Emergency Response Vehicle and Equipment Security

The first responder community relies on the availability of specialized equipment, including emergency response vehicles, to perform their service to the public. When incidents compromising emergency response vehicles or equipment occur, they can not only affect the safety of emergency responders, but also jeopardize emergency responders' ability to provide public safety services in a timely and effective manner. As a result, it is paramount that emergency services organizations continue to educate their personnel and implement best practices to prevent the theft or other misuse of emergency response vehicles and equipment.

Secure Your Emergency Response Vehicles and Equipment

When an unauthorized person gains access to emergency response vehicles or equipment, the acquisition could lead to a potentially dangerous situation. The theft of emergency response vehicles and equipment may be potential indicators of pre-operational activity by malicious actors that constitute a potential threat to our Nation's homeland security as stolen emergency vehicles and equipment have been used to exploit site vulnerabilities, destroy critical infrastructure, and harm people and property.[1] In Israel and Afghanistan, terrorists have used ambulances or other emergency vehicles as vehicle-borne improvised explosive devices.[2] In today's interconnected world, these tactics could easily translate domestically, with malicious actors relying on the general public's respect for emergency responders to reduce suspicion or circumvent security measures. Given the reality that homegrown violent extremists or terrorists may attempt to acquire emergency vehicles and equipment, it is imperative that emergency services organizations continue to educate their personnel and implement best practices to prevent theft of emergency response vehicles and equipment.

Destroyed fire truck
(Photography courtesy of WBNS 10TV)

The theft of emergency response vehicles and equipment can also cause personal and financial loss. For example, a civil lawsuit settlement was reached in 2012, stemming from an incident where an individual stole an ambulance from a Texas hospital and later collided with another vehicle, killing one passenger and injuring four others. Both the hospital and paramedics were found to be negligent for leaving the vehicle running unattended and unlocked.[3] In May 2013, another individual broke into an Ohio fire station and stole a fire truck, destroying it at an estimated replacement cost of $250,000 after hitting a guardrail and overturning the vehicle.[4]

[1] DHS, Transportation Security Operations Center (TSOC); Cloned Vehicles: More than Meets the Eye; March 20, 2009.
[2] Soft Target Hardening: Protecting People from Attack, Jennifer Hesterman; CRC Press, Taylor & Francis Group, LLC 2015.
[3] Gary Ludwig, "EMS: Stolen Ambulances", *Firehouse Magazine*, December 3, 2012, accessed September 2, 2015, www.firehouse.com.
[4] Randy Ludlow, "Thief crashes stolen fire truck", *The Columbus Dispatch*, May 10, 2013, accessed September 4, 2015, www.dispatch.com.

Best Practices

- Install a commercial anti-theft or keyless entry device, if possible.
- Institute use of an automatic vehicle locating/tracking system.
- Maintain active observation of vehicles and apparatus at incident sites, hospitals, training events, etc.
- Lock emergency response vehicles, equipment, and external storage compartments, whenever practical.
- Develop and maintain accurate, up-to-date lists of all vehicles and their associated equipment inventories.
- Consider installing exterior safety cameras on larger response vehicles.
- Routinely review organizational and facility physical security measures.
- Ensure emergency vehicle parking lots, storage areas, and maintenance facilities are secure and under recorded video surveillance.
- Utilize "layering" of locking systems to secure access to sensitive items and equipment (e.g. weapons, explosives, and narcotics).
- Develop procedures to quickly identify a legitimately marked or unmarked response vehicle from a cloned vehicle.
- Develop procedures to secure or disable connectivity options within response vehicles to prevent unauthorized access or loading of malware.
- Maintain awareness of how organizational response vehicles are disposed of and to what extent the vehicles are left recognizable and/or usable.

Resources

- **DHS.GOV** (http://www.dhs.gov/criticalinfrastructure) — The Department of Homeland Security's (DHS) Office of Infrastructure Protection (IP) offers a wide array of free training programs to public and private sector partners. These Web-based independent study courses, instructor-led courses, and associated training materials provide government officials and emergency response professionals with the knowledge and skills needed to implement security and resilience activities.
- **Physical Security Assessments** — Through the DHS Protective Security Advisor (PSA) Program, critical infrastructure stakeholders can request vulnerability assessments, training, and access to other DHS infrastructure protection resources. Contact your local PSA or PSCDOperations@hq.dhs.gov to learn more.
- **Homeland Security Information Network - Critical Infrastructure (HSIN-CI)** — HSIN-CI is the primary platform in DHS for information sharing between and within the critical infrastructure sectors and State and local fusion centers. HSIN-CI enables DHS and critical infrastructure sector stakeholders to communicate, coordinate, and share information in support of the Sector Partnership Framework. For access to HSIN-CI contact HSINCI@hq.dhs.gov.
- **Homeland Security Information Network - Emergency Services (HSIN-ES) portal** — HSIN-ES is a portal in HISN-CI that assists Emergency Services Sector (ESS) to communicate on suspicious activities, threats, and infrastructure vulnerabilities; prepare for and mitigate natural or manmade disasters; and collaborate on restoration and recovery activities following an incident. Email the DHS IP's Emergency Services Team (ESSTeam@hq.dhs.gov) to request access to HSIN-ES.
- ***The Infogram*** **and Critical Infrastructure Protection (CIP) bulletins** — Both of these products are produced by the Emergency Management & Response – Information Sharing & Analysis Center (EMR-ISAC) to share critical infrastructure security and resilience and emerging threat information relevant to the ESS nationwide. Email the DHS IP's Emergency Services Team (ESSTeam@hq.dhs.gov) or EMR-ISAC (emr-isac@fema.dhs.gov) to subscribe to *The Infogram* and CIP bulletins.

Contact Information

For more information, contact the Emergency Services Sector-Specific Agency at ESSTeam@hq.dhs.gov or visit www.dhs.gov/emergency-services-sector.

OMB Control Number: 1601-0014
Expiration Date: 10/31/2017

Stakeholder Feedback Form

General Information

Please select the category that best describes your organization: Select one

Overall Assessment

1. Please evaluate the following statement: The information received through this activity or product was current and relevant.

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

2. Please provide any recommendations that you may have on how future activities or products of this type could be improved to enhance their relevance.

3. Please evaluate the following statement: The information received through this activity or product will effectively inform my decision making regarding safety and security risk mitigation and resilience enhancements.

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

4. Please provide any recommendations that you may have on how future activities or products of this type could be improved to increase their value in support of your mission.

5. Please evaluate the following statement: I will encourage my agency/organization to incorporate information I learned through this activity or product into our safety, security, or resilience practices.

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

6. Please provide any recommendations that you may have on how future activities or products of this type could be improved so they can be better incorporated into safety, security, or resilience practices across the critical infrastructure community.

Submit to: essteam@hq.dhs.gov

Privacy Notice

Paperwork Reduction Act Burden Notice