—	—
◆ Communicates regularly with subordinates	—	—	—	—	—
◆ Coaches/counsels employees regularly	—	—	—	—	—
◆ Trust level with subordinates	—	—	—	—	—
◆ Promotes employee empowerment	—	—	—	—	—
◆ Receptive to new ideas	—	—	—	—	—

Now that you have identified those characteristics that you need to improve upon to successfully manage in a virtual environment, determine what you need to do to improve your "rating". Develop a plan to change low indicators to high. In some cases, you need only to experience managing remotely to have a more positive approach. In that case, the best advice is to "just do it".

MANAGERIAL STYLE AND EXPECTATIONS

The style a manager uses in accomplishing day-to-day tasks, and in providing the needed guidance to his/her employees will determine how successful the manager will be at managing employees in a telecommuting environment. The following are some typical issues for managers of telecommuters, and suggested approaches for dealing with them.

The Need for a Flexible Approach

Despite thorough preparation and planning, most telecommuters and their managers will need to do some fine-tuning to the work arrangements once the employee begins telecommuting. For example, after being in the program for awhile, some telecommuters may find they would prefer more or less time at the alternate worksite. Managers may determine that a different work schedule would be more suitable for the organization. Managers should maintain flexibility on program parameters, especially at the beginning when both the manager and the employee are likely to encounter adjustment issues.

Clear Assignments and Expectations

Ensuring that work assignments and performance expectations are clear and mutually understood by the manager and the employee is important regardless of the work arrangement. With telecommuting, however, the importance of clear communications and a mutual understanding of expectations is heightened. Because you are managing by results, it is paramount to the success of the telecommuting arrangement that the employee is made aware of what is expected of him/her in terms of work assignments and performance. Don't assume that the employee knows without your discussing it with him/her.

The manager should discuss the manner and frequency of communication and/or reporting needed between manager and telecommuter. For example, the manager and the employee should discuss how often and when the employee is expected to check e-mails and voice mails.

Here are a few key points to remember when talking with your employees:

- ◆ Describe the work assignments and objectives in clear and concise terms;
- ◆ Ensure that assignments are clearly understood by asking him/her probing questions;
- ◆ Clearly state the date the assignment is to due. If there are various parts to an assignment, state when each is due.
- ◆ Encourage the employee to ask questions, and then answer them honestly.

Using Progress Reporting

With many jobs, work output is not necessarily a concrete product. The work may be part of a long-term project, involving developing relationships, reading, reviewing, studying, conceptualizing, etc. None of these results are tangible. Even with tangible results, the manager may not have a basis, or simply not know, how to determine quality or appropriate time requirements for the completion of a given assignment. For these situations, a progress report can be used as the measurable output. Such reports inform the manager and serve as a useful mechanism during the initial adjustment period. Finally, adequate progress reporting can ascertain what is involved in various assignments and how long they take for completion.

Another way to manage the work of your off-site employee is to develop a formal plan for long term assignments that involve many facets. A well executed plan sets the stage for performance expectations and enables the manager and the employee to jointly prepare and commit to delivering a specific work product in a specific period of time.

Staying Connected

Managers should make the extra effort to help telecommuters stay connected to the organization. When possible, managers should:

- ◆ Ensure that telecommuters receive all office communications in a timely fashion;
- ◆ Schedule meetings on days the telecommuter is in the office or set up meetings to include the telecommuter via audio or video conference or other electronic means;
- ◆ Ensure the telecommuter remains aware of and involved in official events, decision making discussions and group planning sessions;
- ◆ Have an office discussion including the telecommuters and co-workers on ways to maintain communications and preserve teamwork.

Fairness/Morale Problems

An unfortunate issue that has clouded the advent of telecommuting is fairness in assignments and promotions. Favoritism and unfairness in assignments and promotions can occur in any organization; with telecommuting, however, this issue sometimes gets more attention. Simply stated, in many cases, telecommuters will miss choice assignments or opportunities for promotions because they are not around to gain as much favor or have as much face to face contact. In some cases, this unfairness is not intentional; it is the managers overlooking the telecommuter (out of sight, out of mind). To avoid this problem or assuage concern over it, managers should sensitize themselves to this issue

and, most importantly, have a frank and open discussion with telecommuters reassuring them that the managers will not engage in such behavior.

Managers have expressed concern about possible morale problems and/or grievances from employees who are not allowed to participate in telecommuting. Some managers may be inclined to rule out participation for everyone because of such concerns or preconceived notions. One approach for reducing the possibility of morale problems and/or grievances is to establish a clear set of criteria for employee selection into the program (see Selection Criteria section) and then publicize these criteria. This not only gives employees a clear awareness of the selection criteria but also provides an incentive to improve performance among non-participants.

The manager and the employee should have a positive working relationship before beginning telecommuting. If you, as the manager, identify areas of non-performance, lack of trust, or dependency on direct supervision, wait until these problems are resolved before allowing the employee to telecommute. Managers should provide the true reasons for denying an employee's request for telecommuting. In addition, the necessary steps to improve the employee's performance should be identified along with the time frame for re-evaluation of the request. When the criteria are met, the employee should be allowed to begin telecommuting. This positive approach gives the employee the responsibility for showing his/her suitability for telecommuting, rather than the manager having to assume the responsibility of proving that the employee is not suitable.

A common "what if" expressed by managers is when two employees apply for telecommuting and both have acceptable performance appraisals, but the manager is uncomfortable with a subjective quality of one of the employees e.g. the employee does his/her job well but needs a great deal of supervision. In this instance, it is suggested that the manager allow the independent employee to participate and use this as an opportunity to work with the other employee to change. By using telecommuting as a motivational factor the manager has a chance to change the non-independent employee's work habits for the better. By following up later with a reconsideration of the initial request, the problem may be remedied in a period of time. Another approach is for the manager to allow the employee to telecommute on a provisional basis and state in writing that after a mutually agreed upon time frame if the performance aspect has not improved the employee will be removed from the program.

Feedback for Telecommuters

Employees want to know if they are doing a good job, and they also want to know if they are not meeting the manager's expectations. Feedback is important for all employees, but it is especially important for telecommuting employees. Many telecommuters are concerned that they will not receive any feedback, and one day their manager will inform them that they need to return to the office.

Here are a few points to keep in mind when giving feedback to the telecommuter.

- ◆ Make feedback a regular scheduled component of your relationship with the telecommuting employee.
- ◆ If there is a reason for unscheduled feedback try to provide that feedback immediately after the need is recognized.
- ◆ Give the feedback in private and make sure you have time to discuss it with the employee.
- ◆ Balance positive and negative feedback.
- ◆ Discuss the work, not the worker. Also, ensure that you have first hand knowledge of, or written information about, any action you mention.
- ◆ Be honest and direct about your expectations; don't make an employee guess what is expected. For example, if you schedule a meeting on a telecommuting day, let the telecommuter know if you expect him or her to attend and if so if he or she should attend in person or via telephone. Do not make the telecommuter guess or assume what you want.
- ◆ Respect the telecommuting arrangement; it is a contract between you and the employee. Give oral and written signals to all staff members that you support telecommuting and take it seriously. Make sure that all employees know you expect them to do the same. Avoid characterizing telecommuting as "goofing off" or "getting away with not working". Telecommuters may already be anxious about how their telecommuting is viewed and this will only make things worse.

SELECTION CRITERIA

Using standardized selection criteria allows managers to objectively look at individuals rather than general categories. The primary goal is to ensure that a new participant in TIGTA's VRS program has a good chance for success.

Employee characteristics probably will not vary dramatically from the office setting to the remote location. For example, if an employee is an organized, efficient worker in the office he or she will most likely be organized and efficient at a remote work location. Likewise, if employees have poor work habits in the office, he or she probably will have the same difficulties at the remote location. The personality traits below are good indicators of an individual's success at working at an alternate work place.

- Self-motivated and responsible
- Results oriented
- Independent worker
- Understands job requirements
- Understands TIGTA policies and procedures
- Successful in current position
- Communicates well with supervisor, co-workers and clients
- Accepts change easily
- Interested in Telecommuting

When reviewing the individual's application for participation in VRS consider the following characteristics:

- Ability to set clear work objectives
- Ability to clearly define tasks for the days Teleworking
- Ability to schedule face-to-face interaction on specified days of the week
- Ability to meet internal and external needs while Teleworking
- Ability to limit use of on-site stationary resources (both people and paper)
- Ability to control work schedule
- Ability to benefit from quiet or uninterrupted time.

EMPLOYEE ASSESSMENT QUESTIONNAIRE

The following questionnaire is to be used as a guide for evaluating an employee's potential for successful participation in VRS. The sole purpose of this document is to assess an individual's work characteristics, work habits and competencies to ascertain whether he/she would successfully work in a remote or alternative location. It should not be used for purposes of a progress review or performance rating.

The manager should answer the following questions for each employee who indicates a desire to participate in VRS, regardless of the level of participation desired. The manager should discuss the completed questionnaire with the employee. The manager may wish to give the employee a copy of the questionnaire to complete in advance of this discussion. Once the discussion has taken place and agreement has been reached by both the employee and the manager on the responses to the questionnaire, a copy of the completed questionnaire should be provided to the employee. In addition, a copy of the completed questionnaire should be placed in the employee's Drop File. This exercise should be performed on an annual basis or sooner if circumstances change.

Remember this assessment provides an indication of the likelihood of an employee's success for participation in VRS, and not an indication of the employee's performance. TIGTA executives have already determined maximum levels of participation in job categories; however, managers should evaluate specific employee's job functions and may limit the level of participation accordingly.

EMPLOYEE ASSESSMENT QUESTIONNAIRE

Employee Name: _____

Employee Position: _____

1. Provide a brief summary of employee's duties and responsibilities.

2. Evaluate the following work characteristics according to the employee's existing job function (place a check under the appropriate column)

LOW

MEDIUM

HIGH

- ◆ Clarity of goals and objectives for the position.
- ◆ Ability to schedule face-to-face contact (meetings, etc.) on certain days of the week.
- ◆ Degree to which communications can be accomplished using voice mail, e-mail, faxing, electronic file transfer.
- ◆ Ability to control work flow or schedule.
- ◆ Reliability of technology to support employee when tele-working.

NOTE: If your responses were primarily in the medium to high columns, this employee is likely to be a successful teleworker.

3. Evaluate the following work characteristics according to the employee's existing job function (place a check under the appropriate column).

LOW

MEDIUM

HIGH

- ◆ Amount of in office face-to-face contact required.
- ◆ Amount of in-office reference materials of other resources required.
- ◆ Impact on work team when employee is teleworking.

NOTE: If your responses were primarily in the low to medium columns, this employee is likely to be a successful teleworker.

4. Evaluate the employee's work style and level of performance characteristics (place a check under the appropriate column).

LOW

MEDIUM

HIGH

- ◆ Level of job knowledge.
- ◆ Experience on current assignment.
- ◆ Level of organizing and planning skills.
- ◆ Need for supervisor and/or frequent feedback.
- ◆ Self-discipline regarding work.
- ◆ Reliability concerning work hours.

LOW

MEDIUM

HIGH

- ◆ Level of productivity.
- ◆ Quality of work product.
- ◆ Computer literacy.
- ◆ Flexibility.

NOTE: Your response ratings to the questions above depend on the critical nature of the work style and performance characteristics of the employee's existing job. If your responses were primarily in the medium to high columns, this employee is likely to be a successful teleworker.

5. Evaluate the employee's work style and level of performance characteristics (place a check under the appropriate column).

LOW

MEDIUM

HIGH

- ◆ Resistance to change.
- ◆ Need for interpersonal office contact
- ◆ Importance of co-worker input to successful job performance.

NOTE: If your responses were primarily in the low to medium columns, this employee is likely to be a successful teleworker.

6. Does this employee work with information, data or materials requiring secure or special handling?

YES _____

NO _____

7. Rate your willingness to let this employee participate in VRS.

_____ Not willing

_____ Have reservations (but willing)

_____ Completely willing

8. If you indicated the first or second option above, please state your reasons below.

Supervisor's Signature

Date

Employee's Acknowledgement

Date

FROM OFFICE WORKER TO TELEWORKER

Once the employee determines he/she would like to telecommute, there are several steps that he/she needs to follow. The most important step is to open a dialogue between the manager and the employee to iron out all the issues surrounding teleworking.

After gaining his/her manager's approval to begin telecommuting there are several steps that employees need to complete before beginning to telework..

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

THE APPEALS PROCESS

Your employee has submitted an application for participation in VRS and you have determined he/she is not suited for working from a remote environment. You have completed the assessment sheet and discussed your misgivings with the employee, 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 the employee to try to reach agreement on the matter.
- ◆ If agreement cannot be reached, advise the employee that he/she has the right to appeal your decision to his/her next level manager, and how to go about it:
- ◆ Advise the employee the appeal must be in writing (e-mail is acceptable) and must be received by the manager within five (5) workdays.
- ◆ If the employee indicates that he/she appeals your decision, schedule a meeting to be attended by you, your manager and the employee.
- ◆ Allow sufficient time for your manager to listen to both points of view.
- ◆ Discuss with your manager the background and history of why this meeting is necessary.
- ◆ Bring any documentation you have to support your position with you to the meeting and advise the employee to do the same.
- ◆ Present your "case" to your manager.
- ◆ Allow the employee sufficient time to present his/her "case".
- ◆ Answer any questions posed by your manager and/or the employee.
- ◆ Allow your manager reasonable 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 will take place beginning August 20 and running through September 28, 2001.
- ◆ Training will consist of approximately a 1-hour lesson per day over one workweek.
- ◆ Certificates of completion are required to be completed by each participant and are to 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 you 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. 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 phone 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

- An 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 over Ethernet (PPPoE) Protocol

- 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 billing; you need to place a check mark next to the expense line item(s) on your bill that directly relates 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 located under the Forms section of this guidance.

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 15th 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 prior six months billing are to be included on the same SF 1034 as the DSL / Modem reimbursement requests and should cover the same period.

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 the 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; (e.g. 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.).
- ◆ The cardholder should provide the clerk with the name of the person that will be picking up the cabinet when placing the order.
- ◆ 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. Therefore, if using Corporate Express, the employee will need to make the necessary arrangements for picking up the cabinet.

- ◆ Should the employee leave TIGTA or stops 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

MOVING THE WORK PRODUCT ALONG

Whether working in the traditional office environment or working at an alternative worksite there is a formal process for the submission of all work products. With VRS, the process used for submitting finished products for review and approval will be contingent upon specific functional direction. There are some general guidelines however, that should be noted when working in a virtual office environment.

- ◆ Ensure the assignment is clearly given and expectations are understood.
- ◆ Establish due dates and clearly communicate them.
- ◆ Require a first draft to ensure the work is reflective of the desired end product.
- ◆ Pay special attention to the review process, since feedback will be provided remotely.
- ◆ Communicate in writing any desired changes to the work product.
- ◆ Maximize technology to the extent possible.

LEAVE AND ATTENDANCE

Ensuring the teleworker understands the procedures for requesting leave and reporting their time and attendance is an important aspect of the program. 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 time period 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 - An alternative work schedule available to TIGTA employees either 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 the work schedule 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.
- ◆ 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.

PERFORMANCE MANAGEMENT FROM A DISTANCE

Performance management in the Federal Government is difficult from any aspect, yet managing from a distance is even more challenging. The organizational dynamics at work are very different than those dynamics played out from a remote location. The manager's role in VRS must evolve into the role of "coach or facilitator" rather than "enforcer". This means that rather than overseeing behavior the manager of a teleworker must oversee outputs.

Over the next several pages you will find tips to help you, the manager, be effective in your changing role. The success of the VRS Project is dependent upon managers being able to transition to managing in a new environment.

Here are some basic points to keep in mind when you realize you have a performance problem with an employee.

- ◆ Provide a clear and specific performance plan.
- ◆ Provide notice that the employee is performing at an unacceptable level in one or more elements.
- ◆ Provide counseling and assistance in an effort to improve performance.
- ◆ Provide a notice of proposed adverse action.
- ◆ Make a final decision.

GIVING EFFECTIVE FEEDBACK

Feedback is an important aspect of a manager's arsenal. How a manager provides feedback is often the difference between success and failure.

There are four types of feedback:

1. Silence or no response provided.
2. Criticism or the identification of behaviors or results that are undesirable or substandard.
3. Advice or identification of best practices and how to incorporate these practices in future products.
4. Reinforcement or identification of behaviors or results that are desired or exceed standards.

Certainly, the first two forms of feedback are the least desirable, but how do you give effective feedback? Listed below are some pointers.

- ◆ Make your feedback specific and performance related.
- ◆ Consider the timing, either before the event in the form of advice or immediately after the event as positive reinforcement.
- ◆ Consider the needs of the person receiving the feedback as well as your own needs. Are you "dumping" or genuinely trying to improve performance?
- ◆ Focus on behavior the receiver can do something about.
- ◆ Solicit feedback rather than impose it.
- ◆ Avoid labels and judgements by describing rather than evaluating behavior.
- ◆ Define the impact on you, the team, the unit, the organization.
- ◆ Use "I" statements rather than "You" statements to reduce defensiveness.
- ◆ Check to be sure clear communication has occurred.
- ◆ Give feedback in a calm, unemotional language. Pay specific attention to tone and body language.

Finally, there are six additional points to remember.

1. Reinforcement is the most effective form of feedback.
2. Criticism is the most ineffective form of feedback.
3. The difference between criticism and advice is a difference in timing. Most criticism can be given as advice.
4. Mixed feedback dilutes the impact. Most times it serves to confuse the employee.
5. Criticism will overpower all other types of feedback.
6. Silence is not always golden. Many times it can be left to a myriad of interpretations.

COACHING AND COUNSELING

Now that we have learned about the different types of feedback and the art of giving feedback, coaching and counseling share many of the same skills. Coaching and counseling come down to the supervisor telling the employee what he/she wants done and how it should be done. The best way to differentiate between the two is to define each.

Coaching - A directive process by a manager to train and orient an employee to the realities of the workplace and to help the employee remove barriers toward optimum work performance.

Counseling - A supportive process by the manager to help an employee define and work through problems affecting job performance.

Therefore, dealing with an employee who lacks a specific job knowledge would require strong coaching skills; while dealing with a problem employee will require good counseling skills. Knowing the difference between each and knowing when to use one over the other will help the manager in managing an employee's work product from a distance.

Coaching an employee through the learning of a new task or skill is an important aspect of management. Since your employee is no longer sitting outside your doorstep, it is incumbent upon the manager to ensure the employee has the necessary skills to perform his/her job.

Listed below are some characteristics to effective coaching:

- ◆ Capitalize on the employee's strengths.
- ◆ Make performance expectations and priorities clear.
- ◆ Set standards of excellence while providing the employee the freedom to do the job.
- ◆ Hold employee accountable for his/her action/product.

After you have provided the coaching and you believe the employee has all the skills necessary to be a successful performer yet you still do not see the desired level of proficiency you may want to resort to counseling. This next step is very critical in laying the groundwork for identifying precisely where the employee is falling short in your expectations.

The following eleven steps to counseling an employee on his/her performance is neutral, direct and most importantly effective in dealing with early performance problems. Following these steps does not require any great skill in dealing with people; it is a simple technique that can be learned and applied by anyone.

1. Define your goal.
2. Relate your goal to the mission of the organization.
3. Plan in advance the topic, time and location of the discussion. Make sure the telecommuter is to be in the office the day of the meeting.
4. Be assertive rather than accusatory.
5. Acknowledge your own subjectivity.
6. Describe the performance problem succinctly.
7. Ask the employee for suggestions for improvement.
8. Outline specific corrective action to be taken, with specific time frames.
9. Ask the employee to summarize the discussion.
10. Schedule a follow-up meeting to discuss improvement (or lack of).
11. Listen more than talk.

PERFORMANCE BASED ACTION: THE LAST ALTERNATIVE

You have given clear direction; you have provided feedback; you have coached and counseled, but the employee's performance remains below acceptable standards. The next step is to initiate an appropriate performance based action.

When faced with this alternative make sure you work closely with your Employee Relations Specialist. The following provides a high level definition of the options available for a manager to consider when initiating a performance based action.

- ◆ Opportunity to Improve - otherwise known as the Performance Improvement Period is the formal period of time the manager provides the employee to improve his/her performance. There are several factors associated with this phase:
 - Document every assignment given to the employee, and the employee's performance related to the critical element at issue.
 - Provide any advice, assistance, guidance and counseling as specified in the Opportunity Letter; document your efforts.
 - Keep all drafts through the final version of the work product.
 - Evaluate the evidence of the performance during the opportunity period.
- ◆ Postponement or denial of Within-Grade-Increase (WIGI) - This is usually done at the same time the employee is given an opportunity to improve his/her performance. Contrary to many employees' perception WIGI's are not based on longevity alone.
 - Employee must be notified in writing, at least 30 days before the WIGI is due.
 - Memorandum must contain specific reason(s) why the WIGI is postponed or denied.
 - Once performing satisfactorily the manager should notify the employee in writing and initiate the process for granting a WIGI.
- ◆ Downgrade and reassignment to different position - This allows the manager to retain an employee who can still be an asset to the organization, just not in his/her current position. Usually a reassignment to a different position is at a lower grade level than the employee is currently at.
 - This option is most commonly offered when an employee is promoted into a new position and his/her performance in the former position was satisfactory.
 - There is no requirement that a manager offer this option to an employee before considering termination.
- ◆ Termination for poor performance - This is usually the last resort to be

considered when dealing with a poor performer. You, the manager, have made a decision the organization would be better off without this employee's services.

- Consider alternatives to termination:
- ❖ Offer the employee the option to resign rather than be removed for unacceptable performance.
- ❖ Allow the employee a period of time to look for another job before the effective date of resignation.
- ❖ Offer outplacement counseling, if available, through the Human Resources office.
- ❖ Write a factual, yet positive, reference letter for the employee to use when looking for alternative employment.
- ❖ These are options that are decided by the circumstances and by no means mandatory for the manager. However, a smart manager will use every option available in his/her arsenal to benefit themselves and the agency, as well as the under-performing employee.

DEALING WITH A CONDUCT PROBLEM

Generally, there are three reasons why employees do not get their job done. Regardless of the reasons given when confronted by the manager the answer is usually based on the items below:

- ◆ The employee does not know how to do the job.
- ◆ There is something or someone that keeps the employee from getting the job done.
- ◆ The employee simply does not want to do it.

Conduct problems are a result of a "WON'T DO" rather than a "CAN'T DO". It is not a skills deficiency, but rather the employee knows how to perform the assigned task but for some reason refuses to do it. Therefore, conduct or behavior problems involve the breaking of a rule, regulation or other requirement.

In the traditional office environment, employees can come to their manager with a specific problem or the manager sees firsthand the problem occurring. In a remote relationship, the manager must learn to recognize signs of conduct or attitude problems. The following information will help the manager deal with the employee who has a conduct problem.

The following are signs of declining performance:

- ◆ Decreased productivity
- ◆ Poor work quality
- ◆ Missed due dates
- ◆ Disorganization

The following are signs of attitudinal problems:

- ◆ Little or no initiative
- ◆ Disinterest
- ◆ Increased complaining
- ◆ Increased irritability or depression

Be aware of the above signs. Knowing how to deal with each as appropriate can make your job as a manager easier.

The first two steps to take in dealing with a conduct problem are similar to those for a performance problem.

1. Identify that there is a problem
2. Meet with the employee.

The purpose of the meeting with the employee is again similar to that under Performance Problems. When meeting with the employee:

- ◆ Explain what the problem is.
- ◆ Explain why it is a problem.
- ◆ Explain what you expect the employee to do to correct the problem.
- ◆ Document your discussion.

When the employee still will not abide by the requirements of TIGTA, fairness to other employees in the work unit dictates that a manager have the ability to take effective disciplinary action. Remember the purpose of discipline is to help supervisors maintain an efficient and productive work environment. It should be used to correct unacceptable conduct not punish an employee. Therefore, the third step is:

3. Recommending an adverse/disciplinary action.

Before you take this step, you need to ask yourself two questions.

- Was the rule communicated to the employee, or if not, is the offense so obvious that they could be expected to know without being told?
- Has the rule been consistently enforced in the past, and if not, were employees told that it was now going to be enforced before this incident occurred?

If you can answer "Yes" to either of these questions then you are ready to recommend an action. So here we go:

- ◆ Consider all the facts.
- ◆ Consider the employee's side of the story.
- ◆ Apply the basic concepts used in the process (5 CFR 752; Douglas Factors; TIGTA Guideline of Offenses and Penalties)
- ◆ Have a meaningful discussion with the Employee Relations (E/R) Specialist.
- ◆ Recommend the proposed action to be taken.

If the employee continues to engage in the unacceptable behavior or conduct then the action taken to correct the problem will become more severe after each instance. Maintain a discussion with your E/R Specialist so that you have the advice you need.

Remember when dealing with conduct problems the characteristics of a successful disciplinary process should be:

- ◆ Prompt
- ◆ Impartial
- ◆ Consistent
- ◆ Non-punitive
- ◆ Fair
- ◆ Advance warning
- ◆ Follow through

Name of Employee _____

Name of Supervisor _____

MANAGER'S CHECKLIST

Before the employee begins telecommuting, there are many actions that need to be completed. This checklist is designed to ensure that all actions are taken and that you and your employee are properly oriented to the policies and procedures of the VRS program.

<u>Date</u>	<u>Action Taken</u>
_____	1. A. Manager has read TIGTA's VRS Policy.
_____	B. Employee has read the VRS Policy
_____	2. Employee's request received on _____ evaluated.
_____	* Employee Assessment Questionnaire (EAQ) completed.
_____	* Discussed request with the employee, including EAQ and Participant Self-Assessment.
_____	* Copy of EAQ provided to the employee.
_____	* Copy of EAQ filed in the employee's "drop file."
_____	3. Employee Self-Certification Safety/Security Checklist received on _____ discussed with the employee.
_____	4. Decision on Request.
_____	A. Approved.
_____	* Telework Agreement (TA) discussed with the employee and signed. (Remember to file original in the employee's EPF/"drop file" and provide a copy to the employee).
_____	* Performance expectations discussed.
_____	* Work Schedules discussed.
_____	* Requirements for checking for e-mail and voice mail messages and communicating with the office discussed.

_____ * Policies and procedures for care and use of equipment issued by TIGTA discussed.

_____ * Policies and procedures covering classified, secured, or privacy act data discussed.

_____ * Policies and procedures covering reimbursement for telecommunication expenses discussed.

_____ * Policies and procedures for purchasing approved incidentals discussed.

B. Disapproval

_____ * Discussion with the employee on why the request was denied and what he/she needs to do to get approval.

_____ * Notice of appeal rights and how the process works provided to the employee.

_____ * Written appeal filed.

_____ * Scheduled meeting with the second level manager.

_____ * Notice of meeting provided the employee.

_____ * Meeting held.

_____ * Second level manager issues decision. (If manager's decision is overturned, make sure all actions listed under "Approved" are taken before the employee begins telecommuting.)

_____ C. Copy of TA filed in the employee's (EPF/"drop file").

5. Training Completed.

_____ * Supervisor

_____ * Employee

6. Equipment issued by the TIGTA is documented.

Check as applicable, yes or no.

	<u>Yes</u>	<u>No</u>
- computer	_____	_____
- file cabinet	_____	_____
- other (specify)	_____	_____

Manager's signature

Date:

Employee's signature

Date:

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 meeting 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 that 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", who 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, an alternate site, time in the office or leave should be scheduled.

FAIR LABOR STANDARDS ACT (FLSA)

The existing rules in 5 USC 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., 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 the Privacy Act 5 USC Sections 552 and 552a and 26 USC 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.

June 26, 2001

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/mag3/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.
Appendix A

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 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

TIGTA-IT INFORMATION SECURITY PASSWORD POLICY

Treasury Directive 71-10 (TDP 71-10) requires Treasury Bureau systems utilize some form of user authentication (ie. 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, assist 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

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 password 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 which changes 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 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's 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 system is idle greater that ten (10) minutes, an automatic blanking of the screen with password screen saver evoked and suspension of the session shall occur. Re-establishment of the session must 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, in computers without access control, or in 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 (incorporated) into any software developed in house or outsource.

To hardcode (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 give themselves 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 shared password become necessary, wavier request accompanied a business need justification must be submitted to the TIGTA PRINCIPAL ACCREDITING AUTHORITY for approval to waiver 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 (routers, firewalls, access control servers, etc.) must have unique passwords or other access control mechanisms. A compromise in the security of one device will therefore 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," and 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 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 the users to change their password, otherwise the system administrator must provide a temporary password and the user must change provided password immediately. Example of 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 else besides the authorized user.

To do so exposes the authorized user to responsibility for actions that the other party takes with the password. If users need to share computer resident data, they should use electronic mail, public directories on local area network servers, and other 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 can 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 Trail 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 their 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 meet 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 work site.

P. Alternative Workplace Cost

The employee understands that TIGTA will not be responsible for any operating costs that are associated with the used 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, and 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 work site.

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 equipment? Yes ___ No ___
- 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 questions 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 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 17, in this document.



SF1034.doc



SF1034.doc



tigta5081.doc

