

2014 Information Systems Security (ISS) and Privacy Awareness Course

- for Federal Employees and Contractors

Overview

YOU ARE THE DEPARTMENT'S BEST DEFENSE

Against those who seek to disrupt DOT business processes, transportation systems, and negatively affect the security posture of the United States.

Overview 2

As a DOT Federal employee or contractor, you must:

- Become familiar with DOT Information Systems Security (ISS) and Privacy policies, procedures, and best practices,
- Understand the risks associated with your activities while accessing DOT systems and information, and
- Understand **your** responsibilities and obligations for protecting DOT data, information, and information system assets.

Overview 3

This ISS and Privacy Awareness course will:

- Bring your attention to the most pertinent DOT policies, procedures, and best practices as they relate to information security and privacy,
- Highlight the risks associated with accessing DOT systems and information, and
- Identify **your** responsibilities for protecting DOT systems and information from unauthorized access and disclosure.

Policies and Procedures 1

Why must you take this ISS and Privacy Awareness Training?

You must take this training because:

- You are a DOT federal employee, contractor, subcontractor, intern, detailee, temporary worker **(from now on referred to as DOT workforce).**

- You have access to DOT systems and information.
- You have an obligation and responsibility to protect DOT information and systems from unauthorized access or disclosure, and
- It is required by Federal law and DOT policy.

Policies and Procedures 2

What Federal laws and DOT policies identify the ISS and Privacy Awareness Training requirement?

- Federal Requirement
 - Federal Information Security Management Act (FISMA) of 2002
 - OMB Circular A-130, Appendix III, paragraph 3 (2)(a)
 - OMB M-07-16 - Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- DOT Policy
 - DOT Order 1351.37 Departmental Cybersecurity Policy
 - Departmental Cybersecurity Compendium Version 3

Policies and Procedures 3

What is expected of you?

- Before gaining access to DOT systems (or within 30 days of on-boarding), all DOT users must:
 - Read and Agree to the DOT Rules of Behavior
 - Complete the annual Security and Privacy Awareness Training (this course)
- Certain members of the DOT workforce that have Information Technology (IT), Information Systems Security (ISS), or Privacy responsibilities may be required to complete additional specialized training for their assigned role.
- You must complete these items at least annually thereafter.

Policies and Procedures 4

What are the DOT Rules of Behavior?

The DOT Rules of Behavior is a notice to employees and contractors defining how you may use DOT information and information systems.

- Do the *Rules of Behavior* apply to you?

- The rules apply to the DOT workforce that accesses, stores, receives, or transmits DOT information using Information Technology (IT) resources at their primary or alternate worksite (for example, home office).
 - These rules do NOT apply to members of the public accessing publically available DOT information or information systems.
- What are DOT IT resources?
 - Workstations, laptop computers, servers
 - The network infrastructure (for example, wiring and cable, routers, switches, printers, etc.)
 - Personal digital assistants and tablet computers (for example, Palm Pilot, iPad, etc.)
 - Cellular, mobile, smart phones, text messaging systems (for example, BlackBerry Messenger and iPhone)
 - Plug-in and wireless add-ons that employ removable media (for example, USB flash memory (thumb) drives, external drives, diskettes, CDs, DVDs, etc.)
 - DOT Information, data, reports, websites, etc.

NOTE: If you do not agree with the DOT Rules of Behavior, the DOT will not allow you to access its network or systems.

Protecting DOT Data and Information 1

Why protect DOT data and information?

- Much of the information and data you use at work is essential to the Department of Transportation and its Modes to maintain a safe and efficient transportation system.
- Your access to DOT information is important for you to perform your assigned job.
- Some information you use requires ***stronger*** protection and enhanced handling procedures to ensure that it is not misused or accessed by unauthorized individuals.

Protecting DOT Data and Information 2

Types of information used at DOT

- Personally Identifiable Information (PII)
 - Any information about a human being, living or deceased, regardless of nationality, that is maintained by an agency and permits identification of that individual to be reasonably inferred by either direct or indirect means.
 - PII includes but not limited to:
 - Name
 - Social security number
 - Date and place of birth
 - Mother's maiden name

- Biometric records
- Medical records
- Educational
- Financial information
- Employment information

Protecting DOT Data and Information 3

Types of information used at DOT

- Sensitive but Unclassified (SBU), Sensitive Unclassified Information (SUI)
 - Information and data that is necessary to operate DOT systems and to conduct normal DOT operations. Because of the sensitive nature of the information you must place a degree of control over its use and dissemination.
 - Examples of SBU/SUI data include, but are not limited to:
 - IP addresses of DOT systems
 - Account logon information
 - Passwords
 - System vulnerability information
 - Business records
 - Operating procedures
 - Security plans
 - Other information that the DOT deems sensitive
- Classified Information
 - Classified information is material that a government body has determined is sensitive and requires protection of confidentiality, integrity, or availability. Access is restricted by law or regulation to particular groups of people. A formal security clearance is required to handle classified documents or access classified data. Mishandling of classified material can incur criminal penalties.

Protecting DOT Data and Information 4

Protecting Sensitive Data and Information

As a user of DOT information systems, it is your responsibility to protect PII, SBU, SUI, and other DOT sensitive data by:

- Ensuring DOT information and records are properly (stored, handled, disposed) in accordance with DOT policy
- Not disclosing DOT information (in any form), unless
 - Only when authorized
 - On a “need to know” basis
 - Or required by federal law obligations such as the *Freedom of Information Act*
- Not providing DOT information obtained through government employment to another person or organization which is not otherwise available to the public.
- Not using information obtained through government employment which is not otherwise available to the public.

Warning: You must NOT access, process, or store classified information on any device that has not been authorized for such processing!

Protecting DOT Data and Information 5

How do I protect DOT sensitive data and information?

DOT Employees and Contractors must:

- Utilize DOT-approved encryption software when transmitting or storing PII or sensitive data
- Only access PII and other sensitive data for which you are authorized
- Only use DOT approved devices for storing and processing PII and other sensitive data
- Protect PII and sensitive information from unauthorized disclosure
- Obtain proper approval before responding to external agency request for PII or sensitive information
- Lock workstations and laptops while away, even for a short time
- Protect all PII and sensitive data as if it were your own

Protecting DOT Systems : Personally-Owned Technology

Users may only access DOT information systems and networks using DOT-provided or **approved** personally-owned technology (for example, personal computer, laptop, printer, smart phone, tablet, etc.)

- When using personally-owned technology on a DOT network, you must:
 - Complete and sign the appropriate technology agreement(s)
 - Allow authorized personnel to monitor and examine your technology upon request
 - Use DOT-approved security and encryption software for storing or sending DOT-sensitive information or PII
 - Allow the installation and use of strong authentication (for example, PIV card)

- Agree to allow the DOT to wipe the technology if it is lost or stolen
- Understand that a security or privacy incident involving your personally-owned technology may result in:
 - the seizure of your personally-owned technology
 - the loss of software you may have purchased
 - and the loss of all personal data on the technology

Protecting DOT Systems : Accessing DOT Systems

- The DOT provides you access to its network and systems to conduct official business on behalf of the DOT.
 - You are responsible for the security of your account, password, and the information and data you access with your account.
 - Users of DOT systems have **no reasonable expectation of privacy**.
 - To protect the DOT network and systems from misuse or unauthorized access, the DOT **reserves the right to monitor** the DOT network and all attached systems, including **all activity** on your system.
- You must agree to abide by the DOT Rules of Behavior.

NOTE: If you do not agree with the DOT Rules of Behavior or the Monitoring of your activities, you must not use the DOT network or systems.

Protecting DOT Systems: Access to DOT Systems

- DOT provides access to employees and contractors only to systems required to perform their official duties.
- If you access DOT systems, you must complete annual training.
 - Mandatory completion of cybersecurity and privacy awareness training (**this course**)
 - System-specific training may be required
 - Role-based* training is required for individuals in certain positions

*** Refer to the Roles and Responsibilities section of the DOT Cybersecurity Policy for more information on which roles require specialized training.**

Protecting DOT Systems: Use of Government Office Equipment

By using your DOT furnished equipment, you must:

- Agree to the monitoring of your activities
- Not install unauthorized software

- Not allow other users to use your logon ID and password to access DOT systems
- Comply with all software copyrights and license agreements
- Never view or download pornographic or offensive content

Do not make unauthorized changes to your government furnished equipment or attempt to circumvent the implemented security measures.

Protecting DOT Systems: Passwords and Access Control Measures

- Each user must have their own unique logon account.
- Passwords must:
 - Be at least twelve (12)* characters long and have a combination of letters (upper- and lower-case), numbers and special characters, and
 - Be updated at least every 60 days, or immediately if you suspect your password has been compromised.
- Always protect passwords, PINs, and access numbers.
 - Never share a password with anyone, including system administrators.
 - Do not write passwords down or store them in an electronic file on workstations, laptops, or personal technology.
 - Make sure no one is watching as passwords are entered.

*** Some systems have an approved waiver for passwords with fewer than 12 characters**

Protecting DOT Systems: Your Personal Identity Verification (PIV) Card

- Your PIV Card is more than a picture ID. It contain sensitive information about you and your system access rights.
 - Never leave a PIV card unattended on a desk or in a workstation.
- Protecting passwords and PIV Cards is a first-line defense against internal cyber threats.
 - Never share your PIV card or PIN.
- If your PIV Card is lost or stolen, you must report the loss immediately to your supervisor and to your security servicing organization.

Your Responsibilities

Know Your Responsibilities

You should:

- Know your responsibilities for protecting DOT systems and data.
- Understand the risks associated with the actions you take while using DOT systems or accessing DOT information and data.
- Know how to handle and protect the equipment that DOT provides to you for your assigned job.
- Know what you are permitted and NOT permitted to do while using the DOT equipment.
- Understand your responsibilities when teleworking.
- Understand your responsibilities while traveling on official DOT business.

Your Responsibilities: Understanding the Risks

- Hackers are always trying to break in to Government systems for various reasons
 - For bragging rights, for fun, or just to prove that they can
 - To disrupt normal service
 - To gain valuable information on projects for unfair competitive gain
 - To gain access to your personal data so they can steal your identity
- Hackers use many methods to gain unauthorized access to government systems
 - Some take advantage of vulnerabilities in software to break in to government systems
 - Some use emails to entice you to provide your personal information
 - Some lure you to click on malicious links on websites
 - Some call you on the phone and ask for the information they want
 - Offer you free software, subscriptions, USB drives, CDs, or DVDs

Your Responsibilities: Understanding the Risks 2

Phishing

- Phishing is an attempt to convince you to give up your personal information, usually through an email from an authentic looking source (for example, a system administrator, your bank, credit card company, or maybe even from someone you know).
 - You should delete the email so that you don't accidentally click on it in the future.
 - Do not respond to the email.
 - Do not give out your personal information to an unsolicited email request.
 - Never give out your user name or password.
 - Do not subscribe to offers of "Free" services or subscriptions.
 - If you believe that you have opened a suspected malicious email, you must report this to the DOT Cyber Security Management Center (CSMC) immediately.

Spear Phishing

- Spear phishing is a targeted phishing attempt toward a specific person or group of people.
 - Do not respond to any spear phishing messages.
 - You should report spear phishing attempts to the DOT CSMC so they can alert others in the affected group.

Your Responsibilities: Understanding the Risks 3

Whaling

- Whaling is a targeted phishing attempt towards senior company executives, agency officials or their assistants.
 - Do not respond to whaling messages.
 - Report whaling attempts to the DOT CSMC so they can alert other executives.

Malicious Web Links

- Malicious web links are links that can download malware to your system and allow a hacker to gain access your system.
 - Do not click on links in emails that you do not know.
 - Be cautious of links on websites of unknown origins – it could download malicious code.
 - If you click on a malicious web link, you must report this incident immediately to the DOT CSMC.

Your Responsibilities : Understanding the Risks 4

Social Engineering

- Social engineering is a method used by hackers so they may gain information that allows them to access your system. The person usually pretends to be someone in authority such as a system administrator or helpdesk person seeking your help.
 - Never give out your logon ID or password to anyone.
 - Do not respond to surveys.
 - Do not provide any information to anyone that does not have a need to know.
 - Refer the caller to the Public Affairs office.

Other Malware

- Malware is malicious code that may cause harm to your system or data or allow unauthorized access to DOT systems.
 - Never insert unauthorized media (USB devices, CDs, DVDs, etc.) in to any system.
 - Never install unauthorized software on any DOT system.

- Do not download unauthorized files – they might contain malicious code.

Your Responsibilities: Limited Personal Use

- The DOT Internet and email systems are for business use **only**
 - DOT policies permit **limited personal use of the Internet** while at work as defined in DOT Policy.
- The personal use of the Internet and email systems must **not**
 - Compromise the security of DOT information and information systems
 - Interfere with the DOT's normal business operations
 - Keep the employee or contractor from performing their assigned DOT duties
- Certain activities are ***strictly prohibited*** from access to or use on DOT systems and may result in termination from the DOT, and / or other disciplinary actions
 - For example, accessing pornographic material, gambling, operating a private business, etc.

–Warning: Your use of the DOT Internet and all email received, stored or transmitted may be intercepted and monitored by the DOT, including your account logon ID and passwords, credit card numbers, bank account numbers, and other personal information.

Your Responsibilities: Appropriate Use of DOT Internet and Email

Internet

- You may not use the internet to:
 - Stream audio or video (*unless work related*)
 - Download or share files from peer-to-peer networks
 - Attempt unauthorized access to information systems
- Do not host any type of internet server or connect personal devices on any DOT network unless explicitly authorized.

Email

- Never auto-forward DOT e-mail to a personal account.
- Do not respond to, send, or forward jokes, chain emails, or offensive content.
- Do not send DOT sensitive information to your personal accounts.

Your Responsibilities: Social Media

- Use of social media/networking sites, blogs, and instant messaging is outlined in DOT Order 1351.33, Appendix A Employee Conduct Policy.

- You must follow the **DOT Social Media Policy, Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR Part 2635**
- Only authorized individuals are permitted to make statements on behalf of the DOT.
- Do not place work related information on your personal social media sites.
- Exercise care when using social media.

Your Responsibilities: Teleworking

- The DOT permits certain employees to complete job responsibilities from a location other than their normal workplace. *Please refer to the DOT Telework Policy for details.*
- Before you telework, you must:
 - Be designated as a telework employee
 - Have an approved telework agreement in place
 - Have an agreed upon work schedule with your manager
 - Contact your manager or visit the DOT telework website for additional information on teleworking and to see if you are eligible to telework
- While you are teleworking, you must:
 - Follow security practices that are the *same as or equivalent* to those required at your primary workplace
 - Adhere to all provisions of your telework agreement
 - Protect PII and sensitive data at your alternate workplace
 - Downloading and storage of PII and sensitive data must be on government-owned equipment
 - Properly dispose of sensitive information

Your Responsibilities: Laptops and Other Portable Electronic Devices (PED)

- When you use Laptops and other portable devices you must:
 - Only use DOT-issued computers and approved personal electronic devices to access DOT systems
 - Ensure anti-virus and firewall software is installed and up-to-date
 - Utilize DOT-approved encryption software for storing and transmitting all PII and DOT-sensitive information
 - Only use DOT-approved Bluetooth and wireless communication devices with your DOT equipment
 - Be aware of the ***dangers associated with mobile “hot spots”*** and use secure connections when possible

- All DOT Laptops must have the DOT-approved full hard disk encryption installed.
- Do not connect your laptop to a DOT network and a non-DOT network at the same time.

Your Responsibilities: Travel with DOT Laptops and PEDs

When traveling with DOT-provided laptops and mobile devices, you must:

- Take precautions to prevent theft, damage, abuse, or unauthorized use
- Keep equipment under physical control at all times

What does “Physical Control” mean?

- Maintain *sight of equipment* when going through airport security
- Never place DOT equipment in checked luggage
- Never store DOT equipment in public lockers
- If you must leave DOT equipment unattended
 - lock it out of sight in a vehicle trunk
 - lock it in a hotel room if available
- Follow the DOT PED policy when taking a DOT-issued laptop or mobile device on foreign (non-US) travel

Your Responsibilities: Incident Reporting

- Federal law requires you to report all suspected or actual ISS incidents or privacy breaches to the DOT Cyber Security Management Center (CSMC) **within one (1) hour** of their discovery
- The DOT CSMC contact information:
 - **Phone:** 1-866-580-1852
 - **Email:** CSMC@dot.gov or 9-awa-csmc@faa.gov
- You must support the CSMC and the Information Systems Security personnel in the investigation of any incidents
- After contacting CSMC, you must also report suspected or actual privacy breaches to Your immediate supervisor

Protecting Yourself at Home: Your Home Computer and Personal Data 1

Protecting your systems and data at home is just as critical as it is at work. Here are some tips to protect your home computers and your data.

- Keep your home devices up-to-date
 - Install a good anti-virus software on every computer in your home and keep it up-to-date
 - Be cautious of installing free and shareware software – they may contain malicious code
 - Install all security updates to installed software immediately
 - Make sure the software updates are from the software vendor
 - Enable the automatic update feature of your software
- Email
 - Do not open emails and attachments from people that you do not know
 - Do not click on links in emails from people that you do not know
 - Never respond to requests to provide your personal information or account numbers
 - Delete suspect emails so that you do not click on them in the future

Protecting Yourself at Home: Your Home Computer and Personal Data 2

Here are some tips to protect your home computer and your data.

- Internet use
 - Use caution when surfing or searching the web.
 - Use caution when ordering merchandise or services over the Internet.
 - Make sure that the website uses a secure mode (HTTPS) before you enter your password, credit card number, other personal information.
 - Be wary of transfers from the website you visited.
- Social Media
 - Never post work related information on your personal social media sites.
 - Restrict your interactions on social media sites to people you know.
 - Remove geocaching data from your photos before you post them.
- You must have DOT approval for using your personal devices to access the DOT network.

Protecting Yourself at Home: Your Home Computer and Personal Data

Here are some tips to keep your family's computer and data safe.

- Kids and Safe Computer use

- Never allow your children, spouse, or others to use your DOT computer, laptop, smart phone, or other DOT equipment to play games or access the internet.
 - Monitor your kids activity while they are on-line.
 - Restrict their website access to age-appropriate content that you review and approve.
 - Know who your kids are communicating with via email, chat, and other social media sites.
 - Watch for signs of cyber bullying.
 - Teach your kids not place personal information such as home address, age, gender, school information, etc. on websites, social media sites, or in emails.
 - Don't let your kids download software, files, music, videos, etc. without your permission.
- You can find more resources for keeping your kids safe online at <http://www.safekids.org/>.

Summary 1

By completing this ISS and Privacy Awareness course, you should:

- Have a better awareness of DOT Information Systems Security and Privacy policies
- Understand and follow the DOT Rules of Behavior
- Understand the need to protect DOT information and Systems
- Understand your responsibilities for protecting DOT information and systems

Summary 2

Additional Mandatory Training

This course provides employees and contractors with basic Information Systems Security (ISS) and Privacy awareness

- The DOT may require you to complete other mandatory courses including (but not limited to):
 - Privacy Awareness Training
 - Role-based training is required for individuals in certain security-related positions
 - Plain Language
 - Ethics
 - Security Awareness Virtual Initiative (SAVI) which covers physical security (*for FAA users only*)
- Mandatory training courses are loaded into your learning profile
 - DOT - Training Management System (TMS)
 - FAA - electronic Learning Management System (eLMS)

- You must complete each course within the designated timeframe

Summary 3

- This concludes the Information Systems Security and Privacy Awareness portion of the course.
- Certify that you completed this part by pressing the button at the bottom of the screen, then proceed to Knowledge Check portion of this course.