***2018 Security Awareness Training Course Test—Accessible Version***

This version of the 2018 Security Awareness Training (SAT) Course Test for contractors is updated to reflect DOT's commitment to Section 508 and Accessibility. If you do not need to use this version, please complete the test 2018 SAT Course found on SharePoint. (update link)

Please follow these guidelines to complete the course:

1. Print out this test.
2. Manually answer each question.
3. Non-FHWA personnel should scan the document and email your completed test to ASAT@DOT.GOV.
4. FHWA Personnel should email their completed test to FHWA.CTRISSAT@dot.gov.
5. Your test will be graded and returned to you within 5 business days of completion.
6. If you fail the test, you will need to retake it until you pass.
7. Once you pass, you will receive an email notification documenting that you successfully completed the 2018 Security Awareness Training Course.
8. It is your responsibility to follow up with your security staff to ensure your results are recorded properly and reported.

Requirements:

You must answer at least 12 out of 16 questions correct (75%) to receive automatic credit for the 2018 Security Awareness Training course and Knowledge Check. If you do not answer at least 12 questions correctly, you will be required to complete the 2018 Awareness Training course and Knowledge Check.

1. What are DOT IT resources? *(Check all that apply)*
* Workstations, laptop computers, servers
* The network infrastructure (e.g., wiring and cable, printers, etc.)
* Tablet computers (e.g., Android Tablet, Pilot, iPad, etc.)
* Smart phones, text messaging systems (e.g., Android and iPhone)
* Plug-in and wireless add-ons that employ removable media (e.g., USB flash memory aka thumb drives, external drives, diskettes, CDs, DVDs, etc.)
* DOT information, data, reports, websites, etc.
1. Personally Identifiable Information (PII) is any information about a human being, living or deceased, regardless of nationality, that is maintained by a federal agency and permits identification of that individual to be reasonably inferred by either direct or indirect means. *(Select one)*
* True
* False
1. Who is responsible to protect Personally Identifiable Information (PII), Sensitive but Unclassified (SBU), Sensitive Unclassified Information (SUI), and other DOT sensitive data? (*Select one)*
	* All DOT employees and contractors who use DOT information systems.
	* Only DOT employees and contractors authorized to access the data.
	* Supervisors of the DOT employees and contractors with access to the data.
	* The Information System owner of the system where the data resides.
2. When dealing with PII or sensitive data, all DOT Federal Employees and Contractors must: *(Select all that apply)*
	* 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 send PII and other sensitive data to your personal account when teleworking.
	* 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 an external agency request for PII or sensitive information.
	* Lock workstation and laptops while away, even for a short time. (e.g., going to the bathroom, retrieving items from the printer, etc.)
	* Protect all PII and sensitive data as if it were your own.
3. Passwords must: *(Select all that apply)*
	* Be at least twelve (12) characters long.
	* Have a combination of letters (upper and lower case), numbers and special characters.
	* Be updated at least every 60 days.
	* Be updated immediately if you suspect your password has been compromised.
	* Always be shared with your supervisor upon request or in response to an ISS incident.
4. Hackers and social engineering scammers use many methods to gain unauthorized access to government systems. They often: *(Select all that apply)*
	* Take advantage of vulnerabilities in software to break into government systems.
	* Use emails to entice you to provide your personal information.
	* Lure you to click on malicious links on websites.
	* Call you on the phone and ask for information they want.
	* Offer you free software, subscriptions, USB drives, CDs, or DVDs.
5. If you suspect an email phishing attempt, you should? *(Select all that apply)*
	* Forward the email to the DOT Security Operations Center (SOC)(9-AWA-SOC@faa.gov) within one (1) hour of the discovery.
	* Delete the email so that you don’t accidently click on it in the future.
	* Respond to the email informing the sender of your suspicions and request to be removed from the sender’s mailing list.
	* Click on the links provided in the email to confirm it is a valid phishing attempt.
6. Valid uses of the DOT Internet include: *(Select all that apply)*
	* Operating a private business.
	* Exchange of information that supports the DOT mission, goals, and objectives.
	* Accessing pornographic material.
	* Job related professional development for DOT workforce personnel.
	* Access to scientific, technical, and other information that has relevance to the DOT.
	* Business related communications with colleagues in Government agencies, academia, and industry.
	* Gambling.
	* Limited access to social media when you are on break or are having lunch, as to not interfere with your job responsibilities.
7. Before you telework, you must: *(Select all that apply)*
	* Be designated as a telework eligible employee.
	* Purchase a personal laptop or computer to utilize when connecting with DOT information systems.
	* Familiarize yourself with and adhere to the DOT Order 1501.1A Telework Policy (PDF).
	* Have an approved telework agreement in place.
	* Remove all non-DOT issued equipment connections from your offsite Wi-Fi network.
	* Have an agreed upon work schedule with your manager.
	* Visit the DOT telework website for additional information on teleworking and to see if you are eligible.
8. When you use laptops and other portable devices, you must: *(Select all that apply)*
	* Only use DOT issued laptops and portable devices to access DOT systems (unless otherwise explicitly authorized).
	* Ensure anti-virus and firewall software is installed and up-to-date.
	* Ensure your personal laptop has updated virus protection before connecting it to a DOT system.
	* Utilize any type of 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 whenever possible.
9. If you suspect you’ve witnessed or are currently involved in a cyber-incident, you must:*(Select all that apply)*
	* Immediately shutdown and restart your computer to allow anti-virus protocol to address the suspected incident and validate occurrence.
	* Report all suspected or actual ISS incidents or privacy breaches to the DOT Security Operations Center (SOC) within one (1) hour of their discovery.
	* Support the DOT SOC and all related ISS personnel in the investigation of any incident.
	* After contacting the SOC, report the suspected or actual incident to your immediate supervisor.
10. Which of the following examples does not qualify as Sensitive but Unclassified (SBU), Sensitive Unclassified Information (SUI)? *(Select one)*
	* IP addresses of DOT systems.
	* Account logon information.
	* Passwords.
	* System vulnerability information.
	* Business records.
	* Operating procedures.
	* Security plans.
	* None of the above.
11. When are you permitted to leave your Personal Identity Verification (PIV) Card unattended? *(Select one)*
	* Only when it is inserted into your DOT issued computer or laptop, and you are going to your local printer to retrieve DOT related information.
	* Only when it is inserted into your DOT issued computer or laptop, and you are going to the bathroom.
	* Only when it is located within your DOT workstation (but not in the computer or laptop) and the workstation is secured by physical guards.
	* Never.
12. When using personally-owned technology on a DOT network, you must: *(Select all that apply)*
	* 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. (e.g., 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 tech
13. Which is a permitted use of DOT Internet or DOT email? *(Select one)*
	* Stream audio or video (non-work related).
	* Download or share files from peer-to-peer networks
	* Attempt unauthorized access to information systems.
	* Auto-forward DOT email to personal account(s).
	* Respond to, send, or forward jokes, chain emails, or offensive content.
	* Send DOT sensitive information to your personal account(s).
	* None of the above.
14. If you receive an unrequested email, even from a valid sender within the DOT, that has a cryptic message and questionable attachment or links, you must: *(Select all that apply)*
	* Contact sender via a separate communication method (e.g. email, phone call, text, etc.) and verify validity of email.
	* Never download or open attachments, without verification from the sender that the email is valid.
	* Never click links within the email, without verification from the sender that the email is valid.
	* Immediately delete unverifiable email.
	* If unverifiable email appeared to be from a DOT email address, report this suspected phishing attempt to the FAA Cyber Security Management Center
	* All of the above.