# Soft Target and Crowded Places Landscape Assessment Research Roadmap

Science and Technology

## ROADMAP BACKGROUND

Attacks on soft target or crowded places (ST-CPs) represent a significant challenge in the current security environment. In response to this challenge, the Department of Homeland Security (DHS) Science and Technology Directorate released the Soft Target and Crowded Places Security and Enhancement and Coordination Plan in 2018 to provide key stakeholders in the public and private sector with an overview of its mission to enhance the security and resilience of ST-CPs. To reduce the risk to ST-CPs and better understand the threat, vulnerabilities, status of existing programs, and the optimal allocation of ST-CPs security resources, this study aims to deliver guidance on the types of measures and spending that best align with reducing the number and casualties of ST-CP incidents, by addressing the primary research question of this study:

- How can prevention, protection, and response/recovery investments reduce the risk of casualties from attacks on soft targets and crowded places?

## DESIRED OUTCOMES

This effort will deliver guidance on the types of ST-CPs security and enhancement measures and spending that best aligns with reducing the number and casualties of ST-CP incidents and will provide recommendations to help optimize funding for DHS soft target prevention, protection, response, and recovery. Conducting this research and development is necessary to have the results validated, training disseminated, and operational tactics, techniques, and procedures updated nationally, in time to be included in the planning efforts for major international events (e.g., 2026 World Cup Soccer Tournament). The development of these inputs, strategies, and mission improvements also has the potential to increase awareness of threats, contributing to expanding public awareness of approaches to help secure the homeland.

## RESEARCH DESIGN AND METHODOLOGY

There are five tasks in this effort.

1. **Understand the ST-CPs threat through document analysis and interviews.** A quantitative analysis using past datasets, academic, grey literature (e.g., reports, working papers, government documents, white papers, and evaluations), and case studies.
2. **Address vulnerabilities and current and planned solutions through interviews.** Experts will be identified within key agencies in DHS, other federal government agencies, and industry consultants (e.g., insurance experts) who are engaged in ST-CPs security.
3. **Landscape analysis.** Findings from Tasks 1 and 2 will be synthesized to identify major threats and solutions from different types of attacks across different types of ST-CPs and provide needed capabilities and solutions.
4. **Assessment of preparedness in response/recovery spending.** Previous task findings will be used to estimate expenditures, create cost analysis frameworks, and conduct cost/benefit analyses.
5. **Research and implementation roadmap.** The roadmap will identify needed capabilities, status, gaps, and proposed recommendations and ways ahead. It will document this all in a research report and prepare a summary presentation and report for wider audiences.

The research team will use academic and grey literature review to identify top findings on risk and protective factors. Grey literature will consist strictly of governmental, corporate, and civil society open studies and guidance on responding to the ST-CP threat. Lastly, four case studies will be used to compare high- and no-casualty events and will include cause-and-effect analyses of security measures' impacts.

## IMPACT

This study will deliver guidance to DHS and critical infrastructure security operators to help assist in considerations that could decrease the number and lethality of ST-CP attacks. These knowledge products shall inform security and prevention measures for future events while identifying risk and protective factors in hardening ST-CP security.

## MILESTONES

- **FY23 Q4** – Landscape Analysis
- **FY24 Q1** – Assessment of Preparedness and Response/ Recovery Spending
- **FY24 Q2** – Research and Implementation Roadmap
- **FY24 Q3** – Final Report

## PERFORMERS/PARTNERS

- RAND Homeland Security Operational Analysis Center, Arlington, VA
- Cybersecurity and Infrastructure Security Agency, Washington, DC

**Contact Us:** PSVP@hq.dhs.gov