



# CRISIS MANAGEMENT & MOTORCOACH PREPAREDNESS

BEST PRACTICES

## WHAT SECURITY AND EMERGENCY SITUATIONS MAY EMERGE

- Fleet loss by fire or weather emergency
- Catastrophic Accident or over-the-road incident
- On-board violence by passenger or third party
- Missing passenger
- Human Trafficking recognition
- Over-the-road bus fire or system emergency
- On-site maintenance or severe work injury
- Cyber Security Breach



MUTUAL GOAL: SAFE AND SECURE TRAVEL FOR ALL MOTORCOACH PASSENGERS

# MANAGEMENT AND ACCOUNTABILITY

Best Practices:

- Security Planning and Coordination
- Incident Command, Control, Continuity of Operations (COOP)
- Leadership



# GENERAL

- Designate a mix of senior executives, management, key employees and if applicable, union representatives to serve on the security committee
- Ensure the security committee meets regularly to discuss plans, operating procedures, security information and exercises
- Establish and practice a security committee alert / recall plan
- Keep emergency recall / security committee rosters in a secure and accessible place



- Be sure your security committee understands vulnerability assessments, your overarching security plan and your security training plan
- Know how to safeguard Sensitive Security Information (SSI)
- Maintain security incident records
- Conduct vulnerability and continuity of operations assessments of the company's assets, sites and operating units. Identify threats, consequences and action plans designed to deter or mitigate threats

# MESSAGING

- Do NOT wait for an emergency to try and coordinate media messaging or find your marketing/media partner
- Do NOT wait for an emergency that impacts your employees to search for an EAP or emotional support coordinator

# COMMUNICATIONS

- Develop an employee emergency / crisis employee communication plan. Include an emergency response process for drivers to use when communications are disrupted
- Develop processes designed to establish communications with operating units and facility leadership within 60-minutes of the onset of a crisis event
- Establish a reporting process designed to account for all company assets within two hours of the onset of a crisis event
- Participate in industry, Fusion Center and public safety team communications, command and control exercises, committees and conferences
- Establish and test emergency communication processes such as a “call tree” process with employees at all levels of the organization regularly
- Document the company’s enroute emergency communication process
- Ensure members of the security committee or security team can be contacted 24/7/365
- Provide drivers enroute communication devices (two-way radio, cell phone, etc.)
- Determine if “instant” two-way communications using GPS, tracking devices, or commercial tracking programs such as “Teletrack” systems can be incorporated into your company communications plan as back-up to cell phone service (susceptible to tower failure during emergencies)
- Ensure you are aware of which outside agencies require immediate contact (i.e., OSHA, PUC, etc.)
- Safe words?

# COMMUNICATIONS CONTINUED

- Develop a process to monitor federal (DHS, TSA, FEMA) threat reports, news (CNN, emergency broadcast networks, traffic advisories), external events and intelligence briefings
- Subscribe to incident / emergency management information systems capable of delivering timely and accurate threat information.

Sources include:

- State Police
- State Intelligence and Fusion Centers
- State Homeland Security Office
- Transit and Rail Intelligence Daily Reports(TRIADS)

- Develop a process for security management to disseminate security information and issues to operations management
- Plan to integrate company communications processes with local, state, or federal alert systems
- Provide feedback to employees submitting incident reports
- Establish and follow an escalating internal and external incident reporting process
- Decide if legal counsel should be contacted to maintain confidentiality

# PERSONNEL SECURITY

Best Practices:

- Background Checks
- Training
- Enroute Procedures





# GENERAL

- Establish processes verifying employee identity and background
- In compliance with Federal and State laws, establish preemployment screening policies and procedures addressing disqualification
- Develop a robust internal screening redress process for adversely affected applicants and personnel. Include an appeal and waiver process similar to one established for HAZMAT drivers and transportation workers at ports
- Conduct background, criminal history, Social Security verification, driver's license and endorsement checks (all vehicles and equipment) for drivers and "security-sensitive (access to sensitive/classified information and restricted areas)" employees
- Ensure all individuals are lawfully in the country and authorized to work
- Establish licensing, background check and security training plans for contracted workers identical to those plans and processes in place for employees
- Review security clearances on a periodic basis and establish a review process for new security clearances or renewals
- Establish a formal policy addressing negative security clearance or background check results
- Develop formal security policies disqualifying current or prospective personnel from employment should negative results arise from a background check, investigation, declined or revoked CDL HAZMAT or denial of TSA Security Threat Assessment (STA) clearance

# TRAINING

- Train employees to identify and report security threats
- Brief employees on company security organization, objectives, procedures, support process and levels of employee security responsibility
- Provide general security awareness training for all employees. Focus on a quarterly security topic and incorporate an associated drill into the program (fire extinguisher demo, active shooter protocol, suspicious activity reporting, how to activate GPS panic button, duress codes, suspicious package protocol, etc.)
- Document drills, exercises, anti-terrorism and general security training events. Include topic, names of attendees, training date and location in the documentation



- Maintain primary and back-up access control and clearance records
- Provide periodic security re-training no less than every three years
- Train employees how to safely observe, assess and report suspicious activity or behavior
- Train drivers, dispatchers, fleet maintenance and terminal employees how to use the company's internal and external emergency reporting process
- Include emergency management drills (fire, severe weather, shelter-in-place, bomb threat, evacuations, etc.) for employees AND company leadership in your Training and Exercise plan

# TRAINING



- Provide annual refresher training for first responders
- Keep signed Non-Disclosure Agreements (NDAs) on file
- Participate in security exercises or drills annually with local and federal public safety and security teams
- Meet with external security teams (law enforcement, first responders, other public safety teams) to discuss security issues and opportunities to participate in joint training exercises
- Provide crisis management and crisis response training to drivers, dispatchers, fleet maintenance and terminal employees (e.g. TSA Operation Secure Transport – contact your TSA security partner for more information)
- Establish a security awareness bulletin board in a common employee area. Post timely and accurate security and safety information. Discuss this information at security and safety meetings
- Require operators and drivers to report in, out, before and after bus operating duties

---

## FACILITY / TERMINAL SECURITY

Best Practices:

- Access Control
- Physical Security
- Information Security



# GENERAL

- Develop robust terminal, facility and headquarters security plans
- Partner, share information and conduct facility orientation tours with law enforcement, emergency responders and other public safety teams assigned to respond to emergencies at your facility
- Ask local public safety teams to review terminal security plans
- Ask law enforcement teams to randomly patrol company / facility perimeters
- Invite public safety and law enforcement teams to your facility to train on emergency access / entry to your vehicles
- Assess the need for facility, terminal or motor pool security guards during day, evening or weekend hours
- Install, based on the level of risk and resources, intrusion detection systems (alarm system, CCTV, surveillance cameras access control hardware, etc.) at all locations
- Ensure CCTV cameras are functional, used as designed, adequately monitored and record activity at all locations. Inspect frequently
- Post evacuation routes at places easily seen by employees and customers
- Establish vehicle parking, stopping or standing policy at all facilities
- Install security fencing around the company's bus storage, motor pool or operating facilities
- Maintain facility and terminal fences, landscaping, natural and man-made barriers designed to slow or keep unauthorized persons or vehicles away
- Add fence features such as razor or concertina, alarms, locks and other anti-intrusion devices or hardware
- Install physical barriers (fences, gates, planters, bollards, etc.) where needed to prevent high-speed or unauthorized vehicle access
- Control landscaping to allow unobstructed sight lines to vehicles, pedestrians or restricted areas
- Ensure physical barriers intended to prevent high-speed or unauthorized access are functional, used as designed and maintained
- Inspect and maintain electronic monitoring devices and access control systems regularly
- Maintain security hardware and software maintenance records, inspections and tests
- Install appropriate security lighting at bus staging areas, motor pools, lots and parking areas.
- Contact a local or federal physical security expert to determine recommended threat deterrence lighting levels
- Require vendors to provide advance delivery notification, to include driver and vehicle ID numbers, cargo description, number of containers or packages, etc.
- Ensure facility and vehicle locks are tamper-resistant or "tamper-evident"
- Announce or display information requesting passengers to report suspicious activity
- Develop a mail handling security process and plan (screening, awareness posters, etc.).
- Establish primary and alternate delivery locations for all packages and deliveries
- Require employees to display identification cards or badges at work
- Require facilities to document visitor, contractor and vendor visits
- Provide secure locations for employee parking
- Install clearly visible and easily understood signs identifying restricted or off-limit areas at all facilities
- Incorporate random security checks, measures or spot inspections into your organizations' security policy and practice
- Provide secure locations for employee parking
- Coordinate Visible Intermodal Prevention and Response (VIPR) Team deployment to your terminals and facilities with your TSA point of contact. VIPR Teams augment security operations associated with ANY US transportation mode and serve as a excellent threat deterrent. There is no cost to the stakeholder for VIPR Team deployment

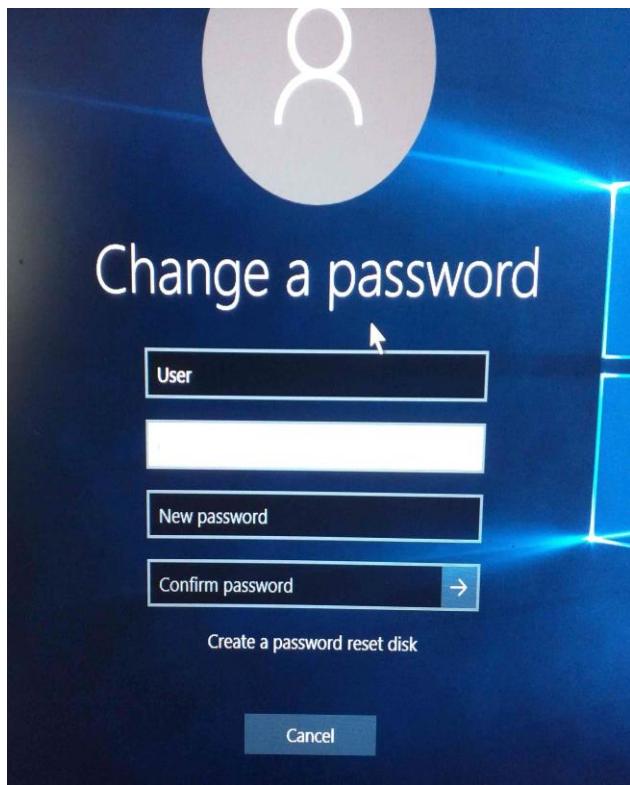
# ACCESS CONTROL

- Equip vehicles with appropriate door/window locks and enforce their use
- Establish a vehicle, facility, terminal and gate key control program, terminals and gates
- Require the use of key card, PIN or biometric input to enter or start vehicles
- Prohibit unauthorized passengers in company vehicles
- Restrict access to a single gate or point-of-entry wherever possible
- Require employees to display / wear badges or photographic ID at company facilities



- Require visitors, vendors and contractors to register or sign in and show photographic ID
- Require employee or security team escorts for business guests
- Develop, publish and disseminate facility access control process to all employees. Clearly sign restricted areas
- Deny access to restricted areas such as computer rooms, administrative areas, dispatch offices for unauthorized personnel
- Randomly spot-check employee identification
- Capture (manually or electronically) employee and visitor entrance and exit data at all terminals and facilities
- Require key cards, PINs or the use of biometric input devices for access to buildings, sites or secure areas

# INFORMATION SECURITY



- Require employees to logon, logoff and to use strong passwords when using company information systems
- Require frequent password changes
- Restrict information system access to sensitive company data to those with internal “need to know” classification
- Restrict information system access with “firewalls” to help prevent internal and external threats
- Establish formal IT security policy and guidelines
- Identify and formally designate an IT security officer or coordinator
- Assign select administrative or security personnel to monitor sector specific DHS Homeland Security Information System (HSIN). If clearances are needed, contact a TSA Motorcoach security specialist
- Develop and conduct vulnerability tests for your IT system
- Designate administrative or security team members to regularly access and review the DHS National Terrorism Alert System (NTAS). Require the same team members to receive automatic electronic NTAS alert updates at [www.dhs.gov/alerts](http://www.dhs.gov/alerts)
- Develop plans to protect company / facility confidential operations information
- Determine and publish your organizations' Bring Your Own Device (BYOD) and bring Your Own Network (BYON) policy

# VEHICLE SECURITY

## Best Practices:

- Passenger, Baggage and Cargo Screening
- Inspections
- Suspicious Activity Reporting (SAR)



# PASSENGER / BAGGAGE / CARGO SCREENING

- Prior to departure, onboard, announce passenger emergency exit features (windows, rear doors, other exits, etc.) of the motorcoach and provide a short demonstration or instruction card detailing how to use the emergency exits
- Announcement, post or provide an instruction card detailing the motorcoach evacuation plan
- Onboard and in terminals or waiting areas post or announce security partnership plans with local, State or Federal law enforcement organizations such as TSA. A sample announce is available for review by contacting your TSA Security Specialist
- Establish a robust passenger, baggage and cargo screening program
- Compile a “prohibited items” list. Publish and post for passengers at terminals, on buses and on web sites
- Restrict or monitor passenger checked bag access at interim points on their trip
- Match checked bags with actual on-board passengers
- Equip vehicles with a safety/security barrier between the driver and passengers
- Participate in a DHS sponsored security inspection or certification program
- Conduct vehicle security and safety inspections prior to vehicle operation (pre- and post-trip inspections)
- Require post-trip vehicle security inspections
- Incorporate “behavior detection” processes in passenger boarding queues
- Provide supplemental equipment for securing vehicles (steering wheel locks, theft alarms, “kill switches,” or similar devices
- Require additional vehicle security inspections in special situations such as vehicle left unattended, driver change, etc.
- Require a “passenger count” or ticket re-verification any time passengers are allowed to exit and re-enter the bus
- Equip vehicles with panic button capability
- Equip vehicles with on-board video cameras
- Secure vehicle cargo / storage areas

Number of items discovered during a 90-day baggage screening pilot at two motor coach terminals	
Knives	7856
Scissors	4439
Sharp Objects	2144
Martial Arts	151
Guns	79
Restricted Tools	550
Alcohol	5948
Drugs	733
Explosive Materials	177
Chemicals	248

## ENROUTE PROCEDURES

- Establish an enroute vehicle tracking and reporting process
- Prior to departure, announce partnerships with local, state and federal security and law enforcement organizations. Mention the partnership recommends random security inspection. Contact TSA for recommended announcement format
- Develop a process to brief drivers, dispatchers and fleet managers on possible security threats along routes before departure
- Equip vehicles with “Emergency-Call Police“ message signs or similar enroute emergency signage program / process
- Conduct regular security inspections  
Require, in addition to any pre-trip safety inspection conducted, a pre-trip vehicle security inspection
- Equip vehicles with GPS or land based tracking system
- Require employees to lock and secure vehicle doors when parked
- Secure luggage bays at all times
- Limit access to baggage storage areas during rest stops





# US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

TAKE ADVANTAGE OF FREE DHS / TSA CYBER SECURITY RESOURCES THAT ALL TRANSPORTATION SECTOR STAKEHOLDERS SHOULD TAKE ADVANTAGE OF:

- **US CERT:** <http://www.us-cert.gov>
  - US-CERT's mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans
- **ICS-CERT:** <http://ics-cert.us-cert.gov>
  - The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors

- Review and incorporate, where applicable, the cyber security framework provided by your TSA point of contact (1st Quarter, 2014)
- Review practice of allowing employees to connect personal devices to company-owned equipment or network, if applicable
- Limit access to sensitive information to those with “need to know”
- Establish clear cyber security policies and procedures; clearly communicate them with all employees
- Require all employees to lock their computers. Unattended / unlocked computers can be easily compromised
- Provide Cyber Security Awareness Training to all employees on an annual basis
- Report unauthorized people in secure IT areas
- Report attempts to get account passwords or other access information by telephone. Secure laptops with a cable lock
- Establish a process for updating your IT system, network and related software via manual or automatic updates to avoid missing critical changes or alerts. Vendors and security researchers identify new vulnerabilities in software and hardware products frequently. Without updates, your systems may be vulnerable to attack
- Use strong passwords to secure your information, and keep different passwords for different accounts
  - Passwords should have at least eight characters and include uppercase and lowercase letters, numerals, and special characters
  - Change all default passwords upon installation, particularly for administrator accounts and control system devices, and regularly thereafter
    - Include passwords for securing wireless routers, CCTV cameras, devices and access points
- Apply firewalls or communication blocking technology to implement network segmentation
  - A firewall or its equivalent is a software or hardware device that filters inbound and outbound traffic between your network or computer and the Internet and between different networks within your enterprise and operational domains
  - Firewalls also act to segment one large network into smaller functional networks so that if one segment of the network or a device is compromised, the threat cannot be spread to others as easily. This strategy is known as “Defense in Depth”
  - Firewalls should be used to separate the Enterprise/IT/ business networks from the Industrial Control networks, and in some cases between different segments of the Industrial Control Networks themselves
- Minimize network exposure for all control system networks
  - Conduct a thorough assessment of your system, including the business network and control system devices. Unless there is a compelling reason, control system devices should not be accessible through the Internet
- Establish “Least Privilege” based access controls to computer systems and networks
  - Least privilege based access control grants or denies access to network resources based on specific job functions. It provides access only to those with specific need and only to those who have achieved proper clearance
- Use secure remote access methods such as a Virtual Private Network (VPN), if remote system / network access is required
  - A VPN is a private data network that uses the infrastructure of the public Internet to transmit data in a secure manner
- Limit use of removable storage devices. Removable storage devices provide valuable functionality but are frequent carriers of malware. Lost or stolen devices can compromise sensitive data, and computers can be infected even without Internet access.
- Develop a cyber security incident response plan. Train employees and exercise the plan. Cyber security incident response plans are a critical yet underdeveloped component of emergency response plans within many organizations

# GENERAL EMERGENCY RESPONSE

- Develop an Incident Response Plan (IRP) for emergency / crisis events
- Exercise the IRP regularly
- Establish a business operations center at an alternate location in the event of a major incident or crisis event. Be sure the alternate location does not share the same power grid as the primary location. Be sure company leadership can communicate with business entities and incident / emergency response teams at the alternate site
- Establish a primary and alternate emergency command center (EOC). Be sure the EOC is equipped to facilitate communication throughout the company and with local public safety teams during emergencies
- Develop a basic emergency response guide suitable for employees describing action to take in the event of disaster or crisis event. Include the guide in your security training curriculum



- Assign a senior leader responsibility for determining the nature, scope, impact and reporting of incidents, disasters or crisis events. Develop plans to be executed in the event of an elevated security alert status from the DHS National Terrorist Alert System (NTAS) or other government source
- Require employees to report security related “suspicious activities” to designated personnel such as management or local law enforcement team
- Establish written suspicious activity notification procedures (who to call, when to call, etc.) for all employees
- Practice response to threat scenarios through tabletop, functional and full scale exercises (coordinated with public safety teams). Response time is measurable and can be improved
- Require “Memorandums of Understanding,” or similar security related agreements with state and local authorities prior to an emergency or incident response

# EMPLOYEE BACKGROUND CHECK REDRESS

- Many stakeholders may use criminal background checks to assess the suitability of employees for positions.
- To the extent a stakeholder chooses to do so for employees with unmonitored access to company-designated critical infrastructure, consider using the federally established list of disqualifying crimes applicable to HAZMAT drivers and transportation workers at ports (see 49 CFR 1572.103).
- While establishing a vigorous internal redress process for adversely affected applicants and personnel, include an appeal and waiver process similar to the system established for HAZMAT drivers and transportation workers at ports (see 49 CFR part 1515).
- Design an appeal process providing an applicant or personnel an opportunity to show he or she does not have a disqualifying conviction, by correcting outdated underlying court records or proving mistaken identity.
- A waiver process can be designed to provide an applicant or personnel with the opportunity to be hired or continue employment by demonstrating rehabilitation or facts surrounding a conviction that mitigate security concerns.
- The industry should consider permitting an applicant or personnel to submit information pertaining to any of the following:
  - • Circumstances of the disqualifying offense
  - • Restitution made;
  - • Letters of reference from clergy, employers, probation/parole officers; and
  - • Other factors the individual believes bear on his or her good character.
- The industry may elect to incorporate the redress process into the disciplinary procedures already used as part of its management/labor relations.



Jill E. Nagy, Esq.  
Summers Nagy Law Offices  
35 South Duke Street  
York, PA 17401

Phone: (717) 812-8100  
E-mail: [jnagy@summersnagy.com](mailto:jnagy@summersnagy.com)

THANK YOU!