

August 2011

Most likely your office maintains space on a DHS shared network drive. Your office controls access to its portion of the shared drive through a folder-based security mechanism. Typically, access to your main folder is restricted to the staff on your office's main email distribution list.

If you want to restrict access to a particular folder within your shared drive, here's what to do:

1. Create/identify the folder you want to control.
2. Find the full path to that folder by:
  - a. Clicking on My Computer on your desktop.
  - b. Finding your network shared drive and right clicking it.
  - c. In the left NAV under "Details", the network drive path will appear, for example:
    - \\ZZA1CE-0350\dhs-g\DHS\Your Office\Your Folder
3. Create the name of an email distribution list that you'd like to use to govern access to the folder. Use something like "officename [folder]". Keep it short, simple, easy to recognize in the GAL. This email list becomes your security group, and as the manager of this group, you have the ability to add and remove names of users, as needed. To do this [once the email list is created], open the security list in the GAL, click "modify members", then add or remove users.
4. Identify who you want to have access to that folder – you will need full DHS email addresses.
5. Email IT Support and tell them you want to:
  - a. Restrict access to a folder. Send them the full path (step 2).
  - b. Create an email distribution list with the names you picked (step 3); and
  - c. Add all the names/email addresses to that distribution list and give each of those individuals "owner" rights to the distribution list – this way anyone in that list can change the list if you want to add/remove names. You can also pick one person and give them ownership rights to add/remove people from the distribution list. However you do it, it's key that someone you know can edit that list of names – this will give you control over who can access the folder.
  - d. Restrict access to that folder so that only users on the distribution list can access it. You can make this a little more complex by changing the tiers of control over the folder.
    - i. Full restriction/access – only those on the list can open the folder and once they're in they can do anything they want.
    - ii. Read only – you can allow anyone to read files in that folder – they cannot edit/delete anything – then only people on the distribution list can change.
6. Then get confirmation from IT Support, and conduct a test –
  - a. See if someone outside your new group can open the folder.
  - b. See if someone inside your group can open the folder and change stuff in it.
  - c. See if someone on your list can change the names on the list.

## Article: Helping Victims of Sexual Assault

Would you be prepared if a sexual assault victim came to you for help? What if you felt that someone was in danger of being sexually assaulted? Or if you witnessed an attack? Would you know what to do?

This article will teach you appropriate methods of interceding to prevent sexually violent situations and responding when someone else has been sexually assaulted.

### What do I do if I witness a sexual assault?

If you witness an assault or a potential assault, become an **active bystander**—look for safe and effective ways to intervene. If you are in a situation to act, remember these ABCs:

- **Assess the situation for safety:** Ensure the victim's safety and your own. Avoid violence. Call the police if the situation is too risky to intervene—they are specifically trained for such situations.
- **Be with others:** Don't intervene alone. Approach both the victim and offender in a courteous manner but be firm. By working with others, you will have greater influence over the outcome, as well as increased safety.
- **Care for the victim:** Even if you perceive a behavior as an assault, be sure to verify this perception by asking the victim how they feel about the behavior. Also ask whether they need medical care, want to talk to an Employee Assistance Program Coordinator (EAPC)/Sexual Assault Response Coordinator (SARC), or need help getting home.

### What are examples of actions I can take as an active bystander?

Here are actions you can take to prevent behavior that could lead to an assault or get involved when one does occur:

- Make up an excuse to give a potential victim a reason to separate himself or herself from a potential perpetrator.
- Let a bartender or host of a party know when someone has had too much to drink.
- Talk to the victim or potential victim to make sure he or she is okay.
- Address any disrespectful behavior in a manner that is courteous but firm to avoid violence.
- Call the police.
- Distract those engaged in sexist behavior (for example, if a man on the street is harassing a woman, you could ask him for directions or the time).

### What do I do if someone tells me that they've been sexually assaulted?

If someone tells you that they have been sexually assaulted, take the following actions:

- Make sure that the victim is safe.
- Ask the victim if he or she needs medical care.
- Transport the victim to receive assistance (such as to the Employee Assistance Program Coordinator (EAPC)/Sexual Assault Program Coordinator (SARC) or to medical care), if requested.
- Contact an EAPC/SARC, a Family Advocacy Specialist (FAS), a Health Care Provider (HCP), or a Victim Advocate (VA).
- Offer to stay with the victim.
- Listen to the victim.
- Ask what you can do to help.

#### Did You Know?

Confronting offenders respectfully, rather than reacting in anger, will discourage violence that would put you, the victim, or others at risk.

#### Did You Know?

Sexist behavior can lead to assault or to tolerance of forceful sexual acts. If you witness such behavior, intercede.

## What if I'd like to be more involved in assisting sexual assault victims?

A volunteer opportunity as a Victim Advocate (VA) may be an option for you. A Victim Advocate is a trained volunteer that gives support and information to victims, acts as a companion during a victim's recovery and during medical and investigative processes, and ensures the victim's safety.

Interested? If you have no unresolved issues with sexual assault, show the maturity to maintain confidentiality, demonstrate good communication and interpersonal skills, and have at least one year remaining at your unit, contact an EAPC/SARC for details.



## Article: Preventing Sexual Assault

Unfortunately, there is always some risk of becoming a victim of sexual assault. However, by practicing some protective habits and knowing some warning signs, you can greatly minimize that risk. In addition, adopting a few practices can help ensure that you don't cross the line and become an offender.

This article provides measures you can take to protect yourself from becoming a victim, as well as avoid inadvertently committing offensive and illegal acts.

### How do I reduce my risk of becoming a victim of sexual assault?

The following are general actions that can help you to minimize the possibility of being victimized:

- Trust your instinct
- Don't overindulge in alcohol
- Don't assume coworkers or other non-strangers would never harm you
- Be aware of your surroundings
- Avoid isolated places
- Ensure someone knows where you are
- Meet first-time dates in a public place
- Travel and socialize in groups
- Always have money to get home
- Have your cell phone with you
- Take a self-defense class
- Don't prop outside doors open
- Always lock your door

### Are date rape drugs a risk?

Date rape drugs, such as Ecstasy or GHB, are drugs that rapists use to subdue their victims, although alcohol is the most commonly used. Some indications that you may have been drugged with a date rape drug are that you:

- Feel a lot more intoxicated than usual after only a few drinks
- Wake up very hung over
- Experience lapse of memory
- Remember taking a drink, but cannot recall what happened afterward

Ways you can avoid an assault by drugging are:

- Going to pubs, clubs, and parties with trustworthy friends
- Appointing a trusted friend to help you watch your drink
- Not leaving your drink unattended
- Avoid sharing or exchanging drinks
- Refusing drinks from anyone you don't know and trust
- Refusing drinks from an open container
- Drinking from a bottle and keeping your thumb on top
- Avoiding drinking anything that tastes or looks unusual
- Seeking help from a trusted friend if you feel really drunk after only a drink or two

### Does the use of alcohol increase the chance of sexual assault?

Excessive alcohol use can increase the risk of committing or being vulnerable to sexual assault. Alcohol can:

- Impair judgment
- Lower inhibitions
- Impair ability to recognize potentially dangerous situations
- Increase sexual aggression

#### Did You Know?

Date rape drugs are easily slipped into a drink at a pub, club, or party and are colorless, odorless, and often tasteless.

#### Did You Know?

Most rapes involve alcohol use, either by the offender, the victim, or both.

- Make it difficult to resist a sexual assault

Offenders may take advantage of the fact that alcohol or other drugs increase vulnerability. Also, while an individual cannot legally consent to sex if they are drunk, those who are drunk when assaulted often feel responsible.

There are measures you can take to minimize your risk of alcohol-related sexual assault:

- Understand the effects alcohol may have
- Watch what and how much you drink
- Never allow yourself to be incapacitated by alcohol – make sure that you always have control
- Ask a trusted friend or call a taxi to take you home if you are drunk

### What are the warning signs that someone may be a non-stranger rapist?

A non-stranger rapist may exhibit the following behaviors:

- Ignores, interrupts, or makes fun of you
- Has a reputation for being a player
- Drinks too much or uses drugs
- Tries to get you to drink or take drugs
- Invades your personal space and sits or stands too close
- Tries to touch or kiss you when you barely know him or her
- Wants to be alone or pressures you to be alone together
- Pressures or tries to guilt you into sex
- Wants to appear strong and in charge
  - Does what he or she wants without asking what you want
  - Becomes angry or mopes if he or she doesn't get their own way

### How do I avoid becoming a sexual assault offender?

The following actions can help you to avoid being an offender:

- Ensure your partner consents (and that they can legally consent – they are not incapacitated, drunk, drugged, or underage)
- Communicate your expectations
- Avoid using drugs and excessive alcohol
- Remember that “No means No”

#### Did You Know?

Over 66% of all rapes are committed by someone the victim knows.

## Article: Recognizing Sexual Assault

All members of the Coast Guard should know how to identify sexual assault. This will allow you to avoid acts that are questionable or can lead to sexual assault. It can also help you know whether you've been sexually assaulted, so you can seek for and receive needed assistance. Finally, it can help you know when to step in to help others.

After completing this article, you should be able to define and recognize sexual assault, as well as know the difference between "consent" and "lack of consent".

### Who becomes involved in sexual assault?

Be aware that, contrary to popular perception, both men and women can commit sexual assault and both can become victims.

In addition, sexual assault can take place between genders (a man assaulting a woman or vice versa) or between people of the same gender. When same-gender assault takes place, neither the victim nor the offender are necessarily homosexual.

Offenders sexually assault their victims to humiliate and dominate them. Sexual assault to them is about gaining power and control, **not** about romance, passion, or even sexual gratification.

### What is sexual assault?

Sexual assault is intentional sexual contact, set apart from legal sexual activity because it includes:

- Force
- Threats
- Intimidation
- Abuse of rank or authority
- A situation where the victim does not consent
- A situation where he or she cannot legally consent, such as when the victim is:
  - Drunk or under the influence of drugs
  - Unconscious or asleep
  - Incapacitated
  - Underage
  - Unable to understand the nature of the sexual act

Specific acts that are included as sexual assault are rape, forcible sodomy, and other unwanted sexual contact that is aggravated, abusive, and/or wrongful.

An attempt to commit one of these acts is also considered sexual assault.

### What is consent?

Consent is words or overt acts by a competent person indicating a freely given agreement to the sexual conduct at issue. Consent can be denied at any point (even if, for example, the two people have had sex in the past or have made suggestive remarks or acts).

#### Did You Know?

According to the Department of Justice, 1 in 4 females and 1 in 6 males are sexually assaulted.

## What is lack of consent?

The following shows a lack of consent:

- Declining or expressing unwillingness to engage in a sexual act (No means NO!)
- Lack of physical resistance to conduct without overt words or acts of consent
- Submission resulting from the offender's
  - use of force,
  - threat of force, or
  - placing another person in fear
- Submission resulting from the victim's
  - intoxication,
  - unconsciousness,
  - incapacitation, or
  - substantial incapability to understand the nature of the sexual acts

In addition, the following does NOT imply consent:

- Current or previous dating relationship—just because two people are dating, have been intimate, or are married doesn't mean that one person can insist on or force sex on the other
- A person's manner of dress— the way another person is dressed does not excuse you from your responsibility to obtain consent from them

## What are examples of situations, words, or actions that show a lack of consent?

Words and actions which indicate that a person does not consent include:

- "Not now"
- "I'd rather be alone"
- "I'm not sure"
- "I'm not ready for this" or "I don't feel good about this"
- "You've been drinking" or "I've been drinking"
- Pushing you away, moving away from you, trying to leave
- Crying
- Silence

If you are in doubt whether the other person consents or not, ask. Communication can help you avoid making bad assumptions about a partner's wants and getting into trouble because of it.

### Myth

"She was asking for it by the way she dressed."  
Fact: Dressing attractively, or even provocatively, is often used simply as a way to get attention, not to invite sexual conduct, and does not constitute consent.

### Myth

"The other person didn't say anything and didn't resist, so it was okay."  
Fact: They may have felt afraid or pressured and were unable to speak or resist. This is not consent.

## Article: Responding as a Sexual Assault Victim

Learning how to act if you are sexually assaulted can prepare you to take action, protect yourself from further harm, and begin healing.

This article will outline reporting options available to sexual assault victims, as well as inform you about what to do immediately after a sexual assault and how to engage assistance to help begin the recovery process.

### What do I do if I'm sexually assaulted?

If you are ever sexually assaulted, immediately after the attack, you need to:

- Get to a safe place
- Get medical care as needed
- Preserve the evidence of the assault if interested in potential prosecution of the offender
- Write down what you can remember of the offender and the attack
- Choose your reporting option (see below)

### How do I preserve the evidence?

To preserve important evidence for possible prosecution of the offender, avoid certain actions until medical personnel (and investigators, if using unrestricted reporting) have had the opportunity to collect evidence. Specifically, do not:

- Bathe, shower, or douche
- Change clothing
- Wash your hands
- Brush your teeth or gargle
- Use the restroom, if possible
- Eat or drink
- Clean, rearrange, or remove items from the scene of the assault.

### What are my reporting options?

Members of the Coast Guard have two options for reporting an assault: restricted reporting and unrestricted reporting.

Restricted reporting:

- is a confidential method of reporting an assault by contacting **ONLY** the Employee Assistance Program Coordinator (EAPC)/Sexual Assault Response Coordinator (SARC), a Family Advocacy Specialist (FAS), a Health Care Provider (HCP), or a Victim Advocate (VA). If the assault is disclosed to anyone other than these individuals, the report must be unrestricted.
- gives victims access to medical and counseling services even if they are not willing to openly report the offense.
- may not be available in every circumstance

Unrestricted reporting:

- allows for a formal investigation to be initiated and the offender to be punished, which is usually done by calling the police or reporting the offense to military authorities.
- Victims can switch to this option after having chosen restricted reporting but evidence will not be available after a year.
- Victims are not required to cooperate with investigators.

For details on reporting options, see Commandant Instruction 1754.10 (series) or an EAPC/SARC.

#### Did You Know?

Preserving evidence is important. Even if a victim initially chooses restricted reporting, evidence will be kept for twelve months and an investigation can be initiated at any time at the victim's request.

#### Myth

"It's better if I pretend like nothing happened."  
Fact: Victims may need assistance to fully recover and may likely need medical care.



## Is there someone who will help me through this?

Yes, a Victim Advocate (VA) will be made available to sexual assault victims. The Victim Advocate is a trained volunteer who supports and informs victims; acts as a companion during recovery and through investigative and medical processes; and ensures the victim's safety.

Victims also have access to:

- Medical support
- Local rape crisis centers
- Employee Assistance Program Counseling Services
- USCG Legal services
- USCG Investigative services

To request services, contact your local EAPC/SARC or any military healthcare provider. Websites that can help you locate USCG resources are:

- [www.worklife4you.com](http://www.worklife4you.com)
- [http://www.uscg.mil/worklife/rape\\_sexual\\_assault.asp](http://www.uscg.mil/worklife/rape_sexual_assault.asp)

Outside resources include the National Sexual Assault Hotline at (800) 656-4673, the Rape, Abuse, and Incest National Network (RAINN) (<http://www.rainn.org>), or Hope for Healing (<http://www.hopeforhealing.org/>).

### Did You Know?

Services are available to Active Duty members, reservists on active duty, full time Civil Service, Exchange System, and MWR employees, as well as their dependents.

## Article: Preventing Sexual Harassment

Sexual harassment takes place all too often. However, measures such as showing respect, using effective communication, asking for help when needed, and evaluating your actions can do much to prevent sexual harassment from continuing, or even happening in the first place.

This article provides preliminary measures you can take to help you stop someone from sexually harassing you, as well as ways you can use to avoid inadvertently becoming a harasser.

### What should I do if I'm sexually harassed?

Take these steps to help put an end to sexual harassment:

Communicate:

- Name the behavior that is offensive, how you feel about it, and what you want to see happen—be specific about the behaviors
- Be assertive but not confrontational—a harasser will be less receptive to the idea of change if he or she feels under attack
- Realize that the harassment is not your fault—it's the harasser's behavior that's an issue and you don't have to tolerate it
- Do not assume it will go away on its own—remaining silent or going along with the harassment usually encourages a harasser

Record:

- Keep a record about the harassment, including keeping a log of incidents and saving any emails and other written media related to the harassment
- In the log, write the dates, times, places, names of witnesses to, and nature of the sexual harassment at issue, in case further action is required.

Report:

- Always try to resolve the issue at the lowest level—many times, an issue can be resolved by speaking to the harasser or asking a supervisor to help out.
- If that does not work or is not a possibility, however, there is an established complaint process—your supervisor or an Equal Opportunity Advisor/Equal Opportunity Specialist (EOA/EOS) can guide you through this.

#### Did You Know?

Keeping a written record of the harassment will better establish your credibility should the harassment require higher level resolution.

### What do I do if I feel I can't confront the harasser?

Many victims find themselves in such a situation, because of intimidation, a desire to avoid conflict, the severe nature of the harassment, or other reasons. Strategies to help you are:

- Direct approach: talk to the harasser and tell them to stop
- Indirect approach: send an email to the harasser and tell them to stop
- Third party approach: ask a friend or coworker to approach the harasser instead
- Report approach: notify his or her supervisor and ask for help in resolving the harassment

### How do I avoid being a sexual harasser?

You can avoid being viewed as a sexual harasser by doing the following:

- Cease and desist when you are told that your behavior is offensive or unwelcome
- Strive to be approachable so others can feel that they can tell you when your behavior needs to change
- Show respect to those around you. For example:
  - not viewing or posting off-color or pornographic materials in public

- not sharing sexual humor or details of your sex life in public
- allowing others their personal space and privacy
- not asking for a date from a person who has already said no to you a couple of times
- refraining from complimenting coworkers on their bodies
- following the military policy on homosexuality: don't ask, don't tell, don't pursue, don't harass
- Periodically evaluate how you behave and how others react to you
- Communicate—if you have questions about appropriate behavior, ask and actively listen

### What are some ways I can evaluate my behavior?

In determining whether your behavior is appropriate or not, try these methods:

- Imagine what someone you deeply care about (a child, sibling, significant other, parent, etc.) would think of your behavior. If you would be embarrassed having them witness you doing it, reconsider the behavior.
- Imagine your loved one being treated by a stranger or slight acquaintance in the way that you're treating others. If you would not want it happening to them, do not do it to others.

#### Myth

"Sexual harassment is really just flirting."

Fact: Flirting is wanted, mutual, and shows interest in the other person as an individual. Sexual harassment is unwanted, one-sided, and often motivated by power.

## Article: Recognizing Sexual Harassment

All members of the Coast Guard should know how to identify sexual harassment and understand the basic standards that are used to determine if behavior is sexually harassing or not. This will allow you to avoid acts that could be considered sexual harassment, know if you are being sexually harassed, and be able to step in to help others in need.

After completing this article, you should be able to define and recognize sexual harassment.

### Who becomes involved in sexual harassment?

Be aware that, contrary to popular perception, both men and women can commit sexual harassment and both can become victims.

In addition, sexual harassment can take place between genders (a man harassing a woman or vice versa) or between people of the same gender.

Offenders often sexually harass their victims to humiliate and dominate them. Sexual harassment to them are about gaining power and control, **not** about romance and flirting.

### What is sexual harassment?

Sexual harassment includes sexual advances, requests for sexual favors, or other sexual conduct (verbal or physical) that is **unwelcome** and where:

- Conditions are placed on someone's employment in return for submission to sexual conduct (can be obvious or hinted);
- Submission or rejection to the conduct is used as a basis for employment decisions; or
- It interferes unreasonably with someone's work performance or creates a working environment that's intimidating, hostile, or offensive.

This means, in the workplace, that:

- Sexual favors or dates cannot be required in return for promotions, leave, positive endorsements, and so on.
- A person cannot be treated differently from his or her colleagues because they have either submitted to or resisted sexual conduct.
- Coworkers cannot create a hostile work environment for any other coworker.

### What is a hostile work environment?

When talking about sexual harassment, a hostile work environment is one that exposes an employee to certain behaviors, including:

- **Verbal harassment:** such as catcalls, whistles, sexually offensive joking or banter, innuendo, spreading sexually-related rumors or lies, playing offensive music publicly, asking for a date after multiple rejections, asking for or suggesting sexual acts
- **Physical harassment:** intimidating behavior (such as stalking, standing too close, intentionally blocking a person's path, leaning over a person) and unwanted touching (such as hugging, patting, stroking)
- **Visual harassment:** such as leering, winking, licking lips, sexual hand or body gestures, checking someone out, displaying offensive pictures

#### Did You Know?

In one poll, 31% of women and 7% of men had been sexually harassed at work (Louis Harris and Associates).

## Can certain kinds of discrimination be sexually harassing?

Yes, certain kinds of discriminatory remarks or behaviors can be considered sexual harassment and are illegal. This includes:

- Harassing a woman (or man) by making an offensive remark about women (or men) in general
- Treating someone differently based on their gender or sexual orientation (whether actually known or just assumed)
- Asking or requiring someone to reveal their sexual orientation (The military policy is don't ask, don't tell, don't pursue, don't harass)

## How do we know if sexual harassment has really taken place?

What matters most in deciding if sexual harassment has taken place is the **impact** of a person's behavior on others, not the **intention** of the accused. A 'reasonable person standard' is used to judge whether behavior is harmless or harassing. What this means is: Would someone with an ordinary level of reasoning ability find the behavior sexually harassing?

## Article: Responding to Sexual Harassment

What if someone will not stop sexually harassing you? What if you saw that someone was suffering because of sexual harassment? How would you respond? Knowing how to respond appropriately can prepare you to take action, begin resolving a difficult and distressing situation, and create a positive working environment for yourself and others.

In this article, you will find information on the steps to take to make a sexual harassment complaint. It will also teach you appropriate methods of responding when someone else is sexually harassed.

### Who is responsible for eliminating and reporting sexual harassment?

**Harasser**—responsible for making corrections when he or she is aware of a problem and resolving any issues with the victim

**Victim**—responsible for letting an offender know that the behavior is offensive and reporting unresolved harassment

**Supervisor**—obligated to correct and help to resolve all sexually harassing behavior in his or her unit that he or she is aware of

**Peers and other witnesses**—responsible for interceding when they know that sexual harassment is taking place and for reporting harassment when necessary

### What should I do before I report sexual harassment?

Try to resolve the issue at the lowest level:

- Let the harasser know that you are offended, either in person, through an email, or through a third party.
- Ask your supervisor to help resolve the issue. He or she can be held accountable if he or she chooses not to address it. If your supervisor is the one harassing you, report it to his or her supervisor.

### How do I file a complaint?

If the issue cannot be resolved at a lower level, you may file an informal complaint. To do this, begin by:

- *Military*: submitting a written notification to the Commanding Officer.
- *Civilian*: contacting the Equal Opportunity Advisor/Equal Opportunity Specialist (EOA/EOS).

There are, however, some similarities between the processes:

- You must file the complaint within 45 days of the last sexually harassing act.
- If, at the end of a specified length of time, the issue is not resolved satisfactorily, you will be issued a Notice of Right to File and can submit a formal complaint.
- Retaliation against reporters and witnesses of sexual harassment is illegal and can be reported.

For more information on the reporting procedure, see Commandant Instruction M5350.4B.

#### Myth

“The harassment will go away on its own if I just ignore it.”

Fact: Harassment can often continue or even worsen if nothing is done to stop it.

## What if my supervisor already knows about the harassment but won't do anything about it?

Remember, if a supervisor, commanding officer, or another in a senior position sees a possible sexual harassment situation, he or she must work to resolve it. If they choose to do nothing, they can be held accountable.

## What can I do if I know that someone is being sexually harassed?

Don't remain silent! When you see inappropriate or offensive behavior happen, take steps to stop it or intercede:

1. Attempt to resolve the issue at the lowest level. Start by addressing the offender. Be assertive but courteous to avoid violence.
2. If that does not stop the behavior, report it to the offender's supervisor. Commanders and supervisors are required to correct sexually harassing behavior.
3. Keep in mind that retaliation is prohibited against someone reporting or acting as a witness to sexual harassment. If backlash against you occurs, report that as well.

### Did You Know?

Sexual harassment victims may not verbally object to the harassment but still suffer from it. Speaking up may help someone who can't or doesn't feel able to help themselves.

## Protecting PII: Telework Best Practices

### Teleworking and Information Security

Telework presents many benefits to the federal workforce, such as managing commutes, saving taxpayer money by decreasing government real estate, and ensuring continuity of essential government functions in the event of emergencies. While telework allows for greater flexibility in managing our workforce, there are risks to privacy and information security<sup>1</sup> that are inherent with a remote workforce. Information security policies do not change when an employee works from home. It is the duty of the employee to safeguard Sensitive information, including personally identifiable information (PII),<sup>2</sup> while teleworking.

### Safeguarding Sensitive PII

Effective teleworking begins with having a signed telework agreement in place. Work with your supervisor to determine what types of documents are appropriate to take home and what documents should stay secured within the DHS work space. Know the sensitivity of your documents, and make sure they are appropriately marked to help mitigate the risk of unauthorized disclosure.

One of the most effective ways to safeguard documents containing Sensitive PII is to keep electronic documents within the DHS network and to properly secure hard copy documents that you take outside of the DHS work space. Stay within the network by logging in remotely through the DHS Virtual Desktop\*, whether you use your DHS-issued laptop or your personal computer. If you choose to work from your personal computer, **do not forward documents to your personal email account** as a way to avoid issues such as slow network connectivity or the inability to print. While there may be instances where you need to send information to an individual's personal account (i.e. job applicant), forwarding unencrypted emails to your own personal email account or sending unencrypted documents outside the DHS network that contain Sensitive PII is considered a privacy incident (or data breach).

If you know you will be teleworking, identify the files you may need to work on in

<sup>1</sup> The Federal Information Security Management Act of 2002 (FISMA) defines information security as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide (A) integrity, which means guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information.

<sup>2</sup> PII is any information that can directly or indirectly lead to the identification of an individual. Sensitive PII is defined as personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

advance, and organize them on your network drive or DHS laptop so that they will be easily accessible to you while teleworking. You may also want to take advantage of DHS-approved collaboration tools, such as SharePoint, to easily access files while teleworking. However, before using SharePoint to store Sensitive PII, make sure your site has been approved for such use and that access is limited to only those individuals whose need for the information is related to his or her official duties. Have a back-up plan in mind in case you experience issues with network connectivity, but never transfer files to your personal computer using thumb drives or other portable electronic devices.

Be able to secure your DHS equipment and information at all times, including while transporting information home or while traveling. If you must leave equipment or documents unattended, secure them (i.e. in the trunk of your car, in a hotel safe, etc.), but only for short periods of time. Inventory your documents before teleworking, and ensure all documents are returned to the office.















### Examples of Privacy Incidents Associated with Telework

Know how to recognize a privacy incident and how to report it.

- Sending an email containing Sensitive PII to your personal email account.
- Sending unencrypted Sensitive PII outside the DHS network (i.e., to another agency, to a private sector partner, to a potential hire).
- Allowing family members access to documents containing Sensitive PII.
- Printing documents containing Sensitive PII to your personal printer.
- Using a thumb drive or other device to transfer data (i.e., Sensitive PII) to your personal computer.

***Report any suspected or confirmed privacy incidents  
to your supervisor  
or your component Help Desk.***



| WHEN                       | DO   | DON'T   | WHY   |
|----------------------------|--|---|---|
| Before you telework...     |  <b>Plan ahead to ensure that Sensitive documents can be safely accessed remotely.</b> Organize your files so that they are easily accessible via the DHS Virtual Desktop*. Use DHS-approved, portable electronic devices, which are encrypted, thereby adding a layer of protection to your data.  |  <b>Don't forward emails to your personal email account or use non-approved portable electronic devices.</b><br>Have a back-up plan in case you experience issues with network connectivity, but never transfer or download data to your personal computer, personal email account, or to non-encrypted devices.   | When you remove data from the DHS network, DHS cannot protect it. There may be instances where you need to send Sensitive PII to job applicants or individuals without DHS accounts, but it must be encrypted. To send it unencrypted is considered a privacy incident. |
|                            |  <b>Obtain authorization from your supervisor to take home Sensitive documents, and make sure documents containing Sensitive PII are marked "For Official Use Only" or "Privacy Data."</b><br>Inventory your hard copy documents when you leave the office and before you return them to the office.  |  <b>Don't take Sensitive PII home that you do not need.</b><br>Limit your removal of Sensitive PII from the office to only that information that is relevant and necessary to the work outlined in your telework agreement.  | Hard copy documents are easily lost or misplaced, putting Sensitive PII at risk. Conducting an inventory and properly marking documents helps mitigate the risk of unauthorized disclosure.   |
| Transport of documents ... |  <b>Be able to secure Sensitive data when not in use.</b><br>If you must leave your laptop or hard copy documents inside a vehicle, lock them in the trunk but only for short periods of time. When traveling, place Sensitive data in a hotel safe when not in use.  |  <b>Don't leave your laptop or hard copy documents unattended overnight.</b><br>Maintain accountability of your data by ensuring documents are secured when not in use.  | Failure to maintain accountability of Sensitive PII can lead to loss, theft, or misuse, resulting in a privacy incident.  |
| At home...                 |  <b>Log in through the DHS Virtual Desktop*</b><br>Organize your work space at home so that work files are separate from personal files and can be properly safeguarded.  |  <b>Don't email or save files containing Sensitive PII to your home computer.</b><br> <b>Don't print agency records to your home printer.</b>  | Your home computer, printer, fax, and copier all contain internal storage or "hard drives." Even when these devices are disposed of, the information stored within is vulnerable.   |
|                            |  <b>Take advantage of DHS collaboration tools such as SharePoint.</b><br>Do not post Sensitive PII on the DHS intranet, Component intranet sites, SharePoint collaboration sites, shared drives, multi-access calendars, or on the Internet (including social networking sites) that can be accessed by individuals who do not have a "need to know." |  <b>Don't store Sensitive PII on SharePoint unless your site has been approved for such use.</b><br>Access must be limited to those that have an official need to know.  | Collaboration tools provide quick, easy access to data, but without proper security controls, can lead to data winding up in the wrong hands. Sharing Sensitive PII with unauthorized users is considered a privacy incident.   |
|                            |  <b>Secure your data, and ensure other household members do not have access to it.</b><br>Organize your work space at home so that government property and information are kept separate from personal property and can be properly safeguarded.  |  <b>Don't leave files containing Sensitive data lying out in the open.</b><br>Never leave Sensitive PII in view of children, spouses, or visitors. Sensitive PII should be secured in locked cabinets and your computer/Blackberry should remain locked when not in use.   | Failure to properly secure Sensitive records could result in inadvertent sharing of Sensitive PII.  |

\*Each Component has a different process for accessing the DHS network remotely. Please contact your Help Desk.



## HOW TO SAFEGUARD SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION

This fact sheet helps you safeguard **Sensitive Personally Identifiable Information (PII)** in paper and electronic form during your everyday work activities. DHS employees, contractors, consultants, interns, and detailees are required by law and DHS policy to properly collect, access, use, safeguard, share, and dispose of PII in order to protect the privacy of individuals.

### **What is PII?**

**PII** is any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to an individual. Some PII is not sensitive, such as that found on a business card. Other PII is **Sensitive PII**, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. **Sensitive PII requires stricter handling guidelines, which are detailed below.**

**Examples of Sensitive PII include:** Social Security numbers (SSN), Alien Registration Numbers (A-number), financial account numbers, and biometric identifiers (e.g., fingerprint, iris scan). Other data elements such as citizenship or immigration status, account passwords, and medical information, in conjunction with the identity of an individual, are also considered Sensitive PII. The context of the PII may also determine its sensitivity, such as a list of employees with poor performance ratings.

## Guidelines for Safeguarding Sensitive PII

### I. Collecting and Accessing Sensitive PII

Before collecting or maintaining Sensitive PII, be sure that: (1) you have the authority to do so; (2) the data collection is consistent with the terms of a Privacy Act System of Records Notice (SORN); and (3) your database or information-technology system has an approved Privacy Impact Assessment. Access to Sensitive PII is based upon your having an official need to know, i.e., when the information relates to your official duties. Limit your access to only the Sensitive PII needed to do your job.

- Ensure that casual visitors, passersby, and other individuals without an official need to know cannot access or view documents containing Sensitive PII. If you leave your work area for any reason, activate your computer's screen saver.
- Ensure privacy while having intra-office or telephone conversations regarding Sensitive PII.
- Do not post Sensitive PII on the DHS intranet, the Internet, social networking sites, shared drives, SharePoint, or multi-access calendars accessible to individuals without an official need to know or proper authorization.
- Do not share account information, especially logins or passwords, with anyone. Do not have login or password information accessible to others (such as on a sticky note on your computer).
- Be alert to phone calls or emails from individuals claiming to be DHS employees attempting to gather or verify personal or non-public information. DHS will never ask you to verify your account login, password, or personal information by email or over the phone.

### II. Using and Safeguarding Sensitive PII

**Limit duplication of Sensitive PII:** Before creating new spreadsheets or databases that contain Sensitive PII from a larger file or database, consult the *DHS Sensitive Systems Policy Directive 4300A*, Attachment S1.

**Protect hard-copy Sensitive PII:** Do not leave Sensitive PII unattended on desks, printers, fax machines, or copiers. Secure Sensitive PII in a locked desk drawer, file cabinet, or similar locked enclosure when not in use. When using Sensitive PII, keep it in an area where access is controlled and limited to persons with an official need to know. Avoid faxing Sensitive PII if other options are available.

**Safeguard DHS media:** Sensitive PII may only be saved, stored, or hosted on DHS-approved portable electronic devices (PEDs), such as laptops, USB flash drives, and external hard drives. All portable media must be encrypted pursuant to *DHS Sensitive Systems Policy Directive 4300A*. Personal computers may not be used *unless you log in through the DHS Virtual Desktop*. If you need to transport your laptop or PED and must leave it in a car, lock it in the trunk and out of sight. Do not leave your laptop or PED in a car overnight. If lost or stolen, immediately report the missing asset according to your component's reporting procedures.

### III. Sharing Sensitive PII

You are authorized to share PII *outside* of DHS only if there is a published routine use in the applicable SORN and an information sharing and access agreement that applies to the information.

#### **Emailing Sensitive PII**

- **Within DHS:** Though DHS policy allows you to email Sensitive PII without protection to a recipient with an official need to know, some components do require encryption. The DHS Privacy Office strongly recommends that you redact, password-protect, or encrypt Sensitive PII you email within DHS.
- **Outside DHS:** Email Sensitive PII within an encrypted attachment with the password provided separately by phone, email, or in person. Before emailing Sensitive PII, confirm that you have the correct email address.
- **Never email Sensitive PII to personal email accounts:** Personal computers should not be used to access, save, store, or host Sensitive PII *unless you log in through the DHS Virtual Desktop*. Each component has different procedures for accessing the DHS network remotely, so check with your Help Desk.

#### **Mailing Sensitive PII**

Encrypt Sensitive PII stored on CDs, DVDs, hard drives, USB flash drives, floppy disks, and other removable media prior to mailing or sharing. *Always verify that the recipient received the information.* Note that FOIA requests may require different handling.

- **Within DHS:** Mail Sensitive PII in a blue messenger envelope provided by your on-site DHS mailroom or courier.
- **External Mail:** Seal Sensitive PII in an opaque envelope or container. Use First Class Mail, Priority Mail, or a traceable commercial delivery service (UPS, FedEx).

### IV. Disposing of Sensitive PII

Sensitive PII, including that found in archived emails, must be disposed of when no longer required, consistent with the applicable records disposition schedules. If destruction is required, take the following steps:

- Shred paper containing Sensitive PII; do not recycle or place in garbage containers. Be especially alert during office moves and times of transition when large numbers of records are at risk.
- Before transferring your computer or PED to another employee, ask your Help Desk to sanitize Sensitive PII from computer drives and other electronic storage devices according to your component's information security standards and the *DHS 4300A Sensitive Systems Handbook*.

### V. Reporting Privacy Incidents

You must **immediately** report all suspected or confirmed privacy incidents involving the loss or compromise of all PII to your supervisor. If your supervisor is unavailable, or if there is a potential conflict of interest, **DON'T WAIT!** Report the incident to your Program Manager, Help Desk, component privacy officer or privacy point of contact. For more information on reporting privacy incidents, download the *Privacy Incident Handling Guidance* on DHS Connect or [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

#### **For More Information**

For more detailed guidelines on the safe handling of Sensitive PII, download the *Handbook for Safeguarding Sensitive PII* from [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

- You must read this form and affirm your agreement with your course facilitator to receive credit for completing this course.



- **PERSONALLY IDENTIFIABLE INFORMATION (PII)  
EMPLOYEE ACKNOWLEDGMENT AND AGREEMENT**



- **Definitions of Personally Identifiable Information (PII) and Sensitive PII**

- Personally identifiable information (**PII**) is any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.
- Sensitive PII is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. **See Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security**, DHS Privacy Office.
- **Employee Acknowledgment and Agreement**
- I attest that I understand my responsibility to safeguard PII, including Sensitive PII; and, that I am familiar with and agree to comply with the standards for handling and protecting PII. I also agree to report the potential loss, theft, improper disclosure or compromise of PII. I acknowledge that I have received proper training regarding the procedures for safeguarding PII, and that I am aware of Department protocols should PII be potentially lost, stolen, improperly disclosed or compromised. I further understand that my failure to act in accordance with my responsibilities outlined above may result in criminal, civil, administrative, or disciplinary action if I am found responsible for an incident involving the loss, theft, unauthorized or improper disclosure or compromise of PII or Sensitive PII. Additionally, as a DHS employee, I am aware that I am subject to the policies contained within 5 CFR 2635, Office of Government Ethics, **Standards of Ethical Conduct for Employees of the Executive Branch** and DHS MD 0480.1, **Ethics/Standards of Conduct** (January 01, 2010).



- Signed: \_\_\_\_\_