Remote Work Best-Practices

What is SSI?

SSI is information that, if publicly released, would be detrimental to transportation security as defined by 49 CFR Part 1520. Although SSI is not classified information, there are specific policies and procedures for recognizing, marking, protecting, safely sharing, and destroying SSI. This guidance may be used as "Best-Practices" by regulated entities to ensure protection of SSI within their organizations.

Protecting SSI

"Duty to protect information. A covered person must:

(1) Take reasonable steps to safeguard SSI in that person's possession or control from unauthorized disclosure…" and

(2) Disclose, or otherwise provide access to, SSI only to covered persons who have a need to know, unless otherwise authorized in writing by TSA, the Coast Guard, or the Secretary of DOT" and

(3) "Dispose of SSI as specified in 1520.19…must destroy SSI completely to preclude recognition or reconstruction of the information…"

The same handling and safeguarding requirements that apply to SSI at your worksite also apply when teleworking or working remotely.

Managing Sensitive Data in Webinars

- ✓ Manage policies to ensure only desired members can attend; for example, verify attendees are covered persons with a need to know, or enable a waiting room to vet attendees.
- ✓ Lock the event once all intended attendees have joined.
- ✓ Ensure that the host can manually admit and remove participants, including quickly removing unwanted attendees, if necessary.
- ✓ Be mindful of how (and to whom) the links are disseminated.
- ✓ When recording meetings, make sure participants are aware and that the host knows how to access and secure the recording.
- ✓ Consider sensitivity of data before exposing it via screen share or uploading it during video conferences.
- ✓ For more helpful hints and information on common video conferencing tools see *Guidance for Securing Video Conferencing* - https://www.cisa.gov/sites/default/files/publications/CISA_Guidance_for_Securing_Video_Conferencing_S508C.pdf.

Security Practices while Working Remotely

- ✓ Change default router and Wi-Fi network passwords to strong, complex passwords.
- ✓ At a minimum, ensure the home router is configured to use WPA2 or WPA3 wireless encryption.
- ✓ Avoid using public hotspots and networks.
- ✓ Only use secure video conferencing tools approved by the organization.
- ✓ Only use official company email and equipment when sending or handling SSI.
- ✓ Do not use personal email or equipment, including mobile devices, printers, or computers, to process, access, or store sensitive information.
- ✓ Ensure that any virtual assistants will not pick up conversations.
- ✓ Do not work in locations where the computer screen may be visible to others.
- ✓ Take measures to prevent eavesdropping, especially when discussing sensitive information.

For more information on SSI, including best practices for handling SSI, please contact the SSI Program at SSI@tsa.dhs.gov.

2022 Version