Federal Mobile Workplace Security:

An Interagency Security Committee Best Practice

Publication: August 2024
Cybersecurity and Infrastructure Security Agency

Message from the Interagency Security Committee

The Interagency Security Committee (ISC) vision statement is: "Federal facilities, the people who work at them, and those who visit them are safe and secure throughout the country." The ISC achieves its vision by establishing security policies, ensuring compliance, and enhancing the quality and effectiveness of security and protection of federal facilities. The ISC consists of 66 departments and agencies who work collaboratively to achieve its vision.

Federal Mobile Workplace Security: An Interagency Security Committee Guide, 2024 Edition is an update to the 2017 *Federal Mobile Workplace Security: An ISC White Paper*. This best practice provides practical resources and information to assist federal employees, their supervisors, and agency security personnel with a framework for understanding and mitigating risks posed to an organization when instituting a mobile workplace policy. Further, it outlines responsibilities for federal executive agencies, managers, and teleworkers in a setting heavily dependent on alternative work environments.

This best practice represents exemplary leadership from the Federal Mobile Workplace Security Working Group and collaboration across the entire ISC membership.

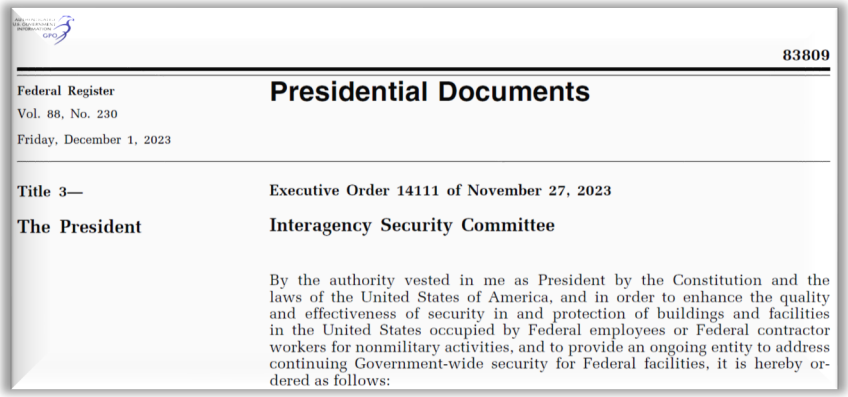
Table of Contents

1.0 Introduction

Federal Mobile Workplace Security has been a focus area for ISC members since the Telework Enhancement Act of 2010. This focus culminated with the publication of *Federal Mobile Workplace Security: An ISC White* Paper, 2017, designed to assist federal employees, supervisors, and agency security personnel with a framework for understanding and mitigating risks posed to organizations when instituting a mobile workforce policy.

The COVID-19 pandemic resulted in an almost immediate move by many federal employees to expand the use of telework and remote work in early 2020. To respond to this expansion of the mobile workforce, the ISC formed a new working group to review the best practices lessons learned by the federal agencies.

Since its establishment in 1995, the ISC has evolved over time, and its efforts have grown to include the virtual or cyber component to the federal facilities security profile. This evolution was recognized when the president signed the EO 14111: Interagency Security Committee tasking the ISC with providing "best practices for securing a mobile federal workforce."



83809

Federal Register
Vol. 88, No. 230
Friday, December 1, 2023

Presidential Documents

Title 3—
The President

Executive Order 14111 of November 27, 2023

Interagency Security Committee

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to enhance the quality and effectiveness of security in and protection of buildings and facilities in the United States occupied by Federal employees or Federal contractor workers for nonmilitary activities, and to provide an ongoing entity to address continuing Government-wide security for Federal facilities, it is hereby ordered as follows:

Continuing the original work, this *Federal Mobile Workplace Security, an Interagency Security Committee Guide, 2024 Edition* offers organizations new and relevant guidance on security considerations, both physical and cyber, for teleworking at home, in alternative workplace arrangements, and in public. Given the ISC's diverse membership, the working group drew upon a variety of subject matter experts to produce this document.

2.0 Applicability and Scope

Pursuant to the Authority of the ISC in EO 14111, Federal Mobile Workplace Security, an Interagency Security Committee Guide, 2024 Edition assists federal employees, supervisors, and agency security personnel with a framework for understanding and mitigating risks posed to an organization when instituting a mobile workplace policy.

Title 41, Code of Federal Regulations (CFR), Part 102-81, Physical Security is applicable to "federally owned and leased facilities and grounds under the jurisdiction, custody, or control of General Services Administration (GSA), including those facilities and grounds that have been delegated by the Administrator of General Services."[1] In 2022, the GSA amended 41 CFR § 102-81.25 "to clarify that federal agencies are responsible for meeting physical security standards at nonmilitary facilities in accordance with ISC standards, policies, and recommendations."[2]

40 United States Code (U.S.C.) § 1315 and the The National Security Memorandum on Critical Infrastructure Security and Resilience codify the U.S. Department of Homeland Security's (DHS) responsibility for protecting buildings, grounds, and property owned, occupied, or secured by the federal government; and establish U.S. policy for enhancing the protection and resilience of the Nation's critical infrastructure, respectively.

- 40 United States Code (U.S.C.) § 1315 vests the DHS Secretary with the authority and responsibility to "protect the buildings, grounds, and property that are owned, occupied, or secured by the federal government (including any agency, instrumentality or wholly owned, or mixed-ownership corporation thereof) and the persons on the property."
- The National Security Memorandum on Critical Infrastructure Security and Resilience "advances our national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure."

[1] …except where the Director of National Intelligence determines that compliance would jeopardize intelligence sources and methods, or the Secretary of Energy determines that compliance would conflict with the authorities of the Secretary of Energy over Restricted Data and Special Nuclear Material.

[2] See 87 FR 51915

3.0 Key Definitions

ANNOTATED SOURCES

1) 2021 OPM Guide to Telework and Remote Work in the Federal Government
2) 2020 GSA Internal Space Allocation, Design, and Management Policy

Table 1: Key Definitions

TERM	DEFINITION
Alternative Worksite (1)	Generally considered an employee's approved telework or remote site (e.g., an employee's home of record).
Desk sharing (2)	Sharing of a single workspace by two or more employees, each with a designated day or time to use of the workspace.
Hot desking (2)	Using non-dedicated, non-permanent workspaces on an unreserved, first come, first served basis (Also known as free address or touchdown workspace).
Hoteling (2)	Reserving and using non-dedicated, non-permanent workspaces as needed.
Telework (1)	An arrangement in which an employee, under a written telework agreement, is scheduled to perform their work at an agency worksite on a regular and recurring basis.
Remote work (1)	An arrangement in which an employee, under a written remote work agreement, is scheduled to perform their work at an alternative worksite and is not expected to perform work at an agency worksite on a regular and recurring basis. A remote worker's official worksite may be within or outside the local commuting area of an agency worksite.

4.0 Telework Enhancement Act

The issuance of the Telework Enhancement Act of 2010 was a pivotal moment in the federal government's ability to achieve greater flexibility in managing its workforce using telework.

With the growing interest in telework and remote work, the Office of Personnel Management (OPM) issued the *2021 Guide to Telework and Remote Work in the Federal Government: Leveraging Telework and Remote Work in the Federal Government to Better Meet Our Human Capital Needs and Improve Mission Delivery* in November, 2021. This guide provides practical resources and information, including a new policy section on remote work, for leveraging workplace flexibilities like telework and remote work as strategic management tools to meet mission-critical organizational needs while balancing the needs of a changing workforce. Further, it outlines responsibilities for federal executive agencies, managers, and employees who telework or engage in remote work.

When establishing a telework program, organizations should review the information found on OPM's Telework.gov website and familiarize themselves with its resources and policy guidance for agency telework managing officers and telework coordinators, managers and employees, including annual telework reports, frequently asked questions, training and legislation.

5.0 Security Considerations for Telework and Remote Work

Federal organizations rely on alternative worksites and workspace strategies to create flexible work environments and schedules, and support continuity of operations. For employees to be optimally productive at an alternative work site, they require access to the same services used at the physical federal facilities, including data, e-mail, collaboration tools, and in some instances, audio and video services. The federal transition to FedRAMP[3] compliant cloud-based services have, in many cases, made the access, delivery, and security of services location independent. Further, FedRAMP is mandatory[4] for cloud-based services utilized by federal agencies and departments.

> "*The term 'telework' or 'teleworking' refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work,*" *5 U.S.C. 6501(3)*.

As stated in the *2021 Guide to Telework and Remote Work in the Federal Government*, "Federal agencies and staff are responsible for the security of Federal Government property, information, and information systems. Telework and remote work do not change this responsibility. If not properly

[3] The Federal Risk and Authorization Management Program (FedRAMP) provides a standard approach to security authorizations for Cloud Service Offerings.

[4] Refer to OMB "MEMORANDUM FOR CHIEF INFORMATION OFFICERS", 8 December 2011.

implemented, telework and remote work arrangements may introduce vulnerabilities into agency systems and networks."

The National Institute of Standards and Technology (NIST) is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all federal agency operations and assets. The Federal Information Security Modernization Act of 2014 amends the Federal Information Security Management Act of 2002 (FISMA) and provides several modifications modernizing federal security practices and addressing evolving security concerns. Organizations should refer to the NIST Computer Security Resources Center for more information.

Real-World Incident

A defense contract employee unlawfully introduced an unapproved external hard drive to his work laptop. The FBI found that he downloaded and stored hundreds of sensitive documents. Search warrants resulted in more than 3100 electronic files and more than 110 paper documents in his possession including over 570 documents marked as containing classified information.

When establishing telework and remote work programs, organizations should consider:

- Security policies outlining who may telework or remote work, services available to those working at approved alternate worksites, information restrictions, maintenance guidelines, Virtual Private Network (VPN) information, training, and user guidelines.
- Written telework and remote work agreements with clearly defined duties, responsibilities (including security considerations), and conditions of participating.
- Approved alternate workspace self-certification checklists to ensure the alternate worksite is safe and suitable. Following a checklist will reduce risk and ensure adherence to organizational telework and remote work policy.
- Implementing training programs encompassing the risks of telework and remote work with topics such as Operational Security (OPSEC), information security, phishing emails, social engineering, and telework and remote work best practices and fundamentals.
- Reasons for decisions to deny, suspend, or limit telework and remote work participation. Supervisors are responsible for enforcing telework and remote work agreement violations. These agreements should specify the conditions warranting disciplinary action.

According to NIST Special Publication 800-46 Rev. 2, Guide to Enterprise Telework Remote Access & BYOD Security | CSRC (nist.gov), organizations should:

- Develop telework and remote work-related security policies and controls based on the assumption that approved alternate worksites contain hostile threats.
- Develop a telework and remote work security policy that defines telework and remote work, remote access, and "Bring Your Own Device" (BYOD) requirements, if applicable.
- Secure remote access servers and configure them to enforce telework and remote work security policies.
- Secure organization-controlled client devices against common threats and maintain their security regularly.

- Establish separate, external, dedicated network for external devices (BYOD, third-party controlled) if permitted in the facility.
- Government Furnished Equipment (GFE) and BYOD may differ in security requirements to mitigate risk. Clearly define each device's purpose in the organization's telework and remote work security policy and user agreement. NIST SP 800-46 *Guide to Enterprise Telework Remote Access and BYOD Security* provides advice on creating GFE and BYOD security policy. **Table 2** provides an example of how an organization may separate access.

Table 2: Example of Access Tiers [5]

Application or System	GFE in Office	GFE Telework/ Remote Work	BYOD in Office	BYOD Telework/ Remote Work	Contractor, Partner, Vendor in Office	Contractor, Partner, Vendor Telework/ Remote Work	Third Party (Internet Café, etc.)
Intellectual Property	Yes	No	No	No	No	No	No
Financial System	Yes	Yes	No	No	No	No	No
Personnel System	Yes	No	No	No	No	No	No
Email	Yes	Yes	Yes	Yes	Yes	No	No
Calendaring	Yes	Yes	Yes	Yes	Yes	No	No

Properly protect sensitive information. The following is a list of key regulations, standards, and guidelines. For additional information, see section 7.

- Federal Information Security Modernization Act (FISMA) of 2014
- Privacy Act of 1974, as amended
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Executive Order 13556 - Controlled Unclassified Information (CUI)

[5] NIST SP 800-46 *Guide to Enterprise Telework Remote Access and BYOD Security*

5.1 General Security Practices

Regardless of how organizations adopt and implement a telework or remote work program, there are several general security practices all participants should follow including:

Complete related training courses:

- Telework / Remote Work
- Cybersecurity Awareness
- Insider Threat
- Security Education and Awareness
- Operations Security

Follow email security best practices:

- Confirm email sender is valid before opening attachments.
- Hover over email links to verify legitimate source.
- Be aware of emails creating a sense of urgency or containing misspellings and grammatical errors.
- Report potential phishing attacks to the designated security office.
- Encrypt emails containing sensitive information.

Use Multi Factor Authentication (MFA):

MFA requires users to present two or more authentication factors at login to verify identity prior to access. A typical MFA login would require some combination of the following:

- Something you know—a password or Personal Identification Number (PIN)
- Something you have—a smart card, mobile token, or hardware token
- Some form of biometric factor (fingerprint, palm print, or voice recognition)

Refer to "Multi-Factor Authentication Fact Sheet," https://www.cisa.gov/sites/default/files/publications/MFA-Fact-Sheet-Jan22-508.pdf

Adopt strong passwords:

Passwords should be adequately complex and should not contain simple patterns or personal data. Birthdays, names, and number sequences are examples of weak passwords that should be avoided, as they can be easily guessed. A strong password should include a combination of the following:

- Be at least 16 characters in length,
- Be randomized using mixed-case letters, numbers, and special characters (!@#$%^&*) or contain a series of unrelated words
- Be unique across each account.

Practice safe internet browsing:

- Verify website address begins with “https” and has a padlock icon in the address bar.
- Review website privacy policies.

Follow your agency’s policies on removable media:

- Only connect familiar/approved devices to your workstation.
- Exercise caution when accessing files on removable media; they may contain malware.

Additional Security Considerations

- Use only authorized mechanisms, such as agency-provided VPN or other authorized remote access applications.
- Keep operating system and antivirus software up-to-date and maintain personal firewalls on devices used to access the agency network.
- Make regular backups of critical data according to agency policies. Refer to agency policies for more information on cyber security measures.
- Only use agency-approved video conferencing, collaboration tools and methods to share files.
- Always secure paper files out of plain view when transporting, such as in a vehicle’s trunk or lockable luggage when commercially travelling.
- Maintain possession at all times of computers or devices (do not leave them unattended or unsecured such as in plain view inside of a vehicle or in a checked luggage when travelling). Always carry them on a commercial carrier.

In addition, all agencies should continue to implement the recommended actions to protect remote information found in the Federal Information Processing Standard (FIPS) 140-3 encryption module.

5.2 Operations Security (OPSEC) Practices

National Security Presidential Memorandum (NSPM)-28, the National OPSEC Program, directs all departments and agencies to implement an OPSEC program. The basic principles of OPSEC for protecting generally unclassified information are applicable at approved telework and remote work sites. Employees should contact the organization's OPSEC program manager regarding threats, risks, and vulnerabilities to information, equipment, operations, etc., critical to mission-essential functions, and possible countermeasures to protect them. Employees should understand the basics of the six-step process to perform OPSEC evaluations and determine practical best practice mitigations for whichever environment they are in. Appendix A provides an OPSEC Reference for employees.

Analyze threat: When it comes to OPSEC, it is important to understand no matter what the job and department or agency, there is an adversary. They might not be a known adversary of the U.S. or a well-known non-governmental organization, but they exist, nevertheless.

Identification of critical information: In its simplest form, critical information is necessary to perform the job to ensure an organization's successful mission accomplishment.

Analyze vulnerabilities: Weaknesses in a device, system, or process adversaries can exploit to gain unauthorized access to critical information or deny access to it by authorized users; the act of obtaining critical information through human exploitation, such as social engineering and phishing.

Assess risk: An OPSEC risk assessment is a determination of what exposure to loss or compromise is acceptable given the value of information deemed critical relative to an organization's operations.

Application of countermeasures: Any action intended to reduce an identified risk and deter exploitation of critical information by an adversary. The intention of countermeasures is to defeat or delay adversarial actions to a point of acceptable risk and they can be employed using existing capabilities.

Assess effectiveness: Determine effectiveness of the program and countermeasures to evaluate if current practices are working or if adjustments need made.

5.3 Revoking Physical and Logical Access for Remote Workers

An agency may determine that a remote work arrangement no longer meets the business needs of the organization or that the arrangement negatively impacts the employee's performance. However, terminating a remote work arrangement, particularly if the employee resides outside the local commuting area of the agency worksite, may require additional considerations. If the decision is made to terminate the remote work arrangement for business reasons, there may be cost implications for the agency to consider (see OPM FAQ: Can a manager terminate an existing remote work arrangement)

Revoking physical and logical access for separating remote workers is both necessary and required but can be more challenging than in a traditional worksite[6]. The best practice is to physically collect the PIV card from the employee.

The process for revoking a PIV card can vary depending on the organization and its specific requirements, but generally this process includes disabling the card from the system, deactivating the card, and destroying physical cards. FIPS 201-3, PIV of Federal Employees and Contractors | CSRC (nist.gov) provides authoritative guidance. Specifically, FIPS 201-3 notes termination procedures must be in place.

- If the PIV Card cannot be collected and destroyed, the certification authority **MUST** be notified, and the PIV authentication key and asymmetric card authentication key **MUST** be revoked.
- The certificates corresponding to the digital signature and key management keys **SHALL** also be revoked, if present.
- Card management systems **SHALL** be updated to reflect PIV Card termination and method of termination (PIV Card destruction for collected PIV Cards or certificate revocations for uncollected PIV Cards).
- If the card cannot be collected, normal termination procedures **SHALL** be completed within 18 hours of notification.
- In certain cases, 18 hours is an unacceptable delay and in those cases emergency procedures **SHOULD** be executed to disseminate the information as rapidly as possible.

Contracting companies should notify their COR as soon as possible in advance of a separation involving a contract employee with logical or physical government access. The organization needs to have procedures in place for this information to get from the COR to those who can affect revoking physical and logical access in a timely manner.[7]

Emergency procedures should include coordinating with the security provider (such as Federal Protective Service) to issue a 60–90-day Be on the Lookout (BOLO) on the separating individual so

[6] For additional considerations for separating remote employees see How should an employer terminate a remote employee? (shrm.org)

[7] See the ISC Guide on Managing Risk of Adverse/Involuntary Separations

that the guard forces at visitor access points are aware. The organization should also consider requesting assistance from the security provider in the event the remote employee refuses to return the PIV card or government furnished equipment.

5.4 Securing Sensitive Systems and Sensitive Information for Employees Working in Alternative Worksites

Sensitive information is defined as any information, which the loss, misuse, or unauthorized access to or modification of, could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled, but which 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[8].

Sensitive Information Includes

- Chemical-Terrorism Vulnerability Information (CVI)
- Protected Critical Infrastructure Information (PCII)
- Sensitive Security Information (SSI)
- Personally Identifiable Information (PII)
- Agency Specific Sensitive Information Markings

Except for certain types of information protected by statute (SSI, PCII), there are no specific federal criteria and no standard terminology for designating types of sensitive information. Such designations are the discretion of each individual federal agency.

There is an online repository listing categories and subcategories of CUI approved by the CUI executive agent for protection at https://www.archives.gov/cui. For Official Use Only (FOUO) and sensitive information may also be CUI; although these terms are interchangeable, this document uses the term "sensitive information" to include all.

Telework and remote work employees should secure all sensitive information when unattended. They should also be familiar with, understand, and comply with their agency's information security policies and complete agency information security training. Depending on the sensitivity of the information and the agency's policies, the home office may require additional security measures such as lockable file cabinets, like those used in the worksite.

The Privacy Act, 5 U.S.C §552a specifically prohibits an agency from disclosing any record contained in a system of records by any means of communication to any person or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains. There are twelve exceptions to the "release without consent" provision of the Privacy Act. The one most applicable to federal agencies allows release to those officers and employees of the agency which maintain the record and need the record in the performance of their duties.

Personally identifiable information (PII) is defined in the Office of Management and Budget (OMB) Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information,* as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information linked or linkable to a specific individual. PII includes

[8] National Institute of Standards and Technology Glossary of Terms.

common data elements such as names, addresses, etc., or documents used for identity theft, such as social security numbers, passport numbers, etc. PII can also be derogatory, medical, or biometric information.

For further protection considerations, please see Appendix C.

5.4.1 Securing Sensitive Information When Working from Home or Alternate Location

Sensitive information would be detrimental to organizational security if publicly released. Employees should take reasonable steps to prevent unauthorized disclosure of sensitive information by demonstrating these best practice examples:

- Minimize printed documents and maintain a secure, lockable container or room to store sensitive materials when not in use.
- Maintain documents containing sensitive information only if necessary. Record copies of documents containing sensitive information as required by agency record disposition schedules and stored in the agency's official records site.
- Properly secure documents containing sensitive information; electronic copies are password protected or encrypted.
- A home office should be in an area where other individuals are not able to see sensitive information or overhear discussions involving sensitive information and that allow for securing sensitive information in a locked room or container.

5.4.2 Reporting a Breach or Loss of Sensitive Material

Safeguarding PII in the possession of the government and preventing its breach are essential to retaining the trust of the American public. Additionally, as indicated above, there are strict requirements for disclosure of PII detailed in The Privacy Act, 5 USC §552a and failure to adhere to these requirements can result in a breach.

Though OMB M-17-12 does not set policy and provides some latitude for agencies to develop forms and procedures based on the needs of their organization, it does set forth the minimum requirements for responding to a breach. A breach includes loss in any media, including physical documents, portable electronic storage media, inadvertent disclosure, public websites, and oral disclosure. Individuals discovering the breach must report the confirmed breach or suspected breach as soon as possible. This includes while working in the office, teleworking, a remote location, or while traveling.

> OMB M-17-12 defines a breach as:
>
> *The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where:*
>
> *(1) a person other than an authorized user accesses or potentially accesses PII, or,*
>
> *(2) an authorized user accesses PII for an unauthorized purpose.*

Agencies should consider a readily available and published e-mail account for agency employees and contractors to notify responsible officials of a breach. Timely reporting can minimize the impact/damage of the breach and it is imperative all employees and contractors know where and how to report a breach.

Agencies are required by OMB M-17-12 to develop a breach response plan tailored to their agency. As a minimum, each agency will develop a standard internal reporting template tailored to their agency. In creating a standard internal reporting template, the agency should include as many of the data elements and information types as are relevant to its missions and functions. A sample of a breach report is available at Appendix 1 to OMB M-17-12.

The level of reporting required depends on several factors, including but not limited to, types of information, number of individuals involved, and extent of the breach, such as an individual e-mail about one person versus a system breach of multiple records. Reporting the breach to the responsible organization official and using the organization's specific template as soon as possible will provide the appropriate information necessary to determine the level of reporting required.

Breaches where the confidentiality, integrity, or availability of a federal information system of a civilian, executive branch agency is potentially compromised must be reported to the DHS NCCIC/US-CERT within one hour of being identified by the agency's top-level Computer Security Incident Response Team (CSIRT). Therefore, providing all available information on agency forms as expeditiously as possible is imperative. Do not delay reporting based on not having all the details; file supplemental reports after the initial report as required.

6.0 Telework or Remote Work Risks

Organizations should consider the security risks, such as theft of identification and passwords, for the various telework and remote work arrangements when creating a telework or remote work policy. NIST SP 800-46 Guide to Enterprise Telework Remote Access and BYOD Security notes "telework devices are used in a variety of locations outside the organization's control, such as users' homes, coffee shops, hotels, and conferences. The mobile nature of these devices makes them more likely to be lost or stolen, which places the data on the devices at increased risk of compromise."

Organizational security elements should consider the baseline threat ratings and target attractiveness found in the *ISC Design-Basis Threat (DBT) Report*[9]. The DBT details the threat of cyber-attacks to include unauthorized access, interruption of services, and modification of services to federal facility Information and Communication Technology (ICT).

Telework locations generally rely on functioning commercial infrastructure (e.g., water, power, internet, etc.). Some tasks with near-zero downtime tolerances or that may be critical during an emergency incur high levels of risk when they are performed at locations susceptible to infrastructure disruptions and outages. The decentralized nature of telework and remote work can

[9] For more information on the DBT, refer to The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard.

also make workforce accountability and developing a common operating picture challenging when commercial communications are degraded or disrupted.

A potentially overlooked risk is the alternate workspace located within federal facilities. With higher rates of telework in alternate office locations, employees are less familiar with their surroundings. This may impede their ability to observe and identify suspicious behavior in the office space. An Occupant Emergency Plan (OEP) should outline procedures specifically addressing workers in alternate workspaces.

Telework and remote work rules or security protocols and procedures may vary by location. For example, it may be acceptable to use a personal computer for reading organizational email but not to access sensitive data.

The following sections discuss specific security considerations for different telework and remote work arrangements.

6.1 Telework or Remote Work at Home

Teleworking and engaging in remote work from an employee's home creates unique challenges and risks. Most home offices do not include physical security countermeasures found in traditional agency worksites, to include integrated access control and intrusion detection features (e.g., security containers, armed guards, card readers, video surveillance). Additionally, for employees working in a home environment, it may be easier to become complacent when it comes to protecting sensitive information.

Each organization should establish policies on types of equipment to use while teleworking or working remotely (GFE, personal computers) designed to reduce identified risks. Organizational policies should specify that use of GFE family members and friends is unauthorized.

Telework and remote workers are responsible for the security of all official data and protection of any GFE and property when working from an approved alternate location.

6.1.1 Physical Security Considerations at Home

Crime Prevention Through Environmental Design (CPTED) is a widely accepted approach that considers environmental conditions and the opportunities they offer for crime and other undesirable behaviors. The application of CPTED concepts and practices can be useful in reducing security vulnerabilities to an employee's home by using elements of the environment to:

- Control access
- Provide opportunities to see and be seen
- Define property ownership
- Encourage the maintenance of the property

The following are selected CPTED best practices employes should consider implementing at their home (at employee expense) if utilizing the home as an approved alternative worksite:

- Trim the landscaping to prevent places of concealment for intruders.
- Ensure that doors and windows are free of obstructions, such as bushes, shrubs, and tree foliage, so that there are clear site lines from inside.
- Consider installing motion sensing external lighting that illuminates areas around the home and eliminates shadowy areas.
- Consider installing a home alarm system with internal motion sensing.

Employees should have a working space separate from their living space and designate one space or area in the home with the best environment to secure and accomplish the work. Additionally, employees should employ the many effective security practices, which include:

DO

- Protect information about yourself and destroy all envelopes or other items revealing your name or other personal information.
- Check references of contractors, landscapers, house cleaners.
- Brief family members on your residential security and safety procedures.
- Advise associates or family members of your destination and anticipated time of arrival.
- Ensure sufficient illumination exists around your residence.
- Be alert to strangers who are on or near property for no apparent reason.
- Secure sliding doors.
- Utilize social media, especially neighborhood oriented social media to learn specifics about your neighborhood.
- Establish and/or participate in a neighborhood security watch program.

DON'T

- Give out information regarding family travel plans or security measures and procedures.
- Use your name on answering machines (landline and cell).
- Identify yourself as a government employee on social media platforms.
- Open the door to anyone without first identifying the person through a side window or peephole viewer.
- Hide any house keys outside your home.
- Keep valuables in-sight.
- Leave windows and doors unlocked.

6.1.2 Cybersecurity Considerations at Home

If the agency policy allows telework and remote workers to use personal equipment, do not allow others to access government files and information, or inadvertently corrupt the files and agency's information system[10]. Practices include:

Update your devices:

- Confirm antivirus software and security patches are up to date on your work and personal devices.
- Enable automatic updates wherever possible.
- Report unexpected computer behavior.
- Reach out to Internet Service Provider (ISP) on a recurring basis to ensure the router is using the most updated firmware.

Secure your home's wireless network (see Appendix B):

- Change the network default administrator password. Do not share network password.
- Only allow people you trust to connect to your network.
- Use strongest available encryption to protect your network activity.
- Segment your home network.

Use organizational provided equipment for work purposes:

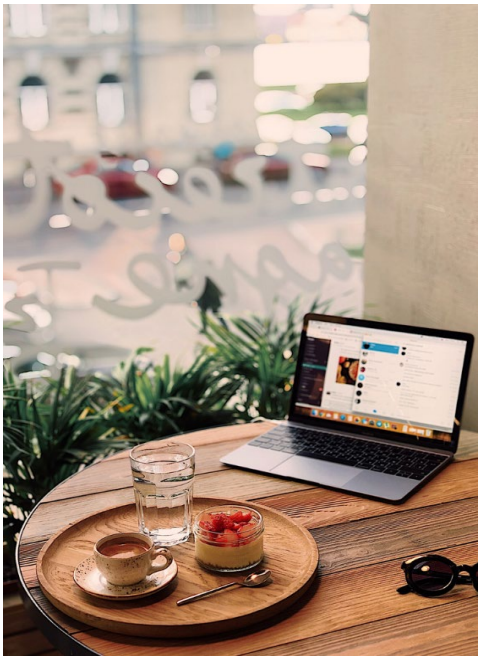
- Use work equipment for work-related business only.
- Inform family and friends not to access your work equipment.
- Confirm you are only connecting authorized devices to your work equipment.
- Lock your screen when leaving work devices unattended.
- Store work-related hard copy materials and equipment in a secure location.

Be smart about smart devices in the home:

- A smart device is any piece of electronic equipment connected to other devices through a wireless network, including phones, thermostats, doorbells, locks, refrigerators, tablets, watches, glasses, etc.
- Employees need to be sensitive to external voice enabled smart devices in their home if they are in the same room the employee is working.
- **Conduct sensitive work-related calls away from voice enabled smart devices.**

[10] See example of compromised equipment; https://krebsonsecurity.com/2022/05/when-your-smart-id-card-reader-comes-with-malware/.

6.2 Teleworking in Public Spaces



Teleworkers should be aware of the potential for physical security and cybersecurity risks when working in public spaces, such as airports, parks, coffee shops, or libraries. Each organization should determine their own policies on teleworking from public spaces based on mission operations and requirements.

External or third-party network connections in public spaces significantly increase the cyber risks for telework devices and communications. The physical risks and threats also increase while using a laptop or mobile devices in public spaces. Additional information to provide a more secure teleworking environment in public spaces can be found in NIST Special Publication 800-114 Revision 1, User's Guide to Telework and Bring Your Own Device (BYOD) Security.

6.2.1 Physical Security Considerations in Public Space

The potential for physical security risks in public spaces may be greater than in the home or office. The single best measure against risk in public spaces is **situational awareness**.

Situational awareness is observations, which assist in assessing risk, thus identifying required protective measures. In physical security, this concept refers to one's ability to be aware of surroundings and respond to immediate or potential threats. Security awareness training should provide employees with the necessary skills to identify risks.

Steps to reduce the physical security risk and threats of working in public spaces include:

DO

- Cover equipment identification markings that may identify your specific organization.
- Be aware of background noise that may cause interruptions or interference during mobile phone or video conference calls or create an impedance to the conversation.
- If using a mobile phone, video conferencing, or instant messaging, speak quietly and choose locations where your conversations and screens remain private.
- Identify multiple exit routes.
- Identify privately owned Video Surveillance System (VSS) camera locations and potential areas of coverage to ensure the screens of your devices are not visible or in "line of sight" to the camera(s).
- Be aware of others recording or live streaming in public.
- Be aware of others utilizing passive listening devices (cell phones, smart watches, and smart assistants).
- When working with a colleague(s), identify a primary and alternate location to meet, if separated.
- Watch for suspicious behavior in others, including individuals asking unusual or inappropriate personal and/or professional questions (social engineering).
- Notice and report suspicious items or objects, visit the If You See Something, Say Something site for more information.
- Consider the use of a screen privacy filter to ensure data is visible only to the user directly in front of the monitor.

DON'T

- Lose possession of computers or devices (do not leave them unattended or unsecured such as in plain view inside of a vehicle or in a checked luggage when travelling).
- Do not leave paperwork files exposed or unsecured for others to read or steal.
- Leave current sessions unlocked when stepping away from the computer laptop or device and remove the PIV card from the reader.
- Do not display a PIV card, wear clothing with government agency symbols or logos or identify yourself as a government employee unless acting in an official capacity.
- Do not develop predictable patterns (going to a coffee shop and sitting in the same seat on the same day of the week).
- Work at areas where others make you uncomfortable or something does not feel right.
- Draw attention to yourself. During travel, stay vigilant by incorporating personal protective measures and be inconspicuous. Be cautious in high-risk areas such as lobbies, nightclubs, and other public spaces. Be aware of potential safety havens such as police stations and hospitals, monitor media where you are staying, and avoid demonstrations.
- Sit where you cannot observe others coming and going or where they can observe your screen. Instead choose a location where you can sit with your back to a wall.

6.2.2 Cybersecurity Considerations in Public Space

Before conducting business in public settings, users should obtain explicit authorization from their organization and not expect any privacy. Vulnerabilities still exist such as masquerading, exploiting via radio interfaces, and network sniffing even when using GFE with a VPN, which carry sensitive information over an unsecure network. Because this often allows full access to an internal government agency network, VPNs are attractive targets to hackers.

The following are tips when connecting from a public unsecured or secured internet connection (public WiFi or Hotspots):

- Update devices over trusted (agency, home) networks.
- Use a VPN or other authorized secure access solution provided by the agency or organization.
- Activate the VPN session immediately after connecting to a third-party network.
- Use firewall and malware protection against intrusion.
- Encrypt files, hard drives, and external memory devices with multi-factor authentication and backed-up on the agency network regularly.
- Remove PIV card from laptop when not in use to prevent inadvertent disclosure of information.

6.3 Using Alternative Workplace Arrangement Strategies

Planning considerations for a secure alternative office workplace are vital. Alternative workplace strategies are work arrangements wherein an employee may not have a dedicated or assigned workspace at the regular (agency) worksite, but instead uses desk sharing or hoteling. In some cases, this may require the employee to work on different floors or even in a different building. As a result, it is important that employees make themselves aware of the different workspaces to include emergency exits.

6.3.1 Securing Sensitive Information

Hoteling, shared workspaces, hot desking, etc., require additional precautions to protecting sensitive information.

- Avoid maintaining hard copy documents containing sensitive information and encrypt or password protect documents stored on shared devices.
- Consider temporary day locker storage for documents, laptops, or electronic media containing sensitive information.
- Enforce a clean desk policy to prevent inadvertent access when employees are away from their workspace.

6.3.2 Hot-Desking and Hoteling

Some organizations use mobile workplace strategies known as "hot-desking" and "hoteling." Although often viewed as the same, they are different, and each has unique security considerations.

Hot-Desking

Using non-dedicate and non-permanent workspaces on an unreserved, first come, first served basis.

- Use an anti-theft cable secured to the laptop.
- Use secure lockers to keep these devices safe, accessible only to the keyholder.
- Provide security escort for visitors hot desking or working in a secure alternative workspace.
- Provide instructions on installing printers and mark all printers with appropriate information to identify during installation.
- Provide ways for locating other employees in the building.

Hoteling

Reserving and using non-dedicated, non-permanent workspaces as needed.

- Use a hoteling app to effectively manage the space.
- Provide a reservation system for securing workspace with check-in and automatic cancelation for no-shows.
- Implement cleaning and sanitization procedures.
- Offer both open office desks and closed offices for diverse types of workers (some need privacy, others prefer being amid the hustle and bustle).
- Offer a quick-read manual with login details, WiFi network and password, phone extension, and answers to frequently asked questions.
- Create a clean-your-desk policy instructing employees on how to reset desks after work.
- Offer storage facilities, such as a locker, to enable employees to leave some of their belonging in the office (without taking up desk space).
- Provide peripherals to support a laptop such as power, computer charger, and mouse.

6.3.3 Emergency Planning

Organizations using alternative workplace arrangement strategies should review their OEPs to accommodate the alternative workspace strategy. Employees may be working on a variety of floors, in different facilities, or with differing numbers of other employees present on any given day. Refer to Occupant Emergency Programs: An Interagency Security Committee Guide for additional guidance.

OEP considerations for alternative workplace arrangements:

- Identify the designated official (DO), responsible for developing, implementing, and maintaining an OEP as defined in Title 41 § 102-71.20).
- Involve key stakeholders, such as building managers; the security organization (Federal Protective Service - FPS); the owning/leasing organization (GSA); medical personnel; human resources; legal counsel; and lessors and union leadership, if applicable.
- Expand the number of employees included in the occupant emergency organization.
- Place emergency items like first aid kits, flashlights, floor warden materials, etc., in a common marked location for each floor and facility.
- Train multiple floor monitors as applicable to ensure coverage of the office/facility when occupied.
- Train employees in basic emergency actions regardless of telework location, to include Run, Hide, Fight for active shooter.
- Train employees to check for evacuation routes and exits for each facility or floor they are occupying.
- Encourage employees to carry small "grab-and-go-kits" to with them to different telework locations.
- Clearly mark exits and place evacuation route maps placed in areas employees can easily find and familiarize themselves.
- Ensure building communication systems are working.

6.4 Telework in an Overseas Environment

Employees must have an approved Domestic Employees Teleworking Overseas (DETO) arrangement to work from a foreign location. DETOs are overseas telework arrangements wherein the federal executive branch employee performs the work requirements and duties of his/her/their domestic Civil Service of Foreign Service (FS) position from an approved overseas location via a DETO Agreement.

Employees should avoid using a PIV as a form of identification and follow their agency cybersecurity guidance and foreign travel policy. Employees with questions on their agency DETO policy should direct inquiries to the agency telework coordinator and/or human resources office. For additional information on DETO policy, email: DETOPolicy@State.gov.

6.4.1 Employee Security Considerations for Overseas Travel

- Review State Department Travel Advisories before taking international trips including to Canada or Mexico.
- Prior to travel, report travel plans and receive area of responsibility (AOR) specific threat briefing by security officer.
- Select an inside hotel room (away from the street- side window), preferably on the 4th–10th floors.
- When traveling via airline or commercial means, store laptops and sensitive documents at your seat. If this is not possible, use an overhead bin immediately adjacent to your seat. Do not put computers or sensitive documents in checked baggage.
- Know the location and contact information for the closest U.S. Embassy or Consulate and other safe locations (Red Cross/Crescent) where you can find refuge or assistance.

The Department of State's Authority Regarding Domestic Employees Teleworking Overseas

On October 14, 2022, the Department of State (DOS) distributed an Executive Secretary Memorandum, entitled '*Policy Requirements for Executive Branch Employees Teleworking from Overseas*,' also known as a Domestic Employee Teleworking Overseas (DETO) arrangement. The memorandum includes policy and DOS guidance on DETO agreement provisions setting forth minimum DETO requirements for inclusion in an agency's DETO policy. It applies to all federal executive branch agencies considering DETO agreements for their agency employees. The DOS policy requirements are in addition to the requirements addressed in the Telework Enhancement Act of 2010, supporting U.S. Office of Personnel Management policy and respective agency telework policies.

Reference: Overseas Telework - Telework.gov; DOMESTIC EMPLOYEE TELEWORKING OVERSEAS (DETO) (state.gov)

7.0 Continuity Planning

Continuity planning efforts can often be augmented with organizational telework and remote work capabilities. Presidential Policy Directive 40 (PPD-40), National Continuity Policy, directs the Secretary of Homeland Security, through the Administrator of the Federal Emergency Management Agency (FEMA), to coordinate the implementation, execution, and assessment of continuity operations and activities among executive departments and agencies. As part of this responsibility, the FEMA Administrator develops and promulgates Federal Continuity Directives (FCDs) that establish continuity program and planning requirements for executive departments and agencies.

Federal Continuity Directives (FCDs)

Establish the framework, requirements, and processes to support the development of continuity programs and defines continuity as the ability to provide uninterrupted services and support, while maintaining organizational viability, before, during, and after an event that disrupts normal operations. It further states that continuity of operations is an effort within the executive office of the president and individual departments and agencies to ensure essential functions continue during disruption of normal operations.

The FCDs, found in FEMA's Continuity Resource Toolkit,[11] provide direction to the federal executive branch for developing continuity plans and programs. Continuity planning facilitates the performance of executive branch essential functions during all-hazards emergencies or other situations disrupting normal operations.

Today's threat environment and the potential for no-notice emergencies (acts of nature, accidents, critical cyber and communication infrastructure emergencies, and nation-state or terrorist attacks) increase the need for robust continuity capabilities and planning. Modern advances in technology now make it possible for an enterprise to take advantage of capabilities allowing for continued operations under most circumstances. Federal entities should consider the benefits and potential risks of teleworking and mobile workplace strategies in their continuity planning.

Federal Continuity Directives (FCDs)

Provide direction and guidance to federal executive branch departments and agencies to assist in validation of mission essential functions (MEFs) and primary mission essential functions (PMEFs). They further outline requirements and provide checklists and resources to assist departments and agencies in identifying and assessing their essential functions through a risk-based process and in identifying candidate PMEFs that support the national essential functions (NEFs).

[11] Continuity Resource Toolkit | FEMA.gov

8.0 Training

Organizations must provide an interactive telework training program to eligible employees and their managers and require successful completion prior to entering a written telework agreement (5 U.S.C. 6503(a)(1), (2)). Employees are to undertake such refresher or modified training as directed by their organization. Organizations should consider a wide spectrum of training designed to assist the employees beyond basic telework requirements. Consulting with security, emergency management, and/or IT professionals helps to ensure adequate training. Suggested on-line training courses include:

Appendix A: OPSEC Reference for Teleworkers

OPSEC for Teleworkers

- Teleworkers should be familiar with their organizations Critical Information List (CIL).
- Teleworkers are responsible for protecting controlled unclassified information (CUI).

Teleworking DOs

- DO coordinate with the OPSEC Coordinator for additional guidance.
- DO use authorized data transfer, virtual meetings and cloud sharing tools.
- DO examine the surroundings while teleworking, not everyone has a need to know.
- DO use authorized document destruction methods.
- DO encrypt emails containing CUI, FOUO and Privacy Act data or critical information.
- DO verify security settings on commercial teleworking platforms.
- DO remember our adversaries continue to find vulnerabilities to exploit.
- DO remove the PIV from GFE whenever not in active use.
- DO turn on automatic patching and run anti-virus software.

Teleworking DON'Ts

- DON'T use workarounds to make teleworking "easier" or "faster."
- DON'T use social media to discuss work related topics or anything containing CUI.
- DON'T use personal cellular devices to discuss sensitive operations containing CUI.
- DON'T use non GFE devices to store or transmit sensitive data containing CUI.
- DON'T leave the device open so others can read the content on the screen.

Additional Resources

- Organization OPSEC Coordinator Info.
- Organization Security Manager.
- Applicable publications.
- Portal information.

Your Company Logo Here

Appendix B: Recommendations to Address Cyber Threats when Teleworking or Working Remotely from Home

B.1 Wired Network

Protect the network from internet threats by purchasing a router or switch with a built-in firewall. The router connects directly to a cable or digital subscriber line (DSL) modem on one interface and allows many computers to plug into the other interface.

Personal software firewalls and anti-virus software installed on a workstation may provide additional endpoint protection from malware when browsing the internet.

Do not install personal firewall software on an agency-furnished computer. Remember to change the router's default administrative password and, if possible, disable any management interfaces that can remotely access from an external Internet Protocol (IP) address (a web management interface that can provide access from outside your residence).

B.2 Wireless Network

Protect the wireless network from internet-based threats while securing the network against local threats to the wireless network. A personal network is accessible by neighbors and war-drivers (hackers who drive around trying to find non-secure wireless networks) up to several blocks away through high-powered antennas. Many of the same wired security principles apply to wireless networking. Ensuring the purchased wireless access points also include a router/switch/firewall is critical. If not, purchase the same type as defined in the wired paragraph above.

Remember to change the router's default administrative password and disable any remotely accessible management interfaces. Once secured from the internet threats, secure the wireless portion of the network. Implement the following settings on the wireless access point and computers:

- Enable WiFi Protected Access 2 (WPA2) on the wireless connection. WPA2 replaced WPA and Wired Equivalent Privacy (WEP) and is based on much stronger security protocols.
- Pick a strong passphrase for WPA2; CISA's Secure Our World[12] recommends making passwords at least 16 characters in length, using randomized mixed-case letters, numbers, and special characters or a memorable passphrase containing a series of unrelated words, and using a unique password for each account.

[12] For more information on creating strong passwords and for other online safety tips, see additional resources at https://www.cisa.gov/secure-our-world/use-strong-passwords

Implementing the settings above will not make the network impenetrable but will go a long way in reducing the risk. The user manual provided with the wireless access point should provide additional guidance for enabling these settings. See WiFi Alliance for additional security settings and enhancements.

B.3 Network Segmentation

Segmentation allows further securing of the wireless home network. It divides the home network into separate sub-networks or groups (for example a different sub-network for guests, Internet of Things (IoT) devices, personal computers, or a work computer). Segmenting the devices prevents them from communicating with each other and can prevent viruses from spreading from one device to the next. Setting up the segments can be as simple as using the guest WiFi network option available in most routers. However, in some cases, configuring the segments can be more complex. Users should refer to their router's manual for instructions and agencies should provide some general information on network segmentation. For more information on Network Segmentation, please see What Is Network Segmentation? - Cisco.

Appendix C: Protection Considerations

Telework and remote work require special precautions when handling agency information, especially sensitive or FOUO information.

Do not transmit classified information through unauthorized or unsecured channels. For transmittal of PII, limit access of PII only to those individuals authorized and with a business need.

C.1 Transmission of PII and Sensitive Information

Encrypt all sensitive information, such as PII, transmitted outside the agency firewall. Use certified encryption modules in accordance with Federal Information Processing Standards (FIPS) Publication 140-3, "Security requirements for Cryptographic Modules.

When sending PII by courier, mark "signature required" to create a chain of custody.

When printing documents containing PII, do not let documents sit on a printer where unauthorized personnel may have access to the information.

When faxing information use a secure fax line. If one is not available, contact the recipient prior to faxing, so they know information is coming. Contact the recipient after transmission to ensure they received it.

C.2 Encryption

When using password generated encryption keys, follow CISA's Secure Our World guidelines for creating a unique, strong password containing at least 16 characters with a randomized combination of mixed-case letters, numbers, and special characters or a passphrase of 4-7 unrelated words.

C.3 Training

Ensure agency training covers transportation of classified information.

C.4 Transporting Sensitive Information:

- When traveling by public conveyance, store laptops or documents containing sensitive information at your seat or, if necessary, under the seat or in the overhead compartment immediately adjacent to your seat. Do not place documents or laptops containing sensitive information in your checked baggage.
- When transporting documents or laptops containing sensitive information by car, do not leave the material unattended. If it is necessary to stop, secure the materials in the trunk or other location where they are not visible.

C.5 Hotel Room Storage:

- When it is necessary to stay in a hotel with sensitive materials, use the hotel safe (United States only) whenever possible to store documents and equipment.
- Avoid traveling with printed documents containing sensitive information when possible and ensure electronic copies are password protected or encrypted.
- Report any loss immediately.

C.6 Media Protection:

Hard copy data:

- Physically control and securely store information within controlled areas.
- Store in a lockable file cabinet or desk drawer restricting access to authorized individuals.
- Comply with federal laws and regulations related to records management.
- Protect information from accidental disclosure by using appropriate cover sheets and folders.

Electronic media:

- Protect documents or files containing sensitive information stored on shared drives, SharePoint, or other accessible sites by encryption, passwords, or access restrictions. Remove individual access when no longer required, such as due to transfer/separation.
- Properly mark documents or files containing sensitive information stored on shared drives, SharePoint, or other accessible sites.
- Deny access to documents and files containing sensitive information stored on to individuals until they have completed required training, including Privacy Act training.
- Sanitize data information systems prior to disposal or transfer to another office or agency.

C.7 Destruction of Sensitive Materials

Organizations should establish a formal process to approve employees and contractors to print and destroy sensitive information at home. An employee's supervisor or a contractor's federal lead in conjunction with the agency's information security office can give the employee/contractor permission to either properly shred PII themselves at home or transport back to the agency for proper disposal.

The employee's supervisor or contractor's federal lead, in conjunction with the agency's CUI, FOUO, or Sensitive Items Program Manager, must approve in writing the National Security Agency (NSA) approved shredder, or the agency must provide an acceptable shredder. See 32 CFR Part 2002 Implementing Directive for delegating authorities.

Appendix D: Individual Preparedness Continuity

FEMA recommends keeping several days' worth of basic supplies on hand when an emergency occurs. Consider location and the unique family needs to customize the kit. Individuals should also consider having multiple emergency go-kits, one for their home and smaller portable kits in their workplace, vehicle, or other places they frequent.

Table 3, Basic Emergency Go Kit contains some basic items to consider when building a personal emergencygo-kit. Please visit www.Ready.gov for more information regarding emergency personal preparedness.

Table 3: Basic Emergency Go Kit

- Water (one gallon per person per day for several days, for drinking and sanitation)
- Dust mask (to help filter contaminated air) and plastic sheeting and duct tape to shelter in place
- Food (at least a several-day supply of non-perishable food)
- Masks (for everyone ages 2 and above), soap, moist towelettes, hand sanitizer, disinfecting wipes to disinfect surfaces
- Manual or non-electric can opener for food (if necessary)
- Toilet paper, baby wipes, plastic gloves, garbage bags and plastic ties for personal sanitation
- Battery powered or hand crank radio with National Oceanic and Atmospheric Administration (NOAA) Weather capability and extra batteries
- Important family documents in waterproof container; including emergency contact lists
- Cell phone chargers and backup battery
- Local maps
- Flashlight and extra batteries, matches and candles
- Prescription medication, glasses, and contact lens solution
- First Aid Kit
- Non-prescription medications such as pain relievers, anti-diarrhea medication, antacids, or laxatives
- Whistle (to signal for help)
- Wrench or pliers (to turn off utilities)
- Cash or travelers checks
- Feminine supplies and other personal hygiene items
- Sleeping bags and warm blankets
- Complete change of clothing appropriate for the climate and sturdy shoes
- Fire extinguishers
- Mess kits, paper cups, plates, paper towels and plastic utensils
- Infant formula, bottles, diapers, wipes, and diaper rash cream
- Paper, pens, and pencils
- Pet food and extra water for any pets
- Books, games, puzzles, or other activities for children

After assembling the go-kit, maintain it so it is ready when needed. Replace expired items and update the kit as family needs change. Additionally, since you do not know where you will be when an emergency occurs, it is a good practice to prepare a go-kit for home, work, and cars.

D.1 Emergency Communications Plan

An emergency communication plan can collect vital information required to locate individuals and keep them connected. It also serves to remind everyone of the basic emergency plan in the event of an incident. The plan can be a training device for younger individuals to help them stay focused during an emergency in the absence of adult supervision. See *Table 4: Emergency Communications Plan* for key components.

Table 4: Emergency Communications Plan

- Personal identification information
- Alternative caretaker information
- School information
- Program emergency numbers into all phones
- Parent/guardian information
- Predetermined locations where the family will reunite
- Emergency meeting locations
- Alternate locations if returning home after an emergency is not feasible
- Important contact information
- Addresses and phone numbers of all meeting places

Familiarizing family members with and training them how to use the plan is also prudent. Steps to take include:

- ☐ Teach your children how to make telephone calls and how to dial 911 for emergency assistance.
- ☐ Know and practice all possible exit routes from your home and neighborhood.
- ☐ Get a copy of your child's school or daycare emergency plans.
- ☐ Make plans for where you can meet your child after an evacuation.
- ☐ Make sure the school has up-to-date contact information for all caregivers.
- ☐ Pre-authorize a friend or family member to pick up your child/children from school in case of an emergency.

Appendix E: Resources

E.1 References Cited

Cybersecurity and Infrastructure Security Agency (CISA)

- Multi-Factor Authentication Fact Sheet

Interagency Security Committee (ISC)

- EO 14111: Interagency Security Committee
- ISC Guide on Managing Risk of Adverse/Involuntary Separations

National Institutes of Standards and Technology (NIST)

- NIST SP 800-46 Guide to Enterprise Telework Remote Access and BYOD Security
- FIPS 201-3, PIV of Federal Employees and Contractors | CSRC (nist.gov)
- Federal Information Processing Standards (FIPS) Publication 140-3, "Security requirements for Cryptographic Modules
- NIST: Security Issues for Telecommuting

Office of Management and Budget (OMB)

- Memorandum M-17-12 Preparing for and Responding to a Breach of Personally Identifiable Information

United States Office of Personnel Management (OPM)

- Telework.Gov
- Telework Enhancement Act of 2010
- 2021 Guide to Telework and Remote Work in the Federal Government

Other

- FMR Bulletin 2006-B3 - Guidelines for Alternative Workplace Arrangements
- DHS If you See Something Say Something
- Federal Continuity Directive 1, Federal Executive Branch National Continuity Program and Requirements, January 2017
- Federal Continuity Directive 2, Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process, June 2017
- The Federal Information Security Modernization Act of 2014
- Federal Information Processing Standard (FIPS) 140-3 encryption module
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Privacy Act of 1974, as amended
- Ready.gov
- State Department Travel Advisories

E.2 List of Abbreviations/Acronyms/Initializations

ADA	Americans with Disabilities Act
AOR	Area of Responsibility
AWA	Alternative Workplace Arrangement
BYOD	Bring Your Own Device
CD	Compact Disc
CFR	Code of Federal Regulations
CIO	Chief Information Officer
COOP	Continuity of Operations
COR	Contracting Officer Representative
CPTED	Crime Prevention Through Environmental Design
CUI	Controlled Unclassified Information
CISA	Cybersecurity and Infrastructure Security Agency
CVI	Chemical-Terrorism Vulnerability Information
DHS	Department of Homeland Security
DOS	U.S. Department of State
DVD	Digital Video Disc
EO	Executive Order
FCD	Federal Continuity Directive
FECA	Federal Employees' Compensation Act
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FLSA	Fair Labor Standards Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FTCA	Federal Tort Claims Act
GFE	Government-Furnished Equipment
GLBA	Gramm-Leach-Bliley Act
GSA	General Services Administration
HIPAA	Health Insurance Portability and Accountability Act
HRO	Human Resource Office
IoT	Internet of Things
ISC	Interagency Security Committee
IT	Information Technology
NCSD	National Communications Systems Directive
NIST	National Institute of Standards and Technology
MEF	Mission Essential Function
OEP	Occupant Emergency Plan
OGC	Office of General Counsel
OMB	Office of Management and Budget
OPM	United States Office of Personnel Management
OS	Operating System

OSHA	Occupational Safety & Health Act
PA	Privacy Act
PCII	Protected Critical Infrastructure Information
PII	Personally Identifiable Information
PIV	Personal Identification Verification
PM	Program Manager
PPD	Presidential Policy Directive
SPII	Sensitive Personally Identifiable Information
SSI	Sensitive Security Information
TMO	Telework Managing Officer
U.S.C.	United States Code
VPN	Virtual Private Network
VSS	Video Surveillance System
WiFi	Wireless Fidelity
WPA	WiFi Protected Access

E.3 Glossary of Terms

Term	Definition
Agency Worksite	The regular worksite for the employee's position of record; the physical address or place where the employee would work if not teleworking.
Alternative Worksite	Generally considered an employee's approved telework or remote site (e.g., an employee's home of record).
Alternative Workplace Arrangement (AWA)	A work arrangement in which an employee uses hoteling, hot desking, or desk sharing when working instead of having dedicated/ assigned workspace at the regular (agency) worksite.
Bring Your Own Device	A telework client device that not controlled by the organization.
Client Device	A system used by a remote worker to access an organization's network and the systems on that network.
Client Site	A space used by a federal employee at a contractor or support contractor's facility on an intermittent basis; a space a contractor or support contractor uses at a federal facility on a regular or intermittent basis.
Consumer Device	A small, usually mobile, computer that does not run a standardPC OS or that runs a standard PC OS but does not permit users to access it directly. Examples of consumer devices are networking-capable personal digital assistants (PDA), cell phones/smart phones, and video game systems.
Controlled Unclassified Information (CUI)	A categorical designation that identifies unclassified information throughout the executive branch requiring the safeguarding of dissemination controls, pursuant to and consistent with applicable law, regulations, and government-wide policies.
Desk Sharing	An AWA in which two or more employees share use of a single workspace where each employee has a designated day or time for use of the workspace.
Direct Application Access	A high-level remote access architecture allowing teleworkers to access an individual application directly,without using remote access software.

Term	Definition
Fair Labor Standards Act (FLSA)	A federal law establishing minimum wage, overtime pay, recordkeeping, and youth employment standards affecting employees in the private sector and in federal, state, and local governments. The FLSA exempts specified employees or groups of employees from the application of certain provisions. Additional guidance may be found in the GSA Time and Leave Administration Policy HRM 6010.1 For more information, visit OPM.gov.
Government-Furnished Equipment (GFE)	Property owned by the government but in the possession of an employee or contractor that is necessary for performance of job or contract.
Hot Desking (also known as freeaddress or touchdown workstations)	An AWA in which employees use non-dedicated, non-permanent workspaces in the primary agency worksite on an unreserved first come, first served basis (typically drop-in).
Hoteling	An AWA where employees use non-dedicated, non-permanent workspaces assigned for use byreservation on an as-needed basis.
Mobile Work (Mobility)	Mobile work (mobility) refers to an employee's ability to work freely inside and outside the office. Mobility also encompasses all remote work functionally required for a job. Telework is a sub-set of mobility in which an employee works specifically at home or at an approved alternative worksite such as a satellite office.
Official Travel	Travel under an official travel authorization from an employee's official station or other authorized point of departure to a temporary duty location and return from a temporary duty location, between two temporary duty locations, or relocation at the direction of a federal agency.

Term	Definition
Official Worksite/Duty Station	Pursuant to the OPM definition and as set forth in 5 CFR 531.605, official worksite is the location where the employeeregularly performs their official work duties. Changes in an employee's official worksite may affect employee pay, locality pay, and travel funding responsibilities. Further, the servicing human resources office (HRO) must process the change. Designation of the official worksite must be determined on a case-by-case basis using the following considerations: • If the employee is to report physically at least twice during every biweekly pay period to an agency worksite, then that location is the official worksite. • If the employee is not to report at least twice per biweekly pay period to the agency worksite, the official site is the location of the AAW, except in certain temporary duty situations. This arrangement includes virtual workers/full time teleworkers. • The agency worksite is the official worksite for an employee if they do not report at least twice per biweekly pay period to the agency worksite and they are performing work within the same geographic area as the agency worksite. This is for the purpose of a given pay entitlement.
Personally Identifiable Information	Any information directly or indirectly inferring the identity of an individual, including information linked or linkable to an individual.
Personal Computer/Equipment	Any computer, laptop, iPAD, or other equipment that can support Windows Vista, Windows XP, Linux/Unix, and Mac OS X, etc.
Portal	A high-level remote access architecture based on a server offering teleworkers access to one or more applications through a single centralized interface.
Public Space	An area within a building with free access to the public, such as a foyer or lobby.
Remote Access	The ability for an organization's users to access its non-public computing resources from external locations other than the organization's facilities.
Remote Desktop Access	A high-level remote access architecture giving teleworkers the ability to remotely control a particular desktop computer at the organization—most often the user's own computer at the organization's office—from a telework client device.

Term	Definition
Sensitive Information	Any information, which if lost, misused, disclosed, or accessed without authorization, or modified, could adversely affect the national or homeland security interest, the conduct of federal programs, or the privacy of individuals, not specifically authorized under criteria established by an executive order or an act of congress to as secret in the interest of national defense, homeland security or foreign policy. Also identified as Controlled Unclassified Information (CUI). Sensitive Information includes: • Chemical-terrorism Vulnerability Information (CVI) • Protected Critical Infrastructure Information (PCII) • Sensitive Security Information (SSI) • Personally Identifiable Information (PII) • Sensitive Personally Identifiable Information (SPII)
Sensitive Systems	Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose, and that may be vulnerable to an adversarial attack through the violation or disruption the system's confidentiality, integrity, or availability.
Session Locking	A feature permitting a user to lock a session upon demand or automatically after the session has been idle for a preset period.
Social Engineering	An attempt to trick someone into revealing information(a password) used to attack systems ornetworks (ref. NIST 800-63-1).
Telecommuting	See "Telework."
Telework	A work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work.
Telework Client Device	A PC or consumer device used by a teleworker forperforming telework.
Telework Agreement	A formal written agreement between a supervisor and an employee permitting the employee to telework as defined within agency policy.
Telework Policy	Agency policy allowing eligible employees to participate in telework to the maximum extent possible without diminished employee performance.
Satellite Office	A small office in a different location from a company orgovernment agency's main office.

Term	Definition
Unscheduled Telework	A form of telework allowing employees to telework without previous supervisory approval in response to specific announcements by OPM or other local governmentdeciding/authorizing officials regarding emergency situations; a means for agency employees to continue work operations and maintain productivity during emergency situations.
Virtual Worker/Employee	A full-time teleworker whose official worksite (duty station) is an appropriate alternative worksite. The appropriate alternativeworksite may be inside or outside the local commuting area of the agency worksite and include such places as the employee'sresidence.
WiFi	A wireless networking technology that uses radio waves to provide wireless high-speed Internet access.

Acknowledgements

The ISC would like to thank the participants of the ***Federal Mobile Workplace Security Working Group.***

Federal Mobile Workplace Security Working Group

David Hess
Chair
Federal Protective Service

Tarkeisha Wills
Co-Chair
Office of Personnel Management

Subcommittee Members

Tonia Cardwell
U.S. Immigration and Customs Enforcement

Bradley Carovani
U.S. Citizenship and Immigration Services

Robert Carter
Department of Homeland Security

Namrata Dhindsa
Department of Energy

Neal Duckworth
Internal Revenue Service

Angela Dupont
National Capital Planning Commission

Derek Gaines
Department of Homeland Security

Jason Groves
Department of Commerce

Roger Hansel
Internal Revenue Service

Aaron Johnson Hearn
Department of Transportation

Jerald Hunter
Internal Revenue Service

Charles King
Federal Trade Commission

Octavia Morgan
National Labor Relations Board

Breanna Palmer
Department of Homeland Security

Liana Roberson
Customs and Border Protection

Vinay Singla
U.S. Citizenship and Immigration Services

Amy Szestak
National Security Council

Reggie Watkins
Customs and Border Protection

Christopher Wilson
U.S. Immigration and Customs Enforcement

Mark Wilson
National Science Foundation

Interagency Security Committee Support Staff

Daryle Hernandez
Branch Chief

Benjamin Adame
Security Specialist

Tarvis Bonner
Program Analyst

Robert Chaiet
Technical Editor

Jamie Craig
Technical Editor

Scott Dunford
Senior Security Specialist

Shawn Fiebiger
Deputy Compliance Program Manager

Harrison Heller
Policy Analyst

Glennell Kelly
Program Analyst