

Consortium Meeting Minutes – January 23, 2019

Welcome – Jake Hoehn, Airport Security Manager

- Jake welcomed and thanked everyone for coming.

Security Topics – Jake Hoehn, Airport Security Manager; Detective Jen Hobbs; Melyssa Meuli, Regulatory Compliance Administrator

- **Door “Shunting” – Jet Bridge Doors** – Gate agents or any individual who “shunts” a door becomes responsible for the security of it. They must remain in the vicinity of the door, maintain visual contact and monitor access to the door. The maximum “shunting” time is 45 mins; setting an alarm on their phone is an easy way to set a reminder and be aware of time remaining. They also need to know the repercussions of a violation. Refer to [MAC Ordinance 117](#) for additional clarification.
- **Challenging** – MSP badge holders are *required* to challenge anyone not displaying proper ID within the SIDA areas and if they cannot produce proper ID, immediately notify the Airport Police. Testing was conducted last week. In some cases, individuals challenged but APD was not notified; need to do BOTH. If you do not have a cell phone, find someone who has one or a radio. Remember to get a good description and direction of travel if they leave the area.
 - As a guideline, repercussions for failure to challenge *and* contact APD are:
 - First Violation could include SIDA retraining and loss of escort privileges
 - Second Violation could include a Hennepin County citation and/or suspension/revocation of badge.

Please pass this information on to everyone. Refer to [MAC Ordinance 117](#) for additional clarification.

- **Concourse Passes** – To obtain a [Concourse Pass](#) full name, date of birth, gender, reason for pass, date and time are required. Also please include the ETA for Concourse Pass pick-up. You can't submit a multi-day request as individuals are vetted daily. Landside has a group template that is available. Concourse Passes should not be requested in lieu of the badging process. This will follow the 7 times rule like being escorted; one exception is for public meetings (Commission Meetings).
- **Escort Procedures** – Please review the [Escort Procedures](#). Refer to [MAC Ordinance 117.2.4](#) Maintaining an Escort – A Person performing as an Escort must, at all times, be in a position to actively monitor, direct and control the movements and actions of the accompanied Person(s). A Person being accompanied by an Escort must be in a position to be actively monitored, directed and controlled in their movements and actions. Failure to follow escort policy could result in civil and/or criminal penalties.
 - As a guideline, repercussions for failure to follow Escort Procedures:
 - First Violation could include SIDA retraining and loss of escort privileges
 - Second Violation could include a Hennepin County citation and/or suspension/revocation of badge. Court fees can be approximately \$400.

Q: If someone has an appointment at badging, can they be escorted?

A: Once the application is turned in, they cannot be escorted.

Q: What if someone is suspended?

A: Notify the badging office and lock up their badge/return it to the badging office until the suspension is over. They cannot be escorted during this time. Upon return, notify the badging office to turn the badge back on.

- **“Tools of the Trade” / Prohibited Items** – DO NOT leave tools/prohibited items unattended; even when going to lunch or getting a drink. This also applies to the AOA, vehicles and open toolboxes. Citations are being issued when this happens. Individuals should call dispatch to report items found unattended and may be eligible for \$AWBUCKS Awards.

MSP Signer Portal Update – Melyssa Meuli, Regulatory Compliance Administrator

- Users continue to be added. Look for a generic email coming for registration (check junk email as well).
- Use Google Chrome as your browser if possible.
- Try copying/pasting the URL into the address bar instead of clicking on the link.
- Updated Authorized Signer Agreement forms are required.
- Get familiar with the Portal – it contains lots of information on your badge holders.
- Currently the reporting does not include Custom Seals; IT is working on this.
- MSPSignerPortal@mspmac.org for questions.

Badging Hot Topics – Anne Thurston, Badging Supervisor

- **Top Reasons for Applicant Denials** – The Badging Office does not want to turn people away, but they have to follow specific rules as they are regulated.
 - Applicant checks a disqualifying crime on the application
 - Address on application is not current (must be where they go home)
 - Address on identification is not current (must be where they go home)
 - Expired documents (only good for 30 days)
 - Applicant doesn't bring old badge with them
 - Applicant doesn't bring application and/or ID with them (Badging Office does not "hold" applications)
 - Applicant is late or doesn't have an appointment
 - Applicant has had a disqualifying crime within 10 years
 - Signer completes application prior to applicant
 - Signer signature appears forged
 - Information has been changed, or whiteout has been used (date can't be crossed out without initials)

Q: What if ID's addresses/names do not match?

A: They must match to move forward in the initial badging process. After individuals obtain a badge and their name/address/phone changes, per [MAC Ordinance 117.3.7](#), they have 10 days to provide updated information to the badging office or they can be issued a citation. **Email any updates/changes to badging@mspmac.org.** The APD does not like to write these citations, but ProWatch needs to be current as there are instances when individuals need to be contacted and the information has not been current.

- **Badge Terminations>Returns** – Effective January 1, 2019 all badges must be returned to the Badging Office within 10 days of deactivation or expiration. If not, the company will be charged a \$200 non-return badge fee. There is a Federal Regulation for Badge Terminations that needs to be followed: Per [US Code of Laws - Title 49](#) “(6) Failure To Collect Airport Security Badges-Notwithstanding paragraph (1), any employer (other than a governmental entity or airport operator) who employs an employee to whom an airport security badge or other identifier used to obtain access to a secure area of an airport is issued before, on, or after the date of enactment of this paragraph **and who does not collect or make reasonable efforts to collect such badge from the employee on the date that the employment of the employee is terminated and does not notify the operator of the airport of such termination within 24 hours of the date of such termination shall be liable to the Government for a civil penalty not to exceed \$10,000.**”
- **Aviation Security Division Emails**
Please use the following e-mail address for quickest response or check the [Badging Website](#) :
 - badging@mspmac.org – Badge deactivations/LOA's/questions/etc.
 - access@mspmac.org – Access questions/requests
 - security@mspmac.org – Signer questions/company documentation/etc.
 - badgingdatarequests@mspmac.org – door swipe requests, etc.
 - mssignerportal@mspmac.org – Authorized Signer Portal questions

Employee Portal Update – Sergeant Jeff Mademann

- Lines have been minimal since the change-over on Jan. 1, 2019.
- Not much is happening right now regarding construction, but we are on schedule for the night of Feb. 4th/morning of Feb. 5th re-opening of Employee Portal 3 and permanent closure of Employee Portal 4.
- Cameras will be installed and there will be more space with the new location.
- **Questions?** – Contact Sergeant Jeff Mademann

Insider Threat Awareness – Detective Dylan Thomas

Anything that may take down an airport will most likely be from an Insider Threat.

- Executive Summary “Insiders” – Potential “insider” threat remains a significant concern:
 - Tightened security in the aviation sector will drive terrorists to adjust tactics
 - Operational planners may seek to recruit or infiltrate airport workers with knowledge and access to secure areas – identify vulnerabilities, help bypass security screening checkpoints & barriers
 - Individuals with criminal and/or known extremist ties have sought or obtained employment at airports – security screeners, vendors inside sterile areas, ramp workers, shuttle drivers, etc.
- Insider Threat Awareness / General Indicators –
 - Airport service workers who are summarily fired with little or no record keeping often reappear at other airports with no indications on their record
 - Significantly altering appearance
 - Burns on hands/body, bleaching of skin or hair
 - Secretive, sweating, avoids eye contact with Police
 - Monitoring access points, use of cell-phone cameras and behavior indicating “photo panning” a hidden camera
 - At airport on their days off, especially if in uniform
 - Avoidance of security cameras, camera sabotage
 - Seeks to work alone and/or unsupervised shifts
 - Presence of unauthorized visitors
 - Threats of violence against the US or individuals
 - Badge sharing and “piggy backing” at security doors
 - Criminal activity and arrests

**An individual with indicators present may or may not be involved in criminal activity

- Aircraft Access and Ramp Access Indicators –
 - Abuse SIDA access or are seen outside of assigned duty areas (especially within aircraft)
 - Overly willing to run sensitive routes and pick-ups
 - Employee arriving or leaving with luggage or items that appear/could be passenger’s
 - Cargo theft and other criminal activity
- Terminal Access Indicators: Food Service, Vendors, Cleaners, Security, Maintenance, Contractors, etc -
 - Seeks additional access or encountered outside of duty areas
 - Theft of official vehicles, uniforms, identification and access cards
 - Unusual inquiries about sterile side security procedures
 - Parking vehicles in restricted zones to observe security responses
 - Monitoring personnel or vehicles entering/leaving secured areas

Further information:

The CBP January Quarterly report is due on the 31st. Please email any questions you may have.

Next MSP Consortium Meeting: April 17, 2019