Impersonation of First Responders

First responders provide the first line of defense for nearly all critical infrastructure sectors and the general public during natural disasters and other physical emergencies. However, malicious actors, both international and domestic, seeking to exploit the public trust first responders have earned, have sought to impersonate first responders in order to do harm to the American people, exploit site vulnerabilities, or destroy critical infrastructure. Malicious actions include the acquisition of authentic or fraudulent uniforms, equipment, vehicles, and other items that may be associated with law enforcement, fire, and emergency services personnel.[1] Therefore, it is imperative emergency services organizations maintain an awareness of the current threat environment and continue to remain vigilant.

Terrorist propaganda, from organizations such as the Islamic State of Iraq and the Levant (ISIL), encourage supporters to engage in local acts of violence. The following examples highlight that extremist propaganda is resonating with audiences in our homeland and that these types of events could extend to the first responder community.

First Responder Emblems
(Courtesy of firefightersupport.org/taking-care-of-each-other)

- In February 2015, Federal Bureau of Investigation (FBI) arrested an individual indicating interest in joining the U.S. military to provide information on U.S. military operations against ISIL and potentially target law enforcement officers or U.S. soldiers.[2]
- In March 2015, the FBI arrested two Illinois residents for conspiring to provide material support and resources to ISIL and planning to use U.S. Army uniforms to enter and attack a local military facility.[3]

Highlighted threats of first responder impersonation internationally include:

- Belgian police raided a house in January 2015 and uncovered police uniforms, weapons, and fraudulent identification documents, raising concern that the suspects may have been seeking to impersonate law enforcement.[4]
- French authorities disrupted a potential terrorist plot in April 2015 after responding to a call at a residence in Paris. A subsequent search of the resident's vehicle and home turned up multiple firearms, ammunition, bulletproof vests, police armbands, notes on potential targets, and other suspicious items suggesting the individual may have been planning to attack a church.[5]

Serving and protecting the public requires Emergency Services personnel to maintain a high degree of vigilance to responder impersonation and the consequences that could occur if successfully exploited. Impersonation of a first responder presents not only a danger to public safety, but also a potential threat to the security of our homeland. Because homegrown violent extremists or terrorists may attempt to impersonate first responders through the acquisition of uniforms, equipment, or emergency vehicles, it is imperative that emergency services organizations continue to maintain threat awareness, report suspicious activity, educate personnel about information sharing resources, and utilize effective measures to prevent theft of emergency response vehicles and equipment.

---

[1] DHS Office of Intelligence and Analysis, *Roll Call Release*, Serial number IA-0264-15, 18 August 2015.
[2] Mariana Regional Fusion Center, *Special Event Threat Assessment*, Serial number SETA-15-007, 16 July 2015.
[3] United States of America v. Hasan R. Edmonds and Jonas M. Edmonds [in-text], Criminal Complaint Case number 15CR 149, U.S. District Court Northern District of Illinois Eastern Division, 25 March 2015.
[4] DHS Office of Intelligence and Analysis, *Roll Call Release*, Serial number IA-0264-15, 18 August 2015.
[5] Ibid.

Best Practices

- Follow established suspicious activity reporting protocols.
- Coordinate information sharing activities with state and major urban area fusion centers.
- Maintain threat awareness by utilizing Federal, State, and local information sharing platforms.
- Routinely review organizational and facility physical security measures.
- Install within emergency vehicles a commercial anti-theft or keyless entry device, if possible.
- Institute use of an automatic vehicle locating/tracking system.
- Ensure emergency vehicle parking lots and maintenance facilities are under recorded video surveillance.
- Develop procedures to quickly identify a legitimately marked response vehicle from a cloned vehicle.

Resources

- **National Network of Fusion Centers** – Located in States and regions throughout the country, fusion centers conduct analysis and facilitate information sharing to empower front-line first responders to understand local implications of national intelligence, thus enabling local officials to better protect their communities. (http://www.dhs.gov/state-and-major-urban-area-fusion-centers)
- **The Joint Counterterrorism Assessment Team (JCAT)** – Comprised of State, local, tribal, and territorial first responders and public safety professionals from around the country, the JCAT works alongside Federal intelligence analysts from the National Counterterrorism Center, Department of Homeland Security (DHS), and the FBI to research, produce, and disseminate counterterrorism intelligence. (http://www.nctc.gov/jcat.html)
- **Homeland Security Information Network - Emergency Services (HSIN-ES) portal** – HSIN-ES is used to communicate on suspicious activities, threats, and infrastructure vulnerabilities; prepare for and mitigate expected natural or manmade disasters; and collaborate on restoration and recovery activities following a serious incident. Email the DHS Office of Infrastructure Protection's Emergency Services Team at essteam@hq.dhs.gov to request access to HSIN-ES. Please include your first and last name along with an email address.
- **Emergency Management and Response-Information Sharing and Analysis Center (EMR-ISAC)** – The EMR-ISAC provides the Emergency Services Sector (ESS) with threat, vulnerability and critical infrastructure protection information and no-cost technical assistance consultation services to ESS leaders. (http://www.usfa.fema.gov/index.html)
- **First Responder Communities of Practice (FRCOP)** – The FRCOP is a professional networking, collaboration, and communication platform created by the DHS Science & Technology Directorate to support improved collaboration and information sharing among the Nation's first responders, other Federal, State, tribal, territorial, and local governments, and private sector stakeholders supporting homeland security efforts. (https://communities.firstresponder.gov/web/guest)
- **Technical Resource for Incident Prevention (TRIP*wire*)** – TRIP*wire* is a free online resource that collects, analyzes, and disseminates information on global explosives-related incidents, terrorist tactics, techniques, and procedures, and related protective measures. (http://www.dhs.gov/tripwire)
- **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.

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