U.S. Department of Commerce

OFFICE OF THE CHIEF INFORMATION OFFICER (OCIO)

Telework Implementation Plan
March 2015

Approved by: _____ 13 APRIL 15

Steven I. Cooper
Chief Information Officer

Date

TABLE OF CONTENTS

Office of the Chief Information (OCIO))
Telework Implementation Plan

I. INTRODUCTION

Telework is a flexible work arrangement under which an employee performs the duties and responsibilities of his/her position and other authorized activities from an approved alternate worksite other than the employee's designated Federal workplace.

The OCIO Telework Implementation Plan is consistent with the provisions of the **Telework Enhancement Act** (Act) of 2010 (Public Law 111-292, October 9, 2010), the Department of Commerce (Department) Telework Policy (October 2014), and the Office of Personnel Management's (OPM) policies contained in their **Guide to Telework in the Federal Government** and **Washington, DC Area Dismissal and Closure Procedures** (December 2013).

The law and policies are intended to promote:

- recruiting and retaining the best possible workforce;
- continuing operations during emergency conditions;
- management effectiveness; and
- enhancing work-life balance by allowing employees to better manage their work and personal obligations.

Telework is a workplace flexibility management option to facilitate the timely and effective accomplishment of the work of the office. Telework is not an entitlement and employees may not care for dependents if they are in a duty status while teleworking. An employee's decision to elect to telework is entirely voluntary (except if the employee is designated an "emergency" employee or is designated as a part of the Continuation of Operations Plan (COOP)).

II. REFERENCES

- Telework Enhancement Act of 2010, Public Law 111-292, December 9, 2010 (Title 5, United States Code (U.S.C.) Chapter 65)
- U.S. Office of Personnel Management (OPM) *Guide to Telework in the Federal Government* (2010)
- OPM, Washington, DC, Area Dismissal and Closure Procedures (December 2013)
- Department of Commerce, *Teleworking Policy*, October 2014

III. DEFINITIONS

ALTERNATE WORKSITE – The employee's residence or another location other than the employee's traditional worksite that has been approved by the manager/supervisor for the performance of the employee's official duties. For purposes of telework, the alternate worksite is considered an official Government worksite.

APPROVING OFFICIAL – The employee designated by the office director to approve individual telework agreements.

ELIGIBLE EMPLOYEE – All employees are considered eligible to telework unless (1) the employee has been officially disciplined for being absent without permission for more than five days in any calendar year (there are no exceptions); (2) the employee has been officially disciplined for violations of 5 CFR Part 2635 (Standards of Ethical Conduct for Employees of the Executive Branch) for viewing, downloading, or exchanging pornography, including child pornography, on a Federal Government computer or while performing official Federal Government duties (there are no exceptions); or (3) the employee's performance does not comply with the terms of the written agreement between the approving official and the employee.

ELIGIBLE POSITION – A position is an eligible position unless the official duties require on a daily basis (every workday) the direct handling of secure materials determined to be inappropriate for telework by the head of the bureau/operating unit; *or* the employee performs on-site activities that cannot be handled at an alternate worksite.

OFFICIAL DUTY STATION – The location of an employee's position of record where the employee regularly performs his or her duties. If the employee's work involves recurring travel or their work location varies on a recurring basis, the duty station is the location where the work activities of the employee's position of record are based, as determined by the manager/ supervisor. An employee's official duty station determines the appropriate locality area for pay purposes for General Schedule or equivalent employees.

REGULAR/RECURRING TELEWORK – Telework that is performed on the same day(s) of the week on the employee's regularly scheduled tour of duty.

REMOTE WORKER – The employee is teleworking full-time from an alternate work site. The alternate work site becomes the employee's official duty station for pay purposes.

TELEWORK – Telework, known as "telecommuting," refers to a paid, flexible work arrangement under which an employee performs the duties and responsibilities of his/her position, and other authorized activities, from an alternate worksite, not the traditional worksite.

TELEWORK-READY EMPLOYEE – An employee who has completed **Telework 101 for Employees** via the Commerce Learning Center (CLC); has a signed individual telework agreement; and has the required necessities to telework for their entire work schedule.

TRADITIONAL WORKSITE – The traditional worksite is where the employee would work absent a telework arrangement.

IV. POLICY

A. Conformance to terms of written agreement. An employee may not be authorized to telework if the performance of that employee does not comply with the terms of the written agreement between the agency manager and that employee

B. Agreeing to Telework. An employee's decision to telework is voluntary unless telework is a condition of employment (i.e., the employee is designated an "emergency employee") or is required to continue Government operations in times of emergency (COOP). In these instances, an employee may be required to work at home, or at another approved alternate worksite.

C. Types of telework. It is the policy of the Office of the Chief Information Officer (OCIO) to allow eligible employee to work at alternate work sites away from their official duty stations, consistent with the needs of their office, during their regular tour of duty. There are three (3) types of telework:

1. Regular/recurring in which telework occurs as part of a preapproved ongoing, regular schedule. Once the schedule is established, the employee may not change the assigned telework day(s) without prior approval of the approving official. An employee may combine teleworking with an alternative work schedule with the prior approval of the approving official;
2. "Unscheduled telework" in which telework occurs under an announcement by the Office of Personnel Management (OPM) (but the employee's office is open). When OPM makes an announcement of "Unscheduled Telework" and it is not the employee's regularly scheduled telework day, the employee may choose to perform unscheduled telework. The employee's decision is not subject to prior approval by the supervisor. However, in rare circumstances, management may find it necessary to require a non-emergency, telework-ready employee to report for an assignment that requires presence at the worksite (e.g., providing a presentation or performing administrative duties at a pre-scheduled conference). This should not be a last-minute surprise, but a special work circumstance that both the supervisor and employee know about, discuss, and plan in advance as the special work requires. The employee must notify his/her supervisor in accordance with the applicable policy of the office; and
3. Ad hoc telework which is telework on an irregular basis, chosen by the employee, to address a specific need of the employee. Ad hoc telework must be requested and approved by the supervisor in advance.

D. Telework May Not be used as a Substitute for Dependent Care. It is the policy of OCIO that employees may not care for a dependent while in a duty status and teleworking.

E. Teleworkers and Non-Teleworkers Shall be Treated the Same for Certain Purposes. It is the policy of the OCIO that teleworkers and non-teleworkers will be treated the same for the purposes of:

1. Periodic appraisals of job performance of employees;
2. Training, rewarding, reassigning, promoting, reducing in grade, retaining, and removing employees;
3. Work requirements; and
4. Other acts involving managerial discretion.

F. Training requirements. It is the policy of OCIO that all eligible employees must successfully complete **Telework 101 for Employees** via the Commerce Learning Center (CLC) before they can request to telework. The approving official for individual telework agreements must have completed **Telework 101 for Managers** via CLC before he/she can approve any individual telework agreements.

G. Maximum amount of teleworking. The maximum number of days an employee (including part-time employees) may telework during a pay period is left to the discretion of the office director. This includes regular/recurring telework and ad hoc telework.

V. ELIGIBILITY CRITERIA

A. Employee eligibility. Participation in telework is open to all eligible employees without regard to race, color, religion, sex (including pregnancy and gender identity), national origin, political affiliation, sexual orientation, marital status, disability, genetic information, age, membership in an employee organization, retaliation, parental status, military service, or other non-merit factors. **5 U.S.C. § 6502(a)(2)**.

1. Employee exceptions. OCIO employees who meet any of the following exceptions are ineligible to telework:
   a. The employee has been officially disciplined for being absent without leave (AWOL) for more than five days in any calendar year;
   b. The employee has been officially disciplined[1] for violations of 5 CFR Part 2635 (Standards of Ethical Conduct for Employees of the Executive Branch) for viewing, downloading, or exchanging pornography, including child pornography, on a Federal Government computer or while performing official Federal Government duties[2]; or
   c. The performance of the employee does not comply with the terms of the individual telework agreement between the supervisor and that employee. **5 U.S.C. § 6502 (b)(3)**.[3]
2. All OCIO employees are initially considered eligible to telework. If an employee is determined to be ineligible to work due to **5 U.S.C. § 6502(a)(2)**, the employee will receive a written determination from the office director within 10 working days of the employee's request to telework.

B. Precluded Due to Nature of Work of Position. If the official duties of the employee's position require the employee to perform direct handling of secure materials determined to be inappropriate for telework by the agency head or on-site activity that cannot be handled remotely or at an alternate worksite, then the employee' position is not eligible

---

[1] Definition of Officially Disciplined – A disciplinary action that results in the placement of a document in an employee's official personnel file (OPF); the bar on telework participation remains in effect as long as the document stays in an employee's OPF. A suspension or termination related to the items mentioned in Public Law 111-292 that results in a document (Standard Form 50) that permanently remains in the OPF would result in permanent prohibition in telework participation

[2] No authority to waive provisions "a" or "b."

[3] The length of this exclusion is at the office director's discretion.

for telework.

VI. ACCOMMODATIONS FOR EMPLOYEES WITH DISABILITIES

It is important to distinguish between ordinary requests to telework and requests from persons with disabilities for reasonable accommodation. Approving officials/supervisors should consult Department Administrative Order (DAO) 215-10, "**Reasonable Accommodation Policy**," and the Disability Program Manager as part of the interactive process established by the Rehabilitation Act, in order to fully understand supervisors' responsibilities under the law. As governed by Section 501 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. § 791 et. seq., the Rehabilitation Act and **DAO 215-10**, the determination as to whether an employee may be granted telework as a reasonable accommodation due to a disability should be made through the Reasonable Accommodation Coordinator, the employee's first-line supervisor, and the employee.

VII. LEVELS OF TELEWORK.

The OCIO recognizes that some employees will opt not to telework at all, while others will choose to telework only on a limited ad hoc basis, and others will telework to the maximum extent possible. The OCIO offers two plans of telework.

A. Plan A (for ad hoc/unscheduled teleworking)

1. Telework-ready employees (employee) limited to a maximum of 80 hours of ad hoc/unscheduled telework during the term of the individual telework agreement;
2. Employee performing unscheduled telework under an OPM announcement may do so without prior supervisory permission[4] but they must first contact their supervisor in accordance with the policies in their individual telework (written) agreement;
3. An employee wishing to perform ad hoc telework must first obtain supervisory approval before performing ad hoc telework;
4. The employee is responsible for ensuring he/she has sufficient work for the planned period of telework; and
5. The employee is not required to telework when the office is closed due to emergency situations.

B. Plan B (for employees on regular/recurring telework schedule)

1. Employees on a regular/recurring telework schedule;
2. Employees who desire the option of doing an unlimited amount of ad hoc telework and/or unscheduled telework during the term of the agreement;

[4] In rare circumstances, management may deny unscheduled telework when it finds it necessary to require a non-emergency, telework-ready employee to report for an assignment that requires presence at the worksite (e.g., providing a presentation or performing administrative duties at a pre-scheduled conference). This should not be a last-minute surprise, but a special work circumstance that both the supervisor and employee know about, discuss, and plan in advance as the special work requires

3. The employee must obtain supervisory approval before performing ad hoc telework;
4. Employee may perform unscheduled telework without prior supervisory approval but must first contact his/her supervisor in accordance with OCIO policies;
5. The employee is responsible for ensuring that he/she has sufficient work for his/her scheduled tour of duty for the telework day;
6. Less than 80 hours of ad hoc/unscheduled telework. Performing less than 80 hours of ad hoc/unscheduled telework during term of agreement does not change the employee's election of Plan B; and
7. The employee must telework when his/her office is closed due to emergency reasons.

VIII. TELEWORKING

A. Systems are to be in place to support telework in an emergency, including a communication process to notify COOP personnel, emergency, and non-emergency employees of the activation of the agency's emergency plan, and the agency's operating status during the emergency.

B. Telework-ready employees scheduled to telework during their regular tour of duty on a day when their office is closed (or when other employees are dismissed early) are not entitled to receive overtime pay, credit hours, or compensatory time off in lieu of overtime payment for performing work during their regularly scheduled hours.

C. All time teleworked in a pay period will be recorded per instructions in the appropriate time and attendance system.

D. All employees designated as "emergency" or with COOP responsibility must have an approved individual telework agreement.

IX. EXCUSED FROM TELEWORKING

A. The approving official, on a case-by-case basis, may excuse a telework-ready employee from duty without charge to paid personal leave or loss of pay during an emergency situation if: (1) the emergency adversely affects the telework site (e.g., disruption of electricity, or network connection problems that prevent telework); or (2) the telework-ready employee's duties are such that he/she cannot continue to work without contact with the regular worksite.

B. If the telework-ready employee faces a personal hardship that prevents him/her from working successfully at the telework site, the employee may request his/her supervisor for the appropriate leave (annual, sick, compensatory, credit hours, compensatory time for travel). The employee may also switch to an alternative work schedule day off, or use "flexing" consistent with the employee's alternative work schedule, if any with the prior approval of his/her supervisor.

X. PERFORMANCE STANDARDS

Performance standards for telework-ready employees must be the same as performance standards for non-telework-ready employees. Expectations for performance should be clearly addressed in each employee's performance plan, and the performance plan should be reviewed to ensure the standards do not create inequities or inconsistencies between telework-ready and non-telework-ready employees. Like non-telework-ready employees, telework-ready employees are held accountable for the results they produce. Resources for performance management are available from OPM at **www.opm.gov/perform**.

XI. RESPONSIBILITIES

A. OHRM is responsible for oversight of the Department Telework Program and for any reporting requirements to OPM. OHRM will review and monitor the various plans to ensure consistency across the bureaus/operating units with implementing the program.

The TC for OCIO is the Director, Administration and Business Management.

B. Approving Officials. Approving officials are responsible for the overall management and success of teleworking within their offices, including day-to-day operations. Telework-ready employees and their approving officials are responsible for annually reviewing the individual telework agreement to ensure that it is current. The date of the review must be documented on the agreement by both parties.

C. TCs
   1. In consultation with the Telework Program Manager (TPM)
      a. provide OCIO policy and procedural program guidance to management and telework-ready employees;
      b. provide advice and assistance to OCIO personnel tasked with policy and implementation plan development, including working with senior-level managers in establishing and obtaining office telework goals, objectives, and reporting requirements;
   2. Provide each employee and appropriate management official a copy of the "Telework Assessment Tool" (**Appendix B**).
   3. Maintain a central file of all approved individual telework agreements for the personnel in the office as well as a record of all written denials or terminations;
   4. Responsible for answering telework related questions and providing guidance to the employees in OCIO offices;
   5. Develop and implement a reporting system capturing telework participation, hours teleworked, terminations, and denials; and
   6. Responsible for providing the following information to the TPM upon request:
      a. The degree of participation by employees of each office during the period covered by the report;
      b. The method for gathering telework data in each office;

c. The reasons for positive or negative variations in telework participation if the total number of employees teleworking is 10 percent higher or lower than in the previous year of the reporting activity;
d. The office's goal for increasing telework participation if applicable;
e. An explanation of whether or not the office met its established goal(s) for the last reporting period and, if not, what actions are being taken to identify and eliminate barriers;
f. An assessment of the progress made in meeting the office's participation rate goal(s) and other goal(s) related to telework, e.g., the impact of telework on recruitment and retention, performance, etc.; and
g. A description of best practices, if applicable.

XII. PREPARING FOR THE INDIVIDUAL TELEWORK AGREEMENT

The following actions are to be taken when establishing an individual telework agreement:

A. Each employee will have an opportunity, prior to meeting with the designated management official, to review and complete the "Telework Assessment Tool" (**Appendix B**) as a preliminary self-determination of whether teleworking is appropriate for the employee.

B. The appropriate management official(s) should review the "Telework Assessment Tool" and complete its questions based on observations of the employee's work habits. This should provide the official(s) with an indication of the employee's ability to telework.

C. The employee completes the "Telework Application/Agreement and Modification of Telework Agreement" (**See Appendix A**) and submits it to his/her supervisor along with the certificate showing successful completion of **Telework 101 for Employees**.

D. The employee and supervisor discuss the expectations in the proposed telework agreement, including the performance levels required of the employee.

E. If the supervisor is not the approving official, the supervisor will forward the agreement to the approving official with his/her recommendations.

XIII. TELEWORK AGREEMENTS

A. Length of telework agreements.
1. The length of the written agreement is established by the employee and the approving official. The expiration date of the agreement is to be included in the written agreement.
2. An employee may not telework if they do not have a current telework agreement in place.
3. In accordance with **5 U.S.C. § 6502(b)(3)**, an employee is not be authorized to continue teleworking if the performance of that employee does not comply with the terms of the written agreement between the approving official and the employee.

B. Modification and Termination of Agreement. The operational needs of OCIO are paramount and employees who telework do not have an automatic right to continue to telework.

1. Modification.
   a. An employee may request to modify the current agreement (e.g., change the regular teleworking day) by submitting a new "Telework Application/Agreement and Modification of Telework Agreement" (check "Modification") with only the requested changes indicated;
   b. The supervisor and employee shall discuss the employee's requested modifications within three working days;
   c. If the supervisor is not the approving official, the supervisor will forward the request to the approving official with his/her recommendations within three working days;
   d. The approving official will issue a written decision within five working days;
   e. If management is proposing to modify an employee's existing agreement, it will provide the employee with five working days advance notice in order for the employee to submit his/her response to the approving official; and
   f. The approving official will issue a final decision within five working days.

2. Termination.
   a. An employee may terminate his/her written agreement by providing the approving official with written notice of a decision to terminate his/her written agreement;
   b. The approving official must deny or terminate the agreement, as applicable, if the employee fails to be eligible to telework due to **5 U.S.C. §§ 6502(a)(2) or (b)(3)**;
   c. If management is proposing to terminate the agreement, it shall provide 10 working days advance written notice before terminating the agreement to allow the affected employee to make necessary arrangements;
   d. The approving official must provide documentation for the termination to the affected employee. Consent or acknowledgement via signature by the affected employee is not required for the termination of telework to take effect; and
   e. Management may terminate or deny telework requests as long as the denial or termination decision is based on operational needs, conduct, or performance in accordance with the law.

C. Appeals. The deciding official will issue a written decision on an employee's request to telework within 10 working days of the request being received by the deciding official. If the deciding official disapproves the request, he/she must provide written justification to the employee indicating when or if the employee would be eligible to reapply, and if applicable, what actions the employee should take to improve his/her chance of future approval. Deciding officials are to provide employees copies of signed written denials or terminations of telework agreements.

D. Administrative Grievance Procedure. OCIO employees must use the procedures in the **DAO 202-771**, "Administrative Grievance Procedure" to appeal issues relating to their

request to telework, modification to an existing telework agreement, and terminations of telework agreements.

E. Discrimination. Employees who believe they are the victims of prohibited discrimination must use the procedures in **DAO 215-9**, "Filing Discrimination Complaints," to appeal the alleged discrimination.

XIV. ESTABLISHING THE WORK SCHEDULE

Work schedules identify the days and times an employee will work while teleworking. Normally, telework schedules parallel those at the traditional worksite; however, they can differ to meet the needs of the organization and participating employees' needs. Work schedules may also include fixed times during the day for manager/supervisor/employee telephone conversations, which may be helpful to ensure ongoing communication. For additional information on hours of duty, please visit **http://hr.commerce.gov/Practitioners/CompensationAndLeave/DEV01_006627.**

XV. DETERMINING THE OFFICIAL DUTY STATION

A. Pay during Telework Agreements.
   1. Traditional worksite and telework site are within the same locality pay area; the official duty station is the location of the traditional worksite;
   2. Traditional worksite and the telework site are NOT within the same locality pay area:
      a. The official duty station is the location of the traditional worksite as long as the employee physically reports to the traditional work site at least twice each biweekly pay period on a regular and recurring basis;
      b. The official duty station is the telework location (i.e., home or other alternate worksite) if the employee does NOT report at least twice each biweekly pay period on a regular and recurring basis to the traditional worksite;
   3. If a telework employee with a varying work location works at least twice each biweekly pay period on a regular and recurring basis in the same locality pay area in which the traditional worksite is located, the employee **does not** have to report twice each pay period to the official worksite to maintain the locality payment for that area.

B. Pay during Temporary Telework Arrangements.
   1. In certain temporary situations, OCIO may designate the location of the traditional worksite as the official duty station of an employee who teleworks on a regular basis in a different locality pay area as the traditional worksite even though the employee is not able to report at least twice each biweekly pay period on a regular and recurring basis to the traditional worksite. The intent of this exception is to address certain situations where the employee is retaining a residence in the commuting area for the traditional worksite but is temporarily unable to report to the worksite for reasons beyond the employee's control (e.g., on a special assignment or working while recuperating from an operation);
   2. One key consideration is the need to preserve equity between telework-ready and non-telework ready employees working in the same areas as the telework location.

Also, the temporary exception should generally be used only in cases where: (1) the employee is expected to stop teleworking and return to work at the traditional worksite in the near future, or (2) the employee is expected to continue teleworking but will be able to report in the near future to the traditional worksite at least twice each biweekly pay period on a regular and recurring basis.

XVI. PAY AND LEAVE

A. Pay. An employee's locality rate of pay is based on the employee's official duty station, and is determined in accordance with 5 CFR 531.604(b). The bureau/operating unit must determine and designate the official duty station for an employee covered by a telework agreement using the criteria above.

B. Premium Pay. The same premium pay rules apply to employees when they telework as when they are working at the traditional worksite.

C. Leave and Work Scheduling Flexibilities. Telework-ready employees are governed by the same procedures as non-telework-ready employees for requesting and obtaining leave approval.

See the Department's Web page, **Leave Policies**,. For additional information on pay administration, premium pay, leave administration, and work scheduling, please visit **http://www.opm.gov/oca/leave/index.asp**.

XVII. IT SECURITY REQUIREMENTS FOR TELEWORK-READY EMPLOYEES

Telework-ready employees must abide by the IT security requirements conveyed in the DOC Information Technology Security Program Policy (ITSPP), Commerce Information Technology Requirements (CITRs), Frequently Asked Questions (FAQs), and IT Security Policy memos. The Telework Agreement signed by the telework-ready employee and his/her supervisor may describe additional security requirements. A complete list of DOC IT security documentation can be accessed at:
http://home.commerce.gov/CIO/ITSITnew/IT_Security_Program_Documentation.html

Telework-ready employees must also abide by office-specified IT security requirements. Supervisors are responsible for ensuring that telework-ready employees agree to comply with all existing IT security requirements and to ensure employees are accountable.

XVIII. THE PRIVACY ACT OF 1974, SENSITIVE PII AND BII – REQUIREMENTS FOR TELEWORK-READY EMPLOYEES

All telework-ready employees are responsible for ensuring that records subject to the Privacy Act of 1974, sensitive Personally Identifiable Information (PII), and Business Identifiable Information (BII) are not disclosed to anyone except those who have been authorized access to such information in order to perform their duties. Bureaus/operating units must ensure that appropriate physical, administrative, and technical safeguards are used to protect the security and confidentiality of such records.

A. Disclosure of Records from an Agency System of Records
   1. Telework-ready employees are responsible for ensuring that their disclosure of a record (information) from any agency system of record complies with the Privacy Act of 1974;
   2. The Privacy Act of 1974 defines a "system of records" as a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Department of Commerce system of record notices (SORNs) are posted at: **http://www.gpo.gov/fdsys/browse/collection.action?collectionCode=PAI&browsePath=2005&isCollapsed=false&leafLevelBrowse=false&ycord=0**.
   3. The Privacy Act of 1974 prohibits the disclosure of a record [information] from an agency system of record that is not identified as a routine use in that system's SORN, does not comply with an exemption identified in the SORN, or does not comply with 1 of the 12 exceptions to the non-disclosure-(to third parties)-without-consent rule.
   4. A Privacy Act incident occurs when an officer or employee of the agency, who by virtue of his/her employment or official position, has possession of or access to agency records that contain individually identifiable information the disclosure of which is prohibited by 5 U.S.C. § 552a (or regulations established thereunder) and discloses the material in any manner to any person or agency not entitled to receive it. Knowing misuse or release of information protected by the Privacy Act of 1974 can subject an employee to fines and/or criminal sanctions; and
   5. Telework-ready employees must immediately report a suspected or confirmed Privacy Act incident to his/her bureau/operating unit privacy officer or Computer Incident Response Team (CIRT) and immediate supervisor.

B. Proper Handling of PII and BII
   1. Telework-ready employees are responsible for the safeguarding of PII and BII;
   2. PII is information that can be used to distinguish or trace an individual's identity, such as name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Sensitive PII, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual;
   3. Types of PII considered sensitive when associated with an individual are: social security number (including truncated form), place of birth, date of birth, mother's maiden name, biometric information, medical information (except brief references to absences from work), personal financial information, credit card or purchase card account numbers, passport numbers, potentially sensitive employment information (e.g., personnel ratings, disciplinary actions, and results of background investigations), criminal history, and any information that may stigmatize or adversely affect an individual. The Department IT Privacy Policy provides that breaches of sensitive PII are subject to notification/reporting requirements;
   4. When deciding whether PII is sensitive or non-sensitive, it is important to consider the type of information, obligations, or expectations regarding the protection of information, risk (probability and consequences) of loss or compromise of

information, and context of information. Context is particularly important. The same types of information can be sensitive or non-sensitive depending upon the context. For example, a list of names and phone numbers for the Department softball roster is very different from a list of names and phone numbers for individuals being treated for an infectious disease. It is important to use good judgment when deciding whether PII is sensitive or non-sensitive. When in doubt, treat PII as sensitive;

5. The Department's policy states that if sensitive PII must be electronically transmitted, then it must be protected by secure methodologies such as encryption, Public Key Infrastructure (PKI), or secure sockets layer (SSL). Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules" provides the standard to which encryption methodologies must conform. The transmission of sensitive PII, even if it is protected by secure means, must be kept to a minimum.
6. In addition to sensitive PII, telework-ready employees must ensure the safeguarding of BII. BII is information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." Commercial is not confined to records that reveal "basic commercial operations" but includes any records [information] in which the submitter has a "commercial interest" and can include information submitted by a non-profit entity. Terms for BII that must be protected from disclosure include "confidential business information," "confidential commercial information," and "proprietary information";
7. Sensitive PII and BII can be stored on Government systems only and saved, stored, or hosted only on Department-authorized equipment (including contractor-owned equipment or a system that is approved to be used as a Government system). Personally-owned computers may not be used to save, store, or host sensitive PII and BII that is collected or maintained by the Department;
8. Sensitive PII and BII must be sent encrypted as an e-mail attachment and encrypted on mobile computers, media (e.g., CDs, DVDs, USB drives), and devices (e.g., laptops, hard drives). When faxing sensitive PII and BII, an advisory statement about the contents must be included on the cover sheet and the recipient must be notified immediately before and after transmission. When mailing sensitive PII and BII, it must be physically secured when in transit. Do not mail or send by courier sensitive PII and BII on CDs, DVDs, hard drives, flash drives, USB drives, floppy disks, or other removable media unless the data is encrypted. Sensitive PII and BII must be sealed in an opaque envelop or container and mailed using First Class or Priority Mail, or a commercial delivery service (e.g., FedEx or DHL). Appropriate methods must be used to destroy sensitive paper PII and BII (e.g., shredding, using a burn bag) and securely delete sensitive electronic PII and BII (e.g., empty the Windows "recycle bin");
9. Telework-ready employees and supervisors are responsible for complying with all office guidelines on reporting PII and BII incidents. The Office of Management and Budget (OMB) Memorandum M-07-16 defines a PII incident as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users, and for an other than authorized purpose, have access or potential access to PII,

whether physical or electronic. Telework-ready employees must immediately report a suspected or confirmed PII and BII incident to his/her bureau privacy officer or CIRT and immediate supervisor. Additional information regarding the PII and BII incident reporting process can be found at: **http://home.commerce.gov/CIO/ITSITnew/DOC_Breach_Response_Plan_v2_final.pdf.**

XIX. IT SECURITY REQUIREMENTS FOR TELEWORK-READY EMPLOYEES

Telework-ready employees must abide by the IT security requirements conveyed in the DOC Information Technology Security Program Policy (ITSPP), Commerce Information Technology Requirements (CITRs), Frequently Asked Questions (FAQs), and IT Security Policy memos. The Telework Agreement signed by the telework-ready employee and his/her supervisor may describe additional security requirements. A complete list of DOC IT security documentation can be accessed at:
http://home.commerce.gov/CIO/ITSITnew/IT_Security_Program_Documentation.html

Telework-ready employees must also abide by office-specified IT security requirements. Supervisors are responsible for ensuring that telework-ready employees agree to comply with all existing IT security requirements and to ensure employees are accountable.

XX. SENSITIVE AND HIGHLY SENSITIVE INFORMATION REQUIREMENTS FOR TELEWORK-READY EMPLOYEES

A. Decisions on the proper use and handling of Sensitive Information will be made by the approving official who permits the employee to work at home or at an alternate worksite. A telework agreement will be signed by the telework-ready employee and his/her approving official that contains the specific data types allowed to be accessed. Information is generally categorized into the following groups: Non-Sensitive Information; Sensitive Information; and Classified National Security Information.

B. The physical security standards for PII and other Sensitive and Administratively Controlled Information must be addressed prior to allowing telework. **Chapter 35 of the OSY Security Manual** provides minimum physical security standards for the office environment that are also applicable during telework. At a minimum, Controlled Unclassified Information (CUI), including PII, should be afforded protection to prevent unauthorized access to the information.

C. The National Archives and Records Administration's (NARA) CUI Office developed the CUI Registry that allows anyone to access the Safeguarding and Dissemination requirements for CUI that must be afforded to information like PII (Privacy) and other unclassified information. The registry may not be all inclusive, as only those categories of unclassified information that have a law, regulation, or government-wide policy governing dissemination and/or safeguarding are provided. Therefore, any Sensitive and Administratively Controlled Information in hard-copy form that does not fall within the parameters of the manual or the registry should be brought to the attention of the Information and Personnel Security Division of OSY.

Teleworkers and supervisors should visit **http://www.archives.gov/cui/registry/category-list.html** prior to allowing hard copy PII and other administratively controlled information outside the workplace for telework purposes.

Controlled Unclassified Information, Title 13, Title 26, and Title 35, U.S.C. Information, which are legally protected, are covered under the Sensitive Information category.

D. Highly Sensitive Information is subject to the most stringent security and access control rules, such as courier authorization, hand-to-hand transmission, or agency-specific rules not included in the Department telework policy/handbook. Classified information that requires Secret or Top Secret security clearances for protecting national security information is included in this category. Classified information (Confidential, Secret, or Top Secret) may only be transmitted or removed from official worksites by classified networks or authorized official couriers. This type of information may not be used or accessed in any manner by teleworkers

XXI. TELEWORK INFORMATION TECHNOLOGY SECURITY POLICY

The Department's Chief Information Officer (CIO) is responsible for issuing and maintaining information technology (IT) and eGov policies and minimum implementation standards, including remote access and safeguarding sensitive information. These policies and minimum implementation standards outline responsibilities of teleworkers to enable an effective working environment for the teleworker and the protection of Department systems from undue risk. Offices, with the support of their IT security officers, are responsible for establishing teleworking IT security procedures specific to their office providing secure telecommuting resources and operational controls commensurate with the sensitivity of the data processed and with policies and minimum implementation standards provided by the Department's CIO. The Department's policy on remote access is accessible via intranet at **http://home.commerce.gov/CIO/ITSITnew/CITR_008_Remote_Access.pdf**

Managers/supervisors are responsible for ensuring that telework-ready employees agree to comply with all existing security policies and procedures, including IT security. Telework-ready employees also agree that their responsibilities, remain in effect while on telework status. Other pertinent bureau or operating unit policies on IT security may also exist; managers/supervisors are responsible for ensuring that telework-ready employees agree to follow all applicable policies.

The workplace and workstation must be set up to accomplish secure information processing, including the proper storage of Sensitive Information in both electronic and paper form. The telework-ready employee, following bureau/operating unit policies, must minimize security vulnerabilities to the workstation and the Departmental network.

XXII. TELEWORKING DURING EMERGENCY SITUATIONS

A. Unscheduled Telework. This type of telework allows telework-ready employees to work from home or at an approved alternate location upon notification to their supervisor in accordance with the terms of the written agreement.

B. Federal/Departmental Offices Are Closed. Employees on Plan B **must** telework consistent with their written agreements when Federal/Departmental offices in their local commuting area are closed. Excused absences may be granted on a case-by-case basis for telework-ready employees in the above situation.

C. Early Dismissal/Delayed Arrival. When an early dismissal/delayed arrival is provided, those who are teleworking from their home are not dismissed from duty for any part of the workday. However, supervisors may grant excused absence on a case-by-case basis, if the employee is unable to continue teleworking.

D. Emergency at the Alternate Worksite. When an emergency affects the alternate worksite, the employee may request his/her supervisor approve administrative leave for the duration of the emergency. The supervisor may excuse, without charge to paid personal leave or loss of pay, a telework employee from duty during an emergency if: (1) the emergency adversely affects the telework site; (2) the telework-ready employee is unable to access another alternate telework site; or (3) the telework-ready employee's duties are such that he/she cannot continue to work without contact with the traditional worksite.

XXIII. TELEWORK AND THE CONTINUITY OF OPERATIONS PLAN (COOP)

If an employee occupies a position deemed an "emergency employee" or serves as an ERG member (these designations may vary based on the nature of the emergency) for inclement weather or natural or man-made emergencies, he/she may be required to report to work.

If an employee is an ERG member for COOP purposes, management, along with the employee and supervisor, should make advance and/or situational decisions as to whether the employee must physically report for duty or may work from home or an alternate worksite. For example, if the purpose of the employee reporting for duty at the traditional worksite is to provide policy guidance or to notify specific individuals of emergency requirements, this may be able to be accomplished from home, provided the employee has access to the resources necessary to perform the required services. However, in some cases, the only way to obtain the services of the employee may be through telework from an alternate worksite. For example, if inclement weather or other emergency situation results in a transportation shutdown, but phone lines remain working, the employee may be able to work from home rather than reporting to the traditional worksite or COOP site.

Employees designated as COOP Team Members may be required to telework during emergency closures or other emergencies, including pandemics and for COOP exercises, on any day, even if that day is not a regular telework day or a day with specific approval for situational/episodic telework. Telework-ready employees may also be required to perform duties outside of their usual or customary duties to ensure continuation of agency-essential missions or activities.

In accordance with Public Law 111-292 Section 6504(d)(2) "Continuity of Operations Plans Supersede Telework Policy – During any period that an executive agency is operating under a continuity of operations plan, that plan shall supersede any telework policy."