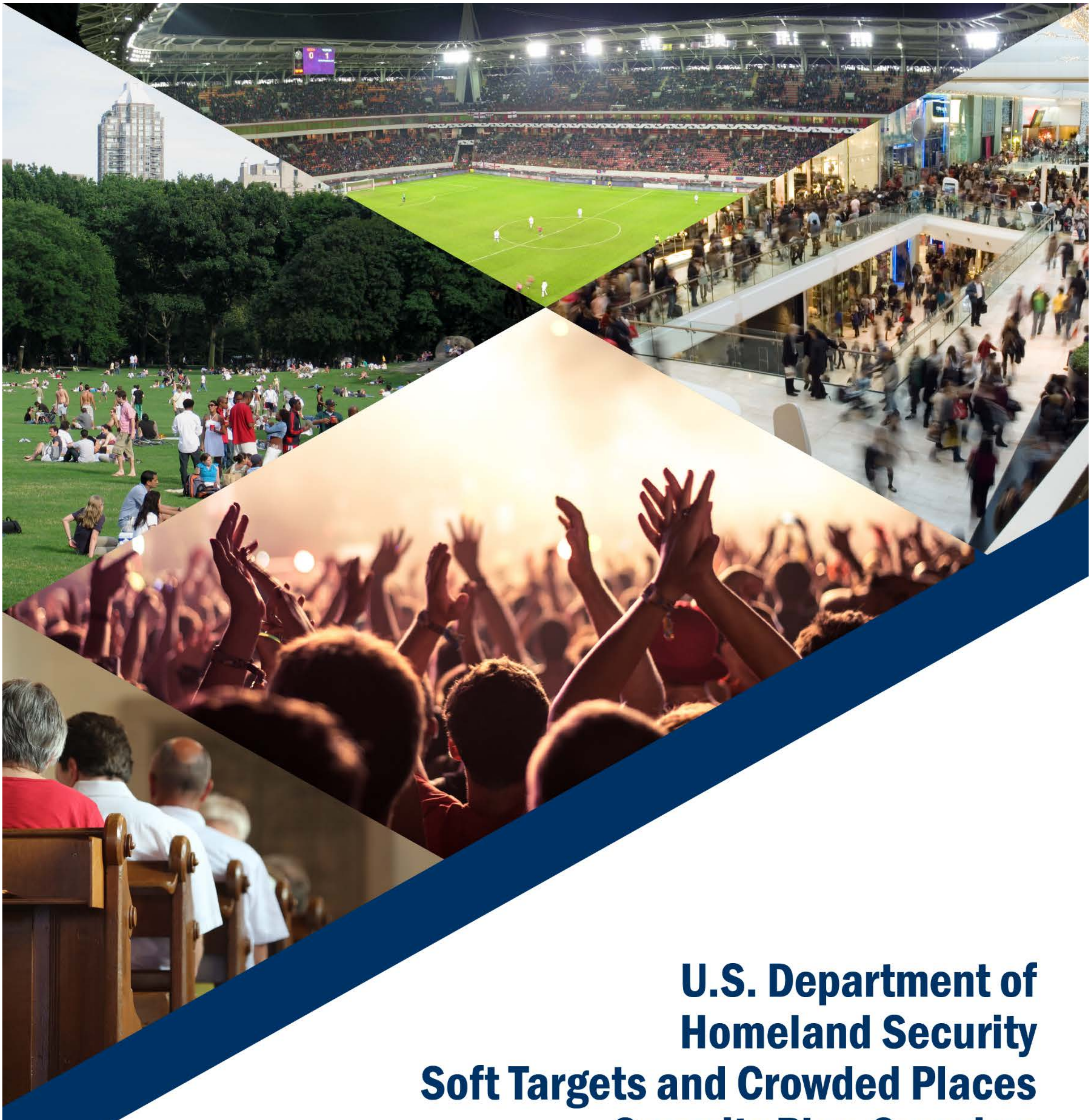


U.S. Department of Homeland Security Soft Targets and Crowded Places Security Plan Overview

May 2018

(This Page Intentionally Left Blank)

Contents

EXECUTIVE SUMMARY III

I. INTRODUCTION 1

II. THREAT ENVIRONMENT 1

III. SHARED MISSION FOR SOFT TARGET AND CROWDED PLACE SECURITY 2

THE GENERAL PUBLIC 2
OWNERS AND OPERATORS OF ST-CPS 3
PRIVATE INDUSTRY 3
STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS 4
FEDERAL GOVERNMENT 4

IV. DHS ROLES AND APPROACH TO SECURITY OF SOFT TARGETS AND CROWDED PLACES 5

DIRECT SECURITY OPERATIONS AND SUPPORT 5
DIRECT SECURITY OPERATIONS AT ST-CPS 5
SPECIAL EVENT SUPPORT 6

AWARENESS, INTELLIGENCE, AND INFORMATION SHARING 7
PROMOTING PUBLIC AWARENESS 7
INTELLIGENCE AND INFORMATION SHARING 8

PARTNER CAPABILITY AND CAPACITY BUILDING 9
PARTNERSHIP BUILDING 9
CAPABILITY-BASED PLANNING AND CAPABILITY ASSESSMENTS 9
RISK AND VULNERABILITY ASSESSMENTS 11
BEST PRACTICES, GUIDANCE, STANDARDS, AND PLANNING SUPPORT 11
TRAINING 12
GRANTS 13

RESEARCH AND DEVELOPMENT 13

V. INITIAL GAP IDENTIFICATION AND ANALYSIS 14

VI. ENHANCING UNITY OF EFFORT AND SECURITY OF SOFT TARGETS AND CROWDED PLACES 14

ENHANCING UNITY OF EFFORT ACROSS THE DEPARTMENT 14
ESTABLISH A ST-CP SECURITY EXECUTIVE STEERING COMMITTEE 15
ENHANCE THREAT-DRIVEN COORDINATION 15

SETTING THE FOUNDATION FOR FUTURE SUCCESS 15
DHS ST-CP SECURITY CAMPAIGN PLAN 15
BUILDING AWARENESS AND EDUCATING STAKEHOLDERS 16
ENGAGING KEY INTERNATIONAL PARTNERS TO SHARE BEST PRACTICES AND LESSONS LEARNED 16
INCREASING AWARENESS OF, AND ACCESS TO, ST-CP SECURITY RESOURCES 16
FOCUSING AND INCENTIVIZING INVESTMENTS IN ST-CP SECURITY 17
FOCUSING RESEARCH AND DEVELOPMENT ON ST-CP SECURITY 17

ANNEX A: LIST OF ACRONYMS 19

(This Page Intentionally Left Blank)

Executive Summary

Soft Targets and Crowded Places (ST-CPs), such as sports venues, shopping venues, schools, and transportation systems, are locations that are easily accessible to large numbers of people and that have limited security or protective measures in place making them vulnerable to attack. DHS has been working for many years to address ST-CP security and preparedness, with recent shifts in the threat landscape calling for renewed departmental focus on leveraging and maximizing its ST-CP security authorities, capabilities, and resources in an integrated and coordinated manner. To help the Department accomplish this, the Department has developed a *ST-CP Security Enhancement and Coordination Plan* (Plan). This document, the *DHS Soft Target and Crowded Places Security Plan Overview*, is meant to provide interested members within the public and private sector—including representatives from industry; academia; associations; state, local, tribal and territorial governments; law enforcement; faith based communities; non-governmental organizations; and international partners—with an overview of the Plan through which the Department is coordinating its mission to enhance the security and resilience of ST-CPs across the United States.

Shared Mission for Soft Target and Crowded Place Security

Reducing the risk of attacks against ST-CPs and reducing impacts of attacks that do occur is a shared mission among many stakeholders, including the general public; ST-CP owners and operators; security industry partners; State, local, tribal, and territorial (SLTT) government partners; and the Federal government. Individuals have a role within their community to help detect and prevent possible attacks against ST-CPs. ST-CP owners and operators have a responsibility to protect their sites and the people that work, use, or visit them. In addition to the critical role the security industry plays in directly securing ST-CPs and providing other security related services, the security industry also develops security related technologies and protective measures critical to the success of the overall effort. SLTT governments have the primary responsibility for preventing, protecting against, responding to, and mitigating incidents and attacks in their jurisdiction. This includes considering security in the design of public and civic spaces in these jurisdictions. Finally, Federal departments and agencies play various roles in both directly securing select ST-CPs and in helping other stakeholders achieve their ST-CP security responsibilities.

DHS Roles and Approach to Security of Soft Targets and Crowded Places

The Department has a significant responsibility for preventing terrorist attacks within the U.S.; reducing the vulnerability of the U.S. to terrorism; and minimizing damage and assisting in the recovery from terrorist attacks that do occur. The complementary nature of the Department's mission with others and the shared responsibility for securing most ST-CPs means the Department must work with and support SLTT governments and ST-CP owners and operators to enhance security of ST-CPs. The Department works through four principal lines of effort to provide security for those places for which it is responsible and to support other stakeholders in implementing their responsibilities for ST-CP security.

Direct Security Operations and Support. DHS is responsible for direct security operations at some facilities and locations that can be considered ST-CPs. This includes authorities for protecting transportation infrastructure, ports, waterways, and Federal facilities and property. Additionally, DHS coordinates Federal support for major special events.

Awareness, Intelligence, and Information Sharing. An informed and empowered public is DHS's greatest ally in its work to enhance the security of ST-CPs. Additionally, ST-CP owners and operators and SLTT government partners require information and intelligence to inform security related decisions. DHS educates, informs, and empowers these partners to perform their respective roles in securing ST-CPs through a variety of awareness, intelligence, and information sharing mechanisms.

Partner Capability and Capacity Building. The shared responsibility for ST-CP security makes SLTT and ST-CP owner and operator capability and capacity building central to the Department's approach. DHS supports building partner capability and capacity by establishing and facilitating partnerships; enabling capability-based planning; performing risk, vulnerability, and capability assessments; developing and promulgating best practices, guidance, and standards; supporting partner security and preparedness planning efforts; developing and delivering training; and by providing grant funding.

Research and Development. Through its research and development (R&D) programs, DHS reaches across the public, private, and international arenas to gather and deliver best practices and tangible solutions to mitigate ST-CP threats. DHS's current portfolio of R&D includes several programs, ranging from basic and applied research for technological solutions development, with direct and indirect application and benefit to enhancing ST-CP security across the spectrum of prevention, protection, response, and mitigation. These include programs designed to enhance the base of knowledge regarding ST-CP threats and risks; advance screening and detection capabilities; and enhance situational awareness, emergency response, and emergency communications.

Enhancing Unity of Effort Across the Department

Enhancing ST-CP security and preparedness requires leveraging the authorities, capabilities, and resources of nearly every DHS Component in a unified manner, ensuring the efforts of individual Components are aligned to departmental objectives and mutually supportive of each other. To this end, the Secretary directed the establishment of an ST-CP Security Executive Steering Committee (ESC) comprising representatives from across DHS Components and charged with maximizing the authorities, capabilities, resources, and programs resident across DHS to enhance security of ST-CPs nationally.

Setting the Foundation for Future Success

While the way ahead for the Department will largely be guided by the work of the ST-CP ESC, the Department will undertake several initiatives to set the foundation for future success, including but not limited to:

- Enhancing a culture of awareness through a major education and awareness campaign;
- Engaging with key international partners to share best practices and lessons learned;
- Increasing awareness of and access to DHS ST-CP resources through:
  - ➢ Development of ST-CP resource guides and webpages;
  - ➢ Increasing availability of self-help guidance, resources, and tools;
- Focusing and incentivizing investments in ST-CP security by:
  - ➢ Leveraging grants and technical assistance to enhance ST-CP security;
  - ➢ Incentivizing investments in ST-CP security; and

- Focusing research and development on ST-CP security.

External stakeholders who are interested in learning more about how they can access capability and capacity building tools and services offered through the Department can contact a Protective Security Advisor by emailing NICC@hq.dhs.gov. Alternatively, visitors to DHS.gov can find many of the Department's soft target and crowded spaces resources at www.dhs.gov/hometownsecurity. This page includes links to the Active Shooter Preparedness Program as well the *Security of Soft Targets and Crowded Places Resource Guide* released in April 2018.

I. Introduction

Soft Targets and Crowded Places (ST-CPs) are locations that are easily accessible to large numbers of people and that have limited security or protective measures in place making them vulnerable to attack. ST-CPs can include, but are not limited to, schools, sports venues, transportation systems or hubs, shopping venues, bars and restaurants, hotels, places of worship, tourist attractions, theaters, and civic spaces. ST-CPs do not have to be buildings and can include open spaces such as parks and pedestrian malls. ST-CPs will not necessarily be crowded at all times – crowd densities may vary between day and night, by season, and may be temporary, as in the case of sporting events, festivals, or other special events.

Preventing attacks against ST-CPs and reducing impacts of attacks that do occur is a shared mission among many stakeholders, including the general public; ST-CP owners and operators; private industry; State, local, tribal, and territorial (SLTT) partners; and the Federal government. Since its inception, the Department of Homeland Security (DHS or Department) has played a role in this area, executing programs intended, directly or indirectly, to enhance the security of ST-CPs. Recent changes in the threat landscape and trends in global and domestic incidents call for a renewed level of focus on this problem.

In recognition of this, the Department has developed a *ST-CP Security Enhancement and Coordination Plan* (Plan). That Plan, which is an internal Department document meant to help guide the Department's ST-CP security efforts, categorizes the Department's current and near-term ST-CP security efforts and identifies the mechanisms through which the Department will ensure unity of effort across the Department in designing and implementing ST-CP security initiatives. This document, the *DHS Soft Target and Crowded Places Security Plan Overview,* is meant to provide interested members within the public and private sector—including representatives from industry; academia; associations; state, local, tribal and territorial governments; law enforcement; faith based communities; non-governmental organizations; and international partners—with an overview of the means through which the Department executes its mission to enhance the security and resilience of ST-CPs across the United States under the Plan.

External stakeholders who are interested in learning more about how they can access capability and capacity building tools and services offered through the Department can contact a Protective Security Advisor by emailing NICC@hq.dhs.gov. Alternatively, visitors to DHS.gov can find many of the Department's soft target and crowded spaces resources at www.dhs.gov/hometownsecurity. This page includes links to the Active Shooter Preparedness Program as well the *Security of Soft Targets and Crowded Places Resource Guide* released in April 2018.

II. Threat Environment

Attacks on ST-CPs have occurred with unfortunate frequency both in the U.S. and abroad over the past decade. Among other incidents, the U.S. has experienced mass shootings in schools, a community center, a movie theater, and a concert; an edged weapon attack at a shopping mall; vehicles used as weapons to target individuals on a pedestrian walkway and at a public rally; and detonation or attempted detonation of improvised explosive devices at sporting events and other places of mass gatherings. The Intelligence Community has assessed that, for the foreseeable future, ST-CPs will continue to remain attractive targets for various threat actors.

The types of threat actors who would attempt to target ST-CPs are many, but share a common purpose—to harm Americans through the use of violence. They include Foreign Terrorist Organizations; “foreign fighters” (i.e., Americans and other Westerners who travel to conflict zones, learn bomb-making and other combat skills, and return to the U.S. to conduct attacks or facilitate the spread of tactics and techniques in their communities); and other threat actors, such as domestic criminals and lone actors.

These bad actors are evolving tactics through observation of actual or perceived successes in the U.S. and elsewhere, trial and error, and the exchange of information over the internet and social media. Extremist literature and other media not only call for disaffected individuals to conduct attacks by any available means, but also provide the know-how through simple and clear instructions for making explosives and improvised explosive devices (IEDs), and using guns, knives, vehicles, and other readily accessible tools to kill and maim unsuspecting individuals. The fact that highly lethal attacks on ST-CPs can be executed with little planning or expertise and are often able to remain undetected until operational, together with the sheer volume of ST-CPs, presents a significant security challenge.

III. Shared Mission for Soft Target and Crowded Place Security

As noted above, preventing attacks against ST-CPs and reducing impacts of attacks that do occur is a shared mission among many stakeholders, including the general public; ST-CP owners and operators; private industry; SLTT partners; and the Federal government. Each of these groups have a unique role in preventing attacks and protecting ST-CPs and the people in them.

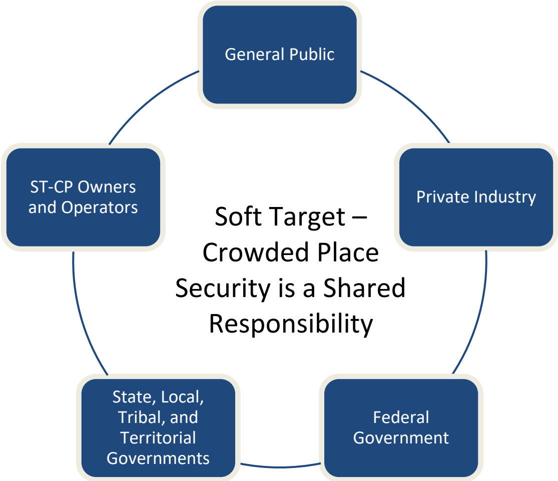

General Public
Private Industry
Federal Government
State, Local, Tribal, and Territorial Governments
ST-CP Owners and Operators
Soft Target – Crowded Place Security is a Shared Responsibility

Figure 1: Stakeholders with a Shared Responsibility for ST-CP Security

The General Public

Members of the general public, including individuals working in or using a soft target or crowded place, often are in the best position to help detect and prevent possible attacks against ST-CPs. It is important for these individuals to be aware of their surroundings and report suspicious or unusual behavior to authorities. Moreover, during an incident or attack, members of the general public and ST-CP employees often become “first responders” – i.e., the first persons in a position to take positive action to reduce loss of life and other consequences. A public with a basic knowledge of indicators of suspicious activity, how to report them, and what to do in life threatening situations (e.g., “Run – Hide – Fight” in the face of an active assailant; basic first aid for

General Public’s Role in ST-CP Security

- Be aware of one’s surroundings
- Report suspicious behavior
- Know what to do in life threatening situations

traumatic injuries) can prevent attacks before they occur and dramatically lessen the consequences of attacks that do occur.

Owners and Operators of ST-CPs

Owners and operators of ST-CPs include, but are not limited to, schools, businesses, event organizers, sports venues, and transportation providers. All owners and operators of ST-CPs have a responsibility to take steps to protect people that work in, use, or visit their site from foreseeable threats, including attacks by terrorists and other bad actors. Specific responsibilities include:

- *Understanding threats to and risks associated with their venue.* ST-CP owners and operators should work with their SLTT partners to understand the current threat environment and assess the risk and vulnerability of their venue. This information can help ST-CP owners and operators design appropriate security plans for their venues.
- *Designing and implementing appropriate security measures.* Developing, implementing, and regularly testing a comprehensive security plan is a matter of good business and corporate responsibility. Once in place, ST-CP owners and operators should monitor the security plans for effectiveness, and review them at appropriate junctures, taking into account costs and business considerations.
- *Raising awareness among staff and patrons.* ST-CP owners and operators should seek to raise awareness of possible security threats among their staff and patrons. This includes ensuring staff receive the requisite training to ensure they are prepared to execute their role in preventing, protecting against, and responding to attacks.
- *Reporting security incidents or suspicious activities.* ST-CP owners and operators should report any security incidents or suspicious activity to law enforcement at the earliest opportunity.

Private Security Providers

Private security personnel often are the first line of defense against an attack. Consequently, they must be well-trained, professional, and held to a standard of excellence.

Private Industry

Private industry, primarily through private security providers and professionals, play a key part in protecting ST-CPs. In many cases, private security personnel—including security contractors, risk analysis experts, and private security officers—are directly responsible for strengthening the security of ST-CPs. They often are the first line of defense against an attack. Consequently, they must be well-trained, professional, and held to a standard of excellence. Governments have a role in supporting the private security sector to achieve this as well as in ensuring private sector security operators meet certain standards.

The security industry also helps develop security products and technologies that enable security professionals to address threats to ST-CPs. Through public-private partnerships, cooperative research and development agreements, industry days, and other forums, the private security industry can learn more about identified capability gaps, enabling the development of more effective security products and technological solutions.

State, Local, Tribal, and Territorial Governments

While responsibility for building and sustaining resilience to all hazards is shared between government, owners and operators, and communities, SLTT governments have the primary responsibility for preventing, protecting against, responding to, and mitigating incidents and attacks in their jurisdiction. SLTT governments perform a variety of activities in support of this responsibility, to include:

- *Managing security at various ST-CP venues and events.* SLTT governments often are responsible for managing civic spaces, public activities, celebrations, agricultural shows, and community days. As part of this, they should develop, implement, and regularly test protective security measures. SLTT governments also play an important role in designing and approving public spaces—providing a unique opportunity to consider and creatively apply protective security during the design stages of areas that may become ST-CPs.
- *Overseeing local emergency management capabilities.* SLTT governments are responsible for overseeing and performing emergency management activities within their jurisdictions. SLTT emergency managers must routinely work with stakeholders from all elements of the community to assess capacity and readiness to deliver the capabilities most likely required during an incident and identify and correct any shortfalls.
- *Sharing of information and intelligence.* SLTT law enforcement organizations serve as conduits of information and intelligence to ST-CP owners and operators, helping to build awareness of the evolving threat environment. This includes reports and analysis developed by the federal government, SLTT government, and other sources.
- *Managing fusion centers.* States and localities also manage fusion centers, the primary focal points within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information. Fusion centers also provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government, assisting law enforcement and homeland security partners in preventing, protecting against, and responding to crime and terrorism.

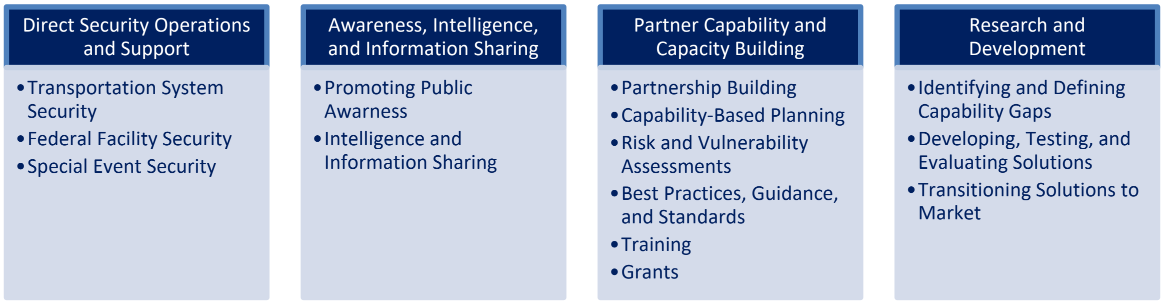
Federal Government

The U.S. Government has no greater responsibility than protecting the American people. This obligation extends across the entire government and necessitates the employment of a cohesive, risk-based strategy to guard against terrorism while preserving the civil liberties that define the American way of life. The essential services that underpin American society must remain secure in the face of diverse threats and hazards, including violent acts committed by foreign terrorist organizations, homegrown violent extremists, lone actors, or other offenders in ST-CPs. The Federal government, through Federal departments and agencies, works ceaselessly to conduct intelligence and targeted counterterrorism operations, perform direct security services, and exchange information and initiate action with SLTT and private sector partners to enhance the security and preparedness of our communities and Nation.

Various Federal departments and agencies have statutory responsibilities and roles based upon the complexity of ST-CP security. The Department of Homeland Security ensures that Federal actions are unified, complete, and synchronized to prevent unfilled gaps in the Federal Government's overarching effort. This coordinated approach ensures the actions undertaken by DHS and other Federal departments and agencies are harmonized and mutually supportive.

IV. DHS Roles and Approach to Security of Soft Targets and Crowded Places

Pursuant to the Homeland Security Act of 2002 as amended, the Department's primary mission is to prevent terrorist attacks within the U.S., reduce the vulnerability of the U.S. to terrorism, and minimize the damage and assist in the recovery from terrorist attacks that do occur, including those in ST-CPs. The Department's activities to enhance the security of ST-CPs in coordination with or in support of SLTT governments, ST-CP owners and operators, and other stakeholders generally fall within four lines of effort – Direct Security Operations and Support; Awareness, Intelligence, and Information Sharing; Partner Capability and Capacity Building; and Research and Development. Through these lines of effort, the Department plays a vital role fostering preparedness and resiliency across stakeholder communities.



Direct Security Operations and Support

- Transportation System Security
- Federal Facility Security
- Special Event Security

Awareness, Intelligence, and Information Sharing

- Promoting Public Awarness
- Intelligence and Information Sharing

Partner Capability and Capacity Building

- Partnership Building
- Capability-Based Planning
- Risk and Vulnerability Assessments
- Best Practices, Guidance, and Standards
- Training
- Grants

Research and Development

- Identifying and Defining Capability Gaps
- Developing, Testing, and Evaluating Solutions
- Transitioning Solutions to Market

Figure 2: DHS ST-CP Security Lines of Effort and Primary Activities

Direct Security Operations and Support

Direct Security Operations at ST-CPs

Direct Security Operations are those missions and associated activities that the Department performs to directly secure ST-CPs in accordance with its statutory authorities. This includes, but is not limited to, the security of transportation infrastructure, ports, waterways, and certain Federal facilities and property. Additionally, primarily through the U.S. Secret Service, DHS is responsible for protecting key leadership, such as national leaders and visiting heads of state and government, including in ST-CP environments.

Transportation System Security

By design, many transportation systems are open in nature in order to accommodate the high throughput they receive, and thus fall within the definition of ST-CPs. The Department's Transportation Security Administration (TSA) is the lead Federal agency responsible for safeguarding all non-maritime modes of transportation—e.g., aviation, mass transit, rail, highways—while the U.S. Coast Guard has the lead for securing maritime vessels, maritime transportation facilities, and other waterside ST-CPs.

TSA focuses its efforts on securing aviation and high-risk locations with the largest congregations of passengers. TSA applies a layered, risk-based approach, working closely with system operators, service providers, law enforcement, and the intelligence communities. TSA enhances security and creates a visible deterrent at select public transportation sites through targeted, risk-based deployment of Visible Intermodal Prevention and Response (VIPR) teams and over 1,000 explosive detection canine units. Additionally, in situations of credible threat to transportation systems, TSA has authority to mandate transportation operators enact certain security procedures required by the situation.

The U.S. Coast Guard protects ST-CPs within the maritime domain, such as waterside facilities, ferries, and cruise ship operations. The U.S. Coast Guard collaborates with SLTT partners to measure, prioritize, and mitigate threats under the authorities of the Captain of the Port as the Federal Maritime Security Coordinator. Vulnerabilities are measured using several risk modeling tools, and possibilities for risk mitigation of ST-CPs are discussed with partners sharing security responsibilities. Mitigation measures include waterside and shoreside patrols, security boardings, searches and inspections, escorts of high capacity passenger vessels, explosive detection canine teams, and ferry security operations. In addition, U.S. Coast Guard units coordinate with SLTT partners to support responses to attacks on ST-CPs by setting security zones, conducting mass evacuations, or conducting direct threat engagement.

Protection of Federal Facilities and Property

The Department has the statutory responsibility to protect property owned, occupied, or secured by the U.S., and, through the National Protection and Program Directorate's (NPPD) Federal Protective Service (FPS), directly protects more than 9,000 Federal facilities and the 1.4 million people who work in, use, or visit those facilities every day. Many Federal facilities have elements that constitute ST-CPs because people queue while waiting for security screening and government services, crowds gather outside and within the facilities, special events are hosted at the facilities, major venues are located adjacent to the facilities, and many are in major urban centers where people travel on, near, or through Federal property. The symbolism of some Federal facilities makes them especially desirable targets for those who are intent on threatening our way of life.

FPS protects these ST-CPs through a broad array of countermeasures, tactics, techniques, and procedures, including Facility Security Assessments, intelligence analysis, explosive detection canine activities, law enforcement response, and tenant training to mitigate emerging threats. These activities are selectively integrated into the protection of ST-CPs to mitigate identified gaps in protection. When needed, FPS deploys its Rapid Protection Force to increase presence and capability in response to specific threats. FPS also assists tenant agencies with the development of Occupant Emergency Plans and provides training for facility occupants that addresses the dynamic threat environment and results in a better informed and better prepared citizenry.

Special Event Support

The Department frequently plays a direct security role in special events, with the specific role depending on the classification of the event and other factors. For events designated to be National Special Security Events (NSSEs), the Department, through the U.S. Secret Service, leads the design and implementation of security for the event. For significant events that do not rise to the level of an NSSE, the Department, through the Special Events Program, coordinates risk assessments, information sharing, and Federal support for security at those events. DHS collects special event information from Federal and SLTT partners via an annual data call and, through the Special Event Assessment Rating methodology, applies a mixed qualitative-quantitative analysis to determine the relative risk of terrorist attack for each event. The resultant risk ratings are used to inform security posture support and policy decisions. For the highest risk non-NSSE special events, the Department generally will appoint a Federal Coordinator to work with State and local event planners on planning guidance and assistance, security best practices, and intelligence and threat assessments, as well as to facilitate the provision of Federal support to State and local public safety agencies where there are capability shortfalls.

The Department may also provide direct support to other special events based on capabilities, statutory authorities, and resource availability. Examples of such support include vulnerability assessments performed by NPPD's Protective Security Advisors; onsite intelligence and information sharing provided by Office of Intelligence and Analysis personnel; deployment of screening and detection capabilities, including explosive detection canines; deployment of TSA VIPR teams to key transportation nodes in close proximity to events; and pre-event training on a range of topics from incident management to active shooter prevention and response.

Awareness, Intelligence, and Information Sharing

n informed and empowered American public is the greatest ally the Department has in its work to enhance the security of ST-CPs. Additionally, ST-CP owners and operators and SLTT government partners require information and intelligence to inform security related decisions. The Department has a responsibility to educate, inform, and empower these partners to perform their respective roles in securing ST-CPs, and does so through a variety of awareness, intelligence, and information sharing mechanisms while protecting individual privacy, civil rights, and civil liberties.

Promoting Public Awareness

DHS, through the Office of Public Affairs, the Office of Partnership and Engagement (OPE), and Component-level outreach, ensures key stakeholders are informed about Departmental programs and key issues impacting homeland security. This includes regular communications and engagements with the media, industry partners, the American public, SLTT officials, law enforcement, academia, the private sector, and the national associations that represent these stakeholders. All of these engagement efforts not only are conducted nationally, but also regionally through DHS operational field personnel. Information also is disseminated through the Department's website (www.dhs.gov) and across various social media platforms. Some significant examples include:

- *Public Awareness Campaigns.* DHS currently manages a number of public awareness campaigns and outreach efforts, such as those that serve to educate the public on how to identify and report suspicious activity to State and local law enforcement. These include the "If You See Something, Say Something^{TM}" campaign and the America's Waterway Watch program. Other efforts, like the Ready Campaign, America's PrepareAthon!^{TM}, and the Hometown Security Initiative, provide information, training and other resources to help citizens prepare for a range of threats including information on how to prevent or respond to IED and active shooter incidents.
- *National Terrorism Advisory System (NTAS).* Through the NTAS, the Department disseminates information regarding threats or risks of terrorism to SLTT government authorities and the public. NTAS Bulletins, Alerts, and Advisories contain information on

terrorism threat trends, warn of specific and credible threats, and recommended actions for the public and other partner and stakeholder groups to prevent or mitigate risks associated with terrorism, including those involving ST-CPs.

Together, these campaigns and outreach initiatives contribute to the goal of hardening ST-CPs by providing information and training geared to create an American public that is alert, informed, and ready to do their part in combatting threats to their security and to the security of our Nation.

Intelligence and Information Sharing

As the Federal lead for coordinating the protection of critical infrastructure activities, the Department engages in a multitude of activities to ensure the array of critical infrastructure security partners have access to the intelligence and information that they need to effectively perform their roles. Examples include:

- *Intelligence Gathering, Integrating, and Sharing.* The Department, through its Office of Intelligence and Analysis, conducts intelligence activities at a national and local-level. This includes integrating national-level intelligence and information with that from SLTT partners and delivering integrated intelligence and information to stakeholders at all levels of government and the private sector through fusion centers and other mechanisms.
- *Public-Private Partnership Models.* DHS also leverages key public-private partnership models, such as the National Infrastructure Protection Plan (NIPP) partnership framework, to share information. The NIPP partnership framework brings together government and private sector stakeholders, including ST-CP owners and operators, to facilitate the sharing of intelligence, information, and security best practices. Through, classified and unclassified intelligence forums, ST-CP owners and operators sit alongside Department analysts to review intelligence – including classified information for those with security clearances provided through the Private Sector Clearance Program – to inform security decisions.
- *National Operations Center (NOC).* DHS operates the NOC to provide situational awareness and a common operating picture for the entire Federal Government, SLTT governments, private sector, and international partners, as appropriate, for special events, threats, and incidents. The NOC leverages DHS field personnel to ensure DHS has, and is sharing, the most accurate and up-to-date information on emerging incidents to maintain situational awareness and enhance the threat picture.
- *Nationwide Suspicious Activity Reporting Initiative (NSI).* The NSI facilitates the rapid processing and dissemination of suspicious activity reporting. This initiative provides law enforcement and private sector security partners with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing suspicious activity reports.
- *Information Sharing Platforms.* Online information sharing platforms, such as the Homeland Security Information Network, the DHS.gov and Ready.gov websites, and TRIPwire, contain a multitude of intelligence and information products, as wells as a wealth of other general and threat-specific preparedness resources and tools, tailored and made available to many different target audiences.

Partner Capability and Capacity Building

Another way in which the Department helps enhance the ST-CP security enterprise is through capability and capacity building. Capability is the ability to complete a task or execute a course of action under specified conditions at a certain level of performance, while capacity is the amount of the task or action that the performing party has the ability to complete. Capability and capacity building enhances the success of initiatives run by the Department's partners by providing resources to which those partners might not have otherwise had access. Tools used to help build capabilities and capacity include partnership building; capability-based planning and assessment; risk and vulnerability assessments; promulgation of best practices, guidance, and standards; training; and grants. When supporting its partners, the Department must tailor its support to complement the ways that each partner approaches the ST-CP security challenge so that the resources the Department provides reinforce existing capabilities, create new capabilities, or increase capacity.

Partnership Building

The shared responsibility for ST-CP security necessitates building strong partnerships between and among all levels of government, ST-CP owners and operators, and private industry. This includes more than building and strengthening partnerships directly between DHS and these various groups. It includes encouraging and, as necessary, facilitating partnerships in and among these groups themselves so that they are able to maximize their capabilities and resources to enhance ST-CP security.

Consistent with the Federal Advisory Committee Act, the Department engages in outreach efforts with critical stakeholders nationwide, including SLTT governments, elected and appointed officials, law enforcement, the private sector, and institutions of higher education, ensuring a unified approach to external engagement. Additionally, through the NIPP partnership framework, the Department helps brings together Federal, SLTT, and private sector partners, including owners and operators of ST-CPs, to share intelligence and information, exchange security best practices, and collaborate on direct security activities.

Capability-Based Planning and Capability Assessments

The National Preparedness Goal calls for "[a] secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk." The National Preparedness System, which is designed to support achievement of the National Preparedness Goal, outlines an integrated set of guidance, programs, and processes and defines the 'core capabilities' required across the prevention, protection, mitigation, response, and recovery mission areas. These core capabilities serve as the basis for and guide DHS, SLTT, and whole-of-community capability-based planning and capacity building efforts in support of enhancing security of ST-CPs. Additionally, the National Planning Frameworks foster a shared understanding of roles and responsibilities and describe how the whole community works to bring the capabilities resident within each segment to bear to achieve security objectives for ST-CPs and other critical infrastructure.

Capability-based planning typically begins with the completion of capability assessments to determine what capabilities are present and what gaps in capabilities exist. Some ways in which the Department supports capability assessments include:

- *State Preparedness Reports (SPRs).* SPRs are self-assessments of a jurisdiction's current capability levels against the capability targets identified in FEMA's Threat and Hazard Identification and Risk Assessment. SPRs support capability and capacity building by helping to identify State and territory preparedness capability gaps. In cases where preparedness levels fall short of targets, States and territories explain the specific improvements they need to address the capability gaps in their jurisdictions. The outputs of this process inform a variety of emergency management efforts, including emergency operations planning, mutual aid agreements, and hazard mitigation planning.
- *Exercises.* Exercises are a key mechanism for assessing and identifying gaps in ST-CP partner capabilities. Exercises can be tailored to examine particular capabilities and process (e.g., information sharing; mass casualty care) or a range of security and response capabilities collectively. Exercises provide ST-CP officials, decision-makers, resource providers, and other stakeholders across the whole community with the opportunity to assess and validate capabilities, improve coordination, and identify areas for improvement and strengths.

  The National Exercise Program is the principal mechanism for examining and validating core capabilities nationwide, including those that support ST-CP security and preparedness. Exercises selected for the program include facilitated policy discussions, seminars and workshops, tabletop exercises, drills, games and simulations, functional exercises, and full-scale exercises.

  Various Components from across the Department also directly conduct or support exercises with tenants, ST-CP owners and operators, SLTT law enforcement and emergency responders, and other ST-CP stakeholders to test security capabilities and plans and to develop corrective action and mitigation plans to fill identified gaps. The Department also offers toolkits, often referred to as "exercises in a box," that provide all the materials required for ST-CP partners to plan and execute exercises of their own.

TSA's Intermodal Security Training and Exercise Program

U.S. Coast Guard's Area Maritime Security Training and Exercise Program

FEMA's Joint Counterterrorism Awareness Workshop Series

NPPD's Multi-Jurisdiction IED Security Planning and Stakeholder Readiness and Exercise Program

OPE's National Seminar and Tabletop Exercise Series for Institutions of Higher Education

Figure 3: Sample Exercise Programs from Various DHS Components

Risk and Vulnerability Assessments

Various Components throughout the Department conduct vulnerability and risk assessments at ST-CPs to evaluate their overall security posture; identify gaps in protective measures or single points of failure; and provide options for consideration that, if implemented, may improve their overall security and resilience. Examples include:

- *NPPD's Protective Security Advisors* assesses the vulnerabilities of nationally significant infrastructure, including facilities, systems, and networks owned and operated by private industry and public areas and places managed by public institutions including SLTT government. These vulnerability assessments account for not only the physical infrastructure, but also the purpose which it serves, including the individuals who patronize it during special events or their daily life.
- *TSA's Baseline Assessments for Security Enhancement* is one of many programs that TSA manages that provide security assessments. The Baseline Assessments for Security Enhancement evaluates the security of mass transit and passenger railroad systems.
- *U.S. Coast Guard's Maritime Security Risk Analysis Model and Domestic Port Security Assessment Program* review potential vulnerabilities to ST-CPs within and adjacent to ports and waterways, ultimately producing risk mitigation recommendations that account for the inherent vulnerabilities of ST-CPs.
- *S&T Technical Assessment Assistance* facilitates continuous innovation and adaptation of the Department's vulnerability assessment programs by incorporating new data based on emergent threats, such as those that threaten ST-CPs.
- *FEMA's Threat and Hazard Identification and Risk Assessment* process supports State and urban area identification of threats and hazards of concern to their communities, evaluation of potential impacts should the threat or hazard become realized, identification of capabilities and associated capability targets required to address the threats, and estimation of the resources required to achieve the capability targets through the use of community assets and mutual aid, while also considering preparedness activities, including mitigation opportunities. This process informs security-related policy, decision-making, and resource allocation, not only by the State or urban area, but also by DHS in targeting capability building technical assistance and in making grant policy decision.

By leveraging these various programs and resources to increase understanding of ST-CP risks, vulnerabilities, and the capabilities required to mitigate them, ST-CP owners and operators, SLTT government partners, and DHS are provided a solid foundation from which to make informed enhancements in security plans and posture and focus investments to enhance security capabilities where they can have the greatest impact.

Best Practices, Guidance, Standards, and Planning Support

The Department provides support to its ST-CP partners by gathering, validating, and endorsing those techniques, tactics, and procedures that have proven reliable and effective in improving the security of ST-CPs. These best practices often take the form of guidance or standards ST-CP partners can use to inform how they design and implement protective measures and security protocols for their sites. The Department also provides instruction that covers how to develop plans tailored to the appropriate threats, hazards, and risks ST-CP partners must address in their efforts to improve their overall security posture. This planning support fosters the development of emergency operations or action plans that outline how individuals, communities, and organizations can design their approach to the challenges they face.

Various DHS Components compile best practices and develop guidance for their SLTT and private sector constituents, including ST-CP stakeholders. Often these products are developed in partnership with these constituents and other subject matter experts. The products cover a wide range of topics such as emergency management and response; security and protection of facilities, venues, events, and individuals; and detection and reporting of suspicious behavior. Examples include the *First Responder Guide for Improving Survivability in IED and Active Shooter Incidents*, the *K-12 School Security Practices Guide*, the *Public Area Security Framework*, and FEMA's *Comprehensive Preparedness Guide* 101. These products inform individuals, communities, organizations, and businesses of actions that can be taken before, during, and after incidents to prevent and protect against attacks and ensure proper response and mitigate consequences and loss of life when attacks occur.

The Department also supports a number of standard setting activities. For example, the Interagency Security Committee is a DHS-led group of Chief Security Officers and other senior executives representing 60 Federal departments and independent agencies that develops physical security policies and standards, promotes key management practices, and facilitates mitigation of threats to all non-military, Federal facilities in the U.S., their employees, and the visiting public. These policies and standards frequently address threats common to ST-CP such as vehicle ramming, active shooters, and IEDs. Similarly, U.S. Coast Guard Captains of the Port can establish, convene, and direct their jurisdiction's Area Maritime Security Committee to identify critical infrastructure and risks in their specific zones, determine mitigation strategies, and support the development of an Area Maritime Security Plan. Additionally, through its authorities for securing of transportation systems, TSA issues Security Directives to transportation system owners and operators that require the implementation of certain security measures in response to specific threats or the results of a vulnerability assessment.

Training

Training plays a critical role in capability and capacity building. Through the development and delivery of training, the Department builds the essential knowledge, skills, and abilities required across the spectrum of partners central to ST-CP security. The Department tailors training, in both content and method of delivery, to the knowledge, skill, and ability requirements of the target audience in order to most effectively build capability and capacity of ST-CP partners.

The Department's training portfolio covers a wide spectrum of topics. The Department offers general awareness and preparedness training intended for nearly all segments of the ST-CP partnership base, such as the suspicious activity reporting training associated with the "If you See Something Say Something™" Campaign and TSA's First Observer Plus ™, and trauma response training, such as FEMA's "Stop the Bleed" Campaign, and the "You Are the Help Until Help Arrives" training. The Department also offers training on a range of ST-CP security topics tailored to the needs of particular segments of the partnership base, such as ST-CP owners and operators, law enforcement officers, first responders, emergency managers, and community leaders. Topics include, but are not limited to, detecting surveillance, venue protective measures, evacuation planning, and active shooter and IED preparedness.

The Department delivers training through a variety of mechanisms, including public awareness and messaging campaigns; computer- and web-based training; mobile training teams; and in-residence training at the Department's training centers, such as the Federal Law Enforcement Training Centers and FEMA's Emergency Management Institute. Basic knowledge and abilities, required by the broadest number of partners, are typically delivered through cost efficient mechanisms such as computer- and web-based training, while more advanced knowledge and skills often use more resource intensive mechanisms such as mobile training teams or in-residence training. Additionally, in order to maximize its limited resources and more effectively reach the broad ST-CP stakeholder community, the Department executes several "train-the-trainer" programs, where the Department focuses on developing SLTT-level instructors certified to deliver curriculum on the Department's behalf.

Grants

DHS distributes approximately $1 billion dollars in homeland security preparedness grant funds each year. These funds support building, sustaining, and delivering core capabilities to prevent, protect against, mitigate, respond to, and recover from terrorist attacks and other hazards. DHS' grant portfolio includes both broad risk-based grant programs aimed at enhancing preparedness of State and local jurisdictions, such as the State Homeland Security Program, Urban Area Security Initiative, and Securing the Cities Program, and more focused programs that target certain infrastructure that falls within the scope of ST-CPs, such as the Transit Security Grant Program, Intercity Bus Security Grant Program, Intercity Passenger Rail Grant Program, and Port Security Grant Program.

As part of distributing grant dollars, DHS requires recipients and subrecipients to provide details on their grant funding investments. From this reporting, DHS is able to discern positive impact on ST-CP security and preparedness. While not specific to ST-CPs, funding provided through grants is being used across the Nation to build core capabilities like interoperable communications, screening and detection, and risk management, which ultimately increases the baseline level of preparedness and resilience in and around soft targets.

Research and Development

DHS, primarily through its S&T Directorate, works to identify and define capability gaps in ST-CP security and develop, test, evaluate, certify, and transition technologies, protocols, and processes to better address those gaps. Since ST-CP owners and operators and SLTT governments bear the burden of protecting the vast majority of ST-CPs, S&T reaches across the public, private, and international arenas to gather and deliver best practices and tangible solutions to those seeking to mitigate ST-CP threats. By leveraging Integrated Product Teams performing technology foraging across the private sector, national labs, and Federal R&D arena, DHS applies a systems-based approach to identify, prioritize, and facilitate the development and transition of solutions that address operational requirements that align with high-priority R&D gaps. R&D efforts performed by the Department to date that may have applications in the ST-CP security space include projects aimed to increase the base of knowledge regarding threats and risks, such as homemade explosive characterization studies and explosives effects testing; enhance screening and detection capabilities; and leverage modern communication platforms and applications to enhance emergency response and communications.

V. Initial Gap Identification and Analysis

Initial analysis of Department efforts, including development of an inventory of all ST-CP related programs, plans, and processes; interviews with all major Components and program offices; and elicitation sessions with various ST-CP owners and operators revealed several opportunities to enhance DHS ST-CP efforts.

Lack of a Standing Coordinating Body. The mission of enhancing ST-CP security and preparedness cuts across nearly the entire Department, yet there historically has not been a standing body or mechanism to ensure these various efforts are coordinated and mutually supportive of one another. Creating an intra-Departmental coordinating group to set standards, identify priorities, and make resource recommendations related to ST-CP security could improve the effectiveness of the Department's programs in that area.

No Unified Picture of the Department's Programs. Based on the understanding that shared equities in a single mission space can reinforce one another, a unified picture of the Department's ST-CP programs will allow the Department to more effectively support ST-CP security efforts. At present, the Department does not possess a unified picture or vision of its ST-CP related programs that is easily accessible to the whole community.

Need for ST-CP Security to be Affordable and Scalable. The ST-CP landscape includes hundreds of thousands of venues and services millions of people daily. Thus, to truly enhance ST-CP security and preparedness, the Department must find ways to expand the scale and reach of its programs, such as through partnership and empowerment approaches and cost-sharing. Additionally, in recognition that the resources available to dedicate to security are limited across the spectrum of ST-CP partners, the Department must work to make security technologies, tools, and resources as affordable as possible.

Challenge of Maintaining Vigilance and the Shift to New Normal. The limits of human capacity for sustaining a heightened sense of awareness, focus, and action eventually lead to decreased effectiveness and complacency. To counter this, the Department must help set a new expectation for what constitutes the normal, steady-state risk environment and change public perception about its essential role in ST-CP security and preparedness.

VI. Enhancing Unity of Effort and Security of Soft Targets and Crowded Places

Enhancing Unity of Effort Across the Department

The ubiquity of ST-CPs makes the responsibility for improving their security one that the Department's Components share according to the overlapping equities that transcend their mission areas. By their nature, ST-CPs exist within every aspect of American society, which taken as a whole is the Department's responsibility to protect. To leverage its resources and capabilities to correspond to the magnitude of the threat and the inherent vulnerability associated with ST-CPs, the Department must enhance unity of effort across its Components and within their mission areas by building upon the existing coordination and collaboration mechanisms that have proven successful.

Establish a ST-CP Security Executive Steering Committee

In order to enhance unity of effort across the Department, DHS will establish a ST-CP Security Executive Steering Committee (ST-CP ESC). Chaired by NPPD and comprised of senior executives representing all DHS offices and Components that play a role in ST-CP preparedness and response, the ST-CP ESC is charged with ensuring DHS maximizes the authorities, capabilities, resources, and programs resident across DHS to enhance security of ST-CPs nationally. Authority and responsibility for ST-CP mission execution, however, will remain with the respective Components. The ST-CP ESC has authority to establish standing and task-specific working groups staffed by representatives from amongst its membership or drawing from staff resources within each Component as required.

Enhance Threat-Driven Coordination

In situations where the Department becomes aware of an emerging or imminent threat that may impact ST-CPs, the ST-CP ESC will convene to identify and coordinate possible Component-specific and/or cross-Component courses of action designed to address the changes in the risk environment. The recommended courses of action provided by the ST-CP ESC will consider all available options—including interagency and field operations based on input from key leaders from the Department's field forces and consultation with interagency partners—and identify the headquarters and field-level cross-Component coordination mechanisms that may be required to execute the selected course of action.

Setting the Foundation for Future Success

Based on the initial gap analysis and lessons learned from other security efforts, the Department has identified six areas to focus on immediately to set the foundation for success across the ST-CP security enterprise.

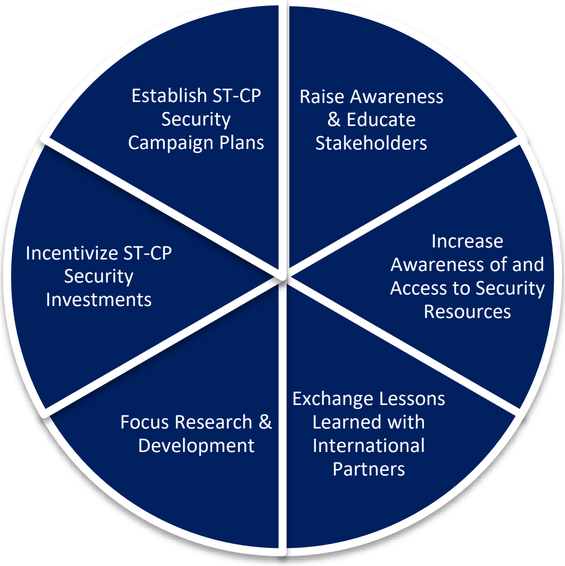

Establish ST-CP Security Campaign Plans
Raise Awareness & Educate Stakeholders
Increase Awareness of and Access to Security Resources
Exchange Lessons Learned with International Partners
Focus Research & Development
Incentivize ST-CP Security Investments

Figure 4: Focus Areas for Setting the Foundation for Future Success

DHS ST-CP Security Campaign Plans

The ST-CP ESC will work to execute enterprise-wide ST-CP Security Enhancement and Coordination Campaign Plans around particular issues, such as school security, which will serve to further integrate DHS lines of effort. ST-CP Campaign Plans will guide the integration of Departmental ST-CP security activities around an organizing framework designed to improve understanding and build ST-CP security capabilities of departmental stakeholders, partners, and the general public.

Building Awareness and Educating Stakeholders

National Education and Awareness Campaign. An informed and empowered American public is the greatest ally the Department and other ST-CP partners have in any effort to enhance the security of ST-CPs, detect and prevent attacks, and respond during an incident. To help empower the public, the Department will enhance national awareness building upon and integrates lessons from existing national campaigns including the "If You See Something, Say Something™" campaign, the "Stop the Bleed," campaign, the Blue Campaign, and the "You Are the Help Until Help Arrives" campaign. The objectives of the enhanced awareness include: (1) fostering recognition across the general public and the business community about ST-CP related threats; (2) empowering the public by teaching individuals how to recognize and report suspicious activities and how to respond appropriately should an incident occur; and (3) preparing the next generation to build a culture of awareness and preparedness.

Department-wide ST-CP Security Stakeholder Engagement Plan. Alongside the broader public awareness campaign, the Department will develop a ST-CP security stakeholder engagement plan. The objectives of this plan will include: (1) aligning and, where necessary, developing information resources and activities to educate stakeholders, including the general public, ST-CP owners and operators, the security industry, SLTT governments, and other Federal departments and agencies, on ST-CP threats and their respective roles in addressing those threats; and (2) helping stakeholders identify and access the resources and activities that DHS can offer to help them mitigate their vulnerabilities and respond where necessary to an ST-CP incident.

Engaging Key International Partners to Share Best Practices and Lessons Learned

The ST-CP security issue is not limited to the U.S., as many other nations around the globe are faced with similar risks and challenges. Many of our international partner countries, some who have been dealing with threats to ST-CPs for longer than the U.S., have made significant headway in ST-CP security and preparedness. DHS has a history of collaborating with international partners on homeland security issues, and will continue to engage these and other partners in order to share best practices and lessons learned in ST-CP security.

Increasing Awareness of, and Access to, ST-CP Security Resources

ST-CP Security Resource Guides and Webpages. The Department has a wide variety of programs, plans, resources, and tools either specifically geared toward, or that otherwise can benefit, ST-CP stakeholders. One of the greatest barrier of access to these resources, and to enhanced coordination within DHS, is awareness of the wealth of resources offered by the Department. To address this, the Department will leverage the inventory of ST-CP programs, resources, and tools that was compiled in the development of the *ST-CP Security Enhancement and Coordination Plan* and will develop a number of resource guides and user friendly webpages. These guides and webpages will outline the various resources available to ST-CP stakeholders so they can understand what the resource are, how those resources can benefit them, and how they can access them. These resource guides and webpages will also provide the additional benefit of increasing awareness across DHS of all the Department does and offers with respect to ST-CP security and preparedness, helping to enhance Departmental coordination.

Increasing Availability of ‘Self-Help’ Guidance, Resources, and Tools. Enhancing security and preparedness of ST-CPs across the country requires enhancing capability and capacity of a significant number of ST-CP stakeholders. The scale of this stakeholder base is greater than the Department has the resources to directly impact. Thus, the Department must find ways to empower ST-CP partners in enhancing their own security and preparedness. To do this, the Department will assess all of its ST-CP security-related program, plans, and processes to identify opportunities to increase the availability of DHS resources and tools to ST-CP stakeholders on a ‘self-help’ basis or will otherwise work to transition their use to non-government organizations and to the marketplace. Such opportunities may include developing guidance, resources, and tools for ST-CP stakeholders to identify, assess, and analyze their risks or, based on such a risk assessment, to conduct an assessment of their ST-CP’s vulnerabilities.

Focusing and Incentivizing Investments in ST-CP Security

Leveraging Grants to Enhance ST-CP Security. Grants are one of the primary mechanisms by which the Department can effect change of preparedness and security at the SLTT level. To this end, FEMA, in coordination and consultation with other DHS Components through the ST-CP ESC, will identify specific national- and regional-level core capability gaps and recommendations related to ST-CP security and preparedness. Based on this analysis, the Department will evaluate opportunities to leverage its current grant programs to focus SLTT investment on these gaps and identify areas where grants are not sufficient to fill gaps. The resources committed to SLTT ST-CP security and preparedness enhancement through grants in relation to other areas of concern and focus may require prioritization and trade-off decisions.

Incentivizing Investments in ST-CP Security. The Support Anti-Terrorism through Fostering Effective Technologies Act (SAFETY Act) provides incentives for the development and deployment of anti-terrorism technologies through a system of risk and litigation management. The SAFETY Act ensures that the threat of liability does not deter potential manufacturers or sellers from developing and deploying effective anti-terrorism capabilities that could save lives. Recently, SAFETY Act protections have been approved for open venues such as sports arenas and stadia, and the Department continues to work with the ST-CP community to encourage more security procedures that would be eligible for SAFETY Act protections and will look for ways to expand use of the SAFETY Act to promote ST-CP security.

Focusing Research and Development on ST-CP Security

Protecting ST-CPs often requires a different approach than that historically used to secure hardened targets. To help more efficiently and effectively secure ST-CPs, the Department’s R&D enterprise will look for novel ways to develop and transition to operational use affordable and scalable technologies that buy-down risk and that work within a free and open society that values individual rights and privacy. This includes enhanced detection, screening, and countermeasures. In support of this, the Department will:

- Inventory all R&D efforts taking place across the Department that have potential impact on and benefit for ST-CP security enhancement;
- Evaluate existing DHS R&D programs, such as the Apex Screening at Speed projects, for use in alternative ST-CP environments, in consultation with ST-CP owners and operators; and

- Define and implement the processes and mechanisms necessary to ensure the mission and capability needs of ST-CP security partners are incorporated into departmental R&D prioritization and resource allocation processes.

VII. Conclusion

Securing the nation's multitude of ST-CPs is a shared mission among all stakeholders, including the general public; ST-CP owners and operators; security industry partners; SLTT government partners; and the Federal government. Individuals also have a role within their community to help detect and prevent possible attacks against ST-CPs.

The Department of Homeland Security is taking steps to unite its own ST-CP security efforts and close any gaps. DHS already provides direct security operations and support; facilitates awareness, intelligence, and information sharing; supports partner capability and capacity building; and conducts research and development. Within and beyond these core areas, DHS has identified a number of initial gaps and has already started work to close those gaps. These include enhancing unity of effort across the Department and setting a foundation for future success through efforts such as enterprise-wide ST-CP campaign plans; building awareness and educating stakeholders; engaging international partners; increasing awareness of and access to ST-CP security resources; incentivizing investments in ST-CP security; and focusing ST-CP security research and development.

As DHS works to enhance its own efforts, external stakeholders interested in participating in ST-CP security activities can email NICC@hq.dhs.gov to contact a local Protective Security Advisor for assistance accessing capability and capacity building tools and services offered through the Department. Alternatively, visitors to DHS.gov can find many of the Department's ST-CP security resources online at www.dhs.gov/hometownsecurity. This page includes links to the Active Shooter Preparedness Program as well the *Security of Soft Targets and Crowded Places Resource Guide* released in April 2018.

ANNEX A: LIST OF ACRONYMS

DHS	Department of Homeland Security
ESC	Executive Steering Committee
FEMA	Federal Emergency Management Agency
FPS	Federal Protective Service
IED	Improvised Explosive Device
NIPP	National Infrastructure Protection Plan
NOC	National Operations Center
NPPD	National Protection and Programs Directorate
NSI	Nationwide Suspicious Activity Reporting Initiative
NSSE	National Special Security Event
NTAS	National Terrorism Advisory System
OPE	Office of Partnership and Engagement
R&D	Research and Development
S&T	Science and Technology
SAFETY Act	Support Anti-Terrorism through Fostering Effective Technologies Act
SPR	State Preparedness Reports
ST-CP	Soft Targets - Crowded Places
TSA	Transportation Security Administration
U.S.	United States
VIPR	Visible Intermodal Prevention and Response