Department of Homeland Security Strategic Framework for Countering Terrorism and Targeted Violence

Executive Summary

The United States faces an increasingly complex, and evolving, threat of terrorism and targeted violence. As was the case sixteen years ago, at the U.S. Department of Homeland Security's founding, foreign terrorist organizations remain intent on striking the Homeland, whether through directed attacks or by inspiring susceptible individuals in the United States. Today, though, the Nation also faces a growing threat from domestic actors inspired by violent extremist ideologies, as well as from those whose attacks are not ideologically driven. Domestic threat actors often plan and carry out their acts of violence alone and with little apparent warning, in ways that limit the effectiveness of traditional law enforcement investigation and disruption methods. We must confront these evolving challenges by building on existing best practices developed against foreign terrorist threats, identifying promising new approaches, and developing a strategic vision that provides a more holistic approach to preventing terrorism and targeted violence that originates here at home. In an age of online radicalization to violent extremism and disparate threats, we must not only counter foreign enemies trying to strike us from abroad, but also those enemies, foreign and domestic, that seek to spur to violence our youth and our disaffected—encouraging them to strike in the heart of our Nation, and attack the unity of our vibrant, diverse American society.

The Department has experienced clear successes in its mission to thwart foreign terrorist enemies. We have denied them entry, stopping them at our border or even before they reach it. We have integrated and supported the efforts of Federal, state, local, tribal, territorial, private sector, and international partners, gathering and sharing information and intelligence, and providing the resources they require to counter terrorism in their areas of responsibility. We have strengthened our communities. As a Nation, we are more resilient than ever. Our ability to prevent foreign-origin attacks against the Homeland is unmatched across the globe. These successes provide a roadmap for addressing the threat we face today.

This Strategic Framework outlines the Department's vision for reinvesting in programs and efforts that have enhanced our security, while incorporating key strategic changes that will allow us to address the threats we currently face. In addition to addressing terrorism, this Strategic Framework encompasses targeted violence, such as attacks on schools, public spaces, and transportation systems, and other forms of racially, ethnically, and religiously motivated violence that can overlap and intersect with terrorism. The Strategic Framework recognizes the critical role advances in technology have played in facilitating the spread, evolution, and interaction of violent ideologies and narratives of personal grievance, and the subsequent security implications, both for the Homeland and around the world.

Our Strategic Framework is crafted with the conviction that the Department must play a vital role in securing the privacy, civil rights, and civil liberties of Americans and others. Privacy, civil rights, and civil liberties are essential. They should be cherished and safeguarded. This Strategic Framework is designed to promote and preserve them. In addressing terrorism and targeted violence, we are steadfast that the role of the Department is to protect American communities, not to police thought or speech.

The *Department of Homeland Security Strategic Framework for Countering Terrorism and Targeted Violence* is designed to implement the White House's 2017 *National Security Strategy* and 2018 *National Strategy for Counterterrorism*, as well as related national policy guidance. While other departments and agencies have vital roles to play, this Strategic Framework describes the Department's vision for addressing terrorism and targeted violence threatening the Homeland. The goals, objectives, and priority actions promoted herein will also enhance the Department's ability to counter transnational criminal organizations, human traffickers, and other criminal threats.

The challenges facing our Nation are significant, but through a whole-of-society approach that empowers our citizens and our state, local, tribal, and territorial authorities, as well as our private sector, non-governmental, and community leaders, the Department of Homeland Security will continue to adapt ahead of evolving threats, and will enhance the safety of our Nation.

The Strategic Framework outlines the Department's vision around the following goals:

- Goal 1: Understand the evolving terrorism and targeted violence threat environment, and support partners in the homeland security enterprise through this specialized knowledge.

- Goal 2: Prevent terrorists and other hostile actors from entering the United States, and deny them the opportunity to exploit the Nation's trade, immigration, and domestic and international travel systems.

- Goal 3: Prevent terrorism and targeted violence.

- Goal 4: Enhance U.S. infrastructure protections and community preparedness.

Introduction

Nearly two decades after the 9/11 attacks, terrorism and targeted violence continue to pose a grave threat to the Homeland in ways that have discernibly evolved. *Terrorism* is likely a familiar term to most readers.[1] The term *targeted violence* may be less familiar. For purposes of this Strategic Framework, targeted violence refers to any incident of violence that implicates homeland security and/or U.S. Department of Homeland Security (DHS) activities, and in which a known or knowable attacker selects a particular target prior to the violent attack.[2] Unlike terrorism, targeted violence includes attacks otherwise lacking a clearly discernible political, ideological, or religious motivation, but that are of such severity and magnitude as to suggest an intent to inflict a degree of mass injury, destruction, or death commensurate with known terrorist tactics. In the Homeland, targeted violence has a significant impact on the safety and security of our communities, schools, places of worship, and other public gatherings. The threats of terrorism and targeted violence increasingly intersect with one another, and there is likewise some alignment in the tools that can be used to counter them. Thus, rather than dealing with terrorism and targeted violence as distinct phenomena, this Strategic Framework addresses the problems, and the tools that can be wielded to address them, together.[3]

Foreign terrorist organizations (FTOs) continue to plot against the United States, and the Department executes on a daily basis its mission of preventing another attack from abroad.[4] Unfortunately, the severity and number of domestic threats have also grown. Homegrown violent extremists (HVEs) are influenced by the ideologies and messages of FTOs.[5] There has been a concerning rise in attacks by

[1] The Department of Homeland Security defines *terrorism* as any activity involving a criminally unlawful act that is dangerous to human life or potentially destructive of critical infrastructure or key resources, and that appears intended to intimidate or coerce a civilian population, to influence government policy by intimidation or coercion, or to affect the conduct of a government by mass destruction, assassination, or kidnapping.

[2] The concept of *targeted violence* was coined and first defined in Robert A. Fein, Bryan Vossekuil & Gwen A. Holden, "Threat Assessment: An Approach to Prevent Targeted Violence," *Research in Action* (National Institute of Justice, U.S. Department of Justice), July 1995. All major subsequent works that have explored targeted violence—including studies published by the U.S. Secret Service and U.S. Department of Education, among others—have either utilized or based their understanding of the concept on this definition. This Strategic Framework does so as well. Given the growing importance of the concept of targeted violence, a more precise definition is needed, as one of the priority actions outlined in Goal 1.1 makes clear.

[3] This Strategic Framework recognizes that the Federal Government has a role in addressing terrorism and targeted violence when the severity and magnitude of an attack would overwhelm the capacity of State and local government prevention, protection, and response efforts. The Federal Government primarily does this through informing, training, and equipping our SLTT partners. The capabilities or capacity developed from Federal investments also benefit other aspects of SLTT partners' missions. For example, enhanced analysis and information-sharing capabilities may be invested in by the Federal Government to ensure we have an effective two-way information sharing capability between SLTT and the Federal Government to share terrorism threat information, but the capability may also be leveraged by the SLTT partner to address local criminal challenges.

[4] This Strategic Framework defines a *foreign terrorist organization* in the same manner as does 8 U.S.C. § 1189, as a foreign organization that engages in terrorist activity or terrorism, or retains the capability and intent to engage in terrorist activity and terrorism, which threatens the security of United States nationals or the national security of the United States. The Strategic Framework defines it as such regardless of whether the group has been placed on the U.S. Department of State's Foreign Terrorist Organization List.

[5] DHS defines a *homegrown violent extremist* as a person of any citizenship who has lived and/or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically-motivated terrorist activities (including providing support to terrorism) in furtherance of political or social objectives promoted by a FTO, but is acting independently of a FTO's direction.

individuals motivated by a variety of domestic terrorist ideologies,[6] such as racially- and ethnically-motivated violent extremism, including white supremacist violent extremism, anti-government and anti-authority violent extremism, and other ideological strains that drive terrorist violence. Hate crimes and non-ideologically motivated large-scale or disproportionately lethal acts of mass violence, including mass attacks, round out the picture of terrorism and targeted violence afflicting the Homeland.[7]

While the terrorist threat remains serious, the Federal Government—in conjunction with state, local, tribal, and territorial (SLTT), and private sector partners—has had numerous successes in protecting the Homeland and preventing foreign terrorist attacks in the years since 9/11. DHS has played an important role. The Department's achievements in preventing foreign-origin attacks illuminate the strategies, tactics, and tools it must bring to bear to address the disparate challenges of today. The Department has used a multi-tiered approach to protection—employing cutting-edge technology, enhancing its intelligence-gathering and analytic capabilities, providing advanced training to our frontline personnel, and building the capacity of our international partners. This approach "pushes our borders outward" and creates defense-in-depth, a term referring to the creation of multiple mutually supportive layers of defense in lieu of relying on one defensive line that is vulnerable to a single point of failure. The concept has been employed in contexts that include cybersecurity, where layered defensive mechanisms can thwart cyberattacks, and by militaries, where defense-in-depth can be employed against advancing attackers. The Department has applied this concept to many of the Nation's security priorities, including border and aviation security. Multiple layers of security and intelligence can provide awareness of hostile actors long before they try to launch an attack.

DHS has achieved noteworthy successes in extending our borders outward through the National Targeting Center (NTC). Screening and vetting are among the Department's primary counterterrorism functions, and NTC is at the forefront of these efforts. This innovative Center leverages sophisticated targeting tools and all levels of classified and open-source intelligence in proactive ways to identify emerging threats, including those posed by terrorists, terrorist support networks, and transnational criminal organizations. NTC identifies targets and interdicts, across all modes of transportation, the passengers and cargo that pose a threat to national security at the earliest possible point prior to arrival in the United States. NTC's targeting and interdiction prevent terrorists and their suppliers and facilitators from reaching not only our borders, but often our Hemisphere. The NTC is one of the most effective counterterrorism tools we have within the Federal Government, and makes our borders not the first line of defense, but one of many.

DHS has also increased the sharing of information regarding terrorist threats between the Federal Government and SLTT entities, as well as private sector partners. Before 9/11, few mechanisms

[6] The Department defines *domestic terrorism* as an act of unlawful violence, or a threat of force or violence, that is dangerous to human life or potentially destructive of critical infrastructure or key resources, and is intended to effect societal, political, or other change, committed by a group or person based and operating entirely within the United States or its territories. Unlike HVEs, domestic terrorists are not inspired by a foreign terrorist group. It should be noted that many groups and individuals defined as "domestic terrorists" are becoming increasingly transnational in outlook and activities. The current label we employ to describe them, which comes from the Federal Government's lexicon, should not obscure this reality.

[7] This Strategic Framework defines a *hate crime* as a criminal offense against a person or property motivated in whole or in part by an offender's bias against a race, religion, disability, sexual orientation, ethnicity, gender, or gender identity. The Secret Service defines *mass attacks* as acts of intentional violence in public places during which harm was caused to three or more persons. Targeted violence includes, but is not limited to, mass attacks and hate crimes as defined in this Strategic Framework.

existed to facilitate the sharing of threat-related information between SLTT agencies and the Federal Government. For example, a streamlined framework did not exist to easily gather and share Suspicious Activity Reporting (SAR).[8] After identifying this shortcoming, the Department of Justice (DOJ), DHS, the Federal Bureau of Investigation (FBI), and SLTT partners created the Nationwide SAR Initiative (NSI) to establish standards for gathering, documenting, processing, analyzing, and sharing terrorism-related SAR information determined to have a potential nexus to terrorism, while protecting privacy, civil rights, and civil liberties. Fusion Centers also play a critical role in the U.S. Government's information-sharing efforts. These State- and locally-operated Centers existed prior to the attacks of 9/11, primarily assisting law enforcement with criminal intelligence analysis. Their mission expanded after the terrorist attacks, and they were eventually recognized in the 2007 *National Security Strategy* as the primary focal points for receipt, analysis, gathering, and sharing of threat-related information between SLTT, Federal, and private sector partners. Engagement with SLTT and efforts like NSI and National Fusion Centers help DHS to detect, prevent, protect against, and mitigate threats.

DHS also supports American communities in their preparations to respond to and recover from terrorism and targeted violence. The Department has trained SLTT emergency responders and helped connect communities with resources that can support their preparedness efforts. As one example, the Federal Emergency Management Agency (FEMA) is engaged in continuous evaluation of the risks that communities face through the Threat and Hazard Identification and Risk Assessment (THIRA) program, which helps SLTT partners identify risks and capability gaps, develop response plans, and efficiently allocate their resources.

As a contributor to the FBI's interagency Joint Terrorism Task Forces (JTTFs), the Department has experienced numerous successes in investigating and disrupting terrorists and their support systems. JTTFs work diligently to investigate and respond to threats and incidents as they occur. Alongside Federal and SLTT partners, DHS agents have been integral in leading JTTF investigations, especially those involving foreign terrorism and transnational crime suspects.

DHS's successes underscore the Department's capacity to address the evolving challenges of terrorism and targeted violence. This Strategic Framework represents a recommitment to, and strengthening of, what has worked, and an investment in tools capable of addressing the present challenges confronting our Nation. A critical element of the Department's learned expertise is its whole-of-society approach focused on empowering American society.

DHS recognizes that this partnership is only possible if the Department respects and protects the values of the Nation. Since its inception, the Department has prioritized civil rights, civil liberties, and individual privacy protections in its efforts. These rights must be rigorously guarded. The Department's mission can only be achieved when we uphold the rule of law, and earn and maintain the trust of the American people. Domestic terrorism and homegrown violent extremism are inherently tied to ideas and ideologies. Planning or committing acts of violence is a crime, while expressing or holding radical or extreme views is protected by the First Amendment. The Department must take care, while addressing the scourge of violence, to avoid stigmatizing populations, infringing on constitutional rights, or attempting to police what Americans should think. Further, how we identify and detect terrorism and targeted violence requires faithful adherence to fair information

[8] SAR refers to official documentation of observed behavior that is reasonably indicative of pre-operational planning related to terrorism or other criminal activities.

practice principles and privacy-focused Departmental policies. The Department always incorporates privacy protections in information technology systems, technologies, rulemakings, programs, pilot projects, and other activities that involve the planned use of personally identifiable information (PII). The Department must continue to take great care to ensure that its efforts sustain, and do not erode, privacy, civil rights, and civil liberties.

This Strategic Framework addresses terrorism and targeted violence based on four complementary organizational concepts central to the Department's mission: intelligence, border security, domestic prevention, and preparedness.

Strong intelligence capabilities allow the Department and its partners to understand the nature of the threat facing the Homeland, allowing DHS to prevent and mitigate threats, and prepare communities to better respond to and recover from attacks that do occur.

Defending the borders is necessary to prevent foreign terrorists and other hostile actors from entering the country.

Border security cannot stop violence originating from within America, so the Department also focuses on empowering and equipping SLTT prevention and resilience capabilities. Prevention efforts must be multidisciplinary, and include enhanced whole-of-society partnerships with mental health professionals, social service providers, and civil society that can provide "off ramps" away from terrorism and targeted violence, both protecting the American people and reducing the burden on the criminal justice system.

The Department also assists its SLTT partners in enhancing infrastructure protections and community preparedness to ensure that, when an attack does occur, its impact can be contained, and those targeted can recover quickly.

The Evolving Nature of the Threat

The Department was founded in the wake of 9/11, and the persistent threats posed by al-Qa'ida dictated that DHS's early counterterrorism efforts focused on preventing attacks by FTOs. The threats associated with a number of FTOs remain an essential priority of DHS's counterterrorism mission. Yet it is clear that the threat of terrorism and targeted violence has evolved in important ways. We must evolve with the threat.

One change is that **more diverse sets of actors and motivations now pose significant security concerns than at any time since 9/11**. Domestic terrorists, motivated by racially- and ethnically-motivated violent extremism, anti-government and anti-authority violent extremism, and other violent extremist ideologies, represent a growing share of the threat to the Homeland.

A second change relates to how Americans, and people across the globe, communicate. At the time of the 9/11 attacks, only 54% of the U.S. population used the Internet, compared to 90% of the adult population today. The rest of the world has similarly seen an explosion in Internet usage rates. The fact that all of our lives are increasingly touched by online activity has brought profound changes, for good and for ill. Violent extremist groups have often proven adept at exploiting the Internet's potential. Post-9/11 developments in the online space—including the advent and

widespread adoption of social media, the development of the "dark web," and the proliferation of encryption and anonymizing technology—help people see themselves as part of communities and causes that transcend national borders, provide users with a sense of intimacy with people and groups half a world away, and embolden the adoption of identities or causes that may once have been obscure, marginalized, or otherwise unknown. Such dynamics have many positive aspects, but they also have major implications for terrorism and targeted violence. Violent extremists disseminate their messages globally and foster online communities that lure vulnerable individuals. Communication advances have likely contributed to compressed "flash-to-bang" timelines, the period between radicalization to violent extremism and mobilization to violence. Online extremist communities lionize attackers, encouraging others to follow their footsteps. The online space has made attackers more operationally competent, as they use the Web to glean technical information for their attacks.

This change has also magnified our Nation's vulnerability to disinformation campaigns, in which foreign states and hostile foreign non-state actors exploit the online space, social media in particular. These actors seek the polarization of American society, and work to capitalize on and accentuate American political divisions and public anxiety. They seek to foment strife and division, and spur vulnerable individuals or groups to commit acts of violence.

A third change relates to the weaponry attackers can potentially employ. Militant groups across the globe increasingly use technologies that were either crude or unavailable to consumers at the time of the 9/11 attacks. One example is unmanned systems. Improvements in the range and payload of unmanned aircraft systems (UAS) have allowed terrorist groups like the Islamic State of Iraq and Syria (ISIS) to use consumer drones to drop explosives on security forces; to surveil enemies; and to use airborne video capabilities to film propaganda. Unmanned systems could also potentially facilitate terrorists' deployment of chemical, biological, radiological, and nuclear (CBRN) materials. While UAS have not been successfully employed in a terrorist attack in the United States, they factored into a disrupted plot targeting the Pentagon.[9] UAS is just one example of a technology that terrorists and other violent actors can now employ. Other emerging technologies that pose concerns in the wrong hands include artificial intelligence, biotechnology, 3D printing, and cryptocurrencies.

Major Threat Actors

One of the aforementioned changes to the challenge posed by terrorism and targeted violence is that DHS must address a wider variety of threat actors. The Department will continue to devote itself to preventing, protecting against, mitigating the effects of, responding to, and recovering from terrorist attacks against the United States directed by FTOs. But DHS will now also amplify its focus on the growing domestic challenge.

The Radical Islamist Terrorist Threat. The radical Islamist movement is in a transitional period following ISIS's loss of the territory that constituted its self-proclaimed "caliphate," as well as the overall movement's metastasization across multiple regions. ISIS and al-Qa'ida remain the two most pressing radical Islamist terrorist threats to the Homeland, through their potential to direct plots and inspire HVEs. But a number of other organizations remain significant threats as well, such as the Iran-backed

[9] Malicious uses of UAS have also resulted in significant public burdens, including extended airport closures, that further underscore the harm that terrorists could potentially inflict with this technology. In one incident in December 2018, drone interference forced the closure of London's Gatwick airport for 36 hours. Hundreds of flights were canceled.

terrorist group Hizballah, which continues to exploit Western commerce, and seeks to further establish logistics and facilitation networks in South America.

The radical Islamist terrorist threat's growth over the past decade is related to the 2011 "Arab Spring" revolutions that shook the Middle East and North Africa. Regional instability, social unrest, political upheavals, and dashed expectations provided radical Islamist terrorist groups opportunities to recruit and geographically expand. The Syrian civil war directly enabled the rise of ISIS, which by late 2014 controlled territory stretching from Syria into Iraq that was approximately the size of the State of Oregon. While the vast majority of this territory has now been freed from ISIS's grip, the group appears to be mounting an insurgency while it tries to regroup and refocus.

Given its losses in Iraq and Syria, a key ISIS priority has been building up affiliates elsewhere in the world. One example is ISIS's Khorasan Province, primarily based in Afghanistan, which has recruited from the Tehrik-i-Taliban Pakistan terrorist group.[10] ISIS has also co-opted militant groups in other regions. The ISIS affiliate based in Egypt's Sinai Peninsula has conducted increasingly bloody attacks, including detonating a bomb on Metrojet Flight 9268 in October 2015, killing 224 passengers and crew members. In the Philippines, ISIS-affiliated militants seized the city of Marawi in 2017 and held it for five months. Other ISIS affiliates and cells can be found in such places as Nigeria, where ISIS absorbed a leading faction of the notorious terrorist group Boko Haram, and Sri Lanka, where nine ISIS-linked suicide bombers attacked hotels and churches on Easter Sunday of 2019, leaving more than 250 dead and 500 injured.

While ISIS has made more headlines in recent years, al-Qa'ida's approach has been quieter and perhaps more challenging. Since 2011, al-Qa'ida has focused on growing its resources, ranks, and geographic footholds in multiple regions. Al-Qa'ida's affiliates—al-Qa'ida in the Arabian Peninsula (AQAP) in Yemen, al-Qa'ida in the Islamic Maghreb, al-Shabaab in Somalia, and al-Qa'ida in the Indian Subcontinent—wage insurgencies, recruit from local populations, and target Western interests in the Middle East, Africa, South Asia, and beyond.

Both al-Qa'ida and ISIS work not only to attack the Homeland directly but also to inspire HVEs to conduct attacks in their name. This approach has supplanted an overarching focus on complex coordinated attacks that may have characterized al-Qa'ida's approach at the time of the 9/11 attacks, but that no longer holds true of major radical Islamist terrorist organizations today. HVEs have conducted eight lethal terrorist attacks in the United States since 2014, claiming 83 lives.[11] Seven of the eight attacks were ISIS-inspired.

Regardless of organization, two demographics from the conflict in Syria and Iraq represent critical concerns for the United States and, indeed, much of the world: 1) foreign fighters and 2) violent extremists in regional prisons. The Syria conflict attracted some 40,000 individuals, including foreign terrorist fighters and supporters who wanted to help ISIS grow its "state," from more than 100 countries.[12] While many died on the battlefield, thousands have left the region, returning to their home

[10] Tehrik-i-Taliban Pakistan previously trained an American citizen to attempt a car bombing in New York City's Times Square in May 2010.

[11] See statistics in Peter Bergen & David Sterman, *Jihadist Terrorism 17 Years After 9/11* (Washington, D.C.: New America Foundation, 2018).

[12] See estimate in Russell E. Travers, Deputy Director of the U.S. National Counterterrorism Center, "Counterterrorism in a World of Competing Priorities," remarks at the World Counter Terror Congress in London, March 5, 2019.

countries or leaving for remote geographic areas where they may continue to plan, facilitate, or conduct attacks, or propagandize in support of radical Islamist causes. Some of the individuals who remain imprisoned in the region work to radicalize vulnerable people to violent extremism. Due to the international movement of this volume of returning foreign terrorist fighters and the potential for further radicalization to violent extremism in prisons, it is critical that the Department be able to identify the locations, travel patterns, and facilitation networks of these individuals, and prevent them from entering the United States and our partner nations.

Domestic Terrorism. Domestic terrorists—a phrase typically used to denote terrorists who are not directed or inspired by FTOs—have caused more deaths in the United States in recent years than have terrorists connected to FTOs. Domestic terrorist attacks and hate crimes sometimes overlap, as perpetrators of prominent domestic terrorist attacks have selected their targets based on factors such as race, ethnicity, national origin, religion, sexual orientation, gender, and gender identity.

White supremacist violent extremism, one type of racially- and ethnically-motivated violent extremism, is one of the most potent forces driving domestic terrorism. Lone attackers, as opposed to cells or organizations, generally perpetrate these kinds of attacks. But they are also part of a broader movement. White supremacist violent extremists' outlook can generally be characterized by hatred for immigrants and ethnic minorities, often combining these prejudices with virulent anti-Semitism or anti-Muslim views.

White supremacist violent extremists have adopted an increasingly transnational outlook in recent years, largely driven by the technological forces described earlier in this Strategic Framework. Similar to how ISIS inspired and connected with potential radical Islamist terrorists, white supremacist violent extremists connect with like-minded individuals online. In addition to mainstream social media platforms, white supremacist violent extremists use lesser-known sites like Gab, 8chan, and EndChan, as well as encrypted channels. Celebration of violence and conspiracy theories about the "ethnic replacement" of whites as the majority ethnicity in various Western countries are prominent in their online circles.

Prior to Anders Breivik's notorious July 2011 attacks in Norway that claimed 77 lives, he posted a manifesto highlighting the threat of Europeans' ethnic replacement by Muslim migrants. Subsequent terrorists have praised Breivik's attacks and voiced similar grievances. On March 15, 2019, a gunman killed 51 worshipers at Christchurch's Al Noor Mosque and Linwood Islamic Center. The shooter's manifesto espoused anti-immigrant conspiracy theories and noted that the gunman had been in brief contact with Breivik. Several months later, another gunman launched an attack at a Walmart in El Paso, Texas, killing 22 and wounding 24. His online manifesto, which reflected elements of multiple ideologies, noted the attacker's fear of ethnic replacement by people of Hispanic descent and praised the Christchurch attacker.

White supremacist violent extremists often scapegoat the Jewish people, voicing anti-Semitic conspiracy theories. On October 27, 2018, a gunman attacked a synagogue in Pittsburgh, Pennsylvania, where the Tree of Life, D'Or Hadash and Or L'Simcha congregations were gathered, killing 11 people and wounding six. Before the attack, he posted messages on Gab accusing a Jewish charity that assisted refugees of bringing in "invaders" to kill "our people." Six months later, on April 27, 2019, a gunman opened fire on a synagogue in Poway, California, killing one. The shooter

published an anti-Semitic manifesto on 8chan, citing the Christchurch and Pittsburgh gunmen as inspirations, and echoing similar anti-immigrant conspiracy theories.

Another significant motivating force behind domestic terrorism has been anti-government/anti-authority violent extremism. This ideology has been associated with multiple plots and attacks, and hostile nation-states often promote it in their disinformation efforts. In July 2019, an anarchist claiming affiliation with the "antifa" movement attempted to firebomb a U.S. Immigrations and Customs Enforcement facility in Tacoma, Washington, and threatened responding law enforcement officers with a firearm. On multiple other occasions, self-proclaimed "sovereign citizens" claiming their independence from Federal law have targeted law enforcement officers and other officials.

Various forms of violent extremism possess overlapping motives, tactics, and targets. In recent years, adherents to particular violent extremist ideologies have sometimes abandoned them for other ideologies with similar sets of perceived enemies. Some violent extremists may simultaneously embrace or find inspiration in multiple ideologies, some of which may appear in tension with one another. Individuals can often use the ideologies' shared sets of enemies to reconcile the surmised tensions between them.

Targeted Violence. Many perpetrators of mass attacks do not appear to fit the definition of terrorists because they lack a clear ideological motive. They may often be responding to a perceived grievance, whether domestic, workplace, or of some other nature. Mass attacks are a persistent problem and a grave concern. According to the U.S. Secret Service, 27 mass attacks were carried out in public spaces in the United States in 2018, killing 91 people. In 2017, 28 mass attacks claimed 147 lives. In the past three years, the Nation witnessed the two deadliest mass attacks in its modern history, including a 2017 shooting at an outdoor concert in Las Vegas that killed 58 and injured 869. The impact of such attacks on the victims, their families, friends, local communities, and the Nation is immense.

Even if the underlying rationale and ideologies motivating them differ, terrorism and targeted violence are addressed together in this Strategic Framework because they necessitate a shared set of solutions. They overlap, intersect, and interact. Addressing one threat can require or lend itself to addressing another. Perpetrators and supporters of terrorism and targeted violence use much of the same toolkit to validate their worldviews, engage with like-minded sympathizers, devise plans, and prepare for attacks. Terrorists and perpetrators of targeted violence may be motivated by different ideologies or narratives of personal grievance, and in some cases by none at all, but they often find the online space crucial as they grow closer to mobilizing to violence. These threats may be exacerbated by foreign actors seeking to undermine the Homeland through disinformation campaigns. Terrorists and perpetrators of targeted violence attack targets with similar characteristics, often with similar tactics. Thus, the goals and objectives in this Strategic Framework address these challenges as a coherent whole, emphasizing solutions that can increase the security of the Homeland against multiple threats.

Guiding Principles

The key goals described above represent the Department's strategic priorities in the counterterrorism and targeted violence space. As we developed our plan to achieve them—and as we operationalize that plan in the days, weeks, months, and years to come—we leverage five guiding principles to ensure that we build on our past successes while identifying and anticipating future threats, and remaining true to the mission we are charged with by the American people.

1. **Understand and Adapt to the Threat Environment:** As threats against the Homeland evolve, the Department must adapt its intelligence capabilities to new security landscapes and craft innovative responses.

2. **Understand Positive and Potentially Malicious Uses of Technology:** Technology can provide important new solutions to the challenges of terrorism and targeted violence. But technological developments can also magnify these challenges. Technological advances influence how people radicalize to violent extremism and mobilize to violence; empower violent extremists to portray attackers as role models; provide attackers with new tactical avenues and means of destruction; and create vulnerabilities to information operations, including by foreign states, that are designed to enhance the attractiveness of violent extremist causes.

3. **Collaborate with Domestic and International Partners:** Terrorism and targeted violence often transcend national boundaries. The Department must address these threats with interagency and international collaboration, including effective intelligence and information sharing, as well as capacity building.

4. **Emphasize Locally-Based Solutions:** No matter the threat, mobilization to violence occurs at the local level, in communities across the country. The Department must support SLTT efforts to ensure they are equipped to play a central role in vital tasks like identifying signs of violent extremism and "off-ramping" susceptible individuals before they mobilize to violence.

5. **Uphold Individual Rights:** The Department must defend individual rights, including privacy, civil rights, and civil liberties.

Goal 1: Understand the Evolving Terrorism and Targeted Violence Threat Environment, and Support Partners in the Homeland Security Enterprise Through This Specialized Knowledge.

Our capacity to respond to terrorism and targeted violence depends on our ability to understand these phenomena, and to adapt as they evolve. The Department will work alongside its domestic and international partners to gather, produce, and share information regarding current and emerging threats, and use innovative technologies to better anticipate changes and prepare responses.

Objective 1.1: Conduct in-depth analysis of current and emerging threats, and share with the homeland security enterprise.

The Department must understand not only the threats of terrorism and targeted violence as they stand today, but also how they are likely to evolve. DHS engages in integrating and analyzing intelligence about multiple threat streams, and disseminating it across operational and support Components, SLTT partners, and the private sector to inform their actions against those threats. DHS's Office of Intelligence and Analysis (I&A) is the only intelligence community element statutorily charged with delivering intelligence to SLTT and private sector partners, and developing intelligence derived from those partners to benefit the Department and the broader intelligence community.

DHS has invested in a multidirectional information-gathering and -sharing infrastructure, focused on four key elements: the National Network of Fusion Centers, the NSI, the National Terrorism Advisory System, and the "If You See Something, Say Something" public awareness campaign. Most recently, the Department enhanced the existing NSI effort, bringing it within the new the National Threat Evaluation and Reporting (NTER) Program, which looks at threats beyond terrorism—thus allowing a focus on all threats regardless of motive or ideology. NTER provides law enforcement and homeland security partners with resources and training to identify and prevent terrorism, targeted violence, and mass attacks. It facilitates a national capacity for identifying, evaluating, and sharing tips and leads related to those threats as appropriate. In addition, the Homeland Security Information Network is DHS's official system for sharing sensitive but unclassified information between Federal, SLTT, international, and private sector partners.

Through this multidirectional approach to gathering and sharing intelligence and information, DHS has enabled all levels of government and the private sector to better understand and consequently prepare for threats of terrorism and targeted violence. Successful information sharing builds connectivity between DHS and SLTT and private sector partners, and lays the groundwork for DHS to provide these partners with additional resources.

Priority Actions

Develop an Annual State of the Homeland Threat Assessment: The Department will, in coordination with the FBI, National Counterterrorism Center (NCTC), and any other appropriate partners, produce an annual product that evaluates the strategic threat environment within the Homeland related to terrorism and targeted violence, and anticipates future or emerging threats. This product will help to inform Federal and SLTT partners, as well as private sector partners and the broader public. A common baseline understanding of threats within the Homeland will support

interagency policymaking, agency prioritizations, resource allocations, and inter-governmental partnerships.

In order to encourage new perspectives and challenge long standing assumptions, the Department will continuously evaluate and measure the impact over time of anticipatory intelligence that appears in the State of the Homeland Threat Assessment—that is, intelligence in the annual report that utilizes specialized tradecraft to make anticipatory judgments regarding the future as foresight, forecasting, or warning. The point of anticipatory intelligence is not to predict *who* will become a terrorist or attacker, but rather to understand such factors as: 1) the impact that changes in the world will have on the problem set, 2) the trajectory of terrorist organizations or movements that may influence attackers, or 3) specific adaptations in tactics, techniques, and procedures (TTPs) that these actors will undertake. A strong methodology for evaluating anticipatory intelligence will allow continual improvements in the Department's ability to produce intelligence that highlights emerging trends, changing conditions in the strategic environment and threats from hostile actors.

Craft a New Definition of *Targeted Violence*: The concept of *targeted violence* was introduced in a 1995 study supported by the U.S. Department of Justice's National Institute of Justice. Major subsequent works, including this Strategic Framework, are reliant on how the concept was defined in the 1995 study.[13] The term *targeted violence* does not appear in the current DHS Lexicon, and the definition that has been employed over the years is insufficiently specific. DHS will consult with other departments and agencies, academia, and relevant non-governmental organizations to fashion a definition of targeted violence that is more precise and actionable for the Department's mission. Following this process, the new definition will be introduced into the DHS Lexicon, and will be employed to further shape the mission of the Department and its Components and Offices as it pertains to targeted violence. This effort will help to build a common understanding of the threat for all people and organizations focused on combating targeted violence, allowing for better discussion, approaches to mitigation, and resource allocation.

Enhance DHS Methods of Collecting and Analyzing Data and Information on Relevant Patterns of Violence: Current national-level statistics on terrorism and targeted violence in all its forms are not comprehensive.[14] The Department will work with other departments and agencies and, as appropriate, academic and non-governmental organizations, to determine the best methods of collecting accurate and comprehensive national-level statistics on terrorism and targeted violence, including hate crimes. After determining the best methods, the Department will prioritize resources toward the collection of this data and encourage its partners to do the same. Accurate nationwide statistics will better position DHS to protect communities from these threats.

Maximize Actionable Transportation-Related Intelligence: The Department will improve intelligence-driven operations with increased information sharing to produce and disseminate actionable intelligence and information that can identify and characterize terrorist and related threats to the Nation's various modes of transportation, including: 1) aviation, 2) freight rail, 3) mass transit and passenger rail, 4) pipeline, 5) highway and motor carrier, and 6) maritime. The Department will seek to close gaps between traveler information available within the aviation transportation and

[13] See discussion in footnote 2.

[14] Multiple factors have contributed to noncomprehensive national-level statistics on terrorism and targeted violence. For example, Federal statistics on hate and bias-motivated incidents rely on voluntary SLTT law enforcement reporting, which is inconsistent in part because of these authorities' confusion over appropriate classification.

maritime transportation systems to facilitate the same level of passenger/crew vetting across both domains.

Assess Technological Advances and Risks from Emerging Technologies: The Department requires a sound understanding of technological advances that attackers will employ, and those that can help to counter terrorism and targeted violence. DHS will conduct risk-based assessments of technological advances in the near-, medium-, and long-term, examining the promise and peril of emerging technologies, including unmanned systems. The Department will collaborate with other Federal agencies, SLTT organizations, and industry partners to share findings and promote awareness of the risks and potential mitigation measures.

Detect Anomalies and Provide Early Warning of Terrorist Weapons of Mass Destruction Plots: DHS will improve Department processes for production and dissemination of intelligence, information, and other data to accurately characterize terrorists' interest in and capability to use CBRN materials in an attack.

Improve Information Sharing with SLTT Partners: SLTT partners are often best positioned to address threats in their jurisdictions, and require access to timely and actionable information from DHS. The Department will collaborate with SLTT partners to share developed intelligence and enhance analytic and information-sharing processes, with a focus on standardizing product and reporting processes and dissemination mechanisms across the DHS intelligence enterprise. The Department will initiate a shared services program to facilitate common processes for managing production, reporting dissemination, tracking, and providing feedback on products and reports across the entire DHS intelligence enterprise. This effort will help SLTT partners have relevant and actionable information.

Further Improve Upon SAR Reporting: The Department will continue to grow the NTER program to facilitate its partners' ability to identify, evaluate, and report or share tips and leads associated with targeted violence.

Provide Transparency Regarding How the Department Protects PII: DHS's mission relies on protecting individuals by embedding and enforcing privacy protections and transparency in all of its activities, including its information-sharing processes. Information shared with or by foreign governments may be sensitive, and requires careful attention to data protection, as well as data quality and reliability standards. As such, the Department commits to expanding its transparency efforts related to how the Department ensures data quality and reliability, as well as its efforts to safeguard PII.

Objective 1.2: Deploy the most effective technological solutions for addressing current and emerging threats.

The Department will invest in researching, testing, and enabling the deployment of important technological solutions to terrorism and targeted violence. DHS will employ research and development (R&D) internally, and will engage with other Federal agencies, the private sector, and academia externally to better understand emerging threats, and avoid technological surprise related to terrorist techniques and means of attack. It will further its partnerships with the technology sector.

Priority Actions

Identify Key Technologies to Enhance Our Homeland Security Posture: The Department will identify existing technologies, or those that can be developed in the near- to medium-term, capable of supporting current or anticipated DHS operational needs to address threats, without eroding individual protections and rights. The Department's efforts will be as forward-looking as possible, and will include exploration of common operating systems that allow for more effective and efficient deployment of diverse, multi-jurisdictional law enforcement and response/recovery assets across priority locations, such as at ports and airports, and along coastal waterways.

Establish Flexible Development, Contracting, and Adoption: Slow-moving bureaucracies can pose an obstacle to adoption of the newest and most promising or effective technologies. The Department and its Components will enhance their ability to flexibly purchase or create, and rapidly adopt and deploy, technologies that can counter terrorism and targeted violence, including investing in a tailored R&D program. The Department will expand existing public-private partnership programs and form new public-private partnership programs where needed.

Objective 1.3: Leverage the Department's specialized knowledge to support law enforcement investigations.

One critical purpose of understanding the strategic environment is to leverage the Department's knowledge, including highly specialized knowledge, to support active missions to protect the Homeland. Law enforcement investigations are a critical area into which Departmental knowledge about the strategic environment is directly applied. DHS's Homeland Security Investigations (HSI) is the largest and longest standing Federal contributor to JTTFs nationwide. HSI's partnership with JTTFs ensures that the Department's legal, strategic, and tactical capabilities, as well as its exclusive authorities, are fully utilized in furtherance of the counterterrorism mission. HSI Special Agents assigned to JTTFs are uniquely trained and resourced to initiate and support global investigations. HSI's international force is the Department's largest investigative presence abroad, and its legal authority to investigate all types of cross-border criminal activity positions it to investigate individuals of national security concern.

U.S. Customs and Border Protection (CBP) also contributes officers, agents, and intelligence professionals to JTTF investigations. CBP's Tactical Terrorism Response Teams (TTRTs)—units specially trained in counterterrorism investigations and responses—work closely with JTTF officers on national-security investigations. The U.S. Coast Guard Investigative Service (CGIS) also contributes agents to support JTTF missions, most notably to assist transnational smuggling cases and other cases with a maritime nexus. The Secret Service supports JTTFs with nationwide assignments of Special Agent personnel. Its global network of Electronic Crimes Task Forces (ECTFs) provide further investigative and forensic capabilities. The Transportation Security Administration's (TSA) Law Enforcement/Federal Air Marshal Service has Federal Air Marshals assigned to the FBI's National Joint Terrorism Task Force and to JTTFs nationwide to provide investigative support related to aviation security. U.S. Citizenship and Immigrations Services contributes immigration officers from the Fraud Detection and National Security Directorate as task force members who can assist intelligence and law enforcement personnel in understanding immigration laws, processes, and procedures.

Priority Actions

Enhance Intelligence Sharing for JTTFs: The Department will work to enhance information sharing between JTTFs, Fusion Centers, and other stakeholders. Increasing cooperation between JTTFs and Fusion Centers will further support investigative efforts of the Department and our Federal and SLTT law enforcement partners.

Enable DHS Resources and Ensure a Highly-Trained Workforce: The Department will provide the most up-to-date technologies to teams and personnel assigned to JTTFs and invest in this part of the workforce through HSI's Counterterrorism Professional Development Training Program. These efforts will help these teams and personnel to best contribute to the JTTFs.

Goal 2: Prevent Terrorists and Other Hostile Actors from Entering the United States, and Deny Them the Opportunity to Exploit the Nation's Trade, Immigration, and Domestic and International Travel Systems.

Terrorists and other hostile foreign actors frequently attempt to exploit our trade, travel, and immigration systems. The Department will continue to enhance our robust screening, vetting, detection, and deterrence capabilities, and secure our trade, travel, and transportation systems.

Objective 2.1: Detect terrorists attempting to travel to, or gain or maintain access to, the United States. Stop them from exploiting the trade, immigration, and travel systems.

Every year, DHS prevents several thousand terrorist watch-listed individuals from traveling to or entering the United States. The Department employs a range of tools to detect such actors and prevent them from entering the country. To ensure that they cannot enter through designated ports of entry or exploit the immigration system, the Department maintains numerous vetting programs and capabilities. DHS Components patrol and rigorously enforce land, air, and sea borders.

The Department is expanding cooperation with foreign governments to better confirm individuals' identities and detect threats before they can cause harm in the United States. DHS engages in comprehensive vetting of refugees and asylum seekers, and works with other departments and agencies to gather and share biometric and biographic information to identify potential exploitation of the Nation's visa and border security programs. DHS leverages its investigative resources, such as the Visa Security Program (VSP), to augment its targeting and vetting initiatives.

The Department is working to maximize its vetting capabilities. As an example, as directed by the President in NSPM-9, DHS worked with its interagency partners to establish the National Vetting Center (NVC) in December 2018. NVC provides a common technology platform and process to allow for a coordinated and comprehensive review of relevant sensitive and classified information to support the vetting of applicants for travel and immigration benefits. NVC will enhance the Federal Government's capacity to detect and prevent hostile actors from entering the country or exploiting the legal visa process.

Priority Actions

Expand America's Virtual Borders: Threats to the Homeland often originate from failed states or countries that lack the ability to identify and prevent terrorists from traveling to the United States, thus necessitating that the Department extend its reach beyond U.S. borders. DHS enacts cooperative programs that make it harder for terrorists to exploit the travel continuum. These efforts take various forms, from the deployment of DHS personnel abroad to work with foreign counterparts, to focused information sharing to confirm identities and illuminate threats, to standards development and enforcement. DHS will maximize the impact of such efforts by developing an international information-sharing framework that prioritizes partnerships based on risk-based analysis of threats to the United States, and partners' political will and capability to reduce risks. This framework will identify weaknesses in the international travel continuum, critical international partnerships to address them, and the most effective approach to mitigating the threats caused by these weaknesses. DHS's prioritized partnerships will help facilitate rapid access to relevant information.

Prioritize Interoperability of Information Sharing: The Department will prioritize interoperability and automation in its information-sharing relationships with trustworthy partners. While personal networks and operational coordination are useful means to share information, we will increasingly supplement these relationships with technology that can share high-volume data—governed by appropriate privacy protections and rules—at a level of speed and accuracy that human networks cannot replicate. These efforts should achieve or beat the "near real-time" information-sharing goal set by the 2018 *National Strategy to Combat Terrorist Travel.*

Improve Vetting Capabilities: Significant work remains to ensure that the NVC reaches its full potential, enabling DHS and other adjudicating agencies to have timely access to the information they need to properly vet travelers and immigrants, and identify threats. The NVC will support additional vetting programs, extending its support beyond the current counterterrorism focus and deepening its capabilities through biometrics and advanced analytics. This will improve information sharing to provide greater intelligence and feedback on vetting decisions to DHS adjudicators, U.S. Department of State (DoS) Consular officers, and others responsible for vetting individuals for access to the United States or immigration benefits.

Enhance Support for the VSP: The Department leverages investigative resources like the VSP to augment its targeting and vetting initiatives to investigate suspect travelers during the visa application process. VSP differs from other Federal screening efforts by leveraging its capabilities to identify previously unknown threats instead of solely denying travel. The Department will support the VSP by expanding the presence of VSP units worldwide.

Stop WMD from Entering the Country: DHS will work to enhance its capabilities to detect and interdict the shipment of WMD, components, and related materials through technical detection and other targeting efforts at and between ports of entry.

Disrupt Illicit Trade Activity That Funds Terrorism: Law enforcement efforts have identified links between terrorist groups and the sale of counterfeit goods and illicit material in e-commerce. DHS will work to enhance end-to-end visibility into supply chains, implement technological solutions to more effectively segment risk among millions of daily trade transactions, and better align targeting efforts to detect and disrupt these illicit financial operations.

Objective 2.2: Improve DHS's security posture governing aviation, surface,

and maritime transportation.

The size of the Nation's transportation systems, coupled with the need for them to be accessible and efficient, creates vulnerabilities. Terrorists and other hostile actors have demonstrated an enduring interest in exploiting global aviation, surface transportation, and maritime transportation systems for a range of dangerous activities, including conducting attacks,[15] transporting weapons, and interfering with mass transit, supply chain networks, and critical infrastructure. Malicious insiders, including personnel employed by government agencies and transportation stakeholders, pose a risk because terrorists and criminals can exploit their knowledge to evade security measures.

TSA, established in the wake of 9/11, has improved the Nation's ability to respond to threats to the transportation system. DHS is working to raise the baseline for aviation transportation system security globally by implementing enhanced security measures, both seen and unseen, at all airports that are last points of departure to the United States in 105 countries. The measures include: 1) enhanced screening and vetting systems for travelers and cargo, 2) updated security inspection regulations at airports, and 3) refined mechanisms for mitigating insider threats. The Coast Guard leads an interagency maritime security effort focused on enforcing security zones, conducting law enforcement boardings, detecting WMD, and securing waterfront facilities. TSA assists the Coast Guard in various maritime security efforts, notably by working to implement passenger security and secure connection between ports. In addition, TSA works with the Department of Transportation, Federal Aviation Administration (FAA), private sector organizations, and Federal and SLTT partners to enhance the safety and security of the other transportation systems, including rail and pipeline security.

The Department also has counterterrorism capabilities in the transportation sector through TSA's Visible Intermodal Prevention and Response (VIPR) assets. VIPR teams promote confidence in and protect our Nation's transportation systems through targeted deployments of integrated TSA assets utilizing law enforcement and screening capabilities to augment security of any mode of transportation.

The Department will continue to adjust and improve its existing measures and introduce new ones as terrorists and other hostile actors adapt their TTPs for exploiting or threatening our Nation's transportation systems.

Priority Actions

Prevent Insider Threats: Criminal and terrorist networks recruit and coerce corrupt or vulnerable personnel employed by government and transportation stakeholders. These individuals possess insider privileges and knowledge that can facilitate, on behalf of the hostile organization, intelligence-gathering and counter-surveillance activities; theft; smuggling; tampering with or sabotaging security systems and devices; and, in some cases, terrorist attacks. Terrorists have used aviation insiders to plot and conduct attacks. The Department will improve protections against insider threats to all modes of transportation by ensuring the effectiveness of employee screening efforts, particularly at secure access

[15] Attacks against aviation and mass transit throughout the world demonstrate that terrorists remain interested in and capable of conducting such attacks. Though they did not succeed in killing anybody in these attempts, terrorists managed to place bombs aboard passenger planes bound for the United States on multiple occasions after the 9/11 attacks. Terrorists have downed passenger planes and carried out attacks against rail systems elsewhere in the world—including in Britain, Egypt, India, Russia, and Spain—since the 9/11 attacks.

points; increasing employees' understanding of insider threats by providing enhanced security training; conducting additional vulnerability assessments; and improving cooperation between industry and government stakeholders.[16]

Improve and Adapt Screening Capabilities: The Department will continually refine screening procedures of travelers, transportation sector workers, and cargo prior to departure. It will proactively identify and address vulnerabilities that can be exploited by terrorists.

Objective 2.3: Strengthen counterterrorism capabilities of foreign partners.

In the digital age, acts of terrorism and targeted violence often have transnational elements, even when not directly coordinated, facilitated, or inspired by FTOs. Terrorist travel, particularly as foreign terrorist fighter returnees gain greater salience, poses a threat worldwide. Many nations now face growing threats of terrorism and targeted violence originating from within their borders, much as the United States does. As a result, it is critical that international partners not only improve their ability to identify fraud and mitigate threats, but also supplement the Department's ability to establish identity and assess risk on an individual, as they often have information about their citizens' and residents' identities, and about risks that are not readily available in U.S. databases. These efforts should also prioritize identifying the connections between known illicit foreign actors and the United States.

DHS contributes to strengthening foreign capacity in many ways. Through DoS, DHS provides training to extend its experience in modern security policies and procedures to foreign counterparts, and develops valuable relationships. Such work is of critical importance in countries that historically have not invested in their homeland security tools, or are just emerging from repressive regimes that used such tools as a weapon against their own citizens. DHS encourages these partners to adopt compatible tools that are effective and protective of privacy and civil liberties. DHS, in partnership with DoS or the U.S. Department of Defense, also provides hardware, software, and other equipment and capabilities that help foreign governments improve the effectiveness of their programs and their ability to interact with technology-savvy DHS Components in such activities as the collection, analysis, and sharing of biographic and biometrics information.

Priority Actions

Improve Security Sector Assistance Procedures: DHS will continue to provide counterterrorism-related security sector assistance (SSA) to foreign partners in partnership with DoS to ensure that these partners have adequate capacity to detect, target, and interdict terrorists. DHS will target its SSA efforts strategically, ensuring that assistance to allies is based on threat assessments, U.S. strategic objectives, and resource constraints.

Improve International Coordination of Counterterrorism Efforts: To disrupt the range of threats facing the United States and its allies, DHS will continue to prioritize information sharing, interoperability, and collaboration with international partners to support the U.S. Government's pursuit of an effective global counterterrorism strategy. We can enhance our own capabilities by strengthening those around us.

[16] Compare the recommendations in U.S. House Homeland Security Subcommittee on Transportation and Protective Security, Majority Staff Report, *America's Airports: The Threat from Within* (February 2017), pp. 4–5, 11.

Improve International Standards for Counterterrorism: DHS will work with our partners to improve international standards governing border and aviation security, travel document security, and other efforts described in this Strategic Framework. We will work with international partners to develop international standards for the collection and use of passenger data and biometrics to implement United Nations Security Council Resolution 2396, which was adopted in 2017 as the global community sought to address the shared risk posed by foreign terrorist fighter returnees.

Objective 2.4: Enhance maritime security operational capabilities.

The Department oversees maritime counterterrorism operations. A lead contributor is the Coast Guard's Maritime Security Response Teams (MSRTs). As first responders specialized in responding to terrorist threats in the maritime domain, MSRTs help interdict and neutralize terrorists. MSRTs have the capability to search, detect, isolate, and triage CBRN threats in the maritime domain in an opposed environment. MSRTs have law enforcement authority in addition to their counterterrorism capabilities, and are thus able to assist other Federal entities in their domestic and international counterterrorism efforts.

The Department will further integrate the Coast Guard's MSRTs with other Federal counterterrorism actors, including TSA's VIPR assets, and will allocate resources accordingly.

Priority Actions

Improve the Flow of Information to Maritime Field Operators: DHS will lead in the production of an enhanced framework for gathering, documenting, processing, analyzing, and sharing information with field operators to advance counterterrorism and other national security interests in the maritime domain.

Integrate Maritime Operations with Other Counterterrorism Actors: To ensure that its teams are best able to contribute to maritime counterterrorism operations, the Department will further integrate them with other departments and agencies' counterterrorism efforts.

Goal 3: Prevent Terrorism and Targeted Violence.

The 2018 *National Strategy for Counterterrorism* acknowledges that, despite a "robust counterterrorism architecture" designed to thwart attacks, the United States does not have "a prevention architecture to thwart terrorist radicalization and recruitment." Thus, the National Strategy calls for the U.S. Government to "champion and institutionalize prevention and create a global prevention architecture with the help of civil society, private partners, and the technology industry." As DHS is charged with informing, equipping, and training SLTT governments, civil society, and the private sector to take preventive and protective actions, the Department is committed to developing this architecture domestically and implementing the priority actions of the National Strategy's "Counter Terrorist Radicalization and Recruitment" line of effort in coordination with our Federal partners.[17]

Prevention is not prediction. However, evidence-based research on individuals who carry out acts of targeted violence demonstrates that regardless of whether the attacks were acts of workplace violence, domestic violence, school-based violence, or terrorism, similar themes are evident among the perpetrators. A 2018 U.S. Secret Service National Threat Assessment Center (NTAC) review of mass attacks in public spaces found:

- Most of the attackers utilized firearms, and half departed the site on their own or committed suicide.
- Half were motivated by a grievance related to a domestic situation, workplace, or other personal issue.
- Two-thirds had histories of mental health symptoms, including depressive, suicidal, and psychotic symptoms.
- Nearly all had at least one significant stressor within the last five years, and over half had indications of financial instability in that timeframe.
- Nearly all made threatening or concerning communications and more than three-quarters elicited concern from others prior to carrying out their attacks.[18]

Over the past five years, Federal and SLTT officials have worked closely with academia, mental health professionals, educators, and faith leaders to better understand the threat we face and develop strategies to address it. The results of these efforts—through pilot and grant programs, and research studies—tell us that prevention works. It can save lives. The best way DHS can enhance the efficacy of prevention programs is by taking a whole-of-society approach, working with our Federal and SLTT partners to employ strategic frameworks that integrate various programs to increase societal resiliency and reduce the number of individuals likely to radicalize to violent extremism, while identifying and intervening with individuals ("off-ramping") before violent or criminal acts occur.

[17] The objectives and priority actions identified here flow directly from and support this section of the National Strategy.
[18] National Threat Assessment Center, *Mass Attacks in Public Spaces – 2018* (Washington, DC: U.S. Secret Service, July 2019), p. 2.

Objective 3.1: Strengthen societal resistance against the drivers of violent extremism and ensure broad awareness of the threat of terrorism and targeted violence.

An aware society is the best foundation for preventing terrorism and targeted violence. Peers are best positioned to recognize individuals exhibiting signs of radicalization to violent extremism and mobilization to violence, but the Federal Government is best positioned to generate the evidence-based research that identifies risk factors, behaviors, and other information that informs this awareness.

The DHS Science and Technology Directorate (S&T) supports the Department's mission by sponsoring scientific data collection and analysis to characterize threats and opportunities for prevention, and evaluating terrorism and targeted violence prevention programs and interventions. Research efforts are further supported by NTAC, which has a twenty-year history of conducting research, training, and consultations on the prevention of all forms of targeted violence, and I&A's NTER program.

Leveraging the latest research, DHS provides a variety of awareness briefings, engagement strategies, and outreach efforts to help the widest cross-section of society know what to look for and how to respond if an individual is mobilizing to violence. Past experience and behavioral research tell us that our most vulnerable individuals are the most susceptible to radicalization to violent extremism. We will prioritize the development of focused resilience programs designed to reach our youth across various stages of development and adolescence. Assisting vulnerable individuals requires open channels of trusted communication between government and civic leaders and other members of the public in any state and locality. As part of the Department's efforts to raise awareness of the threat, DHS intentionally invests in efforts that build trust among these stakeholders. These briefings, engagement strategies, and outreach efforts undergo detailed review to ensure they are built to protect First Amendment rights and maintain the Department's political neutrality.

Priority Actions

Form Partnerships That Support Locally-Based Prevention: Since individuals mobilize to violence due to various grievances and ideologies, collaboration among the widest possible cross-section of any locality is important for effective identification of problems and intervention.[19] The Department will form partnerships with key local stakeholders nationwide to share information that supports the mitigation of risk factors, addresses individuals radicalizing to violent extremism and mobilizing to violence, and enhances practices for prevention and intervention.

[19] A good definition of what *intervention* means in this context can be found in Brian A. Jackson et al., *Practical Terrorism Prevention: Reexamining U.S. National Approaches to Addressing the Threat of Ideologically Motivated Violence* (Homeland Security Operational Analysis Center, 2019), pp. 44–45. Noting that *intervention* and *off-ramping* have often been used synonymously, the authors explain: "The goal is to help an individual move away from violence through noncoercive counseling, service provision, and other resources. Although some of the elements of intervention … may be specific to individuals at risk of perpetrating violence who are driven by particular ideologies (e.g., religious counseling, tolerance-focused programming), many of the elements are not…. [K]ey elements of terrorism prevention intervention include job training, mental health services, life skills counseling, and other services that might be provided to at-risk youth because of concern about gang involvement, as components of substance abuse treatment, or through programs aimed at addressing other social ills. As is the case in those areas, entities involved in intervention can be government agencies, including law enforcement; social service agencies and NGOs; and community and other groups."

Increase Societal Awareness of Violent Extremism and Mobilization to Violence: The Department will standardize its approach to awareness briefings and ensure they are updated frequently to reflect the latest threat trends and research. Leveraging the Department's existing field presence and willing SLTT, non-governmental organization, and private sector partners, we will enhance society's awareness about radicalization to all forms of violent extremism and mobilization to violence, including imparting knowledge of the threat environment, relevant risk factors and behavioral indicators, and increased bystander knowledge of available referral networks (*i.e.*, what to do upon recognizing concerning behavior).

Build Trust Through Engagement and Exercises: Individuals must have an understanding of how information they provide will support prevention and protection efforts, and trust that those receiving this information will act promptly and responsibly. To build this trust, DHS will enhance its efforts to convene state and local practical exercises that bring together key stakeholders to review how information is gathered, shared, and used for prevention and protection missions. Examples include continuing and expanding upon the Community Roundtables, Community Resilience Exercises, the Building Communities of Trust program, and field-based Prevention Coordinators.

Objective 3.2: Counter terrorists and violent extremists' influence online.

As this Strategic Framework has explained, the way that Americans and people across the globe communicate has been fundamentally transformed by the online environment. For some violent extremist movements—including white supremacist violent extremists and radical Islamist terrorists—the online space appears essential to their recent growth. It is vital that the Department help its state and local partners counter the influence of terrorists and violent extremists in the online space.

Priority Actions

Engage with Partners in the Private Sector: The Department will strengthen its partnership with the private sector, highlighting the important role private sector companies can play in social resilience, and identifying tools and methods for private sector partners to play a larger role in prevention efforts at a local level. In particular, the Department will build upon its relationships with the technology sector, including Internet service providers and social media companies, to address the spread of violent extremist content on their platforms. DHS will encourage the tech sector to help inform the public of the risks associated with the spread of violent extremist ideology, and to participate in and contribute to prevention and resilience efforts. Examples of DHS's engagement include awareness briefings tailored to the needs of technology sector experts to recognize and react to violent extremist content on their platforms, and the convening of Digital Forums for Terrorism Prevention that connect technology sector experts with civic leaders to catalyze prevention activities online.

Support Counter-Messaging Efforts by Tech Companies, Non-Governmental Organizations, and Civic Partners: Private organizations and technology companies have engaged in counter-messaging campaigns seeking to steer individuals away from messages of violence. DHS will support these efforts by sharing threat information when possible, evaluating the efficacy of counternarrative efforts, and providing grant funding to effective campaigns. DHS will engage the technology sector to identify and amplify credible voices online, and promote counternarratives against violent extremist

messaging. In these efforts, DHS will prioritize freedom of expression, privacy, civil rights, and civil liberties, while seeking to convey the harm done by targeted violence and terrorism.

Protect First Amendment Rights and Maintain the Department's Political Neutrality: The Department will support an online civic culture that not only protects but prioritizes freedom of expression, robust exchange of ideas, privacy, and civil liberties while simultaneously countering attempts to incite terrorism and acts of targeted violence.

Objective 3.3: Develop prevention frameworks with SLTT partners to enhance their ability to identify and respond to individuals at risk of mobilizing to violence.

DHS is committed to empowering SLTT partners to have the capabilities needed to identify and respond to at-risk individuals. Prevention programs must reside at the local level. Numerous studies have confirmed that peers with the closest proximity to individuals at risk of radicalization to violent extremism are uniquely positioned to detect, prevent, and counter this process.

The Department will keep SLTT stakeholders informed of evidence-based practices and protocols that can inform local prevention frameworks. In April 2019, DHS announced the establishment of the Office for Targeted Violence and Terrorism Prevention (TVTP), which built off previous Department prevention efforts. TVTP widens the scope of previous efforts by ensuring that all forms of violent extremism or targeted violence that threaten homeland security, regardless of the grievances driving them, are addressed. TVTP field staff deliver trainings and technical assistance to support the development of local prevention frameworks. The Office also engages key local stakeholders (*e.g.*, civil society groups, mental health professionals, non-profit organizations, academia, law enforcement agencies, social services, and other government offices) to develop the trust and information sharing that is critical to forming effective prevention frameworks.

Priority Actions

Work with SLTT Partners and Civil Society to Identify Best Practices and Document the Baseline Capabilities for SLTT Prevention Frameworks: A critical aspect of prevention is accessible options for intervention with individuals radicalizing to violent extremism and mobilizing to violence. Intervention is inherently multidisciplinary, requiring coordination and cooperation among SLTT partners, non-profit organizations, professional associations, and academia. DHS, working with appropriate Federal partners—including the U.S. Department of Health and Human Services (HHS), the U.S. Department of Education, and DOJ—will build on existing work being conducted by our SLTT partners and civil society members. DHS will document the best practices and baseline capabilities for establishing local referral networks and multi-disciplinary threat management/threat assessment capabilities, as well as conducting interventions. Once developed, DHS will encourage the adoption of these best practices and baseline capabilities through grant programs, prevention field coordinators, training, and technical assistance, so that any member of society has options for accessing intervention capacity to prevent terrorism and targeted violence. NTAC will expand its training on threat assessments to better identify persons of concern and assess whether they may pose a risk.

Enhance Grant Program Support to SLTT, Law Enforcement, and Emergency Management

Partners: DHS will expand the ability of field personnel to support prevention programming activities with SLTT partners by expanding existing counterterrorism grant programs to also support prevention programming. The Department will also seek additional funding for these grant programs.

Institutionalize Threat Assessment and Management: A successful prevention system is contingent on non-government behavioral professionals and practitioners utilizing their professional capabilities to assess and implement individual threat management plans with individuals of concern. DHS, with partners at DOJ, HHS, and other agencies, will consult with behavioral experts and other professionals to institutionalize the capacity to respond to individual cases of mobilization to violence. This includes but is not limited to the most effective utilization of existing resources, expanding the training of new professionals in educational institutions or professional training, and the creation of accepted professional standards or credentialing for threat assessment and management.

Train SLTT Law Enforcement Partners and Connect Them with Local Referral Networks and Intervention Resources: DHS will work with partners to train SLTT law enforcement partners on intervention options available in their communities. Effective prevention frameworks require law enforcement to work closely with civil society professionals participating in intervention networks to ensure that individuals radicalizing to violent extremism are referred to the appropriate services, while law enforcement is notified in the appropriate circumstances. In addition, DHS training should provide guidance on privacy, civil rights, and civil liberties concerns that non-government partners may have in partnering with law enforcement for countering violent extremism (CVE) activities, and how SLTT law enforcement may ameliorate barriers to cooperation.

Encourage Ongoing Whole-of-Government Assessment of Federal Prevention Programs: This whole-of-society approach to prevention requires the engagement of a variety of professionals, experts, departments, and organizations specializing in various aspects of prevention programming. It is important for the whole Federal Government, including HHS, DOJ, the Department of Education, and others, to coordinate their prevention activities and efforts. The Department will take leadership in encouraging its Federal partners to collaborate with DHS to conduct ongoing comprehensive whole-of-government assessments of the architecture of Federal Government programs that may be used in or considered a part of a holistic Federal Government prevention toolbox.

Evaluate Prevention Programming and Expand Research and Training on Threat Assessment, Intervention, Reintegration, and Counter-Recidivism: The prevention efforts described in Goal 3 are relatively young, with only a few years of demonstrated success. The nature of the fast-evolving threat demands that we try new and innovative approaches—including some that might fail. DHS is committed to being transparent about both our failures and successes, and rapidly updating our programming based on the results of such evaluations and any new research that becomes available. S&T will expand efforts to evaluate the prevention programs described in this goal, as well as continue to research best practices and effectiveness of threat assessments, interventions, re-integrations, and counter-recidivism. The Department will continue to rely on NTAC's expertise in conducting behavioral studies on attacks at K-12 schools, attacks on government, mass attacks, and other forms of targeted violence directed at schools, workplaces, and communities.

Objective 3.4: Working with DOJ and SLTT partners, develop and implement recidivism reduction programming to address individuals convicted of crimes related to terrorism and targeted violence.

People convicted of crimes related to terrorism and targeted violence pose a unique risk during and after incarceration. Hundreds of people have been convicted of terrorism-related offenses since 9/11, and many more have been convicted of offenses related to targeted violence. Most perpetrators will eventually be released to their home localities and states. Likewise, the return to the United States of the spouses and children of individuals who joined terrorist organizations abroad to participate in foreign conflicts requires specialized skill sets for successful reintegration into our localities. Some of these individuals have not committed a crime yet may support violent extremism. Regardless of their beliefs, they are a vulnerable population, facing a difficult transition. Effective support for reintegration is an important factor in reducing the risks they pose. Recidivism reduction programming for terrorism-related offenses is currently limited at the SLTT level. Efforts are hampered by limited funding, in addition to a lack of research into the impact of incarceration on radicalization to violent extremism, the reliability of risk assessments, and the effectiveness of risk-reduction efforts.

The Department will seek to address these problems by developing evidence-based best practices and standards for recidivism programming. It will work with Federal and SLTT partners and non-governmental agencies to disseminate and implement these practices across our justice and correctional system. DHS will continue to prioritize R&D efforts to ensure that all guidelines are grounded in sound evidence. The Department will also work to develop best practices specifically tailored to reintegrating the returning spouses and children of U.S. citizens who joined terrorist organizations abroad.

Throughout these efforts, DHS will continue to prioritize the protection of privacy, civil rights, and civil liberties. The Department aims to manage risks associated with these individuals while recognizing that successful reintegration is an important step in reducing the risk of future terrorism and targeted violence. The protection of rights is especially important in the context of reintegrating spouses and children of individuals who joined terrorist organizations as foreign terrorist fighters. These individuals may themselves be victims of violence and other trauma.

Priority Actions

Develop and Implement Awareness Briefings and Trainings for Corrections Officials: Corrections officials at the Federal and SLTT level need to be aware of current national and local threats from terrorism and targeted violence. DHS will coordinate with DOJ to determine roles and responsibilities as well as division of labor in providing regular briefings, modeled on the Community Awareness Briefings program, to maintain awareness and disseminate updated intelligence, analysis, and information on best practices.

Coordinate with and Provide Support to Federal, SLTT and Non-Governmental Organizations Engaged in Recidivism Reduction Programming: While the Department is uniquely situated to develop and disseminate knowledge on best practices for reducing recidivism, other Federal and SLTT actors, along with non-governmental service providers, will be responsible for implementing recidivism reduction programming. DHS will coordinate with DOJ to determine the best ways in which DHS can support recidivism reduction programming, to include potentially updating grant guidance to support recidivism reduction efforts by SLTT governments and non-governmental service providers.

Develop and Disseminate Best Practices for Reintegrating Returning Spouses and Children of Foreign Terrorist Fighters: TVTP and S&T, in partnership with DOJ, will identify best practices for reintegration programming for the returning spouses and children of individuals who joined terrorist organizations to fight in foreign conflicts.

Support R&D Focused on Recidivism Reduction: Significant gaps exist in our knowledge of recidivism among currently or formerly incarcerated individuals convicted of terrorism or targeted violence-related offenses. DHS, in coordination with DOJ, will support research seeking to address major questions in this area, including evaluation of the efficacy of specific recidivism reduction programs and practices, the reliability of risk assessments, and the impact of incarceration on the spread of violent extremist ideologies. This includes examination of the efforts and best practices undertaken by our allies abroad in dealing with radicalization to violent extremism in prisons, recidivism, and reintegration. DHS will support the development of new risk assessment techniques and recidivism reduction programming where current methods are found lacking.

Objective 3.5: Build resilience to malign information operations initiated by foreign states and foreign non-state actors.[20]

Information operations are undertaken to shape public opinion or undermine trust in the authenticity of legitimate information. Hostile foreign actors—both states and non-state actors—leverage false information or information that is so highly selective as to be misleading with the intention to actively target segments of the American public. Such operations are frequently referred to as *disinformation campaigns*. Information operations by nation-states and hostile foreign non-state actors have had a direct nexus with terrorism and other forms of targeted violence, with recent campaigns promoting violent extremist ideologies and stoking tensions within our diverse Nation.

The Department is committed to implementing a more comprehensive effort to tackle disinformation operations threatening the American polity, particularly those that promote violence. In the counter-disinformation sphere, everything the Department does is designed to improve societal resilience, which has been a DHS focus since the Department's creation. The following priority actions are what DHS will do to counter foreign disinformation campaigns.

Priority Actions

Develop a Media/Information Literacy Toolkit: The Department will spearhead initiatives to raise awareness of disinformation campaigns targeting communities in the United States, providing citizens the tools necessary to identify and halt the spread of information operations intended to promote radicalization to violent extremism or mobilization to violence. DHS already has the tools and expertise to leverage large-scale national campaigns to empower the American people with knowledge at the grassroots level. A gap exists, though, in the form of a public awareness campaign that includes information on media literacy and disinformation campaigns. DHS will now address this gap. The American people need to be equipped with a toolkit to help them better understand and withstand

[20] Foreign state and non-state information operations can be malign in a variety of ways. We consider them relevant to this Strategic Framework only where they promote grievances or ideas that will make individuals more likely to mobilize to violence. Other parts of the Department and the Federal Government, and other strategies, address disinformation campaigns in other contexts.

disinformation campaigns, similar to the toolkit offered through the Department's cybersecurity campaign "STOP. THINK. CONNECT."

Bolster Information Sharing About Foreign Disinformation Campaigns: The Department will build societal resilience to disinformation campaigns through strategic multi-sector partnerships, as well as by bolstering engagement with SLTT actors and the public. When a disinformation campaign targeting a specific community is identified, DHS will, where possible and prudent, make community stakeholders—namely, appropriate SLTT entities—aware of the campaign. DHS will empower SLTT actors, who are often trusted voices in their communities, to shed light on and counter disinformation campaigns.

Goal 4: Enhance U.S. Infrastructure Protections and Community Preparedness.

Our Nation's infrastructure and public spaces are high-value targets for terrorism and targeted violence. The Department will work alongside its Federal and SLTT partners to enhance our protections of critical infrastructure and vulnerable soft targets. We will enhance the preparedness of Federal and SLTT entities, the private sector, the public, and other stakeholders.

Objective 4.1: Enhance preparedness and promote readiness for potential attacks.

The Department is committed to strengthening community preparedness and readiness for attacks. While terrorism and targeted attacks are difficult to predict, fortifying our communities against them is within our control.

DHS led the development of the National Preparedness Goal, a capabilities-based vision for preparedness for all types of disasters and emergencies. It is designed to establish a secure and resilient Nation. The National Preparedness System outlines a six-part process through which communities can organize and execute preparedness in support of the National Preparedness Goal.[21]

The Department has expanded its preparedness efforts to empower a wide variety of stakeholders. For example, in 2018, FEMA expanded required participation in THIRA and Stakeholder Preparedness Review (SPR), which are interconnected processes that communities can use to evaluate their preparedness. The THIRA/SPR most directly addresses the first two components of the National Preparedness System—identifying and assessing risks, and estimating capability requirements—but it supports implementation of all six. The THIRA/SPR is a whole community process: Communities completing this assessment should include partners in the private and non-profit sectors, and at all levels of government. With many communities leveraging the THIRA/SPR, FEMA moved THIRA/SPR to a new online platform, PrepToolkit. Communities may request access, so they can complete the THIRA/SPR using this convenient online portal. Completing the THIRA/SPR helps communities identify and understand their risks, set goals for addressing the risks, identify gaps between their current capabilities and their goals, and develop approaches for addressing those gaps.

It is imperative to increase the number of communities prepared to perform their role in preventing, protecting against, mitigating, responding to, and recovering from attacks. Preparedness is a shared responsibility, calling for everyone's involvement, not just that of the government.

Priority Actions

Enable Preparedness: DHS will continue to enable all levels of government and the private sector to execute the National Preparedness System by building and sustaining the core capabilities required to prevent, protect against, mitigate, respond to, and recover from threats that pose the greatest risk.

[21] The six-part process is: *identifying and assessing risk*; *estimating capability requirements*; *building and sustaining capabilities*; *planning to deliver capabilities*; *validating capabilities*; and *reviewing and updating*.

Facilitate Resource Availability for Preparedness: Since community preparedness relies on SLTT and private partners, it is vital that stakeholders have access to the resources they need to reach relevant goals. The Department facilitates resource accessibility, in part, through its DHS Homeland Security Grants, which provide financial support to SLTT partners, non-governmental organizations, and select critical infrastructure sectors, among others, to address self-assessed capability gaps.

Foster a Whole Community Approach to Preparedness: Preparedness takes different forms for different communities, making whole community involvement necessary to establish true resilience. The Department will foster a whole community approach by incentivizing collaboration across jurisdictional boundaries, across levels of government, and with private sector and non-governmental partners. This work will include increasing active shooter preparedness by broadening the awareness of local law enforcement and community leaders about DHS resources, tools, and trainings.

Objective 4.2: Enhance defensive measures for infrastructure and soft targets, and against high-impact threats.

Americans expect that they will be safe and secure as they cheer a favorite team at a sporting event, shop at a mall, attend a house of worship, go to school, dine out with family and friends, or go to a concert. Maintaining the integrity of our open society is vital to the future of the Nation. Soft targets and crowded places—which DHS defines as locations that are easily accessible to large numbers of people and that have limited security or protective measures in place, thus making them vulnerable to attack—are an urgent focus area. Terrorists and other violent actors have plotted against or attacked such places using simple, low-cost methods with minimal identifiable indicators.

DHS's Cybersecurity and Infrastructure Security Agency (CISA), in partnership with public and private sector stakeholders, leads Federal efforts to mitigate risks to the Nation's critical infrastructure and key assets. Also noteworthy are Federal efforts concerning special events, which are non-routine national, regional, or community activities like concerts, major sports events, or political rallies. These events require additional planning, prevention, and response services to ensure public safety. SLTT and Federal partners voluntarily submit special events not designated as National Special Security Events to the DHS Operations and Coordination (OPS) Special Events Program. OPS analyzes submitted events using the Special Events Assessment Rating methodology, which applies a quantitative/qualitative analytic approach to each event, calculating threat, vulnerability, and consequence in order to create the National Special Events List used to maintain situational awareness and determine the level of Federal support that may be provided.

There is also a growing interconnectedness and interdependence of critical infrastructure on converged cyber and physical systems. Transportation, electricity, and water systems are just a few examples. The *National Preparedness Report* has identified infrastructure systems and cybersecurity as areas for improvement every year since 2012. States consistently rate cybersecurity as their least proficient core capability in their SPRs.

Priority Actions

Enhance Security of Soft Targets: The Department will work with Federal and SLTT partners and the private sector to produce and disseminate products, tools, and best practices to mitigate risks at places where people gather, such as schools, workplaces, entertainment venues, transportation nodes,

and houses of worship. DHS will tailor its approach to enhancing soft-target security based on the nature of the location, respecting the varying levels of security these places deem appropriate. For example, some shopping outlets or houses of worship may be reluctant to have their venues appear overly "securitized," in which case the Department can offer alternative resources. The Department will continue to develop new techniques that incentivize the private sector to invest in protective practices.

Enable Nationwide Cybersecurity and Infrastructure Security: The cyber domain and critical infrastructure are significant targets to protect from terrorism and targeted violence, yet both have vulnerabilities. The Department will work to enable and incentivize cybersecurity and infrastructure security across all levels of government and the private sector. DHS will help partners to build and sustain capabilities required to prevent, protect against, mitigate, respond to, and recover from the most significant threats. Efforts will include executing capability-based planning; performing risk, vulnerability, and capability assessments; developing and promulgating best practices, guidance, and standards; and developing and delivering training and exercises.

Upgrade Biodetection Technology: The Department will strengthen its ability to detect a pending biological attack through air-monitoring, analysis, notification procedures, and risk assessment. The Department will upgrade its technologies to address a wider range of bioterrorism threats; provide real-time data across the homeland security enterprise; and improve information sharing between Federal and SLTT partners.

Integrate Frontline Operator Capabilities with DHS Response and Recovery Efforts in the Event of a WMD Attack: SLTT authorities will likely be the first to respond to any WMD terrorist incident. To ensure that local and regional resources are not overwhelmed, DHS will assist with supplemental capability and technical support.

Objective 4.3: Enhance protections against hostile actors' use of unmanned systems and other emerging technologies.

Unmanned systems and autonomous technology, which includes UAS,[22] are becoming increasingly sophisticated and widely used for commercial, recreational, and security applications. This technology is quickly becoming an integral part of the aviation, maritime, and surface transportation landscape. While the vast majority of uses are legitimate, authorized, and benign, these systems can be exploited by terrorists, criminal organizations, and other malicious actors. Violent non-state actors across the globe have already used unmanned systems to carry out attacks, transport weaponized payloads, conduct surveillance, monitor targets, smuggle illicit goods, and interfere with critical infrastructure. They have been used to monitor law enforcement and first responder movement, and to facilitate the movement of narcotics across the U.S. border, as well as into prisons. Malicious uses of UAS have resulted in significant public burdens, including extended airport closures, which further underscore the harm that terrorists could potentially inflict with this technology. As unmanned systems technology improves, and as innovations like jet propulsion capabilities become more commonplace in them, this technology will pose a growing challenge in the wrong hands. The 2018 *National Strategy for Aviation Security* recognizes that continued improvements in UAS technologies will generate

[22] *Unmanned aircraft* is defined in section 331(8) of the Federal Aviation Administration Modernization and Reform Act of 2012, P.L. 112-95 (2012), as "[a]n aircraft that is operated without the possibility of direct human intervention from within or on the aircraft."

economic and social benefits, but it emphasizes the need for a holistic and adaptive approach to securing the aviation ecosystem.

Unmanned systems are not the only new or emerging technology likely to be used in support of terrorism and targeted violence. In 2014–16, ISIS's use of social media captured the public imagination due to the group's innovative approach to publicizing itself and inspiring sympathizers to carry out attacks in its name. The group's operatives even used the digital space, coupled with encryption, to remotely direct terrorist attacks outside of ISIS's core operational territory. The numerous attacks in France directed by ISIS "virtual plotter" Rachid Kassim exemplify this phenomenon.[23] Moving forward, emerging technologies that pose a concern in the hands of terrorists and other hostile actors include artificial intelligence (including potential use of "deepfakes"), biotechnology, 3D printing, and cryptocurrencies.

Congress passed the Preventing Emerging Threats Act of 2018 to provide counter-UAS (C-UAS) authority to DHS and the DOJ. DHS continues to implement its new authorities to mitigate credible threats of UAS-driven attacks. The Department is investing in research into methods for protecting against and mitigating the UAS threat, but these efforts need to be expanded. The threat of unmanned systems being employed in terrorism and targeted violence, as well as the potential for other emerging technologies to be used in a similar way, affects a range of stakeholders. These challenges require the Department to take a collaborative approach internally, and with its Federal, SLTT, and industry partners.

Priority Actions

Further Develop Public Awareness Campaigns Addressing Misuse of Unmanned Systems and Other Emerging Technologies: The Department, in coordination with Federal and SLTT partners, will engage in campaigns and outreach to educate the public about the potential use of unmanned systems and other emerging technologies in acts of terrorism and targeted violence. These campaigns, which will be similar to the Department's "If You See Something, Say Something" initiative, will highlight security concerns and measures the public can follow for safely operating UAS in the national airspace.

Establish Partnerships to Address Misuse of Unmanned Systems and Other Emerging Technologies: Our Nation has a strong interest in encouraging the legitimate use of unmanned systems and other emerging technologies, while guarding against their use in terrorism and targeted violence. The Department will team with other Federal agencies, as well as private industry and other stakeholders, in countering the misuse of unmanned systems and other emerging technologies by terrorists and other violent actors.

Sponsor Research on Unmanned Systems and Other Emerging Technologies: The Department will sponsor research into domain awareness and countermeasures to unmanned systems threats, including R&D that can produce technical breakthroughs, and it will undertake research

[23] *Virtual plotters* are operatives in ISIS's external operations division who use the online space to inspire, guide, and direct attacks outside of the group's core territory. These operatives often play a key role in conceptualizing plots, from target selection through attack execution. Using encrypted digital communications, virtual plotters are capable of performing most of the key functions of supporting an attack that were previously reserved for physical networks.

related to other emerging technologies that could pose similar threats. The Department will coordinate with Federal and SLTT partners, and other stakeholders, to make domain awareness and countermeasures available for deployment in a timely fashion.

Defend Against Threats from Unmanned Systems and Other Emerging Technologies: The Department will work with Federal and SLTT law enforcement organizations and industry partners to identify potential gaps in authorities, and work with Congress to ensure that the necessary authorities and capabilities exist to defend against these emerging threats.

Promulgate Best Practices for Action Against Misuse of Unmanned Systems and Other Emerging Technologies: The Department will work with Federal and SLTT partners to produce and disseminate best practices, policies, and regulations to support legitimate use of unmanned systems and other emerging technologies, while addressing effective means to restrict access to such technology by terrorists and other malicious actors. DHS will work with and support the efforts of international partners like the Global Counterterrorism Forum (GCTF) that have been active in codifying and promulgating best practices related to terrorist use of UAS and other aspects of the intersection of technological developments with terrorism and targeted violence. Balancing safety, data privacy, and security in the aviation ecosystem is critical to ensuring the growth of these beneficial technologies.

Conclusion

In the aftermath of 9/11, the U.S. Department of Homeland Security was designed as a last line of defense for the Homeland. Our Department was created to prevent, protect against, mitigate, respond to, and enhance recovery from multidimensional threats to the Homeland and their ensuing fallout. DHS's personnel and capabilities are intentionally as diverse as the threats we face, designed to allow for maximum flexibility in response to any number of attacks, disasters, and crises that may befall the Nation.

As the Department has evolved, it has developed recognized capabilities that play a forward-leaning role in the Nation's defense. DHS personnel are now forward deployed around the globe, proactively advancing our Nation's interests, virtually "pushing our borders outward," and enhancing our national defense-in-depth. The Department operates across theaters, threats, and mission sets, supporting multiple national priorities and Federal partners each day.

Countering multiple terrorist threats simultaneously, both those of foreign origin *and* those originating here at home, is not only something our Components and support elements empower us to do, but is also a core responsibility of our modern Department. Our *Strategic Framework for Countering Terrorism and Targeted Violence* clearly identifies the need for the Department to expand its counterterrorism approach, enhancing our pressure on our traditional foreign adversaries while applying new attention and resources to an evolving domestic threat.

The *Strategic Framework for Countering Terrorism and Targeted Violence* marks the Department's recognition of the changing nature of terrorism and targeted violence in America. It explains the Department's approach to further developing its flexible toolkit to counter all forms of terrorism and targeted violence as they emerge, evolve, and intersect. By fundamentally improving our understanding of the evolving landscape for terrorism and targeted violence, and supporting partners in the homeland

security enterprise through this specialized knowledge, we will improve our ability to prioritize threats and subsequently more effectively allocate resources and personnel across the Department. This in turn will allow us to better prevent terrorists and other hostile actors from entering the United States, and deny them the opportunity to exploit the Nation's trade, travel, and immigration systems. It will allow us to better prevent terrorism and targeted violence here at home.

In 2019, we not only face adversaries employing traditional TTPs to attack the Homeland in new ways, but also new TTPs that create previously unanticipated threats. Though often quite beneficial to society, emerging technologies and digital-age innovations that facilitate the rapid spread of information and ideas will always include the potential to be used for violence and hate. We will continue to face hostile actors exploiting this freedom to sow discord and promote violent extremism.

As a Nation, we can and must resist these calls to violence. The Department's strategy to counter terrorism and targeted violence places a new emphasis on our domestic prevention mission, drawing on proven methods for integrating the efforts of Federal, SLTT, and private sector partners toward our collective national security during a period of evolving threats. It calls for a renewed effort to build and sustain the resiliency of American communities. To be secure, we must emphasize locally-based solutions that identify signs of risk before acts of terrorism or targeted violence can be carried out. Not only must we develop frameworks for prevention, but we must also enhance infrastructure protections and community preparedness to better protect against, respond to, and recover from attacks when they do occur.

As we operate in an evolving terrorism landscape, our initiatives must be grounded in respect for individuals' privacy, rights, and liberties. We must remember that freedom of speech is—and always should be—protected as one of our foundational values. This is critical as we address the potential threat of new and emerging technologies, particularly those used to facilitate online radicalization to violent extremism.

The U.S. Department of Homeland Security remains vigilant and forward-looking, prepared to adapt and evolve to multiple threats and crises, just as the threats we confront adapt and evolve. We will safeguard the American people, our Homeland, and our values with honor and integrity. The source and nature of the terrorist threat may have expanded, but we will continue to fight to ensure that all Americans are able to live free from the fear of violence, no matter the ideology behind it.