NUMBER 920.01

DIRECTIVE

DATE 1/30/2006

FINANCIAL CRIMES ENFORCEMENT NETWORK

Check one: ☐ Issuance ☐ Bulletin ☐ Manual ☐ Supplement ☐ Amendment ☒ Revision

SUBJECT: **TELEWORK PROGRAM**

1. PURPOSE:

This directive establishes the Financial Crimes Enforcement Network Telework policy for alternative workplace arrangements. This program provides an opportunity for an employee to work at an alternate worksite without changing an employee's official duty station or other conditions of employment.

It is our policy is to provide employees the opportunity to participate in the Telework Program where practical and consistent in meeting mission objectives. Telework programs are designed to allow employees to perform their duties at a worksite other than the traditional office setting on a full, expanded, limited, or episodic basis, depending on the organizational mission and the roles and responsibilities of a particular office and its employees.

Participation in the Telework Program is voluntary and subject to first-level supervisory approval based on mission requirements and the efficiency of the Federal service. All arrangements must be approved by the employee's immediate supervisor. All employees are eligible for at least episodic teleworking given the appropriate need; however, Bank Secrecy Act data will not be accessed from the home worksite.

2. SCOPE:

Participation is limited to FinCEN employees. This policy does not cover detailees, students, platform, or contractor personnel. The Telework Program currently applies to home and mobile worksites located in the commuting area of the employee's official duty station. General Services Administration telework centers are not initially covered under this policy. In the future, depending on the needs of the bureau and the availability of resources, we may consider other telework locations, such as the telework centers.

3. OFFICE OF PRIMARY INTEREST:

Management Programs Division, Office of Human Resources.

/s/

William J. Fox
Director

TELEWORK PROGRAM

1. PROGRAM DEFINITIONS:

A. Telework is a voluntary, flexible work arrangement that allows an employee to work away from the traditional office or official duty station at an alternate worksite one or more days per pay period. Telework is also referred to as "telecommuting" and "work-at-home". Telework programs may be designed to allow employees to work at an alternate worksite full-time, expanded, limited, or on an episodic basis, depending on the organizational mission and the roles and responsibilities of a particular office and its employees. Telework permits employees to engage in working arrangements at designated locations or other pre-approved alternative worksites known as "flexiplace".

B. Flexiplace refers to an alternative location at which an employee works in lieu of reporting to their official duty station. Examples of flexiplace work environments include home sites, telework centers, and mobile office settings.

C. Telework centers are General Services Administration approved worksites equipped with telecommunications and other office equipment to facilitate communication with the official duty station and other places of business in order to perform daily routine work responsibilities. Those centers are not included as an initial alternate worksite.

D. Mobile office settings include alternate work environments in which employees are engaged in government business away from their office and home worksite environments. Mobile office settings are often established when employees are on a temporary duty or travel status.

E. Episodic participation means approved telework performed on an occasional, one-time, or irregular, medical, or episodical (short duration, project-type work) basis.

F. Limited participation means an employee works 1 day per week at an alternate worksite under a set schedule.

G. Expanded participation means an employee participates in telework for a majority of the workweek, either 2 or 3 days per week under a set schedule.

H. Full participation means an employee works full time (4-5 days per week) at an alternate worksite under a set schedule, only coming into the office at the request of his or her manager and for a specific purpose.

I. Official Duty Station is the official office of assignment. Unless otherwise stated, each employee shall report to and perform his/her duties at this location. All pay, leave, and travel entitlements are based on this location.

J. Sensitive Information: Information for which unauthorized access to, or the loss or misuse of would adversely affect the national interest or the conduct of federal programs,

or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

2. PROGRAM PROCEDURES:

A. Participation. Participation in a telework arrangement is voluntary and is not an employee entitlement. An employee may participate in the program if the respective manager and first-level supervisor:

1. Apply the "Requirements for Participation in Telework Program" contained in the Department of the Treasury Telework and Flexiplace Program, Telework Handbook,
2. Decide that the employee's job duties and responsibilities are appropriate for offsite work, and,
3. Determine that the employee possesses and maintains performance at the Fully Successful level and is suitable for participation in the Telework Program.

B. Training and Guidelines. In addition, all managers, supervisors, and participating employees must attend telework training; follow the applicable guidelines outlined in the Department of the Treasury Telework and Flexiplace Program, Telework Handbook; and comply with this directive and all appendices.

C. Agreement. The telework arrangement under which an employee will perform work must be clearly set forth in a written agreement and signed by the first-level supervisor and employee (Attachment 3). The Telework Agreement may be terminated at will by either the supervisor or the employee, with appropriate notification. Participation in the program will be terminated if an employee's performance does not meet the expected results (e.g., quality, quantity, timeliness) of either party or if the telework arrangement fails to meet organizational needs.

D. Safe Work Environment. Participating employees are required to inspect their alternate worksite using the Home-Office Safety Self Inspection Guidelines and Checklist (Attachment 2). They are responsible for maintaining a safe work environment and by signing the telework agreement (FinForm 040) they certify that they have inspected their alternate worksite and that it is free of significant safety problems.

E. Conditions of Employment. A telework arrangement does not alter the terms and conditions of appointment, including an employee's official duty station, salary, benefits, individual rights, or obligations. All pay, leave, and travel entitlement shall be based on the official duty station. The telework arrangement shall not affect other conditions of employment, e.g., hours of work, time and attendance policies, dismissals, emergency closings, leave or compensation unless otherwise specified in the Telework Agreement Appendix A (FinForm 040).

F. Renewal. Participants continuing in long-term arrangements after a one-year period must complete an annual Telework Renewal Agreement. At this point, the arrangement should be

reassessed to determine the need to revise or update existing participation criteria in Attachment 4 (FinForm 042).

3. PROGRAM RESPONSIBILITIES:

No provisions exist in agreements between employees and supervisors which would preclude management from taking any appropriate disciplinary or adverse action against an employee or supervisor who fails to comply with the provisions of the Telework Program.

A. Senior Management. The Director, Deputy Director, Associate Directors, and Office Chiefs are managers; and as such, may authorize their respective Assistant Directors to oversee this program at their respective level. Management will:

1. Evaluate the impact of the telework program on the efficiency and effectiveness of their work operations.
2. Incorporate teleworking into the Continuity of Operations Plans and Procedures as another alternative for relocating employees to continue providing customer service and carrying out the mission during an emergency situation

B. First Line Managers. All supervisors, managers, and executives who are first-level supervisors are responsible for employees under their charge. In this regard, supervisors will:

1. Review and approve, or disapprove, employee requests to telework, using the criteria contained in the Department of the Treasury Telework and Flexiplace Program, Telework Handbook.

2. Retain the original agreement (Attachment 3) for their files and forward a copy to the Telework Coordinator, Management Programs Division (MPD), Office of Human Resources.

3. Ensure that telecommuting does not burden staff remaining in the office through equitable distribution of workload.

4. Properly certify, approve, and monitor time and attendance for employees working in a telework status including ensuring that employees comply with all overtime and compensatory rules.

5. Reserve the right to require employees to report to the traditional worksite on scheduled telework days, based on operational requirements.

6. Assign appropriate work to be performed at the alternate worksite, and be accountable for the employee's work as in a regular office setting.

7. Maintain performance management records and other appropriate information.

8. Enforce safety and security policies affecting the mission of the Financial Crimes Enforcement Network in telework activities.

9. Attend supervisory telework training before approving telework agreements.

C. Employees. Employees will complete the Telework Agreement (Attachment 3), abide by the parameters of the telework policy as stated in Treasury Directive 74-14, Treasury Telework and Flexiplace Program and the Department of the Treasury Telework and Flexiplace Program, Telework Handbook, and comply with all provisions of this directive and appendices. Additionally, employees agree they will:

1. Dedicate official duty time to government business only, and not conduct personal business while in official duty status at the alternate worksite, for example, caring for dependents or making home repairs.

2. Be available to respond immediately to unexpected tasking or exigent circumstances during scheduled duty hours.

3. Observe existing time and attendance policies in requesting leave, overtime, compensatory time, or working an approved Flexible Work Schedule (FWS), and not work overtime or compensatory hours unless approved in advance in accordance with procedures.

4. Perform a home-office safety self-inspection using the Home-Office Safety Self Inspection Guidelines and Checklist (Attachment 2) prior to participating in teleworking and monitor the alternate worksite accordingly as conditions may change.

5. Maintain a workspace that is free from personal distractions and safety hazards, and immediately report any on-the-job injuries to the first-level supervisor.

6. Protect government property (equipment and software) from possible theft and environmental damage and ensure that work information in both hard copy and electronic format has been adequately secured. In cases of damage to unsecured equipment by non-employees, the employee will be held liable for repair or replacement of the equipment or software in compliance with applicable regulations on negligence.

7. Use Government equipment only for its authorized purposes, complying with Treasury and FinCEN's personal use policy.

8. Observe all rules, policies, and procedures regarding security, including:
    a. Label all media with the highest information identifier (e.g. For Official Use Only) and safeguard it accordingly. No identifier above "For Official Use Only" will be acceptable for teleworking. Be responsible for notifying and coordinating any movement of computer equipment at their telework site with their first level-supervisor and Office of Technology Management.
    b. Be required to transport their laptops and peripheral devices to the principal workplace when in need of repair and upgrade.
    c. If an alternate worksite is approved for and contains sensitive information, such information must be kept secured at all times.

d. Ensure that the alternate worksite has adequate physical and environmental security measures in place to protect the equipment from being accessed by unauthorized individuals.
e. Keep secure any security information such as a secure identification card and password.
f. Immediately report any unauthorized or suspicious activity at the alternate worksite using the same protocols as if they were located at their principal worksite.
g. Information contained on government systems or media will not be transferred or copied to an individually owned personal computer or media.
h. Information contained on a personal computer or media will not be transferred or copied to government systems or media.

9. Report suspected computer operational and security problems (i.e., system intrusion attempts, virus warnings, potential information compromises, etc.) to the Help desk at (703) 905-3767.

10. Take training and be certified by Office of Technology Management to enable employee to troubleshoot common problems and move and reconnect IT equipment as necessary at the alternate worksite.

11. Obtain a long distance phone card from Office of Technology Management to use in making official phone calls, if needed. Teleworking will only be via high speed internet connection (DSL or cable).

12. Attend telework training prior to completing both the remote access agreement and the telework agreement.

D. Office of Chief Information Officer. In addition to standard organizational responsibilities, FinCEN has the right to inspect, during normal work hours with 24 hours of notice to the employee, the alternate worksite and government furnished equipment to monitor safety and security conditions, install, and evaluate the condition and operation of the equipment. The proposed technology support will be provided based on the following framework:

1. Government provided Information Technology (IT): FinCEN will issue equipment to teleworkers. Issuance of government owned IT equipment to the teleworker allows FinCEN to maintain control over what software resides on the equipment, what protections are in place on the equipment, and what kinds of equipment need to be supported by Office of Technology Management.
2. The issuance of equipment will be based on the teleworker's work requirement.
3. For the purposes of IT support, teleworkers fall into one of four categories requiring remote connectivity to the FinCEN Network to access email and/or FinCEN information systems:

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

- Expanded participation - Employee participates in telework for a majority of the workweek, either 2 or 3 days per week under a set schedule.
- Limited participation – The employee works 1 day per week at an alternate worksite under a set schedule.
- Episodic participation – participation in telework is dependent upon the needs of the worker and demands of the work. This is a task based arrangement and the employee works on a particular task at an alternate worksite.

4. The employee must use their own Internet Service Provider (ISP) or Digital Subscriber Line (DSL), or cable modem provider for their connectivity. Workstations and Connectivity requirements based on the category of teleworkers:
   - Full Participation Teleworkers may be issued a laptop computer and two each of the following peripherals as needed: docking station, monitor, keyboard and mouse. They will not be issued a desktop computer for use at the principal workplace.
   - Expanded Participation Teleworkers may be issued one laptop computer and one each of the following peripherals as needed: docking station, monitor, keyboard and mouse. One docking station with peripherals will be available at the principal workplace. They will not be issued a desktop computer for use at the principal workplace.
   - Limited Participation Teleworkers will be issued a laptop computer, without peripherals, only for the duration of the teleworking assignment. They will normally be issued a desktop computer for use at the principal workplace. However, under special circumstances peripherals may be issued, e.g., employee teleworking due to a medical condition.

5. Equipment related services:

   a. Long distance phone cards will be provided to the approved teleworker upon request.

   b. Furnish, maintain, service, and account for all government owned IT equipment, to include loading software to government owned equipment.

   c. Provide anti-virus scanning software as part of the software package. This software will be updated daily when the user logs onto the FinCEN network and automatically checks for infections.

   d. The Help Desk staff will be available to provide assistance, when needed, over the telephone during normal weekday working hours. The Help Desk support hours are from 6:00 AM to 6:00 PM Monday through Friday, Eastern Standard/Daylight Time.

6. Due to the sensitive nature of FinCEN's mission, all information will be handled at a heightened level of security awareness critical to maintaining a safe and secure telework environment. In accordance with TD P 85-01, *Treasury Information Technology Security Program, Volume II, Handbook: Part 1, Sensitive Systems,*

Section 5.4.1, the following criteria must be met to ensure the security of the FinCEN network and the data contained therein:

a. No classified information will be worked at the alternate worksite under any circumstance.

b. First-level supervisors will determine whether or not sensitive information will be worked at the employee's home and will provide specific guidance to the employee once a decision is made to do so. **However, Bank Secrecy Act and Law Enforcement Sensitive information will not be accessed from the home worksite.**

c. In the event the alternate worksite is approved for and contains sensitive information, all such information must be kept secured at all times. Floppy disks or other mobile media (i.e. thumbdrives, CD-Roms, etc.) are not authorized for use at remote locations. All work will be saved on the local hard drive or a network drive when connected to the FinCEN network. **Printing of sensitive information at home is prohibited.**

d. To properly secure FinCEN's data for teleworking purposes:

a. Each laptop will be equipped with personal firewall software, and an encrypted hard drive;
b. FinCEN will employ Intrusion Detection Software;
c. Secure Virtual Private Network (VPN) will secure data communications between the laptop and the FinCEN network;
d. Teleworkers will be provided with a secure identification token and a password;
e. All Teleworkers shall sign a Remote Access Agreement before teleworking is approved.

E. Office of Security. In addition to standard organizational responsibilities, FinCEN has the right to inspect, during normal work hours with 24 hours of notice to the employee, the alternate worksite and government furnished equipment to monitor safety and security conditions.

F. The Management Programs Division is responsible for policy, general oversight, and program evaluation conducted through the Telework Coordinator. Success of the program depends on a close working relationship between the first-level supervisors and participating employees. The Telework Coordinator may request additional data as determined by the Director, Department of the Treasury, or the Office of Personnel Management.

4. REVOCATION OF THE TELEWORK PROGRAM: The Director or Deputy Director may terminate the Telework Program bureau-wide at any time.

Financial Crimes Enforcement Network (FinCEN)
TELEWORK PROGRAM
WORKSTATION DESIGN AND INSPECTION GUIDELINES

The following information can be applied to any alternative work arrangement, either at a telecenter or at a home office. It is provided to assist you in designing, establishing, adjusting, and/or inspecting your workstation at the alternate worksite. An adequate workstation should be safe and comfortable and should facilitate your job performance.

The following guide will familiarize you with many of the desirable aspects as well as hazards in an office work environment. If you suspect that something is hazardous, but are not sure, you can contact the Bureau Safety and Health Officer for assistance. It is recommended that you maintain this Guide as a reference source.

WORKING OR WALKING SURFACES

Surfaces should be level and free of tripping, bumping, or slipping hazards. Things to look for include: torn carpet; electrical or telephone cords in walkways; partition support brackets, waste baskets, portable heaters, fans, etc. placed in walkways; file cabinet drawers and/or bookcase doors that open into an aisle; misaligned furniture; temporary or permanent storage that narrows or obstructs aisles; doors that open into aisles or narrow halls, etc.

ELECTRICAL SAFETY

There are numerous safety considerations involved in the use of electrically powered equipment and appliances. These center around three hazards - shock, burns, and fire.

Grounding: Generally most homes/buildings are provided with three wire grounded electrical outlets. These should be checked for correct wiring and adequacy of grounds by the owner and/or appropriate officials. You should look for cracked or broken outlets, missing covers which expose the wiring or signs of arcing or burns around the outlet.

The subject of grounding for office type equipment is difficult to cover in this amount of space. As a general rule, if an appliance comes from the manufacturer with a three prong plug, the ground pin should not be broken off nor should the device be used ungrounded via a two prong adapter or extension cord. Large appliances such as refrigerators, computers, paper copiers, etc., as well as heating devices such as coffee pots, hot plates, etc., should be grounded.

Electrical Cords: Appliance and equipment cords should be checked for proper connection to the device, frayed or damaged insulation, defective plug, and exposed wires on a regular basis. The use of extension cords in the workplace should be limited and closely controlled. Extension cords are to be used only on a "temporary basis." If the condition where they are used calls for "long term use," then electrical outlets should be moved, added, or whatever proper corrective action may be necessary.

Try rearranging the furniture or adding additional electrical outlets before using extension cords. When they are used, they should be of the same or larger wire size as the cord being extended, and have a compatible connector plug. If an adapter is needed to connect the device to an extension cord, the wrong extension cord is being used.

CAUTION: Extension cords must never be draped over furniture, partitions, equipment, etc., or extended across aisles or walkways, nor extended through doors, walls, ceiling, etc., and never located under carpeting.

Electrical Outlets: A major cause of fire is overloaded electrical circuits.

Fire Extinguishers: Are there enough of the proper type of fire extinguishers and are they properly positioned? Fire extinguishers should be permanently mounted. The location of fire extinguishers must be clearly marked. If the view of an extinguisher is obstructed by partitions, furniture, corners, etc., then a directional arrow fire extinguisher location sign or some kind of marking is needed. The access to a fire extinguisher should never be blocked, even temporarily. The travel distance to reach an extinguisher should not exceed 75 feet.

All fire extinguishers should be checked regularly and inspected at least annually. They must have a tag attached showing the inspection date. Fire extinguishers must be hydrostatically tested every five to twelve years. Look for a metal tag or decal showing the last test date. If the extinguisher has a gauge, check to see that it is "full." Usually, this means that the gauge's arrow/needle is pointing straight up. Examine the fire extinguisher's hose and discharge nozzle for damage. Also check to see that the handle locking pin, or wire is intact. If not, the extinguisher could have been used and now has to be refilled. If the extinguisher has any damage, especially surface damage

such as dents, or has been discharged or tampered with, it must be inspected again by a qualified person.

Sprinkler Systems: Some facilities have automatic sprinkler protection. If your alternate work area has this, check to see that the sprinkler heads have not been painted. Paint can clog the sprinkler head and prevent it from operating properly. Storage under and around sprinkler heads should be limited to no closer than 18 inches in any direction to allow ample clearance for the water spray. Do not permit anything to be attached to or suspended from a sprinkler head. Ideally, the sprinkler system should be tied into the building's fire alarm system so that when a sprinkler head is activated, the proper authorities are notified immediately.

STORAGE

The storing of any item on top of tall furniture or cabinets should be prohibited. To permit this practice sets the stage for many types of injuries. Employees attempting to place things on top of furniture or cabinets can strain themselves, can fall if chairs are used in place of ladders or even if ladders are used incorrectly. The items themselves can fall, striking employees. It is best to limit storage to designated storage rooms/areas.

A good practice is to limit storage height to maintain a minimum of 18 inches clearance from the ceiling in general, and from light fixtures and other electrical equipment in particular. If sprinkler protection is provided in the work or storage room, maintain as much clearance between stored items and the sprinkler head as possible; again, 18 inches is a good minimum clearance. Check to see that heavy items are stored on lower shelves. Have a ladder or approved step stool available so you can safely reach high places within the work or storage area.

HEATERS

Care should be exercised when using portable heaters. Be sure that the heating element is guarded against accidental contact, positioned not too close to furniture or other combustibles, and that a tip-over switch cuts off electrical power to the heating element if the heater is knocked over. This feature could prevent the heater from starting a fire. Kerosene heaters should not be used in the work area.

COFFEE POTS OR SIMILAR ITEMS

Use of coffee pots and similar items in the immediate work area should be placed out of normal walk areas and on a noncombustible surface. Never place such a device in a storeroom, closet, or other location where it cannot be observed. If the device is in a location where it cannot be observed, it could smolder, start a fire and spread beyond control before being detected. Should an electrical short-circuit occur, quick action is necessary to prevent fire hand. CTS can be reduced by stopping or limiting VDT activity, by maintaining proper posture, or as a last resort, surgery.

THE DESK

The height of the work surface should be comfortable for typical uses (computer work, writing, or reading). Conventional desk surfaces are usually about 29 inches high, which is adequate for many tasks. The height recommended for a computing surface is approximately 26 inches.

THE CHAIR

The chair is probably the most important piece of furniture in your work station. The seat should be adjustable, and the height (measured from the floor) of the top surface of the seat should be 15 to 21 inches. The backrest should be adjustable (height and angle) and should provide support for the telecommuter's lower back. Armrests should be substantial enough to provide support, but not so large as to be in the way.

LIGHTING

The lighting in your workstation can affect comfort, visibility, and performance. Whether you're using natural daylight or artificial lighting, it should be directed toward the side or behind your line of vision, not in front or above it. Bright light sources can bounce off working surfaces and diminish your sense of contrast. Northern daylight is the best light for your workstation and for operating a computer.

NOISE

Depending on your personality and work style, noisy or totally noise-free environments can be distracting and stressful. Some background sound such as music can be beneficial in maintaining a level of productivity and reducing boredom.

SELF-CERTIFICATION SAFETY
CHECKLIST FOR HOME-BASED TELEWORKERS

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. Is all electrical equipment free of recognized hazards that would cause physical harm (frayed wires, bare conductors, loose wires, flexible wires running through walls, exposed wires to the ceiling)?	Yes ___ No ___
6. Will the building's electrical system permit the grounding of electrical equipment?	Yes ___ No ___
7. Are aisles, doorways, and corners free of obstructions to permit visibility and movement?	Yes ___ No ___
8. Are file cabinets and storage closets arranged so drawers and doors do not open into walkways?	Yes ___ No ___
9. Do chairs have any loose casters (wheels) and are the rungs and legs of the chairs sturdy?	Yes ___ No ___
10. Are the phone lines, electrical cords, and extension wires secured under a desk or alongside a baseboard?	Yes ___ No ___
11. Is the office space neat, clean, and free of excessive amounts of combustibles?	Yes ___ No ___
12. Are floor surfaces clean, dry, level, and free of worn or frayed seams?	Yes ___ No ___
13. Are carpets well secured to the floor and free of frayed or worn seams?	Yes ___ No ___
14. 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 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 ___

Telework Connectivity **Information** Sheet

To be filled out by User: Contact your ISP and/or Router Vendor if you need help answering the questions below. Return this document to the HelpDesk.

User Name:

High Speed Connection Type ☐ DSL ☐ Cable

Name of Internet Service Provider (Cox, Verizon, etc.)

Router? **Yes** ☐ **No** ☐
(If yes, indicate the I.P. address, make and model)

I.P. Address Make Model

Provide screenshot (Alt Print Screen, Alt Insert to a Word document, File Print)

Wireless Home Networks (Wireless access is not authorized.)
Wireless Router? Yes ☐ No ☐
(If yes, encryption *must* be enabled)

Encryption enabled? Yes ☐ No ☐
Provide screenshot (Alt Print Screen, Alt Insert to a Word document, File Print)

Required Actions
Screenshots must be provided to Helpdesk prior to scheduling One-on-One training. *(Alt Print Screen, Alt Insert to a Word document, File Print)*
Configured wireless routers shall be configured to accept connections from *specified* wireless node MAC addresses only! Users shall work with their ISP and/or router vendors to properly configure their routers for Telework access.

Do you <u>have</u> a SecureID Token? Yes ☐ No ☐ Serial #

To be filled out by Help Desk:

Laptop/ Docking Station

Make Model

Workstation Asset Tag #: SecurID Token Serial #

Has User completed one-on-one training? – yes ☐ no ☐

User's Signature Date

QA Signature Date

Financial Crimes Enforcement Network

User Agreement & Rules of Behavior for Systems and Network Access

1. Systems May Be Used For Approved Purposes Only – All FinCEN office equipment, including the FinCEN network and Information Technology Infrastructure (ITI), and access to the Internet, are only for official FinCEN, Government business, or other authorized purposes. FinCEN permits authorized users of its office equipment the privilege of using that equipment, including Information Systems, for **limited personal use only** when that use: involves minimal additional expense to the Government, does not overburden any FinCEN or Government information resources, occurs only during non-work time, is of a reasonable duration and frequency of use, does not adversely affect the performance of official duties, AND does not interfere with the mission or operations of the Department of Treasury, FinCEN, other bureaus or offices. **Users should have no expectation of privacy when using any U.S. Government resource. Viewing or accessing websites containing pornographic images, gambling, crude or extreme, hate-related, or any other questionable images or material is prohibited.**

All Executive Branch employees are bound by the ethics rules that state, in part:

Use of Government property. "An employee has a duty to protect and conserve Government property and shall not use such property or allow its use, for other than authorized purposes " NOTE Government property includes automated data processing capabilities. 5 CFR § 2635.704

Use of official time. "Unless authorized in accordance with law or regulations to use such time for other purposes, an employee shall use official time in an honest effort to perform official duties." 5 CFR § 2635.705

2. Use The Network and Information Systems Properly- Everything you do while on the FinCEN network, systems, or Internet at work will reflect on FinCEN and on you in your capacity as a FinCEN employee or user. You should avoid any action that may adversely affect the confidence of the public in the integrity of FinCEN.

Executive Branch-wide ethics rules state: *"Public Service is a Public Trust. - Employees shall endeavor to avoid any actions creating the appearance that they are violating the law or the ethical standards set forth in this part." To ensure that every citizen can have complete confidence in the integrity of the Federal Government, each employee shall respect and adhere to the principles of ethical conduct set forth in the section, as well as the implementing standards contained in this part and in supplemental agency regulations. 5 CFR § 2635.101(a).*

3. Safeguard FinCEN Information – The Internet is an open network without the security features found on FinCEN systems. Sensitive FinCEN information will not be transmitted via the Internet except as authorized in business related applications. You should be aware that:

- Anything sent over the Internet and some information sent via e-mail can be intercepted, read, altered or diverted without your knowledge. Exchanging messages or files on the Internet is equivalent to posting public messages that anyone can read.
- You should not have any expectation of privacy while using the Internet or while using any Government resource.
- Information may be modified in transit so there is no guarantee of integrity or delivery for messages sent or received

Executive Branch-wide ethics rule provide: *Use of nonpublic information. "An employee shall not engage in a financial transaction using nonpublic information, nor allow the improper use of nonpublic information to further his own private interest or that of another, whether through advice or recommendation or by knowing unauthorized disclosure." 5 CFR § 2635.703.*

In addition, employees of the Department of the Treasury are bound by the Treasury's Rules of Conduct, which state in part: *"Disclosure of information. Employees shall not disclose official information without proper authority, pursuant to Department or bureau regulation. Employees authorized to make disclosures should respond promptly and courteously to requests from the public for information when permitted to do so by law (31 CFR 1.9, 1.10, and 1.28(b))."* 31 CFR § 0.206.

4. Use Care When Receiving Attached Files - Downloading files from the Internet or received via e-mail can be a danger to our computer systems since attachments may contain viruses or other malicious code. **You must perform a virus scan on all files and documents that you receive via e-mail or download via the Internet.** You should be aware that new viruses are continually being created and files, such as Microsoft Word and Excel files, can contain "macro" viruses and .exe, .bat, .pif and other executable type files can run malicious programs and cause substantial damage to a network.

5. Copyright Issues - You shall not download copies of music, lierature, pictures, software or code unless an approved procurement process is used. LAN Support/Help Desk should review all software before you use it. You are responsible for ensuring that you do not violate copyrights or license agreements.

6. Understanding The Laws And Regulations As It Applies To Data - Data in FinCEN automated information systems is considered "sensitive." Our systems contain personal, financial, law enforcement, regulatory, trade-sensitive/business-confidential and counter-narcotics information. FinCEN is required to protect its data from unauthorized disclosure.

7. Use Only Approved Browsers and Internet Software - You are authorized to use only the approved software and browsers as they are installed by LAN Helpdesk/Administration or as informed by warning messages. You may not download web browsers, Java applets, or any other software scripts from the Internet, unless authorized by the ISSM/ISSO or its use is approved by inclusion on an Authorized Software list. JAVA is a feature that allows programs to be downloaded to the workstation and executed automatically during Web browsing. Java and other similar code (Active X) have the potential of allowing external exploitation of FinCEN internal resources.

8. Sanctions for Misuse --

All users are subject to the criminal provisions relating to exceeding authorized computer access, 18 U.S.C. § 1030. Specifically, 18 U.S.C. § 1030(a)(2)(B) makes it a criminal act to intentionally access a computer without authorization or in excess of authorized access, and obtain information from any department or agency of the U.S. Punishment of an offense under that section is a fine or imprisonment, or both.

Additional criminal provisions apply to Federal employees. Under 18 USC §1905, an unlawful disclosure of certain confidential information may result in a fine or imprisonment, or both, and the statute requires that the employee be removed from employment.

In addition, FinCEN employees who misuse Government office equipment or access to the Internet may be subject to discipline up to and including removal. Other users of government office equipment who misuse the Government office equipment or access to the Internet may be denied access to FinCEN premises and databases.

9. Scope – This agreement applies to all FinCEN employees, assigned detailees, permanent and temporary contractor personnel.

10. I, the undersigned individual, have read this User Agreement & Rules of Behavior and agree to comply with its provisions. I understand that FinCEN may monitor my network and systems use, Email, and Internet communications and that any information that I send and/or receive via the Internet is not to be considered as private communications. I understand that I have no privacy or expectation of privacy whenever I use any Government office equipment. I agree that an audit record of my network and systems use, Email, and/or Internet activity may be taken, retained and reviewed.

Employee/Detailee/Contractor Signature	(Date Signed)
(Printed Name)	(Office Phone)
Return this Signed Agreement to: (FinCEN ISSO)	(Date Received)

Financial Crimes Enforcement Network (FinCEN)
TELEWORK PROGRAM AGREEMENT

The following constitutes an agreement between:

Supervisor: _____ Office: _____ and,

Employee: _____ on the terms and conditions of the Telework Agreement.

1. The employee volunteers to participate in the Telework Program and understands and agrees to adhere to the applicable guidelines and policies. The first-level supervisor approves the employee's participation and agrees to adhere to the applicable guidelines and policies.

2. The employee agrees to begin participation in Telework on:

_____ _____
Pay Period Date

3. The Telework agreement is for (check one):

Full ☐ Expanded ☐ Limited ☐ Episodic ☐

4. Telework Days and Hours of Duty: Indicate desired Telework days and hours of duty for those days (including a one-half hour non-paid lunch period)

WEEK 1 of Pay Period				WEEK 2 of Pay Period			
☐	Monday	a.m. to	p.m.	☐	Monday	a.m. to	p.m.
☐	Tuesday	a.m. to	p.m.	☐	Tuesday	a.m. to	p.m.
☐	Wednesday	a.m. to	p.m.	☐	Wednesday	a.m. to	p.m.
☐	Thursday	a.m. to	p.m.	☐	Thursday	a.m. to	p.m.
☐	Friday	a.m. to	p.m.	☐	Friday	a.m. to	p.m.

(Check if) Episodic schedule ☐

5. The alternate work site will be: Home ☐ Mobile ☐

Address: _____

_____

Phone Number: _____

Computer access will be thru: (check one) Cable modem ☐ DSL ☐

6. The employee and their timekeeper will record the employee's time and attendance. The employee and supervisor are both responsible for ensuring the records are accurate. The employee agrees to follow established procedures for requesting and obtaining supervisory approval for leave.

7. The employee is in a pay status while working at his/her alternate work site. The employee agrees to work overtime (OT) or compensatory time only when it has been ordered and approved by the supervisor in advance and understands that such work without prior approval is not compensated. The employee will be compensated in accordance with applicable law, rule, or regulation. Violations may lead to removal from the Telework Program and/or other disciplinary action. Employees not exempt from the Fair Labor Standards Act (FLSA) are subject to the FLSA overtime rules.

8. Although a variety of circumstances may affect individual situations, the principles governing administrative leave, dismissals, and closings remain the same. If an official duty station or principle office experiences an unscheduled closing, and the Telework employee is dependent on that office for support, information, communication or guidance, and cannot perform his/her duties without support from the principle office, that employee should also be dismissed under the same conditions as are the employees assigned to the principle office. The Telework employee shall remain dismissed as long as this situation persists, unless conditions change allowing the employee to resume working.

   If on the other hand, the Telework employee experiences an emergency that prevents him/her from performing official duties at the alternate work site, but the principle office is not affected, the work status of that employee is at the discretion of the supervisor. Depending on prevailing circumstances, the employee may be required to report to the principal office, or placed on personal or administrative leave. The employee's ability to conduct work under any given circumstance, whether at home or at the office, must be determined by the supervisor based on the specific circumstances of each incident.

9. The employee will protect equipment provided by FinCEN in accordance with the procedures established by FinCEN. FinCEN-owned equipment will be serviced and maintained by FinCEN only.

10. The Government will not be held liable for damages to an employee's personal or real property during the course of performance of official duties or while using government equipment in the employee's alternate worksite, except to the extent the Government is held liable by the Federal Tort Claims Act or the Military Personnel and Civilian Employees Claim Act.

    Provided the employee is given at least 24 hours advance notice, FinCEN may inspect the employee's home worksite during the employee's normal working hours in order to ensure proper maintenance of FinCEN-owned property and conformance to safety standards.

11. The Government will not be responsible for any operating costs that are associated with the employee using his/her home as an alternate worksite, for example, home maintenance, insurance, or utilities. The employee should contact the Office of Systems and Reporting (Office Of Technology Management) to determine connectivity needs. By participating in this program, the employee does not relinquish entitlement to reimbursement for authorized expenses incurred at the alternate worksite while conducting business for the Government, as provided for by statute and implementing regulations.

12. The Federal Employees' Compensation Act is applicable if the employee is injured in the course of actually performing official duties at the alternate worksite. The employee agrees to immediately notify their first-level supervisor of any accident that occurs and to complete any required forms. The supervisor will notify FinCEN's Safety and Health Officer and such reports will be investigated immediately.

13. The employee will meet with the supervisor to receive assignments and to review completed work as necessary or appropriate.

14. The employee will protect all government records from unauthorized disclosure or damage and will comply with the Privacy Act of 1974, as amended, and all FinCEN confidentiality policies and procedures.

15. The employee will continue to be bound by Executive Branch-wide and Department of the Treasury Standards of Ethical Conduct while working at the alternate worksite.

16. The employee may terminate participation in the telework program at any time; however, the employee may be expected to continue working at the alternate worksite for a reasonable period to allow management time to arrange for a workstation. Management has the right to remove the employee and any government owned equipment from the telework arrangement if the employee's work performance declines, or other conditions of the agreement are not met, or if the arrangement fails to benefit organizational needs.

17. If an employee disputes Management's initial determination of the ineligibility of a position to be covered by teleworking, the employee may present a request in writing to the appropriate Associate Director for reconsideration. If the employee is dissatisfied with the reconsideration decision, they may submit a grievance using the procedures set forth in the grievance policy.

18. If an employee disputes the reason(s) given by a supervisor for not approving him or her for telework, or for terminating his or her telework agreement, the employee may submit a grievance using the procedures set forth in the grievance policy.

19. Participants continuing in long-term arrangements must complete an annual renewal agreement; FinCEN Form Fin-042, Telework Renewal Agreement. At this point, the arrangement should be reassessed to determine the need to revise or update existing participation criteria. The Renewal Agreement may also be used to extend short-term arrangements.

SAFETY AND SECURITY CERTIFICATION:

By signing this agreement the employee certifies that:
1. They have been trained on the safety and security requirements of the FinCEN Telework Program,
2. They have inspected their alternate worksite and that the alternate worksite is free of significant safety problems, including but not limited to electrical hazards, inadequate ventilation or temperature control, poor lighting, excessive noise, or tripping hazards,
3. Any computer workstation is free of significant physical hazards, including but not limited to inadequate back support, cramped leg room, or poor work design that would put undue stress on the eyes, wrists or legs, and
4. The alternate worksite provides adequate security for the protection of confidential business information and complies with FinCEN Directive 804.01, Information System Security Policy.

_____

Supervisor's Signature and Date

_____

Employee's Signature and Date

Financial Crimes Enforcement Network (FinCEN)
TELEWORK RENEWAL AGREEMENT

This is to certify that the Telework Program Agreement which was originally approved on (date) _____ and is in effect for the period from (date)_____ to (date) _____, between (employee's name) _____ and the Financial Crimes Enforcement Network, is extended.

The renewal will commence on (date) _____ and end on (date) _____. The employee and the supervisor certify that the arrangement is mutually beneficial. Both parties understand that all applicable policies, procedures, and criteria contained in the original agreement remain in effect.

_____

Supervisor's Printed Name

_____

Supervisor's Signature and Date

_____

Employee's Printed Name

_____

Employee's Signature and Date