Slide 1: Welcome to the latest edition of the Security Awareness Virtual Initiative, SAVI. There are a lot of questions about SAVI, from what it is to when it is required, and why. Over the next couple of slides we will go over some common questions about the SAVI.

Slide 2: Before we begin, the SAVI is equipped with an audio feature. Please adjust your speakers or plug in your headphones prior to proceeding with the course. There is also a transcript available. You are not permitted to jump ahead; you are only allowed to navigate to previously viewed pages. This year’s SAVI also has a glossary of common security terms. Throughout the course, whenever you see a word or term in bold and underlined, the SAVI glossary can be accessed to obtain more information. When prompted, please click on the “Play” button, when it begins to flash, to advance to the next slide.

Slide 3: The Office of Security and Hazardous Materials Safety (ASH), is responsible for ensuring the security of FAA personnel, facilities and information. The SAVI is an awareness initiative that was created to acquaint employees with the general principles or newly adopted security practices to protect FAA facilities and Information. These principles apply to all FAA facilities and FAA employees. SAVI supplements site specific training that is also required annually.

Slide 4: First, everyone will receive the "What's New" training on Workplace violence, Presidential Policy Directive 19 and the release of classified information, Visitors to FAA facilities, Prohibited items at FAA facilities and Counterintelligence. Next, you can choose to take a pretest. If you score at least 80% on the pretest, you can choose to skip the remainder of the awareness training. Even if you pass, you can still choose to see the rest of the course. The rest of the course covers Key Personnel, Your security responsibilities, Reporting security incidents, Protecting government property, Classified National Security Information (CNSI) & Sensitive Unclassified Information (SUI). Most people finish this course in about an hour.

Slide 5: Another question that comes up is, who should take SAVI? In short, anyone who works at FAA facilities, including leased facilities. This includes contractors, subcontractors, military personnel and other federal employees who work at FAA facilities. If someone is new to the FAA they should receive site specific training within 30 days of arrival at an FAA Facility and take the most recent SAVI within 90 days.

Slide 6: The content for SAVI comes from FAA Orders, baseline security measures from the Interagency Security Committee and from an analysis of incident trends that occur at FAA facilities. Here are some of the orders that SAVI is based on, click on each to get more information.

Slide 7: Aside from FAA Orders, there are a number of resources available to assist you with your security responsibilities. Here are some products that you can click on to view or download. These are also available on FAA’s intranet or throughout this course by clicking on the attachments menu.

Slide 8: Workplace Violence

Slide 9a, Workplace Violence Overview: Workplace violence is any physical assault, threatening behavior or verbal abuse directed toward a person at work. A person must fear that harm or violence will take place or that actual violence has already taken place. Workplace violence can be committed by a co-worker; an individual that is known to your co-worker but unknown to you (e.g., friend, relative); someone you provide a service to (e.g., a customer); or an individual without any affiliation to your organization like a stranger.
Slide 9b, Workplace Violence Categories: Workplace violence can fall into any one of the categories listed below:

- Bullying, Harassment, or Intimidation
- Threats or Threatening Behavior
- Verbal Altercations
- Physical Altercations
- Weapons Involvement
- For more information view the Workplace Violence Handbook available in attachments tab.

Slide 9c, Indicators of Potential Violence: While there is no specific profile to predict that an individual will become violent, you should be alert to behaviors that could indicate the potential for violence. Changes in behavior, especially extreme changes, can often signal an increased risk of violent behavior. Working with colleagues and regular customers or clients, you are likely to notice when they become seriously affected by stress, loss, illness or other forms of distress.

Slide 9d: List of Workplace Violence Indicators

- Increased use of alcohol and/or illegal and prescription drugs.
- Unexplained increase in absenteism.
- Noticeable decrease in attention to appearance and hygiene.
- Depression/Withdrawal.
- Resistance and overreaction to changes in policy and procedures.
- Repeated violations of policies and procedures.
- Increased severe mood swings.
- Noticeably unstable, emotional responses.
- Explosive outbursts of anger or rage without provocation.
- Suicidal comments.
- Behavior which is suspect of paranoia, ("everybody is against me.")
- Increased comments about problems at home.
- Escalation of domestic problems into the workplace; talk of severe financial problems.
- Talk of previous incidents of violence.
- Empathy with individuals committing violence.
- Increase in unsolicited comments about firearms, other dangerous weapons and violent crimes.
- The appearance of noticeable injuries (e.g., bruises).
- The co-worker is being harassed or threatened by a known acquaintance.
- Any activity or behavior that causes you alarm or concern.

Slide 9e, Reporting Workplace Violence Events: All workplace violence events or concerns must be reported immediately! Non-Emergency Situations: Contact your manager/supervisor, building security officers or your Servicing Security Element (SSE) as soon as possible. Emergency Situations: For crimes in progress, specific threats of imminent violence, call 911. If possible, use a phone out of sight and hearing of the individual. The police will respond. For detailed information on preventing and responding to incidents, view the Workplace Violence Employee Guide by accessing; https://employees.faa.gov/org/staffoffices/ash/workplace_violence/media/WV_Employee_Guide_Final.pdf

For support with issues related to Workplace Violence contact: FAA Human Resources for your region-https://employees.faa.gov/org/staffoffices/ahr/about_us/regions/

The Security Serving Element for your region- https://employees.faa.gov/org/staffoffices/ash/contact/ and/or the Accountability Board- https://employees.faa.gov/org/staffoffices/ahr/accountability_board/
FAA's Employee Assistance Program (EAP) available 24/7 at 1-800-234-1327, TTY 1-800-456-4006. Contract personnel might have their own EAP.

Slide 10: Active Shooter

Slide 11a, Increase your awareness of a possible Active Shooter: An active shooter is an individual actively engaged in killing or attempting to kill people in a confined and/or populated area. Situations involving extreme violence can be unpredictable but there are steps you can take to increase your chances of surviving.

Slide 11b, Be Prepared: Become familiar with your work environment, building, and your co-workers. Learn alternate routes out of your building or immediate work center. Watch for the warning signs or indicators of potential workplace violence.

- Run. If you have the ability to escape your location, that is your best option.
- Hide. If you can't escape but can hide, then your next best option is to hide.
- Fight. If you can't run or hide, then your last resort is to fight. This means you have no choice but to defend yourself any way you can against an active shooter.

We hope that no one has to face this type of situation. Next, we will provide you with resources that have some additional information on this topic.

Slide 11c, Active Shooter Video: Please click on the link below to watch a short 5 minute video on how to survive these types of situations. This video was produced by the City of Houston Mayor's Office of Public Safety and Homeland Security.

WARNING: The video depicts a realistic active shooter situation and can be graphic at times.

To watch the Active Shooter video visit: https://employees.faa.gov/tv/?mediaId=735
To view the Active Shooter transcript, visit the attachments tab.

Slide 12, Workplace Violence Review Question: You notice that a co-worker, Michael, has been under a lot of stress lately. You can hear him yelling at another co-worker, threatening him. What should you do?

A. Confront Michael, which may escalate the situation.
B. Leave Michael alone, he is usually a calm person.
C. You should seek the assistance of co-workers to try and defuse the situation.
D. You should report the incident to your manager, Facility Manager and SSE immediately.

Correct Answer: D

**Slide 14, Release of Classified Information:** Under Section B of Presidential Policy Directive – 19 (PPD-19), you have a right to appeal adverse actions affecting your eligibility for access to classified information if you believe these actions were made as a result of “whistleblowing.” Whistleblowing generally refers to an employee’s reporting of fraud, waste or abuse. You will not be protected by PPD-19 if you release classified information. The unauthorized disclosure of classified information is a serious offense, and can properly result in revocation of a clearance as well as other disciplinary actions.

**Slide 15: FAA's Visitor Policy**

**Slide 16a, Changes to FAA’s Visitor Policy:**

- **Foreign Nationals.** Updates to the visitor procedures for foreign national visitors to FAA facilities.
- **VIPs.** Policy and procedures for hosting visits by federal executives, other state and local government officials, foreign dignitaries and Heads of State.
- **Process Servers.** Policies and procedures for coordinating with law enforcement agencies (LEAs) and process servers.

**Slide 16b, Visitor Policy Revisions:**

- **Escorts.** All visitors must be assigned a sponsor and must always be escorted within visual and voice control, while in an FAA facility.
- **No Cameras.** Visitors are restricted from using cameras and recording devices while in an FAA facility unless permission is granted by the facility manager.
- **Technology & Systems.** Sponsors, escorts and FAA employees must not allow visitors access to any FAA information technology (IT) or the National Airspace System (NAS).
- **Denials of Access.** If any visitor is denied access, contact the Servicing Security Element (SSE) immediately and provide the information collected about the denied visit request.

**Slide 16c, VIP Visitors:** Safeguard Visit Information. All VIP visit information should be safeguarded at the appropriate level of protection depending upon the classification of the information.

- **Notify the Servicing Security Element (SSE).** The Servicing Security Element must be notified of any visit request by DOT executives, other Federal, State, and local government officials, foreign dignitaries and Heads of State.
- **Protective Details.** All DOT executives and their protective detail members (if any) shall not require facility escorts if they possess and produce a valid, current, HSPD-12, Personal Identity Verification ID Media (PIV Cards). Any persons not able to produce such ID media, must be escorted at all times while on FAA owned/leased property.
- **Air Traffic Facilities.** All visitors to Air Route Traffic Control Centers (ARTCCs), Terminal Radar Approach Control facilities (TRACONs), Combined Enroute Radar Approach Control facilities (CERAPs), and Air Traffic Control Towers (ATCTs), must be escorted at all times.

**Slide 16d, Procedures for Foreign National Visitors to FAA Facilities:**

- **Must have Sponsor.** Every foreign national visitor must have a FAA sponsor. FAA contractors cannot sponsor a visitor.
- **Use IVP.** Requests must be submitted through the automated International Visitors Program (IVP) at least 10 working days prior to the visit. If the request is not done before the visit, the facility manager may, under controlled conditions, allow the visit. To access the IVP website visit: [https://destination.faa.gov/LandingPage.aspx](https://destination.faa.gov/LandingPage.aspx)
• **Continuous Escort.** Foreign national visitors must be under continuous escort by personnel with valid DOT/FAA ID media. Foreign visitors are not authorized unescorted access to any part of the facility.

• **No Cameras.** Foreign national visitors are restricted from the use of cameras and recording devices unless approval has been granted.

• **No access to Information Systems.** Sponsors, escorts and all FAA employees must not allow foreign visitors access to any FAA information technology system.

Slide 16e, Guidance for Cooperating with Law Enforcement Agencies and Process Servers:

Appendix E to the newly published visitor policy provides guidance regarding the service of complaints, summons, subpoenas (civil or criminal), warrants and other legal processes (collectively “legal process”) on Federal, contract, and military personnel while they are present at an FAA facility. It is the FAA’s general policy to cooperate with Law Enforcement Agencies and Law Enforcement Officers (LEOs), acting within the scope of their official duties. Civilians serving legal processes may not have the same authority as Law Enforcement Officers and accordingly may not be entitled to the same access to FAA facilities.

Slide 16f, Process Server Policy: FAA employees are not authorized to accept service of process on behalf of other employees, the FAA, or the Administrator unless authorized by regulation, order or prior approval of the Office of the Chief Counsel through the responsible office. In accordance with FAA order 1600.69, FAA Facility Security Management Program (FSMP), the facility manager is responsible for implementing the security policies for their facility and documenting required implementation details in the Facility Security Plan (FSP). The Facility Security Plan must contain a section on the procedures the facility will follow to ensure cooperation with Law Enforcement Officers and process servers.

Slide 17, Visitor Policy Review Question

Sally wants to sponsor a foreign national visitor for their upcoming training exercise. What should she do?

A. She should advise the foreign national visitor to show up the day of the training exercise.
B. She should submit an electronic request using the International Visitor's Program (IVP) at least 10 days prior to the visit.
C. She should provide the foreign national visitor's information to her manager prior to the training exercise.

Correct answer: B

Slide 18: Prohibited Items at the FAA

Slide 19a, Prohibited Items at the FAA: FAA Order 1600.69 prohibits you from bringing any weapons or items onto government property. When in doubt, ask your Facility Manager or Supervisor before you bring any items to work. In the next 3 slides we will discuss various types of prohibited items. To see a complete list of prohibited items please visit the attachments tab.
Slide 19b, Projectile Weapons and Firearms:

- Prohibited Firearms and Projectile Weapons and their replicas, to include toys.
- BB, Pellet or Compressed air guns
- Flare guns
- Realistic replica or toy firearms
- Starter pistols
- Stun guns and other electric weapons
- Slingshots

Slide 19c, Clubs and Blades:

Clubs:

- Club-Like Items and Striking Devices, to include flashlights used for striking.
- Billy clubs
- Brass Knuckles
- Martial Arts weapons
- Nightsticks

Blades:

- Bladed, Edged, or Sharp Tools
- Axes or hatchets
- Bows and arrows
- Ice picks
- Martial Arts weapons
- Daggers, swords, and blades more than 2½ inches in length

Slide 19d, Explosives and Disabling Chemicals:

Explosives include:

- Destructive Devices and Explosives
- Blasting caps and detonators
- Bombs
- Dynamite
- Fireworks
- Plastic explosives
- Firearm cartridges
- Hand grenades

The list of disabling chemicals and other dangerous items includes, but is not limited to:

- Mace, pepper spray, tear gas, tear gas guns, or other chemical sprays designed for self-defense (unless meeting the exemption listed in 18 U.S.C., sect 930(d))
- Explosive or rapid expanding gasses
- Gas torches
- Flammable liquids
- Chlorine and bleach*
- Toxic industrial chemicals and/or materials

*Except as required for use on the job
Slide 20, Prohibited Items Review Question

Which of the following are prohibited items? (Drag and drop the correct answer)

A. Blades under 2 1/2 inches in length, a book of matches, and a pair of small sheer scissors.
B. Blades over 2 1/2 inches in length, bows and arrows, and firearms.
C. Small utility knife, box cutters office use and a staple gun.
D. None of the above.

Correct Answer: B

Slide 21, Counterintelligence

Slide 22a, The FAA is Concerned: The FAA is concerned with economic espionage and foreign agents/collectors. Economic espionage is the theft of trade secrets, intellectual property, technology, and research by a foreign country for the purpose of gaining or accelerating their own economic and commercial capabilities. Several foreign countries conduct economic espionage—especially in cyberspace—to rapidly grow their civil aerospace or military capabilities. FAA has aerospace information these countries want, and they are attempting to acquire it from us and our civilian U.S. aerospace partners.

Slide 22b, Potential Targets: If you work with information generally not accessible to the public at the FAA, foreign agents/collectors might target:

- Technical information belonging to the FAA, a strategic partner or an aerospace vendor (e.g., Boeing, General Electric, or Department of Defense).
- Pre-release of closely held information (e.g., draft certification decisions, or treaty negotiation points).
- Sensitive research and development activities (e.g. NextGen).
- Information on aerospace components (e.g., advanced materials, or avionic systems).
- Classified or military information.

Remember: Even if you think information is of little value, it might be highly valuable in a foreign country!

Slide 22c, Reporting Espionage Events: Who, When, and to How do I report Espionage Events? If you know or suspect a foreign counterpart or unauthorized person tried to get FAA information generally not publicly available, then contact your SSE immediately. The SSE will pass the information to AEO.

Slide 22d, What can you do about foreign espionage? Never let any foreign visitor use your FAA computer—even supervised—EVER! While on foreign travel, your status as a U.S. official makes you an attractive target for extra searches, surveillance, and possible exploitation. Do not take more electronics or technical material than is absolutely necessary. Don’t reveal to any foreign counterpart more FAA information than is required. Never mention sensitive issues or personal opinions about the FAA with foreign counterparts or on social media sites like Facebook or LinkedIn. Be sensitive to local customs, culture and holiday traditions. Remember, you are an official representative of the U.S. Government. Act responsibly.

Slide 22e, Occurrences while on foreign travel: If the event occurs while on foreign travel contact the Regional Security Officer (RSO) at the nearest U.S. Embassy or Consulate. After you return to your duty station, contact your SSE as soon as possible.
Slide 23: Counterintelligence Review Question

Which of the following are examples of FAA information a foreign government might try to acquire through espionage?

A. Classified or military information.
B. Technical information belonging to the FAA or a partner.
C. Information on aerospace components.
D. Sensitive NextGen research and development activities.
E. All of the above.

Correct Answer: E

Slide 24: This year’s ASH SAVI once again provides employees with the option of taking a pretest. ASH has found that this option significantly decreases the amount of time an employee will spend on this material. If you pass the pretest you will receive credit for taking this year’s SAVI. In order to be credited with completing the course you must answer 16 of the 20 questions correctly. You can always opt out and take the entire SAVI Course.

Slide 25: SAVI Pretest

Slide 26, Pretest Completion: You have successfully completed the Pretest. You have the option of continuing with the remainder of SAVI content or receiving your completion certificate. Receive Certificate of Completion or Continue SAVI.

Slide 27, ASH SAVI: You will now proceed to the remainder of the ASH SAVI Course. Lets Go!

Slide 28: The key personnel with security responsibilities at FAA facilities are:

- The Servicing Security Element (SSE)
- The Facility Manager
- The Facility Security Coordinator (FSC)
- and most importantly you, the FAA Employee

During the next slide we will review these individuals and roles in more detail.

Slide 29a: Servicing Security Elements (SSE)

- Found within the ASH Organization
- FAA Headquarters, Joint Office, Regional or Center organizational element responsible for providing security services to a particular FAA activity
- Provides assistance and advises the Facility Manager on pertinent security issues/concerns that could have an impact on personnel or facilities
- To find your region’s SSE, Click Here.

Slide 29b: Facility Manager

- Responsible for the security at specific FAA facilities.
- Implements corrective action to eliminate security vulnerabilities identified during security inspection
- Collaborates with the Building Security Committee (BSC) to develop and implement the Facility Security Plan (FSP)
- Reports security incidents to Servicing Security Element (SSE)
Slide 29c: Facility Security Coordinator (FSC)

- Acts as the Facility Manager’s representative on various security issues.
- May service more than one facility.
- Often acts as a liaison between Facility Manager and SSE

Slide 30: Key Security Personnel Review Question

Jesse keeps hearing about "SSE". Please help Jesse identify the role of an "SSE".

A. The servicing security elements (SSEs) are not specialists in physical security and do not act as a resource to assist the Facility Manager and FSC in providing the most secure workplace.

B. The servicing security elements (SSEs) are special agents who specialize in security and are responsible for providing security services in their respective regions, service areas or centers.

C. The servicing security elements (SSEs) are special agents for local law enforcement who have the responsibility of assisting their local law enforcement agencies on implementation plans to provide the most secure neighborhoods.

Correct Answer: B

Slide 31: Employee Responsibilities and Incident Reporting

Slide 32, Employee Responsibilities: Employees must follow all security policies and procedures to ensure the safety and security of their fellow employees as well as the physical security of the buildings they work in. All employees must be familiar with the access control measures for their facility, where to meet in the event of a building evacuation or other emergency and how to report suspicious activity and security incidents.

Slide 33, If you see something, report it!

- You are FAA's best security resource. Pay attention to your environment.
- Employees like you prevent harm and stop many crimes because when they notice something, it is reported. Here are examples from the real world where employees made a difference by reporting suspicious activity;
  - Street vendors in Times Square alerted a mounted police officer after they spotted smoke coming from a vehicle that contained a car bomb.
  - Aldrich Ames, a CIA Analyst, was discovered and convicted of espionage after a fellow employee reported that he was living well beyond his means. The information Ames sold led to the death of at least 10 U.S. agents and compromised hundreds of U.S. intelligence operations.

Slide 34, If you see something, report it (cont’d):

- Always be on the look out for suspicious activity, persons, packages and items.
- Report unattended items to security immediately.
- Don't be silent.
Slide 35, **How to Report an Incident:** Contact your SSE to report anything that might indicate a security incident. Include basic information in the Incident Report such as:

- Who was involved?
- Who else might have seen what you saw?
- What did you see?
- When and where did you see it?

Slide 36, **Report a Security Incident Review Question:**

You are walking out of the building and notice the door does not properly close behind you. The door does not latch and remains ajar. You should immediately report the door to your manager and to the facility manager.

A. True
B. False

**Correct Answer:** A

Slide 37, **Protecting Government Property**

Slide 38a, **You are Responsible:** Every employee is responsible for protecting government property; this includes reporting its loss, theft, damage, or misuse. Servicing Security Elements (SSE) advise Facility Managers and Property Custodians on the protective measures necessary to protect Government property.

Slide 38b, **FAA assets need to be protected:** Many FAA assets are valuable or very portable and easy to steal. As such, FAA assets need to be under continuous protection against theft and inventoried regularly to prevent loss.

Slide 38c, **Copper Wiring:** One example is copper wiring in which the FAA has experienced unusually high losses. Sometimes the same location suffered losses multiple times.

Slide 38d, **Report It:** Report any loss, theft, or damage of government property to its Property Custodian and your SSEs using a Report of Survey (ROS).

Slide 38e, **What actions can you take to reduce the risk of property theft?**

- Conduct timely inventories and report the theft/loss of property to SSE's.
- Ensure all property is in a locked cabinet/room.
- Don't leave an office or storage area unlocked.
- Store valuable property separately from cheaper supplies.
- Secure keys and ID's. Report lost/stolen keys and ID's.
- When leaving desk, take ID with you.
Slide 39: Protecting Government Property Review Question

Last night, while at dinner with friends, Diane's car was broken into. Her government issued laptop and cell phone were in one of her stolen bags. What should she do? (Drag and drop the correct answer)

A. Diane needs to call the FAA's Security Guards/Officers and notify them of the theft.
B. Diane should not say anything to anyone and purchase a new laptop and cell phone.
C. Diane should report the theft to her manager and SSE using the report of survey (ROS).
D. Diane should conduct her own investigation and try to locate the stolen property on her own.

Correct Answer: C

Slide 40: Classified Info & Sensitive Unclassified Info (SUI)

Slide 41, Training Requirements for Individuals with access to Classified Information: Individuals who have been granted access to classified information must be trained annually on how to protect it prior to initial access. The course titled "Safeguarding Classified National Security Information (CNSI) within the FAA", available on eLMS, meets the training requirements of FAA Order 1600.2. Information about this course can be found on FAA’s Intranet. Contracting Officers and other acquisition officials associated with classified contracts should also attend a course entitled "Industrial Security and Classified Contracts" (Course ID FAA30200910).

Slide 42, Data Spillage: A data spill occurs when classified or sensitive information is transferred or found on an unapproved computer system, network, or website. If you discover or are involved in a data spill you must report it to your Servicing Security Element (SSE). The SSE will ensure that all appropriate actions and notifications are made within the FAA.

Slide 43: Data Spillage Review Question

You discover an e-mail with an attachment marked as being “Classified.” What should you do?

A. Forward the email to your manager, Facility Manager and SSE immediately.
B. Delete the email, you could get in trouble for receiving a classified document.
C. Do not open, forward, or delete the email. Notify your manager, Facility Manager and SSE immediately.

Correct Answer: C

Slide 44a, Sensitive Unclassified Information: Sensitive unclassified information (SUI) is information that requires protection from unauthorized disclosure. This information may qualify for withholding from the public under the Freedom of Information Act and should not be automatically released to the public. SUI includes, but is not limited to For Official Use Only (FOUO), Sensitive Security Information (SSI), Personally Identifiable Information (PII) and NAS operational data. If you have any questions as to the release of sensitive unclassified information please direct your questions to your manager or the subject matter expert. Additional information can be found in FAA Order 1600.75 available in the attachments tab.
Slide 44b, How do we protect SUI?  SUI must be reviewed and approved for release by the responsible FAA Office (i.e., the information owner) before releasing it to the public.

Ways to protect SUI are:
- Marking documents and using cover sheets
- Storing it in locked desks, file cabinets, or in controlled workspaces that limit access to only authorized individuals
- Using encrypted email transmissions
- Document shredding or using approved destruction bins
- Apply the “need to know” principle before dissemination

Slide 44c, Classified Info & Sensitive Unclassified Info (SUI): When destroying sensitive unclassified information, the best practice is to use cross-cut shredder models. The goal in SUI destruction is to “prevent reconstruction.” Most facilities use lockable destruction bins to meet their paper SUI destruction needs.

Slide 44d, Transmission Methods for SUI: Transmission (electronic or physical): Always consider the sensitivity of the information and verify the address (physical or fax) of the intended recipient prior to transmission.

*Fax transmissions: When sending fax transmissions, verify the recipients fax number and verify that the information reached the intended recipient. You can use a standard FAA fax machine.

*Physical transmission: For physical transmission, use opaque envelopes that bear the name of the intended recipient as well as a return address. So you may wish to use certified or registered mail via the U.S. Postal Service, or you are allowed to use any commercial delivery service.

Posting SUI on the Internet is not authorized. It is permissible to post SUI on the intranet, but you must first consult with the responsible, issuing, FAA Office.

Slide 44e, Reporting Incidents involving Classified Information & SUI: If you see a potential incident involving Classified Information or Sensitive Unclassified Info (SUI), then report it to your SSE, the Facility Manager, and your front-line manager. For example, if you see an envelope marked "Secret" on a desk in an empty, unlocked office, then report it no matter who you are. Timely reporting is essential to protect the information. You can report the incident to an individual's management in addition to the SSE, but don't wait to contact the SSE.

Slide 45, Classified Info & Sensitive Unclassified Info (SUI) Review Question:

You need to send some personally identifiable Information (PII) to another employee via e-mail. What should you do?

A. You should send the email without encrypting it and not be concerned with the Personally Identifiable Information (PII) enclosed in the email.
B. You should encrypt the email that holds the Personally Identifiable Information (PII) before you send it.
C. You should never send Personally Identifiable Information via email. You should contact your Security Servicing Element (SSE) for assistance.
D. You should forward the email containing Personally Identifiable Information (PII) to your manager and have them send it.

Correct Answer: B
Slide 46: Final SAVI Test

Slide 47: Test

Slide 48, Review: The key personnel with security responsibilities at FAA facilities are the Servicing Security Element (SSE), the Facility Manager, the Facility Security Coordinator (FSC).

- Individuals are prohibited from bringing any weapons or items that are intended to be used as weapons on to government property.
- If you see something, report it.
- Protect Government Property.
- Protect Classified Info & Sensitive Unclassified Info (SUI)
- Protect FAA information from economic espionage and foreign spies.
- Visitor Requests should be submitted via the FAA’s automated International Visitors Program (IVP) by the sponsor at least 10 working days prior to the visit.
- All workplace violence events must be reported immediately. Non-Emergencies should be reported your manager, building security or your Servicing Security Element (SSE).

Slide 49, Certificate of Completion: Please follow the instructions to properly close and exit this course. Thank you. End of course.