JBS International

Countering Violent Extremism: Law Enforcement Perspectives

Training and Information Needs

Jill Rhodes
9/20/2013

Contents

Acknowledgments

The study team would like to offer its thanks to all of the Department of Homeland Security (DHS), fusion center, and law enforcement personnel who made this study possible. The team would also like to thank the DHS Science and Technology Directorate's Resilient Systems Division for its guidance and assistance in identifying stakeholders. The team is grateful for the hospitality of the fusion centers, and the support of their directors in allowing the team to impose on the time of their staff. The DHS Intelligence Officers were instrumental in facilitating the selection of interviewees and recruiting focus group participants, and the study would have taken significantly longer without their assistance and support. Finally, the team would like to acknowledge all of the law enforcement departments that very generously volunteered the time of their officers and leadership to this effort. Key individuals played a crucial role in assisting the team to identify and recruit focus group participants, and the study would not have been successful without their assistance.

List of Acronyms

ACIAPT	Advanced Course for Intelligence Analysis to Prevent Terrorism
ADL	Anti-Defamation League
BITAC	Basic Intelligence and Threat Analysis Course
BJA	Bureau of Justice Assistance
CFR	Code of Federal Regulations
CIKR	Critical Infrastructure and Key Resources
CRCL	Office for Civil Rights and Civil Liberties
CT	Counterterrorism
CVE	Countering Violent Extremism
DHS	Department of Homeland Security
DOJ	Department of Justice
DT	Domestic Terrorism
FBI	Federal Bureau of Investigation
FC	Fusion Center
FEMA	Federal Emergency Management Agency
FIAT	Foundations of Intelligence Analysis Training
FLO	Fusion Liaison Officer
FOUO	For Official Use Only
HSDN	Homeland Security Data Network
HS-SLIC	Homeland Security State and Local Intelligence Community of Interest
HSIN	Homeland Security Information Network
HVE	Homegrown Violent Extremism
ICE	Immigration and Customs Enforcement
IFCAT	Intermediate Fusion Center Analyst Training
ILO	Intelligence Liaison Officer
IO	Intelligence Officer
IT	International Terrorism
ITACG	Interagency Threat Assessment and Coordination Group
JTTF	Joint Terrorism Task Force
KIPP	Knowledge and Intelligence Program Professionals
LE	Law Enforcement
LEO	Law Enforcement Online
MITAC	Mid-level Intelligence and Threat Analysis Course
MOU	Memorandum of Understanding
NCTC	National Counterterrorism Center
NOC	National Operations Center
NSI	Nationwide SAR Initiative
NW3C	National White Collar Crime Center Training
ODNI	Office of the Director of National Intelligence
OSINT	Open Source Intelligence
PC	Politically Correct
POST	Peace Officer Standards and Training Commission
RISS	Regional Information Sharing System
SAR	Suspicious Activity Reporting
SLATT	State and Local Anti-Terrorism Training
SLTT	State, Local, Tribal, and Territorial (in reference to law enforcement)

SPLC	Southern Poverty Law Center
SVTC	Secure Video Teleconference
TLO	Terrorism Liaison Officer
VE	Violent Extremism

Executive Summary

Introduction

In August 2011, the White House released the national strategy for *Empowering Local Partners to Prevent Violent Extremism in the United States*.[1] This guiding document, and the subsequent December 2011 *Strategic Implementation Plan*, focuses on three core areas of activity: (1) enhancing engagement with and support to local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise for preventing violent extremism; and (3) countering violent extremist propaganda while promoting U.S. ideals. It also emphasizes the importance of community-based problem solving, local partnerships, and community-oriented policing in building resilience to violent extremism in the United States. This study aimed to support federal government efforts focused on the second objective outlined in the strategy by examining the perspectives of fusion center personnel and local law enforcement on the 1) training and 2) information they receive and need related to countering violent extremism (CVE).

In 2011, the Department of Homeland Security (DHS) Science and Technology Directorate contracted JBS International to gather data from fusion center personnel and local law enforcement across the country to gain a better understanding of their experiences and views. While the team sought feedback on current federal efforts that provide CVE training and information, the study was neither an evaluation nor an assessment of these efforts. Because the goal of this study was to learn more about the perspectives of the participants, these perspectives are represented even when their conceptualizations of CVE differ from that of the federal government.[2]

JBS conducted interviews and focus groups in 17 locations around the country, generally with staff at a fusion center and with law enforcement in surrounding communities. Participants were asked about their experiences with and needs for training and information with respect to CVE and their thoughts on how to improve the training and information they currently receive. Additional areas of inquiry focused on what participants viewed as the primary threats in their communities and their general impressions of current efforts to counter violent extremism.

Methodology

JBS International used qualitative methods of data collection in this study. These methods included focus group discussions and in-depth interviews to explore the experiences and needs of the participants. In-depth interviews were primarily conducted with senior law enforcement personnel and fusion center leadership. The decision to interview leadership individually was based on standard focus group practices, which seek to bring together groups that are homogeneous in nature. The inclusion of participants who are in hierarchical relationships—supervisor and subordinate—in focus groups is not optimal due to concerns that the presence of

[1] The national strategy for *Empowering Local Partners to Prevent Violent Extremism in the United States* can be found at http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf, and the *Strategic Implementation Plan* can be found at http://www.whitehouse.gov/sites/default/files/sip-final.pdf.

[2] For example, several participants discussed the need for more training on source development as a CVE-related training need. The federal government does not view this type of training as CVE-related, but because it was mentioned by participants, it is included in this report.

supervisors may lead participants to censor their comments to align with what they believe are their supervisors' opinions.

JBS worked closely with members of the DHS CVE Working Group in choosing the sites included in the study and developing the focus group and interview guide. Sites were chosen based on where CVE-related training had been previously offered, recommendations by key stakeholders, geographic diversity, and population size. Ultimately, the team selected 17 sites for inclusion in the study. Site visits began in July 2012 and were completed in February 2013.The outreach strategy to these sites primarily involved coordinating with the DHS intelligence officers at fusion centers. The recruitment plan sought to recruit fusion center personnel and local law enforcement who had participated in CVE training. Where little or no CVE training had been provided, JBS requested participants who had taken other CVE-related training or who served in CVE-related capacities. To try to provide uniformity across very different sites, the recruitment plan included participants by functional area, rather than job title, to account for the diversity among fusion centers, different levels of staffing, varying levels of operational complexity, and different areas of focus.

In general, interviews lasted 35 minutes, and focus groups lasted one hour and 15 minutes. Participants were asked 12 questions focused on the types of threats their communities face, the training and information that they have received and need regarding CVE, and what information they would like to convey to those leading government CVE efforts (or what they would do if they led government CVE efforts).

The methodology was structured to facilitate the collection of honest and unfiltered perspectives and included a guarantee that the participants' responses would be reported anonymously. In keeping with this mode of data collection, moderators did not evaluate or challenge participants' responses.

Overall, the team conducted 54 in-depth interviews with law enforcement and 61 in-depth interviews with fusion center personnel (typically those in leadership positions or unique roles that did not have a well-defined peer group). The team also conducted 19 focus groups with a total of 120 law enforcement participants and 17 focus groups with a total of 106 fusion center staff members. Among the 174 law enforcement personnel who participated in the study, 29 were executives, 47 were investigators, 88 were frontline officers, and 10 had other, varied roles. Among the 167 fusion center staff who participated, 36 were senior staff, 41 were liaisons, 75 were analysts, and 15 had other, varied roles.

Fieldwork for this study presented a few challenges. The sensitivity of the topic, the wide range of locations, and the diversity of the participants led to challenges related to recruitment. Additionally, planning for the study began in late 2011 when the phrase "countering violent extremism" was only beginning to enter into the national security lexicon. With little training available that was specifically labeled "CVE training" and participants' varying levels of knowledge concerning what efforts to counter violent extremism might entail, the study team allowed the participants to describe the trainings and information that they viewed as CVE-focused.

Data Analysis

The team used an inductive or "bottom-up" approach in analyzing the data collected. Transcripts and notes from interviews and focus groups were grouped by site and were generally coded by the team members who visited the sites. Personally identifiable information was removed from transcripts prior to them being uploaded to the qualitative data analysis software, ATLAS.ti.

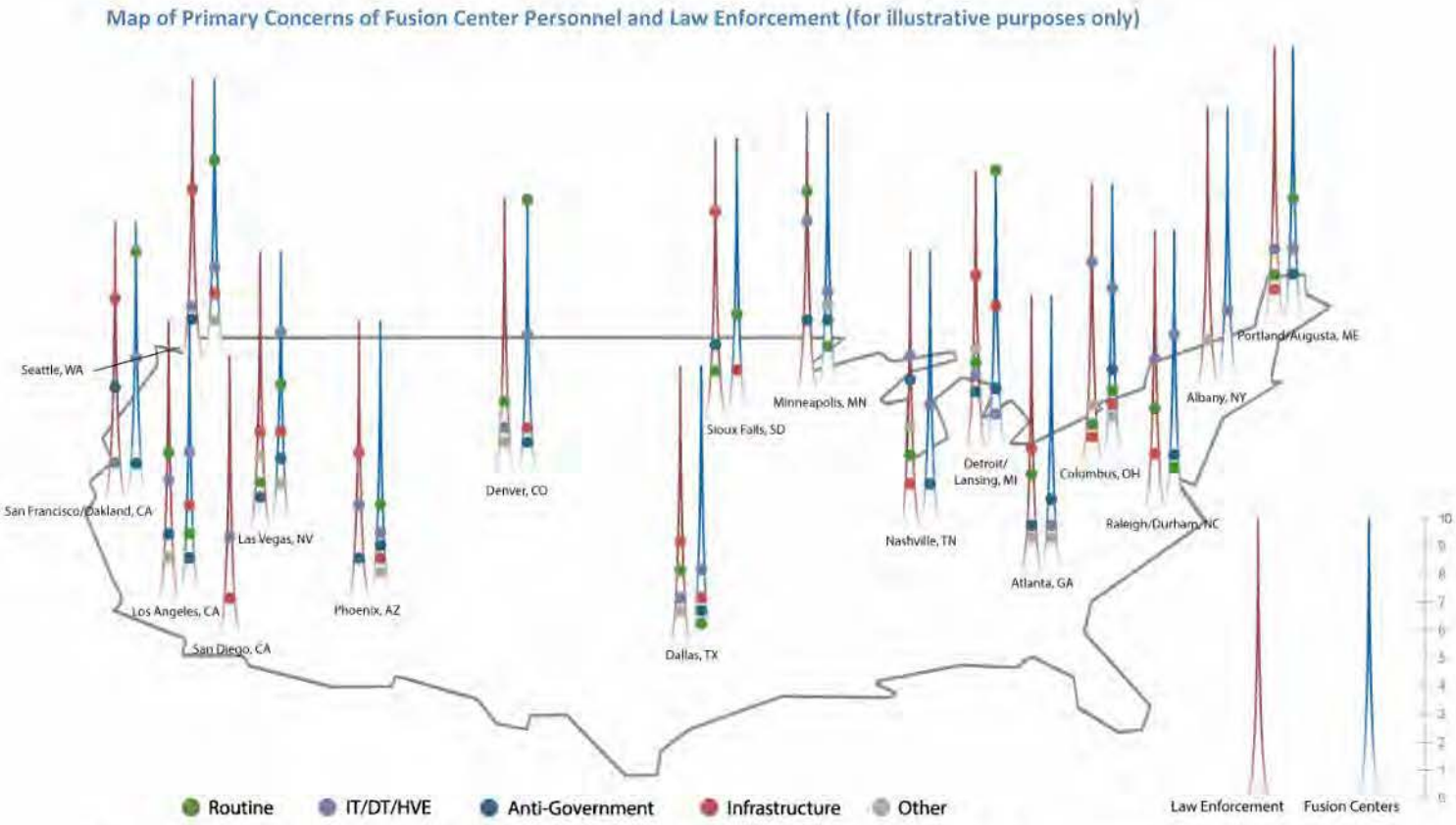
The qualitative software was used to organize the data, including filtering responses by theme and by functional area. Working by theme within a functional area, the team provided a description for each quotation or set of quotations and subsequently grouped similar quotations. Within these groupings, quotations were further described and disaggregated as necessary. Additional analysis then took place to determine the number of participants who noted similar issues and the number of sites at which similar issues were discussed.

The team conducted the analysis and drafted the findings for law enforcement and fusion centers separately before comparing and contrasting these findings. While common themes emerged from the data, there were variations both within and across locations. As a result, broad generalizations were often not possible, and the results reflect these limitations. In addition, while methods such as those used in this study permit a deeper level of understanding of participants' experiences, the findings from focus groups and in-depth interviews are typically limited to the individuals who participated. The findings presented in this report should not be construed as applying to all fusion center personnel or all local law enforcement.

Local Concerns and Understanding about Violent Extremism

Both law enforcement officers and fusion center personnel identified "routine crime," drugs and drug trafficking organizations, gangs, and threats to critical infrastructure as concerns in their areas of responsibility. International terrorism (IT), domestic terrorism (DT), and violent extremism were also concerns for both law enforcement and fusion center personnel. However, whereas fusion center personnel expressed that they were most concerned about DT, violent extremism, and IT, law enforcement communities indicated that they were most concerned about those criminal activities that are most frequent in their jurisdictions and for which they may be called to account by elected officials and the public. These included gang crimes, drug trafficking, threats to the public and officers' safety, threats to critical infrastructure, financial crimes, property crimes, homegrown violent extremism (HVE), terrorism, human trafficking, and sex crimes.

The map below illustrates the different concerns within and across locations, and between fusion center personnel and law enforcement. The different types of concerns are grouped by "routine crime," IT/DT/HVE, anti-government concerns (for example, Sovereign Citizens, militias, anarchists, and "anti-government" groups in general), infrastructure, and other concerns such as issues related to the economy and lone offenders.



This map compares the primary concerns cited by law enforcement (red spindles) and fusion center personnel (blue spindles). Most notable are the relative similarities and differences between the two groups regarding the threats of greatest concern. The scale reflects how often participants noted different types of threats.

Participants were asked to share their thoughts about the extent to which countering violent extremism is similar to or different from countering other types of crime. The majority of fusion center personnel who responded believed that CVE is different from countering other types of crime because the motivations are different (and to counter violent extremism appropriately, one has to understand those motivations); much of the pre-operational activity is not criminal; and responses to routine crimes are generally predicated on perpetrators making decisions based on material gain, which may not be the case with those driven by ideology.

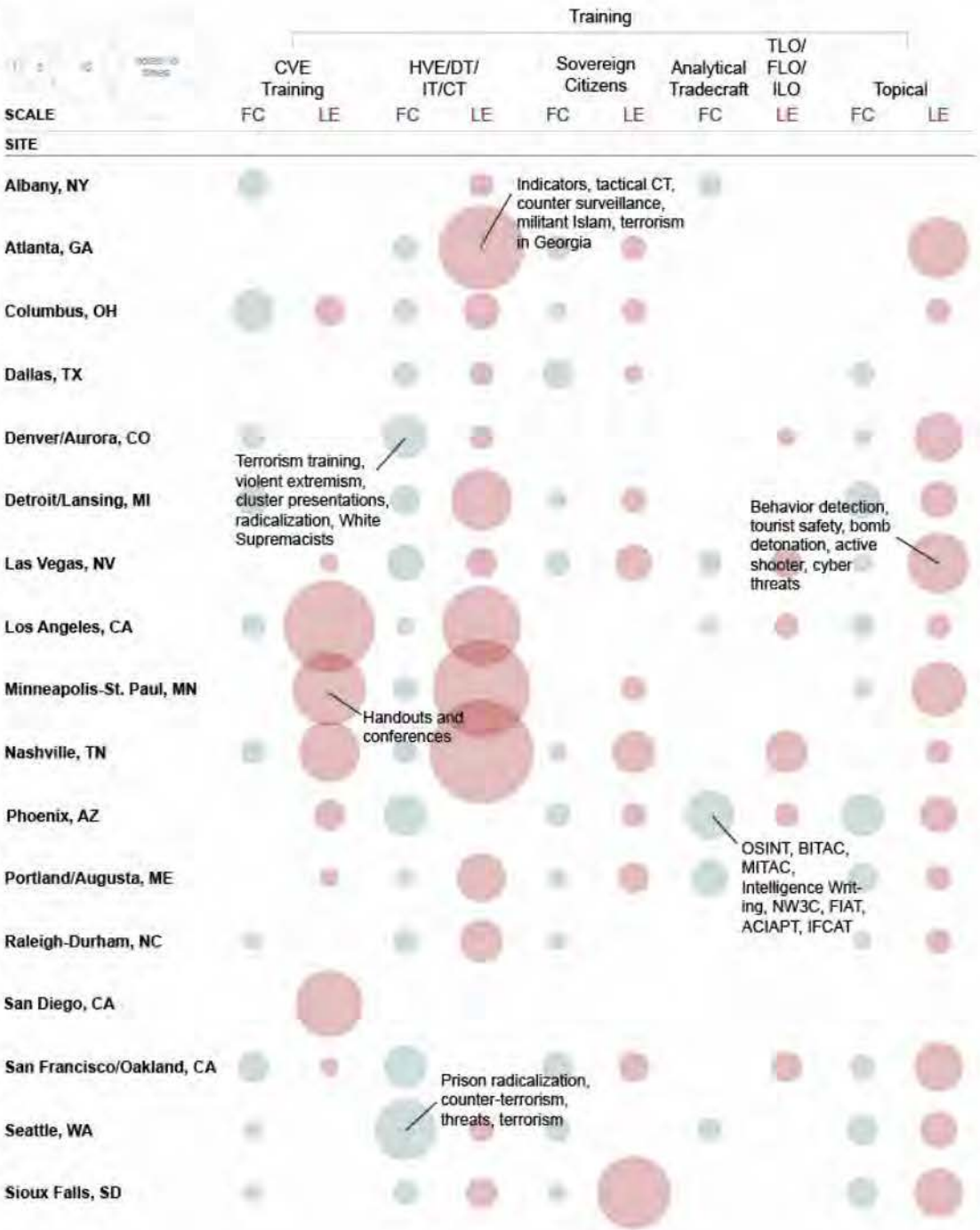
On the whole, law enforcement responded similarly. The vast majority of respondents differentiated between routine criminal behavior and violent extremism, with the latter being driven by a particular ideology, religious belief, or political goal. A few respondents focused primarily on political agendas, while others focused on religious motivations. Among both groups, a sizeable number of respondents thought CVE was similar to countering other types of crime because the police work, both in proactive and response stages, is similar to that for other crimes.

Training on Countering Violent Extremism

At over half of the sites visited (10 sites for fusion centers, 9 sites for law enforcement), participants noted receiving training on CVE. With a few exceptions, fusion center and law enforcement participants expressed confusion about what constituted CVE training or offered examples of what they thought it was. One of the

reasons for the confusion, as articulated by one law enforcement executive, is the lack of an agreed-upon CVE curriculum or lesson plan. Others mentioned that CVE training has not caught up to the need or is not seen as a priority in departments or locations. The graphic below presents the types of CVE-related training participants mentioned receiving. Empty spaces or fewer notations should not necessarily be construed as locations as a whole not receiving CVE-related training.

CVE-related Training Mentioned by Participants (for illustrative purposes only)



This figure juxtaposes the training opportunities reported by fusion center and law enforcement personnel. Fusion center training is represented in blue while law enforcement training is represented in red. The columns represent the training that respondents discussed, and the size of the bubble represents the number of references to each. CVE training relates specifically to training on how to counter violent extremism. The next category, HVE/DT/IT/CT, encompasses training on radicalization, terrorism, and counterterrorism and other training related to violent extremism but not specifically countering it. Because it was such a prominent issue, Sovereign Citizen training has its own column. The remaining columns include analytical tradecraft for fusion center analysts; terrorism liaison officer (TLO), fusion liaison officer (FLO), and intelligence liaison officer (ILO) training for law enforcement; and other trainings that were viewed as relevant to violent extremism but did not fit into the other categories.

Much of the CVE training noted by participants was concentrated in five locations, four of which had developed or served as the host for CVE pilot training. Feedback from participants who attended these pilot trainings is provided below.

CVE Conference, Columbus. Participants felt that the conference was productive, good, and educational, though directed to the wrong audience. Because of this, one participant explained that only a portion of the conference was helpful to him.

Pilot CVE Training, San Diego and Southern California. The pilot trainings in San Diego and Southern California were positively received by almost all attendees who participated in the study. Officers cited appreciation for the community involvement, the group breakout sessions, and the opportunities to develop solutions with diverse input. However, a few others were concerned that the purpose of the pilot training was not clear to officers, and it did not adequately address the range of diverse issues they may face.

CVE Pilot Workshop, Minneapolis-St. Paul. The pilot training in Minneapolis-St. Paul received mostly critical reviews from participants. Criticisms focused on what were described as lengthy and irrelevant presentations by speakers and the misalignment between the content, providers, and audience. The opportunities for practical, hands-on exercises and the inclusion of scenarios received more positive feedback, as did the overall awareness of the need to have more officers conducting community outreach.

CVE Conference, San Diego. Participants provided generally positive reviews of the San Diego conference with a few exceptions. Those who viewed it positively noted that it addressed the need for law enforcement to interact with other agencies and be out among the community. Participants also noted that in addition to focusing on outreach, the conference focused on how to build outreach efforts. A few others cited frustrations in two areas: overuse of the same case study and what they perceived to be a lack of transparency or willingness to address issues that are not considered politically correct. For example, one participant felt conference leaders side-stepped a question about the challenges of integrating large immigrant populations.

Training Needs

Fusion center personnel and law enforcement officers often spoke of similar training needs. Both asked for training delivered by subject

matter experts and experienced trainers. Both cited a need for training on indicators of violent extremism and the radicalization process. Virtually all participants requested training that had local relevance. For fusion center analysts, ideal training on this topic would use in-depth case studies; law enforcement requested case studies as well. Additionally, law enforcement emphasized that CVE training should have practical applications and teach officers how to shift their thinking from the paradigm of traditional criminal behavior to that of violent extremism.

Participants also noted a need for training on interacting with different communities. For some fusion center participants, such training would include best practices and bring the community, community leaders, and other actors together; explain the relationship between fusion centers and social services agencies, including data sharing and its limitations; and assist with developing partnerships with local social service agencies using Memorandums of Understanding. A few fusion center participants sought training on how to develop relationships—built on trust—with communities affected by ties to IT, as well as training on the importance of developing such relationships. Fusion center staff also thought training is needed for the private sector, emergency management, and tribal law enforcement.

Law enforcement officers cited a need for training on how to conduct outreach to community members of all types, including those in more closed ethnic and religious communities. More senior officers noted a need to teach newer law enforcement officers conversation and interviewing skills.

At fusion centers and law enforcement agencies, participants cited a need for a CVE training program that would be planned, offer a menu of courses, be tailored, and be available to all—not just, in the case of law enforcement, community outreach officers or executives. Both requested that training be delivered through a variety of formats. For some fusion center personnel, such training should provide the skills to navigate the nuance and gray areas of CVE. For law enforcement, a variety of delivery methods would provide the flexibility needed for departments facing staffing and funding shortages and allow for more officers to be trained. Of particular importance to law enforcement was the fact that such training should be free or fundable by Federal Emergency Management Agency grants.

Both groups requested training on practical skills related to their roles. For fusion center personnel, this included managing a fusion center, writing analytical reports, writing for a law enforcement audience, conducting background research, and managing intelligence collection. Law enforcement cited a need for scenario-based incident response training and intelligence training. In some cases, participants at both fusion centers and in local law enforcement asked for training on source development.

Training Challenges

Approximately half of fusion center personnel discussed having issues incorporating the training they had received into their jobs. They most often cited the lack of relevance or applicability of what they learned to their duties and the inability to use training immediately. Others noted institutional issues with the acceptance of new training initiatives, whether from their administration or their peers. Other issues mentioned included a lack of post-training support and the complexity of guidelines within the Code of Federal Regulations that pertain to privacy and civil liberties protections for information that is collected, stored, and shared on federally funded criminal intelligence systems.

Law enforcement officers also noted significant challenges in incorporating new skills into their jobs, often due to their workloads and the lack of consistent opportunities to apply new skills. They discussed challenges related to receiving CVE training, including:

- Organizational leadership, or the community, focusing on other priorities;
- The need to take other training more directly relevant to their career goals;
- The lack of availability of training; and
- The lack of time and budget.

Sources of Information on Countering Violent Extremism

Fusion center personnel and law enforcement cited similar sources as their best sources of information about violent extremism and countering it. These included community sources; federal government agencies such as DHS, the Federal Bureau of Investigation (FBI), and the National Counterterrorism Center (NCTC); websites and databases; personal and professional networks; and fusion centers. The following table presents specific products and sources of information described by participants as best sources of information.

Best Sources of Information

Source	Fusion Center	Law Enforcement
Local Community	Law enforcement, business owners, community members, Terrorism Liaison Officers (TLOs), and confidential sources or informants	Informants, confidential sources, social and religious organizations, public officials, kids, reformed (and burned) group members, and those with whom officers have built trusted relationships
DHS	Reports and products, DHS Intelligence Officers (IOs), Joint Intelligence Bulletins (JIBs)	DHS IO, Office of Intelligence and Analysis, bulletins, daily reports, press releases, classified information products
FBI/Joint Terrorism Task Force (JTTF)	Regular updates, products, JIBs	Bulletins, classified information, Special Agents, meetings, JTTF, joint FBI and JTTF bulletins
Other Federal Sources	NCTC, Immigration and Customs Enforcement, Department of Justice, DHS National Operations Center, Intelligence Information Reports, Interagency Threat Assessment and Coordination Group (ITACG), State and Local Anti-Terrorism Training (SLATT)	NCTC, ITACG, U.S. Coast Guard, National Warning System, Nationwide SAR Initiative, National Institute of Justice
Online Sites, Databases	Informational websites, the media and social media, databases, Homeland Security Information Network (HSIN), DHS.gov, LEO.gov, FBI.net, Homeland Security State and Local Intelligence Community, Regional Information Sharing System (RISS), CargoNET, CIAWire, SLATT, COPLINK	HSIN, COPLINK, RISS (including Communities of Interest and Regional Organized Crime Information Center), LEO.gov, Police One, state and national databases, online research, InfraGard, Officer.com, SLATT, media and social media, Google

Source	Fusion Center	Law Enforcement
Personal and Professional Networks	Personal connections	Law enforcement networks, meetings, Major Cities Chief Intel Commanders group, briefings and case coordination meetings, other law enforcement
Fusion Centers	Other fusion centers, fusion center products	Weekly and other fusion center bulletins, case-specific information from fusion centers, coordinated information from other states

Problems Getting Good Information

While some participants reported no problems getting information, many fusion center personnel and local law enforcement identified a number of common challenges related to getting good information, including issues around information sharing, information overload, and the quality of information received. Participants generally used the broad descriptor of "information sharing" to signify issues related to getting access to locally relevant, classified information—requested or not—and receiving feedback on information that had been vertically shared. Fusion center personnel cited frequent issues receiving information from the FBI; occasional issues receiving information from DHS, its component agencies, and local law enforcement agencies; and less frequent issues receiving information from other fusion centers. They also noted issues with access to classified systems. Law enforcement officers overwhelmingly reported problems receiving feedback from federal agencies and, on occasion, fusion centers, after sharing tips or case information with them.

Although some participants felt they were not receiving the "right" information, other participants described being inundated with information, and still others said that both are issues. Fusion center personnel and law enforcement officers often used the phrase "information overload" to describe the amount of information they receive, through emails, bulletins, or other means. Perhaps the major consequence of information overload is missing relevant information, due to the inability of fusion center personnel and local law enforcement to process it all. Participants explained that the constant dissemination of bulletins, reports, and other official intelligence to fusion centers and local law enforcement can lead recipients to develop their own management strategies for dealing with information, including deleting emails, leaving distribution lists, not checking relevant secure sites, and relying on individuals to share important information. As a result of these and other issues, participants noted that frontline officers sometimes do not receive information at all.

Fusion center personnel and law enforcement officers both expressed concerns with the quality, relevance, and timeliness of information that is disseminated. Participants described information as repetitive, too general and not targeted, and lacking in quality. Those with advanced subject matter knowledge did not see a high level of complexity in information products, and others noted a lack of complete reporting, comparing information they receive to that which is available on the news. Law enforcement officers noted issues with the format of reports and bulletins, often describing them as too long, difficult to read, or written for intelligence audiences. The timeliness of information was closely tied with access to classified information. Participants, law enforcement in particular, were frustrated that they seem to receive information at the same time as the public. According to some fusion center personnel, when they receive information late or need clearance to disseminate information to their local partners, they can find themselves justifying their existence as a result.

Problems Getting Good Information

Fusion Centers	Law Enforcement
• Inadequate information sharing at all levels • Difficulty accessing secure and classified systems • Information overload • Lack of quality, timeliness, and relevance of information • Privacy concerns • Lack of clarity on the nature of the threat • Issues related to regulations • Lack of resources • Need to rely on personal contacts	• Inadequate information sharing • Lack of access to classified information • One-sided sharing • Information overload • Lack of quality information • Issues with delivery and format of information • Need to use multiple Web-based resources and databases (no one-stop shop) • Lack of internal dissemination • Issues related to laws governing information sharing • Need to rely on personal contacts

Participants also cited unique concerns with getting good information. For fusion centers, these include the need to protect privacy and the lack of clear policy and definition guidelines. Law enforcement officers cited specific issues with the proliferation of secure websites and databases and lack of dissemination within departments. At some locations, law enforcement working at fusion centers and in the community noted legal limitations on information sharing particular to their locations, including requirements that information be made public if it is shared with federal or other agencies, and the need for a court order or a subpoena to share information across state lines.

Conclusion

Fusion center personnel and local law enforcement made final recommendations on how to improve efforts to counter violent extremism. A summary of these recommendations follows:

Training

Fusion center participants recommended that lead agencies involved in CVE provide access to good, quality training that defines CVE, offers an interactive model, and is locally relevant. They recommended that a comprehensive directory of available CVE training be provided with some indication of how well that training has been received by past participants and the level of difficulty of the training (beginner, intermediate, or advanced).

They also recommended that a train-the-trainer type of program be developed to further decentralize training services. This would improve the subject matter expertise of the centers' staff and create an expanded role for fusion centers beyond their training for TLOs and the other targeted training they provide.

Law enforcement participants recommended that training on CVE be provided and be offered to all law enforcement officers. They recommended that this training focus on identifying behaviors, be specific to particular areas of the country, and be run by experts and former law enforcement officers.

Information

Fusion center participants recommended that agencies leading CVE efforts improve information sharing and communication at all levels. They recommended that national and local databases on violent extremists be compiled and provided.

Law enforcement participants recommended that more information, particularly more quality information, on CVE be available and that federal partners facilitate better and more timely information and intelligence sharing. They recommended that federal partners provide greater clarity about the type of information they are looking for from local law enforcement and how that information should be reported. They also asked that feedback be provided after information is vertically shared. In addition, participants recommended developing a single system or platform that integrates federal, state, and local databases.

Participants also recommended that the federal government engage in more truthful, transparent, and less politically correct communications about CVE. For example, some law enforcement and fusion center personnel cited issues with what they perceived as incomplete reporting due to concerns about offending cultural or religious groups, the perceived political motivations behind the adoption of terminology such as "violent extremism," and the perceived reluctance by the federal government to portray incidents such as the attack at Fort Hood as terrorism.

CVE Policy and Implementation

Fusion center participants requested greater clarity about CVE policy and its implementation. A few also sought clarification on the roles and responsibilities of fusion centers in CVE. They recommended that reforms be made in how federal, state, and local agencies coordinate and interact, as well as for security clearance protocols.

Law enforcement participants also asked that clear leadership for CVE be established and that CVE policy include a prominent role for local law enforcement. Participants recommended that greater weight be given to the changing role of law enforcement in CVE, and to reflect this shift, there be recognition of the need for a cultural shift in how police departments are run.

Law enforcement participants recommended that better cooperation and collaboration occur among all partners involved in CVE efforts and that focus be kept on those partnerships. They recommended ending federal in-fighting and duplication of efforts and developing federal guidelines that would improve cooperation and information sharing, including in locations that have strict information sharing laws. Participants recommended that those leading CVE efforts provide greater support to local law enforcement institutions and help to bring state and local governments on board in efforts to counter violent extremism. They suggested finding ways to increase the cooperation and outreach between law enforcement and the communities they serve and to improve coordination between locations with similar refugee and immigrant communities.

Resources, Funding, and Staffing

Fusion center participants recommended that more resources be provided to fusion centers so that they can more effectively counter violent extremism. Resources, such as funding, are needed to sustain the current

staffing levels in order to maintain operations, increase the number of personnel to expand operations, and provide greater educational and training opportunities for staff.

Law enforcement participants recommended providing resources, consistent funding, and staffing to facilitate efforts to counter violent extremism. Participants also recommended developing a grant that would allow departments to develop CVE-related positions and providing a clearer grant application process for funding CVE-related training.

Other Recommendations

Based on analysis of the data collected for this study and experiences in the field, JBS developed the following recommendations:

- **CVE Training**: JBS recommends that future CVE training be tailored to functional areas and levels of experience and be built on and use current law enforcement protocols and language. This approach to training would enable officers to build on experiences and frameworks they already have, allowing for training and CVE initiatives to be better incorporated into their jobs. Due to the importance of this initiative, such training should be mandatory and offered by experienced professionals.
- **CVE Training Program:** JBS recommends that a CVE training program be developed that includes a certificate option. This training program should offer a menu of courses at different levels (beginning, intermediate, and advanced). Training on skills related to CVE should be offered as well.
- **CVE Information:** JBS recommends that CVE communications be presented in ways that are appropriate for the target audience and that efforts continue to provide documents with higher tear-lines to law enforcement and others. JBS also recommends that CVE communications be streamlined and that a mechanism be developed to allow law enforcement and fusion center personnel to search multiple databases and secure websites simultaneously.

Introduction

Introduction and Background

In August 2011, the White House released the national strategy for *Empowering Local Partners to Prevent Violent Extremism in the United States*.[3] This guiding document, and the subsequent December 2011 *Strategic Implementation Plan*, focuses on three core areas of activity: (1) enhancing engagement with and support to local communities that may be targeted by violent extremists; (2) building government and law enforcement expertise for preventing violent extremism; and (3) countering violent extremist propaganda while promoting U.S. ideals. It also emphasizes the importance of community-based problem solving, local partnerships, and community-oriented policing in building resilience to violent extremism in the United States.

This study aimed to support federal government efforts focused on the second objective outlined in the strategy by examining the views of fusion center personnel and local law enforcement on the 1) training and 2) information they receive and need related to countering violent extremism (CVE). Law enforcement agencies at the state and local levels already have a very broad set of responsibilities, including responding to emergencies; countering, responding to, and solving crimes; and maintaining order. Adding CVE to their portfolio requires them to develop an ability to act on a set of concerns that has not traditionally been central to their roles. Good communication, information sharing, training, and analysis are all necessary to build the foundation for enhancing the roles that state, local, tribal, and territorial (SLTT) law enforcement can assume in CVE.

An important resource in this arena are the 78 fusion centers located in each state and in major metropolitan areas. The mission of these centers includes receiving, gathering, analyzing, and sharing information related to threats—both criminal and terrorism-related. The fusion centers, which grew out of the need for greater coordination between the federal government and SLTT partners after the 9/11 terrorist attacks, are owned and operated by state and local law enforcement entities and receive support from federal partners in the form of deployed staff, training, grant funding, and other assistance. The centers are designed to bridge communication and coordination gaps among state and local law enforcement agencies and between these agencies and federal agencies.

In 2011, the Department of Homeland Security (DHS) Science and Technology Directorate contracted JBS International to gather data on the CVE-related training and information needs identified by personnel at selected fusion centers and state and local law enforcement agencies. JBS conducted interviews and focus groups in 17 locations around the country, generally with staff at a fusion center and with law enforcement in surrounding communities. Participants were asked about their experiences with and needs for training and information with respect to CVE and their thoughts on how to improve the information and training that they currently receive. Additional areas of inquiry focused on what participants viewed as the primary threats in their communities and their general impressions of current efforts to counter violent extremism.

While the JBS team sought feedback on current federal CVE efforts, the study was meant to be neither an evaluation examining outcomes nor an assessment examining participants' performance. Rather, the researchers aimed to explore the experiences and needs of U.S. law enforcement and fusion center personnel

[3] The national strategy for *Empowering Local Partners to Prevent Violent Extremism in the United States* can be found at http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf and the *Strategic Implementation Plan* can be found at http://www.whitehouse.gov/sites/default/files/sip-final.pdf.

and to gather these perspectives in a manner that encouraged open discussion. This report provides the reader with the results of those discussions. In presenting the results, the researchers have sought to represent participants' perspectives, even when their conceptualizations of CVE differ from that of the federal government.[4]

After describing the methodology used in the study, the first section of the report focuses on the perspectives of fusion center staff, and the second turns to the perspectives of local law enforcement. In each section, the perceptions of threats with respect to CVE are examined, touching also on the degree to which both fusion center staff and local law enforcement feel they are prepared to respond to these threats. Training—both training received and needed—is a principal focus of both sections, and the report provides information on the training that participants have received and that they view as relevant to CVE (whether explicitly defined as such); their thoughts on the appropriateness and utility of this training; what training they feel they need, but are not receiving; and how training could be improved or delivered in ways that are most effective. The report then turns in each case to sources of information and examines which sources of information participants view as most useful in understanding CVE and in assisting them in their jobs; what problems they face in getting good information; and what they feel they need in order to access better information. The report concludes with a summary of participants' overall recommendations followed by those of the research team. Finally, an annex to the report details the perspectives of fusion center personnel and law enforcement on broader challenges in implementing the national CVE strategy (Annex 1). Though outside of the study's immediate scope, concerns and confusion around the national CVE strategy and its implementation were often the main issues participants wished to discuss.

[4] For example, several participants discussed the need for more training on source development as a CVE-related training need. The federal government does not view this type of training as related to CVE, but because it was mentioned by participants, it is included in the report.

Research Approach

The research team used qualitative methods of data collection. These methods included focus group discussions and in-depth interviews. The use of focus groups allows study participants to discuss their experiences in depth and encourages interaction among participants. Interviews permit an even deeper understanding of the interviewee's perspectives and complemented the focus groups. Interviews were primarily conducted with senior law enforcement personnel, fusion center leadership, and personnel from other federal agencies (as appropriate) because the perspectives of these stakeholders are typically quite broad and may differ considerably from other staff. The decision to interview leadership was also based on standard focus group practices, which seek to bring together groups that are homogeneous in nature. This similarity may be based on age, gender, race or ethnic background, profession, or even shared experiences. The inclusion of participants who are in hierarchical relationships—supervisor and subordinate—in focus groups is not optimal due to concerns that the presence of supervisors may lead participants to censor their comments to align with what they believe are their supervisors' opinions.

Moderators used a combination of nonreflective listening, or reacting to participants' comments with limited verbal responses, and reflective listening, or paraphrasing and summarizing responses to ensure ideas were properly understood. Moderators also guaranteed that participants' responses would be reported anonymously. In keeping with this mode of data collection, moderators did not evaluate or challenge the perceived correctness of the responses. The methodology was structured in this way to facilitate the collection of honest and unfiltered perspectives.

Instrument Design

JBS developed the focus group and interview guide with input from members of the DHS CVE Working Group. The guide included 12 questions and three general areas of inquiry: local concerns and understanding of violent extremism; experiences, needs, and challenges related to training; and information sources and challenges around getting good CVE-related information (see Annex 2). The guide also included a final question that asked participants what information they would like to convey to those leading government CVE efforts (or what they would do if they led government CVE efforts). Once the guide was developed, two pilot focus groups were held, one with fusion center personnel and one with local law enforcement, to test the questions and elicit feedback. The data from these focus groups are not used in the final report. Based on the feedback from these groups, changes were made in how the questions were presented and how the study was implemented.

Site Selection

JBS worked closely with members of the DHS CVE Working Group in choosing sites. DHS provided the study team information on the locations where DHS and other agencies had conducted previous CVE-related training activities as well as recommendations on fusion centers to potentially be included in the study. JBS drafted a site selection plan that took into account this information as well as geographic diversity and population size. The goal was to hold two focus groups,[5] one with fusion center personnel and one with local law enforcement, in each location. Ideally, at least one group, and in many cases both, had received CVE-related training of some

[5] San Diego was designed to have a law enforcement focus group only. In two locations, Rochester, NY, and Dallas, TX, it was not possible to organize law enforcement focus groups.

kind. A list of the locations included in the study is shown in Table 1. Most often the fusion center and law enforcement interviews and focus groups were held in the same city or in close proximity to each other, but some travel was required between the locations of the fusion centers and the designated law enforcement communities in Maine, Michigan, and New York.

Site Visits and Data Collection

Site visits began in July 2012 and were completed in February 2013. DHS provided JBS with the names and contact information of the DHS Intelligence Officer (IO) at each of the selected fusion centers, and outreach was primarily carried out through these officers. The IOs assisted in coordinating the site visits, setting up interviews and recruiting participants for focus groups at the fusion centers, providing contact information for local law enforcement, and in certain cases, recruiting participants for the law enforcement focus groups.

The time between the initial contact and the site visit took between three weeks to four months. Two-member teams consisting of a team leader and researcher conducted site visits. Site visits were mostly conducted over a two- to three-day period with one day designated for the fusion center interviews and focus group and another day designated for the law enforcement interviews and focus group. In six of the locations, the fusion center served as the venue for all focus groups and most interviews. At the remaining locations, the study team typically traveled to police headquarters for the law enforcement focus group and interviews. In general, interviews lasted 35 minutes and focus groups one hour and 15 minutes.

Participants

The JBS team sought to recruit fusion center personnel and local law enforcement who had participated in DHS CVE training or other training on violent extremism or countering it. JBS developed a general recruitment plan that included participants by functional area, rather than job title, to account for the diversity among fusion centers, the different levels of staffing and complexity of operations, and different areas of focus. This recruitment plan was designed to provide a measure of uniformity across very different locations and was shared with IOs and others. Outreach materials were developed and provided as well. These materials included an introduction to the study and descriptions of possible participants by functional area and the manner in which they would participate (i.e., in interviews or focus groups). Receiving CVE training served as the primary criterion for participation in the study; however, where no or little training had been provided, JBS requested participants who had taken other CVE-related training or who served in CVE-related capacities.

The study team sought six to eight participants for each focus group, three to five interviews with fusion center personnel, and three to five interviews with law enforcement, for a range of 18 to 26 participants per location. For smaller fusion centers and in less urban locations, a more accurate range for the number of participants was 10 to 15. Overall, the team conducted 36 focus groups, which included 226 participants and 115 interviews. Table 1 shows the breakdown of participants by location.

Table 1. Locations and Participants

Location		Law Enforcement				Fusion Center			
	TOTAL Participants	*Total Law Enforcement*	Inter-views	Focus Groups		*Total Fusion Center*	Inter-views	Focus Groups	
				Part*	FG**			Part	FG
Albany, NY	**6**	1	1	0	0	5	0	5	1
Atlanta, GA	**16**	10	3	7	1	6	0	6	1
Augusta / Portland, ME	**11**	6	1	5	2	5	0	5	1
Aurora / Denver, CO	**22**	8	0	8	1	14	8	6	1
Columbus, OH	**25**	12	6	6	1	13	6	7	1
Dallas, TX	**24**	14	14	0	0	10	6	4	1
East Lansing / Detroit, MI	**21**	9	2	7	1	12	4	8	2
Las Vegas, NV	**22**	8	3	5	1	14	6	8	1
Los Angeles, CA	**24**	10	5	5	1	14	4	10	1
Minneapolis / St. Paul, MN	**17**	9	4	5	1	8	3	7	1
Nashville, TN	**39**	29	0	29	4	10	3	7	1
Phoenix, AZ	**36**	14	2	12	1	22	9	13	1
Raleigh-Durham, NC	**19**	8	2	6	1	11	3	8	1
San Diego, CA	**9**	9	N/A	9	1	N/A	N/A	N/A	N/A
San Francisco/ Oakland, CA	**19**	9	4	5	1	10	4	6	1
Seattle, WA	**16**	7	1	6	1	9	5	4	1
Sioux Falls, SD	**15**	11	6	5	1	4	2	2	1
Total	**341**	**174**	**54**	**120**	**19**	**167**	**61**	**106**	**17**

* Number of participants in focus groups
** Number of focus groups

As was expected given the range of sites, recruitment by functional area produced a diverse set of participants. For example, participants classified as "analysts" often work on topics related to terrorism; however, most of the fusion centers the teams visited focus on either "All Crimes" or "All Hazards" or both, and a significant number of analysts work in a criminal intelligence capacity or even as geospatial or maritime analysts. DHS IOs and Federal Bureau of Investigation (FBI) intelligence analysts are also classified as analysts. Fusion center directors, assistant directors, and section managers are included under "senior staff." Those officers who are detailed to the fusion center are classified as "liaisons," while those working in different capacities such as health, fire, or critical infrastructure and key resources (CIKR) are classified as "other." For law enforcement, participants ranked at captain and higher are included under "executives;" "investigative officers" include detectives or those who work in criminal intelligence; and "frontline officers" primarily include patrol and

community outreach officers.[6] Those who work as firefighters, health workers, and security are classified as "other." The team relied on participants to describe their functional areas, and Table 2 shows the number of participants by area.[7]

Table 2. Participants by Functional Area

Fusion Center		Law Enforcement	
Functional Areas	**Total**	**Functional Areas**	**Total**
Senior Staff	36	Executives	29
Liaisons	41	Investigative Officers	47
Analysts	75	Frontline Officers	88
Other (Fire, Health, Corrections, CIKR)	15	Other (Fire, Health, Security)	10

Data Analysis

As with other qualitative analyses, the study team used an inductive or "bottom-up" approach in categorizing and analyzing the data gathered in the field. This allowed the team to remain as close as possible to the participants' language and the ways in which they conceptualized their experiences. Data included in the report reflect the combination of focus groups and individual interviews. Not every participant answered every question. In general, the findings are presented as a narrative, bringing the experiences of the participants together under broad and more refined themes.

The data organization and analysis phase included five main steps:

- Developing codes, establishing data controls and working files (including removing personally identifying information from transcripts and classifying functional areas), and coding using ATLAS.ti qualitative data analysis software.
- Running qualitative cross-tabular reports and creating easily searchable data files.
- Organizing the data further based on functional areas and themes.
- Writing up the results for law enforcement and fusion centers separately.
- Comparing and contrasting the findings.

The study team developed a list of codes, and the team were trained and participated in two practice coding sessions. Transcripts and notes from the interviews and focus groups were grouped by site and were generally coded by site team members. An additional level of review was provided by site leaders with a final review conducted by the study team leader. Personally identifiable information was removed from transcripts prior to their being uploaded to the qualitative software.

[6] Some departments had dedicated community outreach teams while others considered community outreach a collateral duty of patrol officers.

[7] The decision to use these general categories was based on an empirical analysis of participants' roles and the naturally occurring breaks in the data.

The qualitative software was used to organize the data, including filtering responses by functional area and by theme. Working by theme within a functional area, the lead analyst provided a description for each quotation or set of quotations and subsequently grouped similar quotations. Within these groupings, quotations were further described and disaggregated as necessary.

Additional analysis then took place to determine the number of participants who noted similar issues and the number of sites at which these issues were discussed. To show the frequency of similar perspectives, the number of sites at which a particular perspective was expressed is often included in the report.[8] Included as well is the range of ideas that were presented, even if reported by only a few participants, as well as multiple examples participants used to express these ideas. In general, results are reported exclusively using the participants' language and quotations, limiting, as much as possible, the interpretation of the data.

It should be kept in mind that findings from focus group research cannot be generalized to the wider population. Though the findings are often grouped by functional areas across sites, the findings related to, for example, "analysts," should not be interpreted as applying to all analysts who work in fusion centers, or to all fusion center analysts who participated in the study.

Methodological Challenges and Limitations

As with all field research, challenges are inevitable. Fieldwork for this study presented three main challenges. First, planning for the study began in late 2011 when the phrase "countering violent extremism" was only beginning to enter into the national security lexicon. Over the course of the study, DHS and other federal government CVE efforts evolved and became more crystallized and coordinated.

Second, the focus group and interview protocols, developed in late 2011, were designed to elicit feedback on training on, and information about, violent extremism and CVE. With little training available that was specifically labeled "CVE training," and varying levels of knowledge of the phrase by participants, the study team allowed the participants to describe trainings they viewed as CVE-focused. As a consequence, participants discussed trainings that covered everything from briefings on specific violent extremist groups to protocols for collecting and storing information at fusion centers. As a result, this report presents feedback and perspectives on training in three separate sections:

- The section on "CVE-specific Training" provides a summary of participants' perspectives on the availability and quality of training directly focused on CVE;
- The section on "CVE-related Training" provides a similar summary of perspectives, but on training that is related to but not directly focused on CVE; and
- The section on "Training Offered by Federal Government Agencies" provides feedback on CVE-specific and CVE-related training produced by the federal government.

A third challenge occurred when several participants seemed to associate CVE with activities related to source recruitment and long-term investigations, which are often classified, and expressed discomfort discussing issues around training and information in an unclassified study. In order to address some of these concerns, the team

[8] Results from focus group research are generally not reported according to the number of participants because in many cases participants may not respond to every question. Such a method of reporting is usually reserved for survey results.

altered the study protocol so that focus groups only took place at official locations and were not recorded unless prior approval had been received. JBS also clarified the aims of the study and its unclassified nature.

Recruitment and Data Collection Challenges

The sensitivity of this study topic, the wide range of locations, and the diversity of the participants led to significant challenges related to recruitment. Nevertheless, all but two of the fusion centers that were invited ultimately agreed to participate. The ability to recruit law enforcement participants appeared to rest heavily on the type of relationship the federal government, the fusion center, or the DHS IO had with local departments. For example, one law enforcement department's negative experiences with the federal government almost led it to decline participating in the study, and it only agreed after a great deal of outreach explaining that the study's goals were to get feedback on officers' needs. In other cases, the DHS IOs' close relationships with local law enforcement directly facilitated recruiting law enforcement participants for the study.[9]

Logistically, coordinating interviews and focus groups in 17 locations was challenging. Many locations had staff that had previous commitments to training, vacation time, conferences, and other tasks that prevented them from participating in the study. Further, one of the main challenges for law enforcement groups was bringing officers in during their shifts, which entailed receiving approval from superiors. The research team sought to overcome this challenge by introducing the study directly to law enforcement leadership.

Finally, although focus groups were designed to have minimal differences between the ranks of participants, and confidentiality was stressed, inevitably some participants were more hesitant to share bad experiences or problems. In a few cases, participants spoke rarely in the focus group, and it was unclear whether they did not have anything to say, agreed with the others, or were reticent about sharing. However, other participants spoke openly about sensitive topics, including the political nature of their work, the inconsistency of local and federal policies, the problems of federal "territorialism," and challenges with "political correctness" as it relates to CVE.

Other challenges in data collection were the need for familiarity with locations, knowledge of the different types of products that are disseminated by the federal government, and the various information sharing systems currently in use. JBS conducted an extensive review of available literature to become familiar with these issues beforehand, but had no direct access to the products or information systems.

Data Analysis

The main challenge in analyzing the data was the quantity. As noted, the team conducted 36 focus groups, which included 226 participants, and 115 interviews. Transcripts and summaries were coded according to the main questions asked in the focus groups, the themes that emerged throughout these discussions, and the functional areas of participants. The variations across locations and across and within functional areas, as well as the different experiences of the participants required that special attention be paid to subtly articulated nuances. As a result, broad generalizations were often not possible. Where JBS could draw these generalizations, the team did.

[9] It should be noted that it may be the case that the resulting focus groups included law enforcement who had greater awareness of the fusion center and CVE than might have been the case had no such relationship existed.

Fusion Center Perspectives

Local Concerns and Understanding of Violent Extremism

In each of the interviews and focus groups with fusion center personnel, the moderator opened the discussion with a preliminary question about the threats that were of greatest concern to participants in their areas of responsibility. The purpose of this question was two-fold: first, it helped to clarify the overall orientation of the fusion centers, and second, it helped get the conversation flowing, particularly when focus group participants with varying roles within the fusion centers had different perceptions of the relative severity of the threats within their purview. The responses are therefore not representative of the full range of threats that may exist in each area, but rather represent only the perceptions of those participating in the study.

Threats and Perceptions of Threats

Overall, fusion center personnel around the country seemed to be most concerned about domestic terrorism (DT), violent extremism (as defined by DHS), and international terrorism (IT). The extent to which these are a focus of day-to-day activities depended on the characteristics of the fusion centers' states and areas of responsibility, but at least a few respondents in each location cited domestic terrorism or violent extremism as a primary concern. In addition to these, other primary concerns included gangs, drugs and drug trafficking organizations, human trafficking, "routine crime,"[10] cyber crime, the border, and critical infrastructure. Secondary concerns listed also included "paper terrorism"[11] and natural disasters (for some of the fusion centers that focus on all hazards). Which of these was the foremost concern for any participant was related to her or his role within the fusion center and the characteristics of the center's area of responsibility.

There were many similarities in the concerns about threats across all locations. For example, concern about international terrorism was not limited to concerns about one particular group; rather, it encompassed all well-known groups espousing violent rhetoric against the United States. In total, more respondents cited concerns about domestic terrorism and homegrown violent extremism (HVE) than any other threat. Only in two locations were these not a primary concern. Further, Sovereign Citizens were cited as a specific primary concern in all locations except four, and they were cited as a secondary concern in those four locations by at least one of the participants. Similarly, almost all fusion centers recognized gangs, drugs, and drug trafficking organizations as primary or secondary threats in their areas of responsibility, though which threats were most prominent depended on which groups were operating in their areas.

There were a few notable differences, however. In Arizona, California, Maine, Michigan, Minnesota, Nevada, New York, Texas, and Washington, the border was cited as a concern, particularly related to drug trafficking, human trafficking, and the entry of terrorists to the United States. Respondents in states that are part of major transportation corridors, including California, Michigan, Minnesota, Texas, and Washington, noted concerns about what they might encounter as people and goods move through their states. Critical infrastructure was

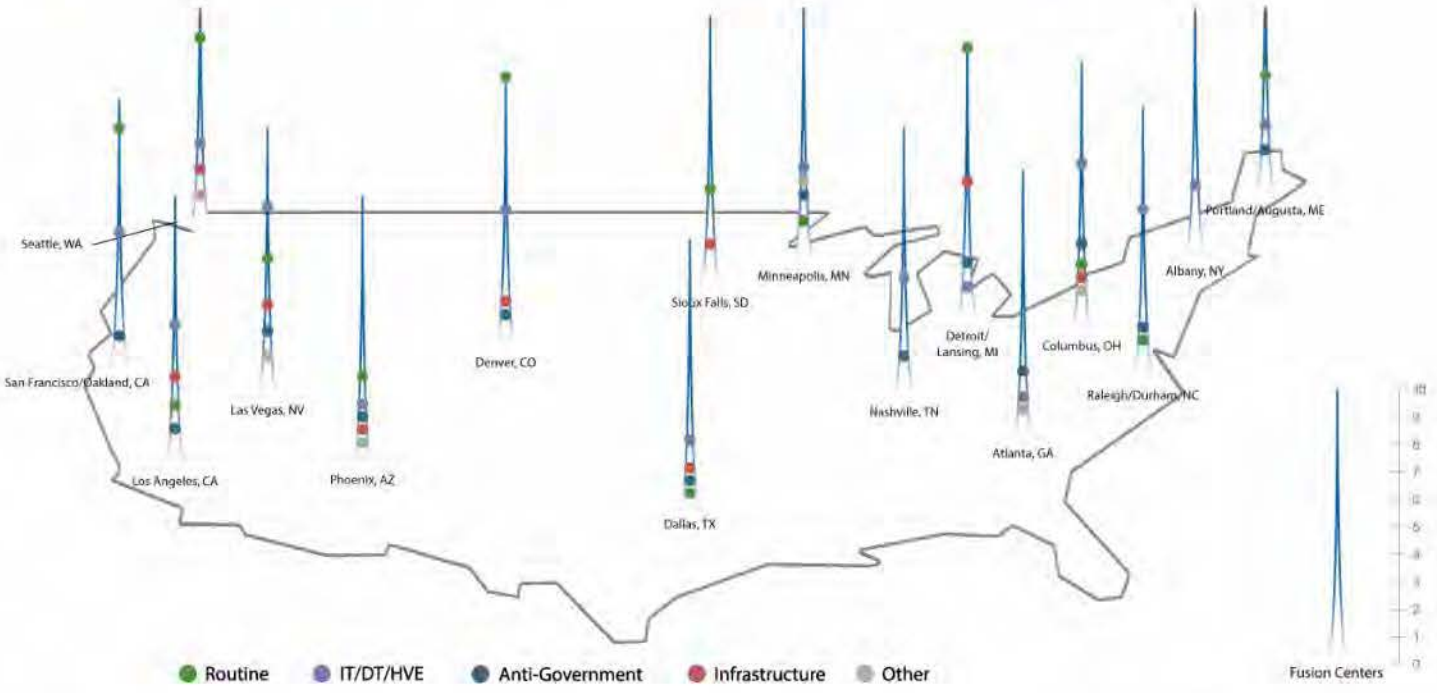
[10] "Routine crime" includes theft, robbery, assault, property crime, etc., that are most common in the communities included in the site visits.

[11] "Paper terrorism" refers to creating and filing baseless complaints and legal actions against law enforcement, including liens against personal property and in at least one instance, a lawsuit for treason. These actions impose a burden on law enforcement, municipal agencies, and local courts (and potentially state agencies and courts as well), as they are required to respond to or resolve these complaints and actions.

also a more frequently cited concern in Los Angeles, Michigan, and Washington than elsewhere, and responses about what constituted critical infrastructure were consistent—ports, bridges, ferry systems, and interstate transportation routes.

The map below illustrates the different concerns within and across locations. The different types of concerns are grouped by "routine crime," IT/DT/HVE, anti-government concerns (e.g., Sovereign Citizens, militias, anarchists, general descriptor of "anti-government"), infrastructure, and other concerns such as issues related to the economy and lone offenders.

Figure 1. Map of Fusion Center Personnel's Primary Concerns (for illustrative purposes only)



This map illustrates the primary concerns cited by fusion center personnel in interviews and focus groups. It is useful to note fusion centers' missions differ somewhat by location, but most have an "all crimes" or "all crimes/all hazards" focus. The scale reflects how often participants noted different types of threats.

Threat of Violent Extremism

As indicated by the discussion of threats, violent extremism is a concern for fusion center staff across the country. As one participant noted, "Violent extremism is perhaps [the] most prevalent topic in many people's minds at the fusion center and especially in the media where any kind of HVE is sensationalized." Only four respondents indicated that they did not think violent extremism was a concern in their communities. Fusion center personnel were concerned about all perpetrators of violent extremism and not necessarily only specific groups known to be operating within their areas of responsibility. In fact, many expressed concern that an attack could come from an individual or group not currently known to be a threat in their communities.

Fusion Center Perspectives

Fusion center participants all cited similar definitions of violent extremism that were generally consistent with the DHS definition. However, participants in most locations noted that the definition had changed over time and seemed somewhat fluid. One analyst found the real difficulty with HVE is the inconsistent terminology that is used. For him, there are two levels of meanings, with some agencies using the term violent extremism as a kind of euphemism for violent jihad, while others state that violent extremism is any kind of radicalized violence, regardless of motivation.

This lack of consistency has led to the definition being applied in centers somewhat differently. Some approach it from the broadest perspective. As one analyst explained, "We cast a wide net in the interest of public safety. There are some real concerns about offending certain communities, so we're equal opportunity offenders. We'll offend everybody." Others thought it was important to take a more constrained approach. As one liaison said, "It's important for us to be able to distinguish what may be of interest to a local law enforcement agency versus what the fusion center and DHS need to know ... To the degree that DHS may highlight the wrong domestic threats, it loses credibility."

Participants were also asked to share their thoughts about the extent to which CVE is similar to or different from countering other types of crime. The majority of fusion center personnel who responded believed that CVE is different from countering other types of crime. The main reasons cited for the difference were that the motivations are different (and to respond to or counter violent extremism appropriately, one has to understand those motivations); that much of the pre-operational activity of violent extremists is not criminal; and that responses to routine crimes are generally predicated on perpetrators making decisions based on material gain, which may not be the case with those driven by ideology. One analyst stated, "For CVE, this is the only time in which law enforcement attempts to react to violent behavior before it happens, before illegal activity takes place. The focus on indicators is quite different from the normal law enforcement reaction to crime, in which action only begins after the behavior has taken place."

However, a sizeable group of respondents thought that CVE was similar to countering other types of crime. For most of these respondents, the reason they see it as being the same is that the police work involved, both in proactive and reactive stages, is similar to that for other crimes: "The work is the same in terms of conducting the investigation, in getting at the facts and disseminating them" (fusion center analyst). As one senior leader noted, "It's [violent extremism is] similar, but on a greater level. Violence is violence."

State of Preparedness

Moving on from the threats about which they are concerned, participants were then asked if they felt prepared to counter the threat of violent extremism while in the pre-operational stages, and there was significant variance in their responses.

Although a handful of participants said that they felt prepared to counter violent extremism without reservations, a greater number of fusion center personnel said that they felt prepared to respond to an incident after the fact but were less positive about their ability to counter an incident in its preoperational stages. "In terms of responding to the situation, yes [we're prepared]. But we're not readily able to identify them," said a fusion center analyst. Several respondents in all roles indicated that they believe the JTTF would be the lead group; respondents also stated they believe the JTTF has the resources to intervene. One participant put it this

way, "The solution to countering it? It wouldn't occur [here]. We're just a cog in the wheel with the prevention of it" (fusion center senior staff).

Further, a significant number were quite blunt about their lack of confidence in their ability to counter violent extremism in its preoperational stages:

> *No. And I want everyone to hear that. When I heard about the countering violent extremism initiative, I was utterly puzzled that this country is embarking on this. With all respect, the premise is flawed. You're assuming that we can change beliefs when they are already … once you're built that way. Isn't the idea that we can catch them like saying we can catch lone wolves? … Every terrorism expert will say … there is nothing you can do by law to catch them.* (fusion center senior staff)

Among those who said they did not feel prepared, the most common issues were lack of resources such as staffing, "unsatisfactory" education and outreach, and legal and constitutional constraints on detecting activities.

In spite of those concerns, almost all respondents indicated that they were better prepared (at least to respond to a situation) than they were several years ago or before 9/11. "We're better than we were since 9/11, because now you're having all communities talking, whereas before the federal government wasn't talking to the state government, or information wasn't going where it needed to go, and the locals weren't getting information. That is better than it was. But we still have a little ways to go" (fusion center analyst). Participants in locations with strong Terrorism Liaison Officer (TLO) and Suspicious Activity Reporting (SAR) programs cited those as being key resources along with developing accurate threat assessments and good relationships with key communities in their areas of responsibility. At the same time, most still identified gaps or areas in which they need additional resources, information, or training to be able to counter violent extremism in its preoperational stages.

Training to Counter Violent Extremism

Respondents were asked questions about the training they had received on violent extremism and CVE. This section presents selected findings from these training-related questions. CVE-specific training and discussions around its availability are presented first. Comments on CVE-related training, or training that is not labeled CVE but is understood to promote the aims of CVE, follow. Training delivered by specific federal agencies is then discussed.

CVE-specific Training

Fusion center senior staff generally answered CVE training questions by either discussing their training or their subordinates' training. A significant minority of senior leadership interviewed received no training or no formal training on CVE. A few explained that there are limited trainings provided on CVE, and they specifically noted a lack of opportunities from DHS. While leadership had participated in few CVE-specific trainings, including CVE workshops and conferences, they did cite trainings that they viewed as broadly related to violent extremism and countering it (e.g., training offered by the Office for Civil Rights and Civil Liberties [CRCL] and the Building Communities of Trust initiative). One leader took care to note that certain trainings, such as those associated with the Nationwide SAR Initiative, were not called CVE training, but in his view they are about CVE.

A number of analysts stated that they had not received CVE-specific training, that training in their area is very limited ("Training is a void"), or that courses are not providing anything specific to violent extremism. In a number of cases, discussions took place on what constituted CVE training, including the broad application of the phrase "CVE" and the differentiation between training—where you learn to do and apply—and the "educational realm." One senior analyst explained that because of the few available trainings in his area, he has no resources to train new analysts, just his own knowledge or the "hope that a class comes along." Others noted that they have had no training on how to stop violent extremism—as compared to general knowledge about HVE and radicalization—or that few classes mention CVE. One analyst explained that for him, there was little difference between terrorism and violent extremism and that "you could just take off 'terrorism' and put 'CVE'" into the title of training courses. He said that he and others in his position have had a lot of training on terrorism.

Fusion center liaisons typically include those who liaise with the fusion centers for investigative or other purposes and those who provide training. At some locations, the training liaisons form a separate training body, while at other locations training appears to be one of their many duties. Because liaisons tend to offer training, they often quickly moved the discussion to training they provided. Most liaisons shared their overall perceptions on training, including their feeling that training is geared toward introductory levels, or, at one location, geared toward command staff and not frontline officers. One participant took care to note that he had not taken a formal class on CVE, though he had taken courses on radicalization, civil liberties, and terrorism. Similarly, one participant explained that most classes do not mention CVE.

CVE-related Training

Participants discussed taking part in CVE-related training related to their roles in the fusion center, whether as directors, analysts, or TLOs. Training generally mentioned by participants included SAR training, the National Fusion Center Conference, and state-level fusion center conferences and workshops.

Senior staff members discussed participating in the Naval Postgraduate School's training for fusion center directors and executives. One senior leader found this training to be great "at hitting all of the topics." Another participant's experience was similar. He relayed his experience in a course in which after a break, the instructor returned to the classroom dressed in traditional male Arab garb. The participant explained that he watched how the students' body language changed and used that exercise to highlight how much stigma is attached to appearance. This participant said that for adult learning, it is "experience around a concept" that is important and that "lecture doesn't work."

Many analysts cited analytical tradecraft development as relevant to understanding violent extremism and how to counter it. Although some training on tradecraft may not have included content about violent extremism, analysts said that it did develop critical thinking and analytical skills that could be used for assessing any threat. Training cited included the Critical Thinking and Analytic Methods course, Principles of Intelligence Writing and Briefing course, Advanced Criminal Intelligence Analysis to Prevent Terrorism (ACIAPT) course, the Mid-level Intelligence and Threat Analysis Course (MITAC), and Anti-Terrorism Intelligence Awareness Training Program.

Many liaisons said they had participated in TLO training that included sections on countering HVE, DT, IT, and prison radicalization. One liaison participated in a conference on prison and jail radicalization put on by another fusion center and found one panel helpful for his work. Another liaison spoke about training from Knowledge

and Intelligence Program Professionals (KIPP). KIPP provided Fusion Liaison Officer (FLO) basic training that was highly regarded.

Training Offered by Federal Government Agencies

The section below summarizes comments participants made about CVE-specific or CVE-related trainings offered by the federal government. Findings in this section should be interpreted as individual reactions to the trainings; these findings do not necessarily generalize to other focus group participants or fusion center personnel in general.

Figure 2. CVE-related Training Mentioned by Fusion Center Personnel (for illustrative purposes only)

This figure shows the types of training related to violent extremism or CVE in which fusion center respondents mentioned participating. The columns represent the training that respondents discussed, and the size of the bubble represents the number of references to each. CVE training relates specifically to training on how to counter violent extremism. HVE/DT/IT/CT training encompasses training on radicalization, terrorism, counter-terrorism, and other trainings related to violent extremism but not specifically countering it. Because it was such a prominent issue, Sovereign Citizen training has its own column. The remaining columns include analytical tradecraft and other trainings that were viewed as relevant to violent extremism but did not fit into the other categories.

Department of Homeland Security

Four fusion center analysts reported attending the DHS CVE workshop in Columbus. One participant noted that he found the workshop productive, well received, and important to have. Another participant explained that he did not find it very useful because much of the focus was on issues not relevant to him, such as assigning patrol officers to community policing.

Three analysts attended the San Diego CVE workshop. One attendee expressed frustration with the lack of relevant case studies. He noted that three different speakers over two days used the Zachary Chesser case study, which is not relevant to his location. One of the key criticisms expressed concerning DHS CVE training, as well as that of other federal agencies, was that it did not draw on intelligence examples or case studies from local environments and did not align with local needs.

Fusion center personnel also discussed participating in a one-day training offered by CRCL that covered protecting civil rights and privacy and emphasized the need to focus on policing behavior rather than ethnicity, culture, or religion. They reported that they generally felt the training was helpful. One analyst, however, described the "required DHS training of Arab/Muslim cultures" as an example of still presenting Muslims as "the Other." Another analyst noted that the privacy training, though dry, was excellent and useful.

Finally, fusion center participants mentioned attending trainings offered by the Office of Intelligence and Analysis. One training that participants attended focused on threats, indicators, and radicalization, as well as activities protected by the First Amendment. One participant said that he found the training helpful because it discussed the "gray area" in many cases of radicalization and violent extremism and why intelligence and law enforcement officers have to be aware of crossing a line in violating a person's rights. Analysts also noted attending training on HVE that was conducted through the fusion center and complemented chats on the Homeland Security Information Network (HSIN) and Homeland Security State and Local Intelligence Community of Interest (HS-SLIC). One analyst described it as "general" and commented that these types of trainings always seem to occur after an incident. On the other hand, a training that covered anarchist groups in the run-up to the 2012 Democratic National Convention in Charlotte, North Carolina, was considered very helpful, as it included information on motivations and indicators.

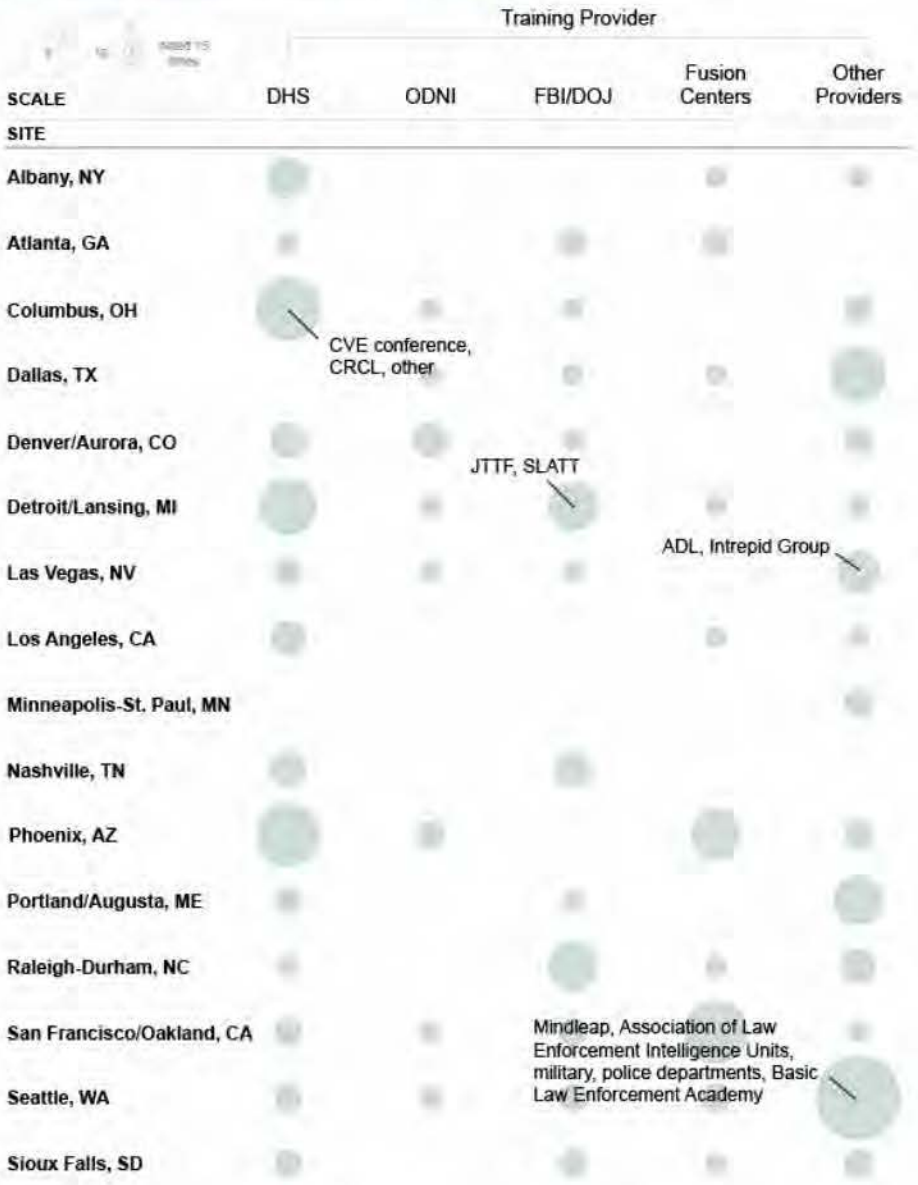
Federal Bureau of Investigations/JTTF

Though few fusion center personnel specifically mentioned participating in FBI training, those who did found the training to be good, extensive, and, in one case, "perhaps too detailed." Other participants mentioned receiving good training from their local JTTF. One liaison, who had worked with the JTTF, found the initial JTTF training at Quantico to be excellent as it provided real-life scenarios, along with PowerPoint presentations and access to case agents. Another liaison's locally taught FBI training on violent extremism was "eye-opening" and discussed the radicalization process among violent extremists promoting "jihadist," Sovereign Citizen, and White Supremacist agendas.

Other fusion center staff spoke positively about presentations made by the FBI in conjunction with former members of groups such as the Lackawanna 6 and the Fort Dix 6. As one participant noted, these presentations are the "true-life story of how this happened."

Figure 3. Training Providers Mentioned by Fusion Center Personnel (for illustrative purposes only)

The columns represent the training providers that respondents discussed, and the size of the bubble represents the number of references to each. Much of the training was provided by DHS, the FBI and DOJ, fusion centers, and the Office of the Director of National Intelligence (ODNI). The remaining column represents training offered by the military, think tanks, academic institutions, police departments, and private organizations.



Department of Justice/State and Local Anti-Terrorism Training (SLATT)

Fusion center senior staff, analysts, and liaisons discussed participating in SLATT training on a variety of subjects, including regional counterterrorism (CT), terrorism, and domestic extremism. Participants tended to think very highly of SLATT, with one noting the training he had received was "excellent." At one SLATT presentation on CT, personnel from one fusion center participated in the final hour to provide the local-level perspective, which participants noted was value added and "how you get buy-in." SLATT also provides background on extremist groups, which a few analysts explained was helpful because that background leads to an understanding of beliefs, ideologies, tactics, and techniques, and the training is provided by those with first-hand experience.

National Counterterrorism Center

Participants noted taking part in training provided by the National Counterterrorism Center (NCTC), as part of the "NCTC/FBI/DHS traveling roadshow." This training discussed violent extremist and HVE threats. Other training provided by the NCTC included training on fundamentalist Islam and social dynamics, as well as classified briefings on extremists, HVE, and radicalization. One participant noted that the NCTC model of bringing in subject matter experts and providing classified briefings is helpful.

Department of Defense

Analysts and liaisons occasionally referred to training they had received as part of the military or while working for the Department of Defense (DOD). A number of analysts who had served in the military noted that most of their training on violent extremism was during their military service. One liaison viewed his training in the military as "the best training" he had participated in. Others referred to training they had participated in at the Defense Intelligence Agency. One participant felt that this training was engaging because it brought in subject matter experts, including those from the foreign media, to speak about how the United States' actions are viewed around the world. Other DOD training included courses at the National Defense University and the Defense Information Systems Agency.

Training Needs

Participants recognize that CVE training needs to emphasize the focus on behaviors and not religion or protected activities. As one fusion center senior staff member said, "We, as a fusion center … we need to be better than that." For something as important as training to counter violent extremism, he noted, "There is nuance, gray areas" and such training cannot be cut and dry. For him, instructors need to be present, and students need to be involved in the training. Many senior staff members saw a need for training that incorporates real-life examples, best practices, and recent case studies. This section presents the diverse training needs as noted by fusion center staff.

> *"If I could develop a training … it would involve a credible instructor who has visual aids, maybe a PowerPoint, but not all PowerPoint. I'd add in a tabletop exercise that is scenario-based. It would be hands-on, with bouncing ideas off each other, updated, and intelligence-based."*
>
> (Fusion center senior staff on ideal training)

Case Studies and Exercises

In-depth case studies were one of the elements of CVE training most consistently requested by analysts and liaisons. They stated that case studies that include local examples can be used to engage participants and to "pull people back" into the lesson.

However, as one analyst explained, true case studies are lacking as most are "cautionary tales, but not full learning experiences." They provide only the "glaring triggers" and not the small items leading up to those triggers. It was suggested that DHS, working with academics, could develop case studies that involve major cases, or other lesser known location-specific cases, of HVE and other violent extremism. These case studies could involve speaking with those who first identified the threat and discussing what was found, how it was noticed, and what was missed. They could include lessons learned, best practices, and discussions about what was prevented "because of X, not Y."

Fusion center personnel also recommended developing case studies that show where extremists crossed the line in their support for, or engagement in, violence. As a corollary to these, they stated that real-world examples of incidents that appeared to be violent extremism but were expressions of First Amendment rights are also needed. Fusion center analysts pointed out that case studies can be used for awareness training on recent events and provide the opportunity to trace the path of indicators from the end to the beginning—these case studies are "walked back," to use the phrase of a senior staff member. Using case studies in this manner "helps staff recognize the value of a tidbit and knowing when something is out of the ordinary. That's key for analysts." Analysts at one center discussed the utility of breaking down a case into its component parts:

> *I want to take Breivik, Oslo, and start from the time he is two years old until today. The most value you could get in a training would be to take one full case and look at everything about it. I don't care if it's online, the delivery. You could do it any way, online, in person, whatever. But show each indicator that led up to an incident … Talk individual variables like blogging, actions, decision-making. People want to read … or be told the details. That is a violent extremist. This is HVE; this is what it is. That is a case study—that is how these things happen. You need to give people what it means.*

Practical exercises that present the big picture were also recommended. Such training could mimic the nature of threats and response. For example, it was suggested that a week-long tabletop exercise would allow staff the opportunity to experience the level of extended effort needed to follow or respond to a situation. As a senior staff member noted, "Threats aren't going to be over in one day. When it really hits, you have to have a long-term understanding" of what is needed. One member of leadership suggested developing a regional CVE activity that brings together all players—the fusion center, law enforcement agencies, and federal agencies. This could be presented as a packaged scenario training that allows for changing the city locations and landmarks. It was noted that scenario drills could include the coordination that needs to occur across law enforcement, fusion centers, and federal agency networks, including tips and leads from the community, where "at the end, because you did all the steps, you made an arrest." It could also include a capstone exercise to review lessons learned.

Training on Indicators, Violent Extremism, and CVE

In addition to case studies, fusion center personnel specifically asked for training on indicators, for their own benefit and for the benefit of the law enforcement officers with whom they interact. Analysts who spoke about working with law enforcement on indicators noted the challenges officers face with identifying suspicious activity based solely on behavior. Some analysts—and others from law enforcement—reported that concerns about being labeled racist have led officers to not report suspicious behavior. This was described as a concern

for analysts, who want the option of making their own determination about suspicious activity and would rather have all reports than none. Participants recommended training on the following types of indicators:

- Indicators to be able to track pre-violent extremist criminal activity;
- Precursors or indicators signifying a more violent uptick of activity;
- Indicators to "differentiate between annoying, but legal behavior" and behavior that is not yet illegal, but could become illegal;
- Key behavioral indicators, even if constitutionally protected behaviors, in order to protect rights and to ensure the safety of officers;
- Normal versus suspicious behavior in immigrant Muslim communities, for officers who have no experience with these communities; and
- Indicators of radicalization.

Fusion center personnel also cited a need for training on various other topics related to violent extremism. These included training focused on:

- Defining CVE and identifying who is susceptible to violent radicalization;
- Identifying the main security threats in a region (and CVE training and documents related to those threats);
- Understanding lone-actor violent extremists;
- Examining the relationship between IT and communities in the United States;
- Understanding various violent extremist groups, such as Sovereign Citizens, neo-Nazis, militias, and homegrown violent extremists;
- Developing narratives to counter violent extremist perspectives; and
- Examining how social media such as Twitter, Instagram, and other emerging networking and blogging services are used for recruitment and radicalization.

Context-relevant Training

Analysts and liaisons most often cited a need for relevant, pertinent, and tailored training, particularly as it relates to their locations. Such training could come from DHS and be adapted to the locality, providing local examples or addressing issues that may potentially involve the location or have a local connection. As one analyst explained:

> *You have to make it relevant, but I don't want to just be focused on [the state], because these violent extremists cross state lines all the time … And a lot of them, they're not even associated with a particular terrorist organization; they're just behind the ideology, every single one of them. Very [few] of them are a member … they just have loose affiliation, right, so that can happen anytime, anywhere, and in any state.*

Training for analysts that uses historical events to create awareness of linkages and methods of analysis may not be considered beneficial if those historical events do not have local relevance. As one liaison noted, because training changes so rapidly, local relevance is even more important. He asked that any training be a "living training" that can be adapted as the needs change. One analyst, whose job prior to working at the fusion center

involved security at a power plant, explained that relevance could involve discussion of local threats, rather than the focus on "al-Qa'ida, al-Qa'ida, al-Qa'ida."

Training on Interacting with Different Communities

A few analysts asked for training related to working with the broader community. Best practices in working with communities, either in the United States or elsewhere, are also needed. As one analyst noted, no "snapshot look" of best practices exists. A few analysts asked for training that could bring the community, community leaders, and other actors together; explain the relationship between fusion centers and social services agencies, including data sharing and its limitations; and assist with developing partnerships with local social services agencies using Memorandums of Understanding (MOUs).

Where communities exist that have been heavily affected by ties to IT, a few analysts and liaisons also sought training on how to develop relationships—built on trust—with these communities. Illustrating the divergent views of these participants, and the liaisons in particular, such training could be on awareness of the importance of developing relationships or developing sources in difficult-to-access communities. Fusion center staff also thought training is needed for the private sector, emergency management, and tribal law enforcement.

Training on Other Topics

Fusion center participants also noted training needs for other practical, job-related skills. As one senior staff member explained, training should be designed to be immediately applied on the job—"I want specific skills I can put to use or that are specific to the threat. Not general." There were several types of practical skills identified for training, including roles and responsibilities within fusion centers, analytical tradecraft skills, and effective brief writing for varied audiences.

Participants across functional roles cited challenges with working in the fusion center environment that could be mitigated by training. For one fusion center director, a federal partners or DHS "Fusion Center 101" course would be helpful. In particular, this director sought information on a fusion center's structure and direction, as well as secure networks and better components needed in a center. Some analysts expressed similar sentiments; as one analyst explained, "Fusion center business is a collateral duty," and personnel have multiple duties that limit the time available for their primary responsibilities. One analyst noted a need for training on classical intelligence, namely teaching what is intelligence, what does it mean, and what will fusion center personnel and law enforcement do differently as a result. Analysts also suggested offering certification for analyst training, so analysts can be viewed as experts and have that expertise recognized by their command.

One senior staff member noted a need for training on how to use systems and databases. As he explained, his staff are really good at open source research, but need information on how to use classified systems; his fusion center has so many, that they do not know where to start. An analyst had a similar request for training on how to use technology for tracking incidents.

Senior staff and analysts both indicated a need for more training on writing briefs. Currently, analysts mostly write for the executive level and receive training for this; however, there is an emerging need to learn how to write for law enforcement, which might require the inclusion of boxes, pictures, maps, and other features.

Better Planning for Training

Currently, the process of providing CVE training is seen as *ad hoc* and "catch as catch can." Analysts cited a need for a more systematic, structured, and organized process for providing CVE training. For example, one analyst requested a four-month period between notice of training and the training date. Others recommended a structured training curriculum that gives analysts—and their managers—the opportunity to choose from a menu of courses over a certain time period and plan for attendance in advance. Beyond offering a menu of courses, such a training curriculum could provide a series of courses that are inter-related, whereby participants can build on and reinforce prior learning. At the same time, other analysts questioned the feasibility of creating a structured CVE training program, due in part to the wide applicability of the phrase "countering violent extremism" and in part to the multiple agencies involved—noting that each agency will be responsible for some part of CVE and have different agency-specific approaches to achieving that mission. However challenging it would be to bring a common training curriculum to different agencies, the analysts did note that having a minimum level of training on CVE was a good thing.

One senior staff member cited a need for a list of available trainings and resources. He also saw a need for a system that rated the available trainings. Even a system that classified different levels of training—beginning, intermediate, and advanced—is seen as a need. Another senior staff member requested that this study develop a list of trainings that could be ranked by fusion centers across the country.

Training Delivery and Availability

Analysts often spoke of different types of training delivery methods. Web-based training was sought by some, and could include virtual training with breakout sessions; others roundly rejected the use of Web-based training. Those who saw a need for such training delivery discussed its cost and efficiency. Web-based training is often inexpensive—some noted that the training they received was "free"—and can provide a simpler way to train new staff. One analyst said that the availability of Web-based CVE training would allow him to bypass previous issues his center has faced with inconsistent invitations to training.

Analysts also sought training delivery methods such as tabletops, red team/blue team exercises, and local or regional in-person training. Analysts requested training by—and access to—subject matter experts. For some, local experts were a priority, rather than national experts. Analysts stated they wanted experts they could ask questions or network with locally or regionally, at both the unclassified and TOP SECRET level. They explicitly asked for a contact list or roster of experts, though one analyst noted HSIN had similar information available.

Participants also mentioned wanting ongoing opportunities for learning. For example, one analyst identified a need for refresher exercises twice a year to keep skills current and suggested using the HSIN portal for these exercises. Also, because only so much information can be covered in courses, two analysts noted a need for more continuity after a class is over, when weekly or monthly "tips for your toolbox" could be distributed. Fusion center personnel also stated that they need access to training at intermediate and advanced levels.

A few analysts felt that the training they receive is helpful and classes offered are sufficient, though it requires knowing where to find them. One analyst cited a need for online training blocks from DHS and training from NCTC. Another asked for a video recording of the DHS weekly analytic chat for those who are not available at the regularly scheduled time. Participants stated that training that is offered through briefing papers is not ideal.

Training Challenges

Roughly half of the participants identified challenges with incorporating the training they received into their jobs. Most often, these challenges were related to the relevance of the training to their jobs and institutional barriers. Other challenges were related to a lack of post-training support from the trainers (especially for software or technical training) and difficulty fully understanding federal guidelines relating to collecting, storing, and sharing information.

Training Relevance

For those participants who mentioned issues incorporating training into their jobs, most cited issues related to relevance or applicability. For example, some mentioned that CVE training is too abstract and has little practical application. Participants also reported that the opportunities to apply training often come weeks or months later when it is forgotten. One senior staff member explained, "I send a group to training, and I anticipate that I will see something change in the products. But I never see changes. I'm not seeing it incorporated into products." For one participant, the ability to apply training should come from the training itself. As he explained, one of the "biggest failure[s] with training is no one says, 'This is what you're going to do differently on Monday morning.'" He explained that organizations also may need to make changes to their policies to allow for skills learned in training to be fully implemented: "Authorize what I need to do, rather than tell me what I need to do. How do you want me to do it? Authorize it."

Institutional Culture

Participants occasionally noted difficulty incorporating their training due to institutional barriers, including the culture of the institution. Participants experience a variety of hurdles, as the following examples illustrate:

- Yes, a lot of times we're hindered by our own administration. We have leadership who don't understand what you've learned … When men and women get training and go back to departments, they're fired up and ready to go, but the administrator says, "We've always done it this way and this is how we're going to do it." (fusion center liaison)
- The biggest problem is people's mindsets. Especially with the cultural side of it. That's not something you can change in one swift motion. One lady asked at a DHS training, "Why are you giving them special rights?" That seems to be more of a problem here. They aren't gonna buy it. There was a DOJ [Department of Justice] training that I was in and they got heckled. Different cultures is where you will run into problems here. (fusion center analyst)

Sources of Information on Violent Extremism and Countering It

Fusion center personnel were asked about their experiences receiving information on violent extremism and countering it, including the sources they value and turn to most often, the challenges with getting good information, and the information they need.

Best Sources of Information

Within and across fusion centers, there was broad agreement on the best sources of information. For example, fusion center personnel noted that they often rely on information that is obtained through personal

connections. The senior leadership across fusion centers agreed that relationships are critically important in order to get good information. This holds true whether the source is a federal (including other fusion centers), state, or local community source. These networks have been built over time, and participants are more likely to trust these sources.

However, it is also important to note that participants indicated that there was no one single best source of information on CVE.

Local Sources

"The community is the best source. They're the eyes and ears." (Fusion center analyst)

Across locations, analysts commonly reported that their best sources of information were local sources, in the form of law enforcement, business owners, community members, fire department personnel, parents reporting their children's behavior, TLOs, or "snitches" from local gangs or prisons. Many analysts described "people on the ground" as the best source of solid information. The views of liaisons and senior leadership were similar. As one senior staff member noted, "It's always human intelligence. There's no substitute for that."

Many senior staff and a few liaisons thought that the TLO/FLO programs in their areas of responsibility were the most valuable bridges between the community and the fusion center. Trained law enforcement personnel and first responders were described as the primary link in the information flow, particularly in states where sheriffs retain a significant amount of authority. For example, one senior staff member described how the TLO programs help fusion centers in the following way:

> *[The] TLO is extremely valuable ... We average 750. When engagement falls off, we reach out. So we have an average of 750 to 800 TLOs. 750 is a good core. We get a lot of Sovereign activity in [region], a sudden uptick in this. And then we'll find a similar incident in other areas of the state. [Our state] is a 'home rule' state. The state doesn't dictate to sheriffs ... Without the TLO program in the state, it would be difficult to get the sheriffs' involvement. Or information from that department. The TLOs bridge that gap.*

A few analysts and liaisons specifically mentioned SARs as the best sources of information. Another liaison mentioned the "If You See Something, Say Something™" campaign as a source of information: "We get most information from [the] law enforcement community, but we do get information from private sector and individuals. If I was a line officer, I'd be interacting with the public on a daily basis, and they are my best source."

Online Sites and Databases

Analysts also frequently reported websites as one of their best sources of information, with social media being of particular interest to analysts in three locations. Senior staff and liaisons also cited social media and online databases, but less frequently than the analysts. Participants discussed using publically available websites and federal/state sites that required some form of clearance. The most commonly mentioned websites were DHS.gov, HSIN (with respondents at two locations specifically mentioning the CVE portal), and Law Enforcement Online (LEO). Other sites included FBI.net, HS-SLIC, Regional Information Sharing System (RISS) (and its component information networks), CargoNET, CIAWire, SLATT, and COPLINK. Media websites named by analysts were CNN, BBC, and local open sources. The social media websites that were commonly cited were Facebook and Twitter. As one analyst noted, "Social media is a gold mine."

Fusion Centers

Analysts from five locations specifically mentioned information from other fusion centers as being a best source of information. The subject matter expertise that the various fusion center staff bring and make available to others is highly valued, particularly cultural expertise that gives the staff insights about populations with which they are less familiar. A few liaisons specifically cited the fusion centers' products as being best because they focus on local issues and are shorter and more timely than other products. One participant provided an example of fusion center products leading to law enforcement to recognize similar trends in two states.

Senior leaders felt that the way the fusion centers are set up, with key personnel all located under one roof, is an important factor in their productivity. A few senior staff members explained that it is the combined resources increasingly brought by state and local entities and their support of the mission that ultimately allows for information to be available to local law enforcement. This "connectivity" can lead to more information sharing and, senior leaders perceive, to greater success at their tasks related to CVE.

Department of Homeland Security

Analysts at seven locations indicated that DHS was a best source of information, citing DHS reports and products. One analyst shared that DHS defines the overarching threat, but locals have to determine what applies to their areas of responsibility. Liaisons from nine locations indicated that DHS was a best source for them. Senior staff members often noted the DHS IO as a best source of information. One liaison, however, stated that DHS products were often outdated by the time they were made available to fusion center personnel and the wider law enforcement community.

Federal Bureau of Investigation

Analysts at seven sites indicated that the FBI is a best source for information, while liaisons in three locations mentioned the FBI and in two locations cited the JTTF. However, participants explained that FBI information is not always forthcoming and that frequently information is provided to the FBI, but not much is given in return. Respondents who did get regular updates or products from the FBI appreciated them, but some felt they were out of date by the time they got to the fusion center staff. As one liaison explained, "Something is better than nothing. If it goes up to the federal government, by the time it is cleared and it gets back down to us, seven other people have already sent it out. It is out of date or there may be redundancy. A number of different agencies end up circulating the same information."

Other Federal Sources

Other federal agencies that were described as best sources of information included the NCTC, Immigration and Customs Enforcement (ICE), DOJ, National Operations Center (NOC), Institute for Intergovernmental Research, Interagency Threat Assessment and Coordination Group (ITACG), and SLATT. However, it was stated that the ability to get timely and accurate information from many of those agencies depended on personal relationships. As one liaison explained, "We have a guy who sits at the NOC, so that's our insider since 2005.He'll collect

information from New York, Pennsylvania, Florida, and others. He reads everything and if it pertains to hospitality, [city], or law enforcement officers, he'll send it. He's a filter. We had people at ITACG. The Sheriff jumped on this in 2005. We've had an advantage there."

Academic and Other Sources

Academic sources were not a primary source for any of the fusion center personnel. Most analysts had to be prompted to think about academic sources as sources of information. Challenges with academic work cited included the lack of timeliness and the length and density of the reading. One analyst felt that academic work was valuable "but not fully appreciated." One senior staff thought academic research could help give the historical component to certain problems while another felt that academic research was "too much fluff." A few senior staff, analysts, and liaisons referenced useful academic contacts at institutions such as Michigan State University, the Naval Postgraduate School, University of North Dakota, West Point's Combating Terrorism Center, and Duke University.

A few fusion center personnel also mentioned other organizations as sources of good information, including the Anti-Defamation League (ADL), Southern Poverty Law Center (SPLC), Brookings Institution, and Rand Corporation.

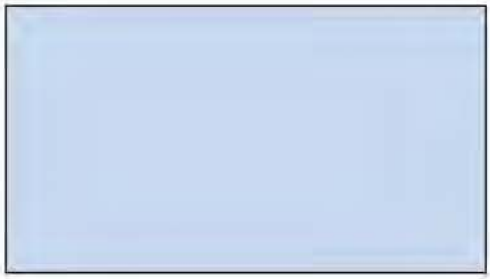
Problems Getting Good Information

No Problems

A few of the participants reported no problems getting good information about violent extremism and countering it. Those who expanded on their answers tended to note that too much information is never enough or that there is always going to be a desire to know more. Others mentioned the access they had to knowledgeable individuals, including the DHS IO. One senior staff member explained that if he had any questions, he would ask the IO, who "would give me everything he's got on HVE. He knows what's out there. He's a resource for direct information."

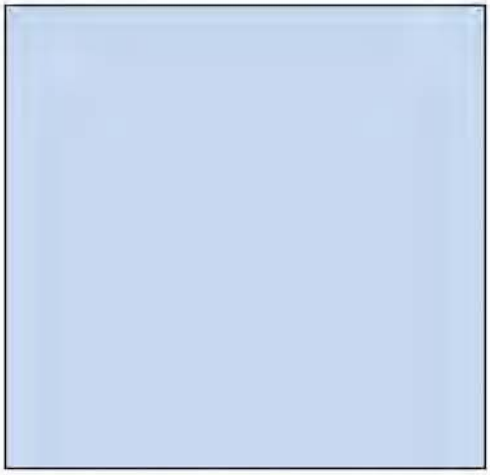
Information Sharing and Relationships with Partners

Participants at 12 locations cited information sharing as the primary obstacle to getting good information and noted ongoing issues with collaboration with federal agencies and between state/local agencies. According to one analyst, "Communication is 100 percent better," and "no one can get away without giving the appearance of collaborating," but "we're still cutting each other off at the knees." Participants said that information is only shared to certain levels of leadership or is shared inconsistently, leading to a flood of information at times. For others, ongoing information silos are still a problem. As one analyst explained, these silos are still present due to "hubris" and an unwillingness to "burn sources." A few participants also noted that access to information still hinges on having personal connections rather than an institutionalized process of information sharing. Those who rely on personal networks expressed similar sentiments. As one analyst explained, "There's a good final product I only know of because I know a guy who knows a guy. They know what questions to ask."



Federal Sharing

Participants' experiences receiving information from other federal and state entities varied. Problems getting information from the FBI were consistently mentioned, with one analyst describing it as "the FBI struggle." One senior staff member explained, "The only time I got good information from everyone was when I was with the JTTF ... I don't mean to bash the FBI, but I've had a lot of trouble getting good information." One analyst noted that the JTTF does "a terrific job," while another analyst explained that information sharing with the JTTF is a one-way flow where "every once in a while they give us a briefer, toss us a bone."



Participants also cited issues dealing with ICE, the DHS IO, and state homeland security units. Some stated that working with DHS component representatives is a challenge as they do not share information, or at one center, tend to take a leadership or administrative role and are not "willing to be part of the team." However, at a number of fusion centers, the DHS IO was seen as one of the best sources of information.

Some of these issues, as two participants noted, may be due to the perception on behalf of federal partners that information is already being disseminated. According to one analyst, "I sometimes see lights go on—'I had no idea you needed to know.'" Or, in other cases, it was stated that some may hold the view that fusion center personnel are not adequately prepared for access to classified information.

Fusion Centers as "the Middleman"

Participants reported that fusion centers as an institution are often placed in situations where they do not receive information from the federal agencies or local agencies, or are limited in what information they can disseminate. Such problems may be related to classification issues, ongoing investigations, or personnel who are not privy to higher-level information requirements. As one analyst noted,

> *The customers are law enforcement, private sector. We can't disseminate it. We can't create docs in HSDN [Homeland Security Data Network], but our job is to share information up and down the line. If we can't understand what's needed higher up, how can we help? ... If we can't see what they're looking at, potential sources, potential leads, we can't do anything.*

For example, at one site, information from an ongoing investigation that, like many cases, began at the local level, could not be shared on information sharing platforms until after an arrest had been made. Such a practice of not providing any information limits the ability of other fusion centers or partners to determine links, if any, to their locations. However, even receiving that investigative information is a problem at other locations where local law enforcement will report information to the JTTF or FBI, but not to the fusion center. One participant explained that a fusion center's role is to aggregate information and having access to the tripwires or indicators of a particular investigation is necessary for that role.

> *"It's already a failed process. It's like an ant pile. You're fighting a never-ending battle to get rid of it. Stop pulling one ant out of an ant hill at a time or they'll keep coming back."*
>
> (Fusion center analyst)

Communications within centers were also occasionally noted as problematic. At one fusion center, sharing information internally was described as an issue. There, liaison officers indicated that they rarely hear feedback on the information they share with the center, and thus cannot provide feedback to the originators of the information—local law enforcement. According to many liaisons, if feedback is not provided to local law enforcement, the average officer will eventually stop providing information. At another center, participants reported that co-workers may not know each other or know what projects co-workers are working on. Here, analysts were also described as "so busy" reviewing information about local threats for the federal government that they did not have time to support their local colleagues' requests for information.

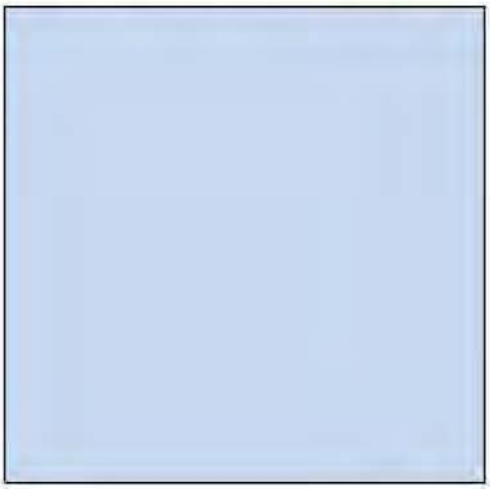
Participants also reported that problems getting good information were the result of a lack of seniority ("I'm low on the totem pole.") or a lack of perceived authority ("You're supposed to be the expert, but you can't get information. You aren't seen as an authority. They don't trust your opinion.").

Local Sharing

Fusion center liaisons noted issues with receiving and disseminating information to local law enforcement and others. At nine sites, participants discussed ongoing, negotiated relationships between fusion centers and local police departments. Possible reasons cited for these issues included trust issues between law enforcement and non-law enforcement, a lack of knowledge on the part of local law enforcement about the fusion centers and their role, institutional barriers, insufficient staffing, or lack of perceived value.

> *We don't have the full support and participation of all the agencies in the state. A lot of partners. It used to be a pull system, but now some agencies are pushing their information to us, but not all. It's still a push/pull system. If everyone did it, we'd need to double or triple in size to handle it. We have a huge chunk of the threat picture missing. It's personality-driven. Not that we haven't tried to get more, but individuals don't think we're of value or valuable to them if we don't provide an analyst to them. They want us to be dedicated to them. We try to work through that.*

While working with local law enforcement across states is generally easier, according to some analysts, some require a court order or a subpoena in order to share information. Analysts at one center noted that information sharing among state and local partners, including fusion center to fusion center, is "getting better." However, as one analyst explained, "Communication with fusion centers—they are all different and reaching out to them doesn't yield consistent results. Some won't even answer their phones."



Developing Products for Dissemination

Analysts spoke about the problems with developing products for local law enforcement and other partners. Discussions about how to present information to local partners included striking a balance between the need to provide information that is unique and interesting with ongoing reminders and not overwhelming the recipients with too much information. One analyst asked, "How are you to provide context if you only want one page to address it?" and

explained that her unit "straddles a fine line" to provide enough information to be useful, but provides limited details to prevent lawsuits.

Participants also discussed how to ensure that products reach a wider audience. Ideas included creating a newspaper-like bulletin with special sections so that recipients could peruse areas of interest to them, preparing targeted bulletins for beat officers or firefighters, and delivering oral briefings followed by analytical products. As one liaison said, each document should contain information relevant for every sector, though the fusion center cannot control how or if that information will be used. Others noted their limited ability to ensure that information, once disseminated, actually reaches all audiences. As a liaison explained,

> *When we pass something down to the department, the people in the precincts have some latitude in deciding what they want to do with it, whether they want to push it out or not. Some may decide that most of what they get they will pass on; others may decide it's not important and the officers may not need to know it.*

Secure Systems/Access to Classified Information

Participants reported issues with accessing and using secure systems. These issues usually pertained to the numerous systems available, the quality of those systems, and appropriate access to information. For participants, the numerous information platforms—combined with a lack of a common effort, MOUs, and jurisdictional boundaries—create barriers to sharing. One participant felt that there are too many agencies involved and too many systems with the result that for his center, it "should be a one-name search, but they have to go into five different systems." Another participant said that he simply will not sign into multiple systems. The number one complaint of two participants is the lack of a single system, or a few systems, that can incorporate the information from other databases or platforms. One senior staff member described the proliferation of systems as everyone "eating off of the same hotdog." He noted that because of quality and ease-of-use issues, no one likes to use them. This proliferation of electronic systems, according to one analyst, is similar to the departmental stove pipes prior to 9/11, only now, there are "electronic stove pipes."

Across four sites, analysts and senior-level staff mentioned issues with the quality of the information systems. Citing HSDN, LEO, HSIN, HS-SLIC, and RISS, they explained that systems are "glitchy," there are issues with connectivity, or they do not work much of the time. Analysts at one site agreed that HSDN "could go away tomorrow and no one would notice or care. Tell DHS to throw it in the basement." One senior staff member explained that he visits LEO.gov once a month, but only to change his password. For one analyst, these systems are the only access he has to classified information, and he noted that their unreliability inhibits the dissemination of timely classified intelligence.

Access to the systems and different levels of information on the systems were identified as problems as well. One senior staff member, citing issues with gaining access to the CVE portal, explained that at his center,

> *We don't all have access here. You must first know the portal is out there on HSIN, but then it's not clear what to do to get on. We have to pick up the phone to call the Help Desk to start the access process. Now the Help Desk nominates you to the managers of the requested Communities of Interest and if they approve it takes 24 to 48 hours to be finalized. But if nothing happens for a week you have to call the Help Desk again. One of ours is still not approved [a*

month later]. I would recommend an online self-nomination tool to request access. Take the Help Desk out of it. Then click on the Community of Interest and behind the scenes some manager of the Community of Interest says "yea" or "nay."

For some analysts, HSDN only offers access to state and local sites with no federal information available. One analyst expressed frustration that the information available through HSDN's White List, or the list of approved sites for state and local partners, is too limited. Consequently, he has to serve as the middleman and pull information that is not accessible by others. At another center, analysts explained that they are told by the DHS IO to access information on HSDN, but the IO does not know that this information is not available to them. Conversely, federal employees are unable to access certain state and local databases, whether due to firewalls or needing approval by the Office of the Chief Information Officer to obtain access.

Analysts experienced other challenges in accessing classified networks. At one site, analysts with SECRET-level clearances do not have access to classified systems, including IntelLink, the full NCTC page, and Intelligence Information Reports. Occasionally, one analyst noted, they receive unclassified information below the tear-line. At another site, where analysts have TOP SECRET clearances, they do not have access to certain classified systems within the fusion center. However, as one analyst explained, as a member of the armed forces, she can access the same systems at the military base.

Without access to such systems, analysts have a difficult time running background checks and searching through vetted information. One analyst, who previously had access to classified systems, now relies on others to run background searches. As he explained, "I knew the system. I didn't have to ask. But now I have to ask for it to be done, and I'm not sure where or how they looked. I don't know if they'll do the search like I would. I'm just told there was 'no derogatory information.' But no information on which sites they visited."

Another analyst explained that limiting access to classified information undercuts the CVE policy's focus on local law enforcement and citizen involvement. According to this analyst, a "very good" and "immensely useful" DHS report outlining the steps toward becoming a homegrown violent extremist was released only at the classified level, thus not allowing local law enforcement or the public access to it.

Information Overload

> *"We're standing under Niagara Falls."*
> (Fusion center analyst)

Participants at nine sites mentioned issues with receiving too much information. One analyst explained, "I'm inundated with information, data—written and electronic. Email has almost become a useless tool for me." Another analyst described the amount of available information as high signal-to-noise ratio, where they are "looking for a needle in a big stack of needles."

With so much information, they explained, determining what is relevant is difficult, and they worry about missing pertinent information. They noted different strategies to deal with the flood of information, including deleting emails manually and automatically, picking and choosing sites they will visit—"If I checked the first five source sites, why should I check the next?"—and relying on individuals, like the DHS IO, to alert them to important information. Reports are skimmed, if read at all.

Participants said that the coordination of the flow of information needs to be better handled. Analysts and liaisons suggested that streamlining and consolidating federal efforts would be helpful, as "it is a federal

government problem." As one analyst explained, "There could be 17 different products, two independent products from DOJ or DHS or others—do they all cover the same thing? I don't know if information in one is the same, so I ignore them all." Others noted that agencies showed no discretion about the information they share, and that the information is generally not targeted.

Quality, Timeliness, and Relevance of Information

Quality

Participants at nine sites perceive the quality of information to be a problem. At five of these sites, information is seen as repetitive and not adequately complex. As one analyst explained,

> *When I was new, I read everything. But it took two years to realize I was rereading the same stuff. It's been a while since there was a new, exciting need to act on … Initially when I didn't know anything, yes, federal communications were helpful. But on a 1 to 10 scale, now they are consistently delivered at a "three" level, which is great when I was a "zero." But then I stayed at "three." Information could be lost there in the information overflow.*

Analysts at one site reported that they receive good information because they check the appropriate sites; however, they noted that HSIN teleconferences that rehash bulletins are "not value added." Others reported that the only opportunity for some fusion centers to interact with federal agencies in Washington, D.C. is through secure video teleconferences (SVTCs), but information shared in these teleconferences is "watered down to the level of FOUO [For Official Use Only]." For one liaison, the information that is available about CVE is repetitive, with a lot of cutting and pasting, and the analytical way in which intelligence publications are written is not "appealing" to law enforcement staffing fusion centers. One senior staff member felt that repetitive information may not be a bad thing, as he, and others, "won't remember past five minutes." The "three-way reporting" among state/local agencies, DHS, and the FBI led one senior staff member to wonder if reporting was "circular or regurgitated." One senior staff member explained that state and local law enforcement often view products that come from DHS and JIBs as "spam" and noted with some concern that federal analysts are evaluated on the number of products they produce, rather than the quality of those products.

> *"… it was written by academics and how it was translated was that 'the Feds are coming and they're going to limit our rights.'"*
>
> (Fusion center analyst, on poorly worded federal communications about tripwires that were perceived as a threat)

One of the analysts stated that most of the information they receive from DHS may make a "marginal improvement for the analysts, but there are no points in which you say, 'This made the difference.'" Another participant questioned whether the fusion center receives complete and accurate reporting and wondered what "was told to leave out" of documents. Other participants noted different motivations for not providing potentially valuable information, including political and investigative concerns. One participant thought that the federal government did not address cultural indicators because it "would be a heavy lift" and "a slippery slope." For another participant, the most valuable information "sits in investigative coffers." Participants at one site noted problems getting demographic information and clarity about ethnic or clan conflicts.

Timeliness

Participants at six sites reported issues with the timeliness of information they receive. For a few of these participants, timeliness was noted as a key component in ensuring successful communications and the exchange of information. Others stated that how and when they receive information has an impact not just on their positions, but also on the role they play in disseminating information. As participants at three centers explained, the secure federal documents they receive are often on the news or radio the next day, or contain information that is already public. In one case, analysts at one center actively sought a classified document, only to be told that it could not be provided to them; however, CNN had the physical document. According to one senior staff member,

> *We get good information, but the problem is timeliness. The fusion centers and law enforcement are taking the backseat. A few here have SCI access. Secret isn't needed for our customers. Our customers are looking for a lower level … We're always looking for the tear-line, the FOUO for customers. We're usually at a disadvantage; by the time it's ready, it's always on CNN or Fox News. And then the customers say, "Why do we need you?"*

Relevance

Participants across five sites cited issues with the relevance of information sent to their centers. Analysts explained that information often lacks appropriate context. For example, analysts at one site would like greater clarity on the reason for distribution of information products and noted that "if there was an understanding of if it is a routine update or unclassified for a potential threat, that would be helpful." Being aware of such context helps analysts know how to react to information. Another analyst explained that he actively reads CT blogs and briefings as a way to round out information provided by DHS. For him, "DHS products are sanitized from the context" and provide a uniform message that is mechanical, with indicators, but not details. He looks for "people's opinions, facts interlaced in those opinions."

Analysts explained that federal products are often generic and are not specific to CVE. For one analyst, the information she receives requires her to follow up with DHS or the FBI and back-track with the analyst who originally prepared it. For her, "If you really want to know what's going on, you have to dig deeper." Another analyst described DHS products as dated, skewed with too high of a view, lacking in detail, and focused on overseas or foreign threats, rather than issues prevalent in the state. She noted, though, that she values the products for what they do and what they are, but she does not expect local relevance.

Privacy Concerns and Lack of Clarity about the Threat

Fusion center personnel in six sites identified concerns about privacy, a lack of consistent agreement and understanding of the nature of the threat, and reluctance by government parties to develop clear policies around collecting and reporting information. For example, for analysts, First Amendment issues create challenges in receiving information, including information on movements and people involved in them. Analysts explained that few federal and state agencies write on domestic movements unless a crime has been committed. It was also said that analysts are concerned about being targeted in the media by groups they study, and as a result, analysis becomes reactive and not proactive.

One senior staff member explained that the issue is confusion around 28 Code of Federal Regulations (CFR) 23, and especially when a fusion center or law enforcement agency can gather, retain, and share information without violating civil rights. At one site, intelligence collection is prohibited by city ordinance. At another site, a senior staff member commented that reporting physical indicators of gang affiliation, such as hand signs and shaved eyebrows, is permissible, but that reporting physical indicators of cultural association, such as the color of turbans that can have a religious affiliation, is not: "You can target a red bandana, but not a black turban."

Analysts also spoke about the lack of clarity around implementing CVE. For example, the definition of HVE or violent extremism is a problem, with analysts wondering what the threshold is for violent extremist activity. One senior staff member noted issues with how the threat is branded. For him, "CVE, HVE, radicalization, eight signs of terrorism" are all labeled different ways but mean the same thing. One analyst discussed issues associated with the inclusion of legal behaviors as indicators, such as visiting websites, adopting a new name, and shunning peer groups. He acknowledged that DHS is struggling to define indicators for law enforcement, but the only true indicator, according to him, is the totality of such information.

Other Problems Getting Good Information

Regulations

Participants at two sites cited issues getting information due to regulations. An analyst at one site sought demographic information, such as the year of arrival and address, about "aliens of special-interest countries" from the United States Citizenship and Immigration Services. However, he found that the sources of information are all protected. A senior staff member at the other site noted issues with getting information protected by the Health Insurance Portability and Accountability Act following an incident.

Resources

Participants at two centers reported that resources, in particular staffing and hardware, are barriers to getting good information. At both locations, insufficient staffing was cited as preventing appropriate focus on homeland security issues. According to participants, this is due in part to budgets of law enforcement and fire departments being cut, limiting their ability to devote personnel to these issues, including those who would process incoming intelligence and information and develop sources.

At one site, access to classified networks is a problem because of hardware issues. Participants discussed the number of available networks and access to computers and jacks. For these participants, they have to use colleagues' computers to conduct searches. Funding for the centers also has an impact on the number of information technology personnel available to work on technology issues.

Information Needs

Fusion center analysts identified information needs that included information about specific groups, case studies, indicators of radicalization and terrorism, and cyber terrorism issues; regionalized threat assessments; and up-to-date trend data.

Senior staff and analysts were interested in receiving information in various formats, depending on the purpose of the document and information being shared. For example, when sharing analytical products, analysts were

interested in receiving the original analysis, not a summary. They also thought that factbooks that provide detailed information on groups of interest (their history, geographic spread, past and current activities, associations, and symbology if applicable) would be an invaluable asset. They also suggested flipbooks, checklists, and posters for wider audiences. Another key information resource they mentioned needing were contacts for questions on specific groups or issues and other networking mechanisms through which they could develop their own resource networks.

Liaisons discussed their interest in receiving products that are targeted to their constituents, typically law enforcement. They suggested short daily or periodic briefs, with current news on top. However, they stated that these should be written with that target audience in mind, be locally relevant, and avoid jargon that may not be commonly understood outside the intelligence and analysis community. Other suggested products included "Go books," indicator books/tools, and other products like DOD's Smart Culture cards.

Two other information formats that fusion center personnel thought would be useful are SVTCs and a one-stop online resource. They suggested using SVTCs to share current information and facilitate interaction across fusion centers and other relevant partner agencies. The second tool, the online one-stop resource, would enable everyone to access information on demand and would concentrate resources on one site, implement security provisions to be able to post classified information to the cloud, create a user interface with a simple dashboard, and support a federated search function that can aggregate results across different components of the site.

Law Enforcement Perspectives

Local Concerns and Understanding of Violent Extremism

Similar to the interviews and focus groups with fusion center personnel, in each of the interviews and focus groups conducted with law enforcement, the moderator opened the discussion with a preliminary question about the threats that were of greatest concern to the respondents in their communities. Once again, the responses are not representative of the full range of threats that may exist in each community, but rather represent only the perceptions of those participating in the study.

Threats and Perceptions of Threats

Overall, law enforcement participants around the country stated that they were most concerned about the criminal activities that are most frequent in their jurisdictions and for which they may be called to account by elected officials and the public. Thus, study participants reported a wide variety of primary concerns, including: gang crimes, drug trafficking, threats to the public and officers' safety, threats to critical infrastructure, financial crimes, property crimes, homegrown violent extremists, terrorism, human trafficking, and sex crimes. Which of these threats was the foremost concern for any participant was related to his or her role within the law enforcement community and the characteristics of the community in which he or she works.

For example, investigative officers who were members of gang units were most concerned about gangs, and similarly, members of drug units or sex crime units noted that those were their primary concerns. Many of the larger cities have units within their criminal investigative divisions that are focused on larger threats, including terrorism and violent extremism, and many investigative officers reported being most concerned about DT, active militias, and violent extremist groups in their jurisdictions, as well as the radicalization of potential terrorists or violent extremists.

The primary concerns among patrol officers were gangs (including outlaw motorcycle gangs), drugs, Sovereign Citizens, property crimes, threats to critical infrastructure, and improving community relations, which influences the frequency, relevancy, and accuracy of information that police officers receive from members of the community. "As a cop on the street, my concerns are street-level robberies, street-level drugs busts; those are the primary things that I think we deal with."

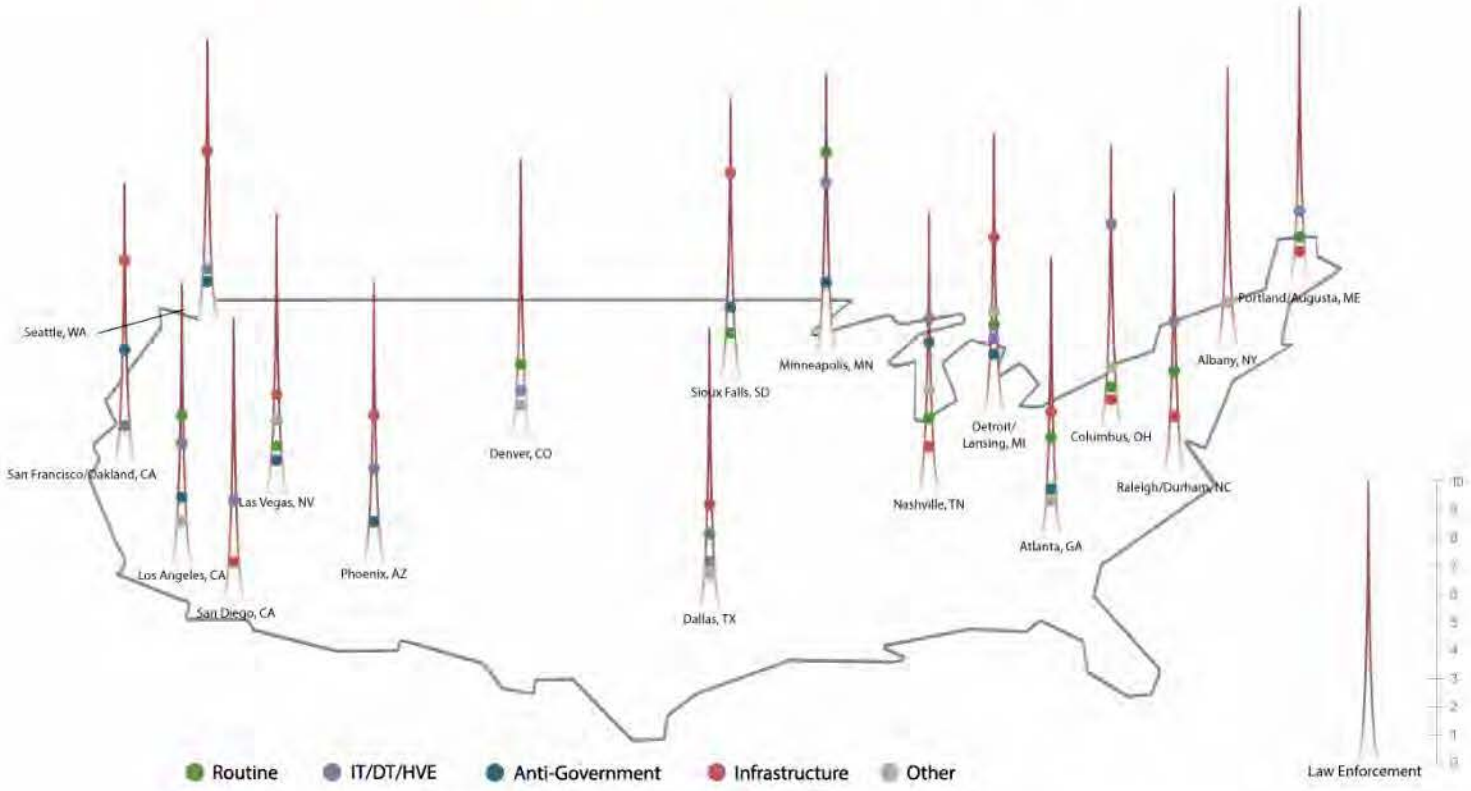
At the executive level, the primary concerns were more varied and were not tied to a specific law enforcement role, but to the overarching concerns of the community and elected officials. Executives' responses were more focused on patterns of criminal activity, such as gang- and drug-related crimes, as well as low probability, high-impact events, such as terrorist or extremist activity and threats to critical infrastructure.

Responses differed by location. For example, in Arizona, Michigan, Texas, and Washington, the border was cited as a concern, particularly related to drug trafficking, human trafficking, and the entry of terrorists into the United States. Respondents in states that are part of major transportation corridors, including Arizona, Colorado, South Dakota, Texas, and Washington, noted concerns about what they might encounter as people and goods move through their states. Concerns related to IT and the presence of international groups also varied by location. For example, in Los Angeles, several officers noted support for Hezbollah being a concern,

while in Columbus, Maine, Minneapolis, and Phoenix, IT-related concerns are predominantly related to al-Shabaab. Al-Qa'ida was noted as a concern in Los Angeles, Ohio, and Tennessee.

On the whole, HVE was reported to be a major concern in many communities, as was the radicalization of vulnerable individuals. In those states where Sovereign Citizens have been highly active, they were reported as a primary concern among many officers. Lone-offender-style attacks were a primary concern for many of the study participants as well. Officers in a number of locations also expressed concerns about activist or non-violent extremist groups, such as animal rights activist groups, white supremacist groups, and environmental activist groups, becoming violent.

Figure 4. Map of Law Enforcement's Primary Concerns (for illustrative purposes only)



This map shows the primary concerns cited by law enforcement interviewees and focus group respondents. The scale reflects how often participants noted different types of threats.

Officers everywhere expressed concern about "routine crime," drugs, and gangs, though which gangs were of greatest concern varied from specific drug cartels in Texas and Colorado to outlaw motorcycle gangs in North Carolina and South Dakota. Similarly, critical infrastructure was a concern in all communities, though what was viewed as constituting critical infrastructure varied.

Threat of Violent Extremism

Violent extremism was mentioned as a concern for the large majority of officers who participated in the study; however, whether it was a daily concern varied. For officers in large cities with significant international

populations considered to be potential targets of terrorist recruiters (including the Somali, Iranian, Yemeni, and Iraqi communities) and particularly officers involved in patrol and community outreach, violent extremism was a primary concern. Other officers mentioned being concerned about a range of groups, including hate groups, Sovereign Citizens, and groups espousing a particular set of ideals (animal rights, right to life, etc.), as well as prisoners from marginalized groups.

Very few respondents said that violent extremism was not a concern. Most of these respondents noted that there was little in their community that would provide a target sufficient to make a political statement, "For extremists, they don't know who we are" (law enforcement patrol), or that it was not a concern because the communities were small and hard to hide in. As one law enforcement investigator stated, "In smaller communities, it's not their [the police's] focus. They know everyone and their moves."

Many study participants, when asked how they defined violent extremism, described it in ways that align with the DHS definition or agreed with the definition provided. However, several respondents indicated there had been dissatisfaction with the "federal" definition initially, as their understanding was that it did not include homegrown violent extremists, and some participants requested clarification on whether the definition included domestic actors. A very small number of participants excluded U.S. citizens as perpetrators in their definitions. This interpretation of violent extremism as coming only from outside the United States is important in recognizing how the term may be understood among local law enforcement.

Law enforcement participants were also asked to share their thoughts about the extent to which CVE is similar to or different from countering other types of crime. The vast majority of respondents differentiated between routine criminal behavior and violent extremism, with the latter being driven by a particular ideology, religious belief, or political goal. A few respondents focused primarily on political agendas, while others focused on religious motivations. As one officer said, "It's the motivation that is different, the political, religious, and ideology. They want to cause harm to as many people as possible and are prepared to die willingly to do it."

State of Preparedness

Law Enforcement Executives

Executives tended to feel more prepared to prevent major international terrorist attacks than attacks by homegrown violent extremists and lone offenders, and more than one executive wondered if any department could ever be truly prepared. Executives at six of the sites visited said they feel prepared to counter violent extremism, depending on the type and scale of the operation, if it is pre-operational, and if key players are involved. They noted that the current strategies in place are not fool-proof. For example, frontline officers tend to become complacent, procedures for reporting suspicious activity may be ineffective, and police departments are

Figure 5. What is needed to counter violent extremism, law enforcement

reliant on good sources or a vigilant public. For these executives, staffing, intelligence, resources, and interagency cooperation all contribute to preparedness.

Executives at seven sites said they did not feel prepared, citing significant gaps between their view of what it means to be prepared and the current abilities of their departments. Five executives identified the gaps as training-related. They thought that departments lack the skills to counter violent extremism effectively, due in no small part to the relative newness of this approach, a lack of deep understanding of it by law enforcement, and competing priorities. For officers, "Drug and gangs grab and keep their attention." Three executives noted insufficient outreach to the community and public awareness. Two executives viewed local law enforcement as serving a supporting role in CVE, relying on the JTTF and federal agencies to fully address it. Other executives cited a lack of sufficient resources, information stove-pipes, too many vulnerabilities in their cities, and laws in place that limit intelligence collection without a criminal nexus.

Law Enforcement Investigators

Investigators across six sites said they felt prepared to counter violent extremism. However, investigators at two of these sites said their role in CVE would be limited, and investigators at three of these sites focused on their ability to respond after an incident occurs. In these cases, though, the investigators felt prepared because the necessary policies were in place, and they knew what was expected of them. Other investigators at those sites stated that information sharing is key, though ultimately, any extremist-related incidents would be handled by intelligence units in cooperation with federal agencies.

At three sites, other investigators said they felt prepared because of the level of support they receive from the community, community awareness, and a locally controlled community outreach program that focuses on threats. At these locations, investigators noted that they are in a position to know about groups before they have acted, and that such knowledge is taken seriously.

Investigators across 11 locations stated they did not feel prepared to counter violent extremism. Law enforcement's traditional focus on responding to incidents led five investigators to feel unprepared. Some investigators explained that when violent extremists work in groups it makes the process of identification much easier because people like to talk. However, they noted that a "tight-knit group within a community that is already standoffish from law enforcement" is difficult to identify. According to participants, establishing relationships with various communities and training officers to develop those relationships is a challenging task. At one site, it was mentioned that developing cooperation between religious organizations and law enforcement has not gone beyond preliminary stages despite efforts; at another site, law enforcement was described as not being comfortable conducting outreach and following up on reports. CVE is not seen as a priority by chiefs and other administrators according to investigators at a number of sites. Lack of resources, insufficient staffing and operational knowledge, and fewer tips were all mentioned as contributing to investigators feeling unprepared.

While some investigators said they felt prepared due to tools such as SARs, the fusion center, and community engagement teams, they noted that they are only prepared to deal with "anything they find out about." Other investigators reported challenges establishing a criminal predicate when activities are generally protected, particularly in jurisdictions that have strict information sharing laws.

Law Enforcement Frontline Officers

Patrol and community resource officers at seven sites said they felt prepared to counter violent extremism. At one site, the scope of the threat was described as small enough that law enforcement can address it. Officers also mentioned feeling prepared to respond to incidents because they have standard operating procedures and coordination with private sector entities. Officers who feel prepared cited the following reasons:

- Community engagement and support;
- Training and awareness, including for reporting;
- Information sharing among law enforcement agencies, including good intelligence; and
- Departments committed to pre-operational planning and information sharing.

Other patrol and community resource officers across 11 sites said that they do not feel prepared to counter violent extremism. Officers often noted that law enforcement is response-oriented and departments lack necessary resources, including funding and staffing. A few officers felt very strongly that attacks cannot be prevented. Other officers deem training to counter violent extremism insufficient. Others point to limited trust between communities and law enforcement.

Many frontline officers said that CVE is not fully within the police culture and that this can make CVE a non-priority, whether by accident or by design. According to some frontline officers, leadership decisions can create institutional barriers that directly or indirectly affect information dissemination and, for patrol officers, the ability to follow up on suspicious activity. Additionally, officers may not see CVE as one of their duties and may not have any incentive to participate. Other issues described as impeding effective CVE included a lack of information sharing, weak coordination and communication among law enforcement agencies (and even among officers within a department at times), and hostility toward DHS initiatives in some local political climates.

Training to Counter Violent Extremism

Respondents were asked questions about training they had received on violent extremism and CVE. This section presents selected findings from these training-related questions. CVE-specific training and discussions around its availability are presented first. Comments on CVE-related training, or training that is not labeled CVE, but is understood to promote the aims of CVE, follow. Training delivered by specific federal agencies is then discussed.

CVE-specific Training

Law enforcement executives expressed a wide variety of views about the availability of CVE-specific training. While some stated that CVE training is widely available from a variety of sources and more CVE-specific training is available now than in the past, others stated that there is not much training on CVE and CVE outreach available and that a lot of what available is "not good." Another executive had heard about CVE training but was unsure what those trainings covered, while others did not know what "countering violent extremism" meant and thus were unaware of, and had not participated in or offered, any training concerning it. One of the issues related to developing CVE training, according to one participant, is the lack of an agreed-upon lesson plan or curriculum; no group is coming together saying, "This is the way to do it."

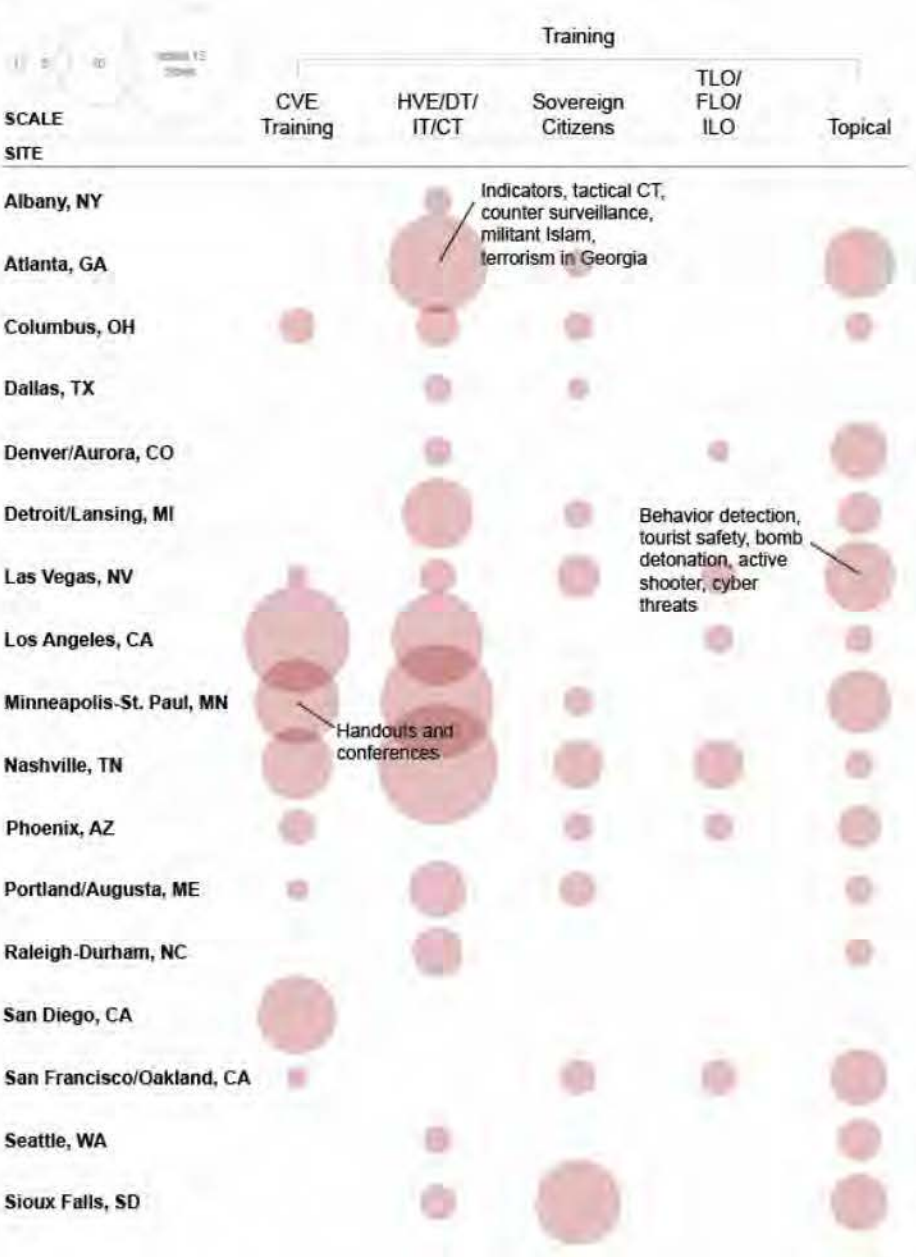
Many officers had participated in cultural awareness training and basic CT-type training, but little to no training on CVE. Officers at all levels wondered what CVE training included, often grouping CVE training in with training

on CT, terrorism, or extremism, broader cultural training, NSI/SAR training, and TLO training. According to participants, training and information on cultural awareness—defined to include awareness of newer immigrant groups—sometimes are delivered by law enforcement officers who specialize in certain topics, but more often are delivered by outside training providers and government agencies.

Officers also mentioned attending terrorism-related courses that covered motorcycle gangs, terrorism, violent Islamist radicalization, traditional neo-Nazi skinheads, Sovereign Citizens, and a spectrum of other groups. In this awareness training, they typically have discussed the groups rather than adopting an operational perspective in how to counter their tactics.

Figure 6. CVE-related Training Mentioned by Law Enforcement (for illustrative purposes only)

This figure shows the types of training in which law enforcement respondents mentioned participating. The columns represent the training that respondents discussed, and the size of the bubble represents the number of references to each. CVE training relates specifically to training on how to counter violent extremism, and the largest clusters reflect where DHS has conducted or sponsored pilot trainings. HVE/DT/IT/CT training encompasses training on radicalization, terrorism, and counterterrorism, as well as other trainings related to violent extremism but not specifically countering it. Because it was such a prominent issue, Sovereign Citizen training also has its own column. The remaining columns include terrorism liaison officer (TLO), fusion liaison officer (FLO), and intelligence liaison officer (ILO) training, as well as other trainings that were viewed as relevant to violent extremism, but did not fit into the other categories.



Officers reported that the CVE training (broadly defined) offered is "pretty minimal," and that "there's no training for patrol officers." In general, the training focus for patrol officers is response training, such as full-gear demonstration management, rapid deployment, and active shooter training. Information, and the ability to identify known groups or even the knowledge that these types of groups exist, is not disseminated well enough among departments. As one officer said of such training, "I've had 20 hours in 17 years of training." Training opportunities for CVE (very broadly defined) have not caught up to the need. Officers stated that because it is "such an evolving process," the training offered is not consistent. A few officers said their departments could no longer provide CVE training in the form of training handouts due to legal restrictions. Some departments have an annual course on violent extremism with little follow-up throughout the year.

CVE-related Training

Officers often spoke of TLO courses that they, or others, have participated in when discussing training related to CVE. Officers also discussed NSI/SAR training as broadly related to CVE and noted receiving such training from the federal government and other providers. One officer reported that the class was helpful in that it provided information on what other things an average cop could pay attention to on a vehicle stop, other than "not getting shot," and how certain crimes may be indicative of something larger—for example, the theft of certain chemicals.

> *Well, they showed a, "Hey, if you stop this guy and he's got this," or, "If you wanna call and you saw this—is it crime?" "Do you do anything?" "Well, what if you add this to it?" That's what I like. He had a step by step, "Well, now are you interested?" "Well, now do you think this could be terrorism?" I thought he did a real good job and then because it showed, well, on face value, this might not be anything, but when you saw it go down to [this level], maybe you should pay attention [and] … just report it, what the heck. I mean what's a report …*

Officers have also participated in classes that discuss different cultures—and the differences between religions and religious practitioners—such as Sikhism and Islam. One department provided a three-hour block of training to 25 percent of its force on interacting with a specific immigrant community in its jurisdiction. The training was developed by the department's community response team with the goal of creating ties and ways to open communications with the community. In some departments, officers have also had opportunities to receive cultural awareness training from universities and other government agencies.

Training Offered by Federal Government Agencies

The section below summarizes comments participants made about CVE-specific or CVE-related trainings offered by the federal government. Findings in this section should be interpreted as individual reactions to the trainings and not as generalizations for other focus group participants or law enforcement in general.

Department of Homeland Security

A few officers discussed attending the CVE conference organized by DHS in Columbus. Attendees thought the majority of the conference was good and educational and that it allowed attendees to learn what is being done in other cities to see if it could be applied in their city. All thought the conference was directed to the wrong

audience, though, and questioned the applicability for all who attended. The audience, one noted, should have been frontline officers, who would have benefited more.

Other officers attended the pilot training provided by DHS in San Diego. Those who participated spoke about the need for more training like it. One participant noted,

> *The single greatest thing I liked about the training we got is we all … just weren't law enforcement talking about something we already knew about. That we got the community involved. That we got community leaders whether … we liked what they were going to say or not, we have to bring them into the picture or we'll never be able to address this issue.*

Attendees also viewed the working group sessions at the training positively as group exercises offered the opportunity to exchange information, especially with other agencies, offices, or divisions.

At the same time, some attendees were confused about what the training was for and what they were supposed to learn. For one officer, the training did not adequately address the different issues patrol officers face because of the diverse communities in their jurisdictions. The course, according to one interviewee, was designed to "let students struggle through things;" however, he noted that "cops learn differently" and it is important to let them know the course's objectives and "what is countering violent extremism and what is not."

Officers who participated in the DHS CVE Workshop in Minnesota had mixed views on its efficacy. One officer acknowledged that DHS and others have a big task, and that they are just getting started. Participants seemed to agree that while some of the information was good, it was not focused on "deliverable services and goods," or practical training, and as a result, was not very helpful.

Participants noted that many of the speakers spoke for too long and that presentations could have been condensed, allowing more time for questions. Others found the propensity for law enforcement to tell "war stories" to be less than helpful and instead asked that presenters with more knowledge of the community be available. At the same time, one participant thought the hands-on opportunities were good and appreciated the inclusion of scenarios.

A few officers attended the final DHS conference in San Diego. One of the participants found the conference very good, noting that it dealt with police duties and signs of radicalization. Another officer who attended the conference appreciated that it addressed the need for law enforcement to interact with other agencies and be out among the community.

Other comments addressed the reason for the conference, noting that some of it was about outreach, but also about how to build outreach. A few officers expressed frustration with what they perceived to be a lack of transparency or willingness to address issues that are not considered politically correct. For example, one officer felt that the conference trainer "danced around" an issue raised by one of the participants about the challenges of integrating a large immigrant population anywhere in the world, especially if that population has a particular national or religious background. One officer noted that DHS offered to provide free CVE training at the conference, and he was "still waiting" for that to materialize.

At one site, all of the law enforcement participants had attended DHS classes delivered by the DHS IO, and at other sites officers occasionally mentioned participating in training from DHS. These trainings included briefings,

an intelligence training class, and information on topics such as combating human smuggling. One officer expressed frustration with how DHS training is not targeted specifically for law enforcement.

Federal Bureau of Investigation

A few officers had participated in various FBI-sponsored trainings, including ones on source development, counterfeiting and extremism, and events that had occurred in their local area. Those who attended the training on local events thought it was more targeted to the broader public and private sector audiences. Another officer had taken a three-month training program at the FBI Academy and reported that it included a number of interesting segments that were very beneficial.

Figure 7. Training Providers Mentioned by Law Enforcement (for illustrative purposes only)

This chart shows the training providers that respondents discussed. Much of the training was provided by DHS, the FBI and DOJ, fusion centers, and ODNI. The remaining column represents training offered by the military, think tanks, academic institutions, police departments, and private organizations.

DOJ/SLATT

Officers generally described SLATT training favorably. One officer noted that the training topics are on point and that "SLATT is hitting the nail on the head there." Another mentioned that SLATT's case studies allow officers to go to a website and see one paragraph summarizing violent extremism incidents. Others stated that SLATT must include law enforcement in the process of developing training and information because they "know what cops need to know."

Fusion Centers

One executive remarked on the high quality and usefulness of a training on Sovereign Citizens prepared and delivered by the South Dakota Fusion Center, commenting that it was the "most valuable stuff they'd had lately" on Sovereign Citizens. Officers who participated in Sovereign Citizen trainings provided by the Northern California Regional Intelligence Center also found them good. Others mentioned valuable trainings on Sovereign Citizens provided by the Information Sharing and Analysis Center in North Carolina and at the Southern Nevada Counter-terrorism Center.

Training Needs

Many participants noted that law enforcement officers are a "tough audience," are "the most critical," and "have a short attention span." Because of their unique profession and the varied roles that officers play, flexibility in training is seen as important. This section presents the diverse training needs noted by law enforcement executives, investigators, and officers.

> Training for law enforcement, according to one community resource officer, does not have to be ***"so formal with thick books and big—big presentations; it can be small little clusters of training that could be valuable to the officer on the street."*** Small trainings, he argues, like the use of language or being introduced to local leaders on a consistent, regular basis, will have a greater impact than a one-time, large conference where the participants say, ***"'Isn't this great,'* and then move on."**

Training Relevant to the Community and the Job

Across all sites, law enforcement asked that training content be presented in a concrete, relatable way. For many, CVE is outside their past experiences or career scope, and as such, they stated that good training on CVE would define the issue and show why it is important and relevant to officers. According to participants, officers need to be able to identify what is in it for them. As one executive explained, "Law enforcement needs to know how to take what is told to him and apply it to his environment. They need local examples. 'Here's the information … '" Without these local examples, "it's as foreign as a foreign language." Officers noted that hearing only about issues in other parts of the country, with no connection or potential connection to their locality, undercuts an officer's motivation "to learn, retain, and expand on" what they learn on their own. If training is focused on the events at the federal level, without being brought down to the local level, one officer noted, "They are going to lose us, our attention."

According to officers, in addition to training that is relevant to the local context, training also has to be relevant to the particular job function of the officer and the length of time he or she has worked in law enforcement. Many officers recommended against one-size-fits-all training and instead suggested that training be developed to reflect how each functional area looks at the world. For example, one interviewee who works both with law

enforcement and a fusion center explained that the frontline officer needs operational information, the analyst needs to know if information is correct, and the intelligence officer needs to be CRCL compliant. Training that is adapted to the job will make it "more meaningful, with greater productivity. It will engage folks at those levels." Officers asked that training not be written "from the DHS/homeland security perspective. Do it from the street level or other levels."

For many officers, these "levels" include years of experience. As one executive said, "You have to know your audience. You can't deliver the same material to rookies and 20-year veterans and expect them to all stay engaged—they have different needs and bring different levels of understanding to the training. That's the quickest way to lose your audience, and I've see it happen a lot." Training on CVE, as one officer explained, should "not just be for specialized units, but for patrol. Something for boots on the ground and something for management. It can't progress if management doesn't understand and support it." One investigator stated that there is sufficient general awareness for those officers who have been in law enforcement since before 9/11. He noted that lessons on Islam were always provided at conferences and were possibly helpful for a younger group, but for individuals with more than a dozen years' experience, he wondered, "What do we train now?"

While many officers wanted training that spoke to their particular roles and levels of experience, in certain cases, training that brought together very different groups is considered useful. Though many noted that "cops like to be trained with cops," in some cases, officers and others thought highly of CVE training that brings together law enforcement and fire personnel, as well as law enforcement and the local community.

Case Studies and Exercises

Law enforcement personnel at all levels stated a preference for case studies because they are less theoretical, can be applied to the local context, and allow officers to "pull on experience." Case studies often provide opportunities to understand indicators and precursors and to bring "thought to action." Just as importantly, cases that permit officers to see where things went wrong are valued. As one investigator explained, the most memorable and engaging case studies are not built on successful cases:

> *You take a case where someone screwed up. It's a critique or debriefing. Those are the best. Take the critique and put a unit together to figure how they would deal with that and identify mistakes. Every year they go through every officer who was killed. They go through and figure out why and mistakes made. You learn from mistakes, not triumphs.*

Officers said they generally enjoy hands-on, scenario-based training that allows them to gain practical experience and get involved more than a presentation. The practical application helps create a common understanding among officers. As many officers noted, they tend to learn and retain more this way.

Training on Indicators, the Radicalization Process, and CVE

Executives noted a need for training on violent extremist groups, indicators and radicalization awareness, and what to expect when dealing with violent extremist groups. Likening the radicalization process to gang recruitment, one executive wanted CVE training that would "tie the principles to a conceptual framework that [officers] already have down." Another executive wanted case studies that provided insights into the radicalization process.

Investigators at over half of the sites noted a need for training on violent extremist groups and indicators. This "Violent Extremism 101" or other training could:

- Provide updated training on currently active groups or when indicators change, including information on new leaders as well as CDs and magazines that promote radicalization;
- Offer a broad overview of extremist groups and then delve into officers' operational process of noting and reporting concerns;
- Give further detail on the definition of violent extremism and its range across domestic and international groups and movements; and
- Offer a structured training program that provides a comprehensive view of individuals and groups that pose threats, rather than covering them piecemeal.

Frontline officers across six sites also cited a need for training on indicators and violent extremist groups, including Sovereign Citizens. This training could cover normal and abnormal behavior, group behaviors, and what "extremism looks like." For officer safety, it could present a discussion of groups' tactics, how to make traffic stops and serve warrants on these groups, and what to do differently with them as compared with the public at large. Officers cited the need for real-world scenarios that would allow them to shift their thinking from the paradigm of traditional criminal behavior to that of violent extremism. These scenarios could cover observation skills or behavior detection, as well as what officers can do, whom they can call, and what information to elicit upon contact. They could also include presentations from reformed extremists. One officer noted a need for training on the radicalization process in prisons and a new movement called "Pris-lam" (or "Pr-Islam").

Finally, executives cited a need for a CVE curriculum that all could agree on, but noted that the first class needs to be with the executives. At two sites, patrol officers cited a need for a CVE 101 course and CVE training after graduating from the training academy.

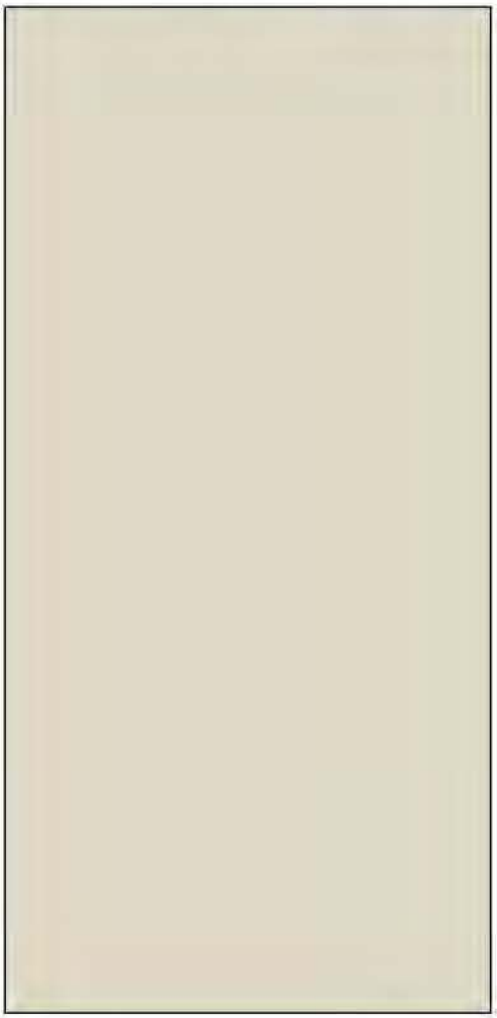
Training on Interacting with Different Communities

Executives cited a need for training officers on how to work with communities, particularly how to move beyond "the activists who ring your bell about once a week" and get to grassroots community members. Investigators noted similar needs and wanted to learn how to get communities to reach out to them when they have concerns. Other topics mentioned included how to approach more closed ethnic and religious communities and how to build relationships with such groups. More experienced patrol officers cited a need for training on conversational and human relations skills for younger law enforcement officers who may spend more time in their patrol cars and less time interacting with communities. Executives also mentioned a need to teach officers how to have a dialogue in an interview. Training is also needed on collaboration among all partners, including local, community, and federal partners, or, as an investigator stated, overcoming the "void" between local, state, and federal agencies.

Training on Other Topics

Executives noted a need for various types of other training, including a need for the community to be trained on awareness, as well on how to police itself; language skills and cultural diversity training; incident response, active shooter, and bomb-related training; and overall education and basic awareness training. A few executives could not think of training that was needed.

Investigators at a quarter of the sites asked for training on intelligence that covers how to gather and store information, as well as intelligence-related roles, skills, and equipment. Source development was also cited as a training need. Other training needs mentioned by investigators include a course on narco-terrorism, social media/Internet training, and training for officers dealing with harassment by Sovereign Citizens. Investigators also saw a need for training that provides success stories from across the country.



Frontline officers also specified they needed training in the following topics: suicide bomber mitigation tactics, standard operating procedures on emerging threats, and how to develop a training bulletin focused on violent extremism issues. Officers also noted that SAR training for the public and court personnel was needed, as well as upgraded SAR training for officers and written instructions for SAR training.

Training Delivery and Availability

In-person Presentation: Seminar/Lecture/Classroom

Law enforcement personnel emphasized a preference for classroom-based learning with intensive interactivity and hands-on activities. Rather than being "lectured to," many officers asked for more dialogue between the presenter and the participants. One executive most appreciated training that was not overly rigid. He noted, "Training has to be almost informal … conversational, and the moderator keeping things on track. Good valuable conversations are when they get off track." This dialogue was necessary, according to an investigator because, "The message has to be understood properly. Otherwise, it will lead to mistakes in the field."

Officers also reported that both an instructor's credentials and ability to teach are key factors in how law enforcement officers experience training. Repeatedly, participants said they want an instructor who is "credible," has subject matter expertise, and can relate to the audience. "Credible" instructors are generally considered those who are either former law enforcement or have hands-on experience with the particular topic being taught. Law enforcement also sought instructors who engaged the audience and who, for example, used PowerPoint as a tool, rather than as the training. As one executive noted, "The police wonder why they are sitting there when they can read the slides themselves."

Many officers explained that because trainers from the FBI and the federal government typically do not have local law enforcement experience and often provide only general, non-classified information (and emphasize that they are only providing the latter), local officers "stop listening" when training is delivered by such trainers. Officers tend also to be wary of academics and analysts. For law enforcement, they lack credibility and often speak in language that officers find difficult to understand. According to one executive, "Academics can be there, but I can't overstate the importance of credibility. It will make or break your case." Developing the capacity of local, internal trainers is a goal towards which some departments are working, and having the local trainer supported by federal training is a "good model."

> *"When [the training] first started, there was one slide with 28 acronyms. I knew one. The presenters, they rattle them off. You get frustrated, you start to tune them out. You start to fiddle with the materials and think, 'Clearly this isn't for me.' That is a huge need for improvement—the use of acronyms."*
>
> (Law enforcement investigator)

Law enforcement officers also stated that physical takeaways—in the form of contact lists and other materials—would be beneficial. Contact lists that include the trainer, subject matter experts, and other attendees "are the best things to get out of these trainings" and provide officers "another number to call to put [them] into contact with the right person." Other materials deemed helpful are PowerPoint handouts, lists of "dos and don'ts," lists of indicators or "what to look for," reference guides, and translation guides.

Briefings-as-training

Frontline officers typically receive training at regularly scheduled briefings, such as shift-based roll calls, where a supervisor or a trainer distributes materials, gives a short presentation, or plays a video. According to participants, the best way to provide information to officers is to make it "short, informative, hard-hitting, relevant, exciting, and make them feel like a part of something bigger." Short briefings, usually between five and 15 minutes, were recommended, because "officers can remember six-minute sound bites. They are not going to remember eight hours of training; they are probably only going to remember five minutes of it. And then you repeat things a lot."

Officers suggested that briefings could include short case studies that provide a summary of what an officer did to counter violent extremism; as one participant said, "This information has real meaning to the officers and describes how an officer did his job." Regularly scheduled briefings could also be part of a single training course, divided into four-week blocks, where each week there is a 10- to 15-minute briefing about groups followed up with examples. Briefings, according to a public safety officer, should be regular, but not daily, to ensure that interest does not wane.

Online Training – Self-paced or Facilitated

Though not a preference for most law enforcement participants, online training has become a viable and valuable method for disseminating training, particularly where resources and staffing are limited. It also complements the busy and unpredictable schedules inherent in police work. Executives noted that getting patrol officers off the street for six hours of training is difficult, but with online training, they can start, then stop, and come back. For those officers who have computer or Internet access in their patrol cars, online training can be done during an overtime 2 am shift or while "running traffic." Online trainings that include videos are also seen as effective, because trainers then know that everyone has seen that particular video. However, because of its

limitations, many officers, at all levels, were not enthusiastic about online training. Some described either watching others "click, click, click" their way through the screens or admitted to doing so themselves, then completing any test at the end by guessing at the answers. For others, online training was described as "good for a refresher," or when provided in conjunction with other methods, such as in-person training and briefings-as-training.

Increasing Attractiveness of Training

Patrol officers at one site suggested that officers would take CVE training more seriously if it provided credits and classes that are certified by the Commission on Peace Officer Standards and Training (POST). They suggested POST training certificates for continuing education through the fusion center.

Videos

Though law enforcement did not always prefer training delivered by video ("People groan" according to one investigator), many saw it as an effective method. For some, videos can accomplish in five minutes "what 45 minutes of talking would do—and even then they might not get it." They can also provide a break from paperwork. Videos are considered effective because their length can vary from a few minutes to hours, offering flexibility for different training needs and audiences, and they can be included as part of a larger training or a short, stand-alone lesson. Those officers who had participated in video-based training noted a preference for "real footage and not a low-paid actor or a government employee. People want to see real video." Real-life footage, according to one officer, "sticks with you more" and allows officers to analyze what occurred. Videos can also be provided to outside agencies or the general public who do not receive training but who can watch a video.

Training Availability

Executives cited a need for consistent, effective training that is free or fundable by Federal Emergency Management Agency (FEMA) grants. They also noted that the training organization should provide advanced notice to departments, ensure that training is delivered to everyone in the department, and make certain that it is tailored to different functions, in particular, the line staff. Investigators at a quarter of the sites also asked that training be delivered to patrol officers and other officers working the streets. As one investigator explained, "You want the most trained person" seeing a suspect vehicle or answering calls. Training for patrol would also develop their talents and allow them to "expand into a whole new lane." Training on CVE, as one investigator noted, appears to be limited to outreach officers. At three sites, patrol officers cited a need for frequent—possibly quarterly—and consistent training, or as described by one officer, "Booster shots throughout the year." Overall, officers wanted more training and training that was mandatory. These trainings could be short videos during roll call that cover topics such as "10 things to know" about particular cultures or indicators of violent extremism. Training content could include local laws and statutes as well, which will let officers know what they can and cannot record.

Training Challenges

Law enforcement most often cited challenges to effective training that related to organizational priorities, lack of opportunities, difficulties incorporating training on the job, individual priorities, and time and budget.

Organizational Priorities

Organizational priorities have an enormous impact on training. As many officers noted, buy-in from administrators is critical, particularly for new initiatives. Changes in leadership may lead to changes in strategic focus and allocation of staffing: As one officer said, "We'll have a new chief come, and he might say you don't need to have many detectives doing this. Might be a guy who wants to do more community policing. I had a lot of support from [the] last two chiefs. I don't know what is coming." As a patrol officer explained, "It boils down to the hot topic of the week. Whatever [the] chief's hot button is."

Leadership's priorities are often driven by the concerns of the community and local civic leadership. Across many sites, participants mentioned that communities are alarmed about car break-ins or other daily crime, not violent extremism. Spending "millions on trainings for things that may not happen as opposed to things that do" is a difficult sell for many law enforcement executives who get "beat up because of murder and rape, not terrorism."

Lack of Opportunities for Training

One major challenge facing law enforcement is the lack of opportunities for training beyond whatever mandatory training is required each year. This may be the result of departments not promoting non-mandatory training or simply that there are fewer available trainings. The ability to offer training can be constrained by a slow approval process at the federal and local levels, which requires "a lot of green lights" to be cleared. Training developed internally may not be offered due to leadership priorities or staffing levels. For example, one investigator reported that his 15-minute training for patrol officers on what intelligence teams do and when and how to flag suspicious comments and follow-up was denied.

While some officers noted that good courses are available, it is a matter of finding them. In some cases, officers must create training on their own. Some police departments are seeking to develop their own internal subject matter expertise by promoting a train-the-trainer policy that will allow them to train all officers in their department rather than just a few. Some officers viewed this positively; however, in at least one department, officers are assigned to training and then "become the expert on that topic," leading co-workers to say, "You're an expert in this today, right? *Okay*."

Incorporating Training on the Job

Law enforcement personnel repeatedly mentioned that they left trainings excited to apply their new knowledge and skills only to find it impossible to do so. Trainings that relate to current job duties, such as burglary, can be applied every day. However, when officers do not have opportunities to practice new skills because they "deal with 911 calls all day," they "revert back to the same officer" they were before the training. Ongoing training helps officers keep issues at the forefront of their minds, particularly when it is not something they deal with daily.

> *"You got your supervisor saying 'Why are you still on that call?' and you're like, 'Cause something just doesn't seem right.'*
>
> *'Have they broken any laws?'*
>
> *'Nope.'*
>
> *'Then go to your next call. You need to clear up.'"*
>
> (Law enforcement patrol)

Individual Priorities

Officers discussed how individual needs and interests determine training priorities. Officers, if given the opportunity, choose their limited, non-mandatory training based on career goals, such as becoming radar-certified or a drug detective. These officers view taking classes on violent extremism as a "waste" of those few available training hours: "If I want to be a drug detective, I want to take all my training that's focused on that. I don't want to waste my hours going to learn about terrorists." However, bringing such classes to departments would not count against limited training hours, because it is considered internal training. Officers who are required to attend classes can be unmotivated as well, as "someone has to want to be there before he learns anything. Some people may have been ordered to go."

Time and Budget

Finding time for officers to participate in training is a significant hurdle for many departments. Longer courses and those that require travel present a major burden, leading departments to turn to online, roll call, and other less time-intensive and costly training options. According to study participants, patrol officers appear to be disproportionally affected by training limits, as leadership needs officers on the street. However, those who work in specialized units, community engagement officers, and officers physically located in buildings appear to have an advantage when it comes to training, as do those who "have the ability to manipulate the system." One participant commented that staffing "is a big thing for us—we have limited training and a limited number of people to go to it." Dedicating time for officers to participate in training is difficult where departments are minimally staffed, since "officers can't take the whole shift off, and they have to plan for training that can cover multiple shifts. Cops have days off."

Training, according to many officers, is the first thing to go when budgets are reduced. Costs associated with off-site training—the officer's time, travel and lodging, and shift coverage—make off-site training unaffordable; instead, leadership pushes to have trainings held online and locally. Budget crises are not shared equally across departments, where, for some, training is on the back burner because posts have to be filled; at another department, they "can release someone for up to three days without creating a crunch." Even keeping officers on the street is a challenge for some departments with severe resource constraints. According to one patrol officer, departments may have traffic units only because "they have a grant for two officers." If grants provided for terrorism or outreach officers, "You're going to see a bunch of departments that have a terrorism outreach officer that they can get a grant for."

Grants and foundation funding offer opportunities for departments to cover the costs of training. However, securing and correctly spending these funds is difficult because for some training, "It is DHS training, but grants won't pay for it. The procedures haven't been followed with FEMA." In some cases, according to participants, the grant requirements are also quite burdensome and become inhibitors in and of themselves.

Sources of Information on Violent Extremism and Countering It

Best Sources of Information

Law enforcement were asked about their experiences receiving information on violent extremism and countering it, including the sources they value and turn to most often, their challenges with getting good information, and the information they need.

Local Community Sources

Executives considered community sources, whether law enforcement informants, confidential sources, or community religious and social organizations, to be among the best sources of information. Most often mentioned were the sources that law enforcement had cultivated, though a few executives noted that these sources are "few and far in-between." Local organizations, such as Planned Parenthood and religious leaders from local mosques and Sikh temples, were also considered good sources. Many investigators also reported that the best sources of information come from the local community, either as a result of outreach or investigations. Often these sources are regular people, public officials, neighborhoods, the corner store, and other businesses within the local community. One investigator said that kids in the community are a best source of information because "kids can see what doesn't look right." Another investigator noted that citizens will come forward when they recognize newcomers to the community who are trying to "stir things up" or who fail to become part of the community.

Many of the frontline officers also named the local community as the best sources of information and noted that these community contacts are often developed over time by building trust. Community contacts may also be more coincidental, as when officers stop by businesses and owners inform them of recent events.

At the same time others noted that community outreach, even extended outreach, does not always provide information. As one investigator explained, ongoing outreach and support to a local Muslim community had not led to a greater trust.

> *We've directed traffic for these guys, we've helped them across the street, we've done it for ten years, and finally our department got to a point where, "Hey, they might have to hire our office," because we've done this for ten years, we've, you know, gone to their luncheons, we've done everything … Constantly free. Footing the bill, sending on-duty people … but they've given us nothing. It's always when we go out there … [t]hey want you out, quickly, and that's just been my take on it, face value, and I've met many of them over there. They've had meals for us. They've had us over thanking us for everything. You know it's a lock down. You know you are escorted. You are, you are watched constantly when you are out there.*

One investigator noted that "people who have been in groups and left them" are one of the best sources of information about groups. In general, informants and criminal contacts were also mentioned as good sources of information. One officer who works on gangs in jails noted that his best sources are the ones who feel wronged by their group or the movement. "We have all kinds of sources coming in in the jails who want to get out early. We pass them along. But the best are those who have given their heart, and when their backs were against the wall, they were betrayed or abandoned by the people they would have died for."

Fusion Centers

Fusion centers were also often mentioned as a best source of information by executives, though with some caveats. Most who mentioned the fusion centers spoke about the weekly bulletins. While they were considered a best source, executives expressed concern that the information contained in them is cut and pasted from other fusion centers and is not relevant to their area. Some also found that information from fusion centers is not timely. While one executive found the senior intelligence analyst at his site's fusion center very helpful,

another executive noted that he does not get what he would like to see from his area's fusion center, as "information goes in, but does not come out." Still, of those who spoke of fusion centers, many saw them as a good mechanism to distribute information and tie information back to national operations.

Overall, investigators across nine sites named fusion centers as a best source of information. Investigators said that centers provide FBI bulletins, case-specific information of a "new thing to look out for," and information from other states about traveling individuals. One investigator said that information from the fusion centers in his state is timely, and another investigator believes that the fusion center in his state "does a little better job" than DHS and the FBI, as it serves as the focal point in disseminating information that is not public knowledge. One investigator appreciated the work that the fusion center had done in terms of developing products that are original. Information from one fusion center led an investigator to open a case on a Sovereign Citizen.

Frontline officers across six sites stated their best information about violent extremism and countering it comes from the fusion centers in their states. One officer noted that the fusion center is his only source of information currently. Fusion centers provide information, typically bulletins, on a regular basis to officers, usually through the department's leadership, TLOs, or through a department's Intranet. This information can come weekly, monthly, or as necessary. Fusion centers were described as providing good intelligence and information, including regional, area, and national perspectives; discussing techniques and tactics; and following up on officers' concerns. One officer, while expressing appreciation for the bulletins, suggested that better organization, with pertinent information up front that is relevant to the immediate area, would make the bulletins and their lengthy attachments easier to read.

Department of Homeland Security

The Department of Homeland Security was mentioned at four sites and by about a third of the executives interviewed as the best source for information about violent extremism and countering it. Often, this information came from the IO at the fusion center, the Office of Intelligence and Analysis, or more generally their "relationship" with DHS. Specific products mentioned included the DHS bulletins; the daily report ("DHS daily reports are fabulous"); press releases (one executive stated that she looks there for information relevant to her city); and classified products. One executive, however, stated that unclassified information often included so many "PC [politically correct] checks" that "it is no longer relevant."

Though a few investigators spoke of DHS as a best source of information, others noted either that the information it provided—along with that from the rest of the federal government—was not useful in opening cases or that the information was readily available on the news. As one investigator explained, information from DHS is open source and they "get the same thing over and over again from different people." Another investigator said that "everyone is trying to produce the same thing, and DHS is no different. They're good at cranking out product one day after everyone else and tweaking it."

Frontline officers across five sites reported that their best information comes from DHS bulletins, pamphlets, and other intelligence DHS provides. One said that the DHS IO at the area fusion center provided a lot of good information. Another officer explained that getting information from DHS is preferable to the FBI, as they have fewer "hoops to jump through."

Federal Bureau of Investigations/JTTF

At five sites, executives cited the FBI as a best source of information for their bulletins and classified information. One executive views the FBI as the best source among all of the federal partners, while another explained that they are a best source because of the relationship he has with them. Investigators at four sites believe that the FBI is a best source of information, whether this information comes from meetings, bulletins, or the FBI's general willingness to answer questions. Meetings with the FBI are considered by some officers to be a good source of information; however, some mentioned that the meetings are not normally held in a timely manner, leading one officer to see a trade-off between them and other, quicker sources of information. The FBI was also viewed as not writing for the street officer; its products are more "academic," according to one investigator. He noted that the FBI's products are classified and do not reach local law enforcement, amid concern that a "Law Enforcement Only" distribution would not be properly secured by officers. A few frontline officers also cited the FBI and its bulletins as the best source of information.

Some executives described the JTTF as a good source of information, though typically because they had officers assigned to the taskforce. While a few investigators mentioned the JTTF in the context of best sources of information, one noted that the information provided is only as good as the officer assigned to the JTTF. One investigator was clearly satisfied with his department's JTTF officers, stating that each agency needs someone to participate in the JTTF. His assigned officers bring back information, letting officers know that "[t]his might affect you guys." In regards to finding specific information on violent extremism, other officers mentioned the JTTF, with whom they have developed strong working relationships. Joint FBI and JTTF bulletins that contain local information are seen as particularly helpful. This is especially true when they are available online, which helps with the timeliness of information. One officer mentioned using resources from the National Institute of Justice at DOJ.

Other Federal Sources

In addition to DHS, fusion centers, the FBI, and DOJ, executives also said that they relied on information from the NCTC; ITACG; Coast Guard Maritime two-page briefer, which includes one page for line officers and one page for executives; and National Warning System. While one investigator receives information from the NSI—"some of it useful"—others were much more general, citing the federal government as a best source. The federal agencies produce a lot of products, and they are well done, according to one investigator. However, he noted, "There is more awareness. But no answers. You can write about al-Qa'ida, but how do you find the al-Qa'ida cell? But they don't have all the answers; there's no end all and be all."

Law Enforcement Online Sites and Databases

Executives said that online sources that are official or targeted to law enforcement are also best sources of information. These include HSIN, COPLINK, and RISS, and in particular their communities of interest, LEO.gov, and Police One. However, one executive who used these sites noted that groups or communities of interest that are commonly used tend to provide the best exchange of information, whereas less commonly used ones have much less value. He went on to say that these online sources seem to be a "little like an 'arms race' between the providers." He explained that information is splintered with each site providing only a portion of the picture. One executive thought that LEO.gov was a wealth of information but underutilized because it is an effort to go to the site and it is "a pain" to even get a log-in.

Investigators said they have found access to state and national databases to be helpful. One investigator explained that they actively use criminal sources and databases, supplementing their "good old-fashioned police work" with creative online research.

Frontline officers found HSIN, InfraGard, the Regional Organized Crime Information Center, and LEO.gov to be the best sources of information. Other law enforcement-related websites mentioned included Officer.com, Police One, and SLATT. One officer said he found SLATT more reliable than HSIN, as HSIN contains more news reports. Two officers mentioned the DHS CVE portal as the best source of information, all on outreach, but noted that it "has lots of information and case studies, but it's completely overwhelming. You can find anything related to CVE, but you have to sift through a lot of stuff." Others cited a number of barriers to using the portal, including the length of time it takes to set up an account. One participant said that this is "a lot of trouble for cops" who are focused on arrests and getting "tick marks." In particular, the inability to bookmark specific content is seen as a weakness of the site, because it can take a long time to find the same information again.

Open Source Information

Executives also cited open source information and the media as best sources of information. One executive stated that the media "do police work better than police officers" and the fusion centers.

At five sites, investigators viewed the media as providing one of the best sources of information, and in one case, more so than DHS, LEO, and HSIN. News sources mentioned included Fox News, CNN, or local news outlets. Frontline line officers also noted local and national news outlets as their best sources of information. Investigators at one site noted that when information is not disseminated in their departments, local news has provided "most of my training" and "briefed me a few times." For these investigators, news organizations provide more up-to-date information and, on some occasions, when information is provided in advance to law enforcement, it is on the news within the hour.

Many investigators and frontline officers cited open sources as the best source of information. A few investigators agreed that they "live by online." One investigator had conducted a search on CVE in the United Kingdom, ultimately reaching out to a think tank run by former extremists. More than a few investigators were particularly impressed by the wealth of information available on the Internet and social media, including Facebook, Twitter, and blogs. Frontline officers noted these as well as Google.

Officers who work with immigrant communities noted that they are aware of the impact that overseas events can have on their community, and as a result, they follow world news related to, in this case, Somalia.

Law Enforcement Meetings and Networking

Local law enforcement meetings and networking were often mentioned by investigators and frontline officers as one of the best sources of information. At a regular law enforcement association meeting that focuses on gangs, one investigator explained, each session includes a two-hour presentation and then information sharing. He said that these meetings are very helpful for solving crimes; he has seen homicides solved in those meetings because "someone knows where this guy hangs out or who he sees." A few investigators spoke of attending over ten meetings per month in order to share information; they see these meetings as extremely important because of the contacts they make. Meetings and one-hour "lunch and learns" with security professionals provide

networking opportunities and connect "a face to a name," which trickles down and helps develop sources. Law enforcement at many sites mentioned this connectivity across law enforcement agencies and with private sector partners. One group meets every other month for training and information sharing purposes. The Major Cities Chief Intel Commanders group was also mentioned as an important source of information. Executives said that they also relied on briefings and case coordination meetings through which they can "close the loop" and can hear how an officer started a case, and that "helps steer our own training."

Other Local Law Enforcement

For many investigators and frontline officers, other law enforcement agencies and officers are one of the best sources of information on violent extremism and countering it. In particular, officers found experienced officers to be the most helpful. Officers who are embedded in, or have deep and personally gained cultural knowledge of, communities that historically have been closed off to law enforcement, such as outlaw gangs, the Somali community, and Middle Eastern Muslim communities, serve as real—and trusted—sources of information. One officer had participated in a course, "Islam for Law Enforcement," taught by a fellow Palestinian-born officer. He explained that this officer's deep cultural knowledge, combined with his law enforcement perspective, allowed him to explain complicated community issues in a way that officers could understand. Another officer shared that officers embedded in communities understand community dynamics, know community leaders (or "shot callers"), and can provide insight and context to communities and issues that are not well understood. As many indicated, one dedicated officer who has ongoing and consistent relations with a designated community will tend to build a rapport with that community, as compared to whichever officers are available for calls or community events. As the officer noted, "It's one of those manpower things."

Investigators and officers also rely on patrol and other law enforcement agencies to provide tips and leads. Frontline officers are in people's homes every day, and many officers noted that "cops are attuned to what is wrong." If officers are educated on the indicators of violent extremism, they will be able to "stabilize a scene or at least filter it up—whatever they do, as long as they don't gloss over it."

Investigators thought that information that came via email, as long as it contained "actual information of whatever took place" was also a good source of information. According to one investigator, email, "forwarded 500 times over," still has value as officers can read the subject line and determine if the email is of interest to them, or not. Roll call briefs were also mentioned as a best source of information, although only the precursor information they provide was considered specific to CVE.

SARs and Bulletins

At two sites, patrol officers mentioned SAR reports as a best source of information as they provide current awareness of issues in their cities. Summaries of reported SARs are provided to law enforcement at one site twice a week. These reports can serve as a back-up source of information when a particular point of contact is away. Bulletins, in general, were viewed as a best source of information by officers across sites, though more than a few officers took issue with how they were written. Officers also mentioned bulletins from their criminal intelligence unit and their TLO watch officer. Additionally, officers found debriefs about recent events to be a good source of information:

> *It's a heads up for the future. It can show one string of an event so [the officers] can look for it in the future. Even a synopsis—what went down and how it ended. That's enough for cops to know that this is happening. Otherwise, they begin to think that it isn't happening. A short summary—you know cops—we'll get through first page and then quit if it is longer.*

Academic Sources and Other Organizations

Investigators who used academic sources, such as studies or research, had been introduced to them as part of training, as part of academic experience, or as part of relationships developed with academics, such as professors who teach about the Middle East. As one investigator noted, "There is no Rolodex of contacts" for academia.

Frontline officers reported using academic sources that were generally related to increasing knowledge about communities, including information provided by the Naval Postgraduate School. Pursuing information outside of the department was occasionally described as an individual effort and not something many officers do. One officer mentioned attending a conference of the East African Area Studies Group. According to the officer, the group's members have helped law enforcement understand the region.

In addition, some officers mentioned information from advocacy and other organizations as best sources of information. One officer found the ADL's magazine, Intelligence, very good, with good information on the "underworld, white supremacists, anti-government groups." Other officers mentioned using information from organizations such as the Arizona People Acting for a Safer Society, SPLC, the American Society for Individual Security, and the Association of Threat Assessment Professionals.

Problems Getting Good Information

No Problems

Executives across five sites perceived no issues with getting good information about violent extremism or countering it. A few felt that this was due to effective liaisons, whether at the JTTF, the fusion center, or other law enforcement agencies. While policies or laws may inhibit sharing, two executives stated that they still received information from state agencies or the FBI when it was needed. At one site, the executive explained, "Sometimes I hear that there are relationships between the FBI, DHS, and local law enforcement that aren't so good. But that's not the case here. We have excellent relationships, and so we get what we need."

Investigators at four sites and frontline officers at five sites said that they have no problems with getting information. At one site, this was said to be due to its small size, where everyone is known and there is continuity and connection. Other patrol officers said the flow of information is good, though one officer explained that he "can't judge the information; I can just say that this is the information that is there. I can't validate it."

Information Sharing

Access to Classified Information

> *"I'm like a hungry dog. I don't mind a cold biscuit, just give me something."*
>
> (Law enforcement investigator on receiving feedback)

> *"It's like wandering around without a flashlight."*
>
> (Law enforcement investigator on not receiving feedback on information provided or knowing what information to provide)

Access to classified information was mentioned as an issue across all sites, though it was often presented in more general terms of information sharing, sharing quality information, and feedback from federal partners. Executives across five sites saw the classification of information as a problem, though it did not always directly affect them. One executive who received regular classified briefings noted, "This is not the way around the rest of the department," as only a handful of officers have clearances. Though executives understood the national security implications of sharing information and agreed that sources and methods need to be protected, they said that there is still a need for information, particularly information that requires immediate action from the local community (such as during a terrorist threat) and accessible information for local law enforcement, emergency management services, and fire communities. First responders are the first to arrive at scenes, but they are often not privy to classified information, including information about the constantly changing trends and techniques of violent extremists. One executive noted that DHS's tear-line approach is designed to provide this information, but it is still a problem because "people are looking for hidden agendas." Other officers discussed potential opportunities to receive Sensitive But Unclassified information that could provide more specific information because of "higher tear-lines," but they have not yet seen it.

Several participants expressed hope that, as cities develop their own threat domains through the National Criminal Intelligence Enterprise and begin to collect information against those identified threats, the FBI, Drug Enforcement Agency, and others will be more willing to share information on these threats. In such cases, local law enforcement would "have the right and the need to know." This focused sharing, in their view, would increase the quality of information and limit the "white noise" of too much information.

Law enforcement at most sites acknowledged that they saw information sharing with the federal government as an issue. For many participants, sharing is one-sided: "What goes up goes up, and nothing comes down." Law enforcement often singled out the FBI. Even at a site where they "have one of the better [FBI] offices," participants described the Bureau as a "huge issue" and "the biggest obstacle" in sharing information with local partners. Law enforcement relationships with their local JTTF tended to be better, with investigators stating the JTTFs "usually try and accommodate" at least one of their officers and provide information. However, some investigators said that they rarely, if ever, receive anything back after sharing case information. Some executives noted that the JTTF "could do a better job of reaching out." They would rather hear, "We know that this is going on, but we can't talk about it" than, "We don't know what you are talking about." It was mentioned that local officers, in part because of these difficult relationships, may keep cases and information "close to the chest" and in-house, making arrests on their own when help could have been needed and offered.

Receiving feedback from other agencies was described as challenging as well. Officers at a few sites said they rarely receive feedback from SARs. While many officers spoke highly of the relationships they have with other

local law enforcement agencies, officers did note that problems sharing information also happens between state and local government agencies. This may be the result of intentional withholding. For example, one participant who works with jails and prisons has found that corrections officers often do not want to reveal sources. Local officers may not share information because "they want to look good." It may also be the result of a lack of coordinated information sharing because there is no database or portal that serves as a nexus for other databases.

Many officers recognize that federal agencies do not share information due to concerns about damaging investigations and cases. However, officers thought other issues were also at play, including a lack of trust and perceptions by federal agencies that local law enforcement officers are not qualified. One officer, after apologizing for being so direct, said, "I think the Feds act like we don't know what we're doing, that we're just local yokels." He relayed discussions he has had with former federal agents and noted that the only difference between federal and local law enforcement is "they have money and we don't." One officer perceives the federal/local issue to be similar to the trust barriers between the police and the public.

> *"When the FBI knocks on the door, you're in trouble, or they're there to develop sources. The community tells us they can't trust [the FBI]."*
>
> (Law enforcement investigator on working with the FBI on community-related issues)

Information Overload

Executives at five sites and investigators at six sites reported issues with too much information. Law enforcement are "overloaded" and "overburdened with information," possibly, as one executive said, because people are afraid to sit on information, thus sending everything out, leading to officers becoming "callous" or inured to information that is shared. Though executives were often appreciative, too much information, described by one executive as "white noise," makes it difficult to find specific information that is relevant or needed. Federal agencies may ask local law enforcement to "read between the lines" in order to understand a classified threat, but executives would rather have straightforward answers.

To demonstrate how much information they received, more than a few investigators pulled out their mobile phones and brought up their email accounts, running through—in general terms—who was sending what and why it was not important. One investigator noted that with electronic delivery of information, the ease of technology has led to officers "struggling" to process the information. Investigators scan emails, but unless they are flagged as important or are relevant to their area, may not read them. In some cases, there can be 10 bulletins a day from just one source. Investigators said that they get so many alerts that they can "spend the whole day reading" them. Officers believe that there is "plenty of superficial information … for the purposes of saying, 'Well, we're sharing information.'"

> One investigator who disseminates information highlights the relevant pages and briefly summarizes why it is important to read, along with the main points—**"Page 16. Read it because this is what you need out of this. Bad guy does this."** He said he has a "surprising number" of officers who read his emails and print out the information, because he had assumed that they delete them.

Even with this information overload, investigators noted that frontline officers are not getting information; rather, it is intelligence units that receive information from and cooperate with federal agencies. Often, one investigator explained, everything remains classified, going from the FBI to the Task

Force, "but whether it has an impact depends on if it gets to the street." Those who have access to classified information and who have been frontline officers are particularly frustrated with being unable to share information with those who need it. One investigator, expressing frustration, complained that "the news is reporting information that I can't share."

Quality, Delivery, and Format of Information

Executives, investigators, and frontline officers discussed the quality of information they receive, how it is prepared, and its delivery. Executives tended to find content to be "watered down," "no longer relevant—completely vanilla," and "too vague and generalized." As one executive shared, "By the time it's unclassified, you can't tell what they are getting at—'Avoid people who might be a threat.'" Investigators at seven sites found content to be "stripped down" to the point that officers are not getting the complete picture. They said that information is outdated, too lengthy, or neither relevant nor easily translatable to a new environment. Some frontline officers, who receive information from federal partners, considered the information to be "whitewashed and useless" and "late." Some officers said they were not receiving federal information at all. Officers tend to come across information relevant to their jurisdictions through indictments, charges, or the news. Many officers said that information that is shared is "not much different than what is on the news."

How information is formatted was mentioned as well. One investigator explained that for information to be clearly presented, it requires more than a few bullet points, but "busy people won't read four paragraphs … Be short and concise." Frontline officers at five sites said that the material they receive may be good, but the long bulletins, particularly when not warranted, are difficult for them to read. As one patrol officer explained, "The first thing an officer looks at is how many pages is it. Oh, that's two pages. Delete. Because again, when I get out of roll call, I gotta get five traffic stops a day, and I gotta serve two warrants, so, no. Delete."

Language and presentation were mentioned as making bulletins difficult to read as well, and officers asked for some type of structured format that does not include classification or police jargon, such as "reference to same and affirmation." Officers said that they found bulletins that had "catchy" titles, were written in plain language and were straightforward summaries of the issue ("This dude is doing bad stuff, and he's doing it this way; this is what you need to counter it") were most useful.

Patrol officers said that they would prefer for more direct communications. More than one officer asked if there was a way to streamline bulletins through one coordinated entity.

Web-based Resources and Databases

A couple of executives cited issues with LEO.gov. One thought it contained "great information" while the other said that he looks on the site and "there's nothing there." However, both mentioned issues with logging in. Investigators at one site mentioned the numerous websites—HSIN, LEO, TripWire, e-Guardian, and others—and the passwords needed for them. They questioned the soundness of a strategy that has information and interaction spread over multiple sites. They also wondered if it was possible to consolidate the sites or set up one central site. At some of the sites, investigators experience challenges when working with databases and said that this was either because of a highly complex process for logging in or because navigation is difficult. One investigator spoke about the multi-day clearance process needed to use a database, which typically becomes an issue because of his need for immediate information. Another investigator noted problems getting other officers

to use HSIN. Though a "great platform," he said it is analysts—more so than officers—who will visit the site on a daily basis. He noted that part of the problem stems from a lack of individual initiative, as officers, not wanting to be inundated, unsubscribe from distribution lists or stop looking at emails and "do not have the discipline" to visit a site such as HSIN every day. Opinions contrasted on the usability of portals for law enforcement: one executive stated that "portals are useless," while others saw the utility in having portals available and in squad cars.

Other Problems Getting Good Information

Locations with few minority officers cited this as a problem in getting good information, particularly where immigrant and refugee communities are growing. Officers in one department explained that there are no African officers or a single person who can speak Somali or Swahili. Recruiting efforts have failed due to lack of qualifications or lack of interest. Even where departments have minority officers who have unique skills or backgrounds, such as speaking Arabic or being of Arab descent, staffing needs may lead departments to assign those officers to areas where such qualities are not fully appreciated.

Internal Dissemination

Patrol officers at many of the sites reported that information is not being disseminated to the patrol level in their departments. Officers explained that external information that begins at the top of their chain of command usually stops there as well. As one officer who had been detailed to a fusion center explained, "I would forward information to the chief. Then it would just die there. He wouldn't send it out to the whole department, and some places do. I think more don't than do." Patrol officers at one site noted that their deputy chief makes a great deal of effort to disseminate information to patrol, but "it is not usually coming down below" from other leadership. Participants took care to explain that even if information is disseminated, officers will not always read it, and many expect that it will be deleted, but at some point "it's like the information just stops." Frontline officers at most sites reported that patrol officers at the street level are not "in the loop" and "are the last to know." Rather than rely on information that is "filtered through a couple of people," officers thought it would be good to have access to a database where officers can "pull" information and not have to rely on having that information "pushed" out to them.

Sharing between the patrol division and investigations was discussed as an issue, as was sharing within units. At one site, officers explained that fears about internal affairs complaints have led to a "sterile environment" with less communication between officers and commands, and this "has really put a wall between everybody."

Within one department, officers reported that there is "no line of communication" for CVE issues and that they "don't even know who to go to in [their] department about that information." Their department provides no information, and were they to inquire about it, they would probably be asked, "Why are you asking?" As these officers explained, "You won't find it written down anywhere, but we're not supposed to inquire, push buttons, or put too much effort into certain ... groups."

Other Barriers to Getting Good Information

At one site, one of the biggest problems with getting good information was the legal limitations on information sharing. As investigators and others at this site explained, information becomes public if it is shared by local law enforcement agencies with federal or other agencies. As a result, communications break down. This has implications for the CVE strategy and its tools, such as SARs, noted one investigator, because officers "feel guilty

and do not want to appear as if they are targeting a certain group" or be labeled as someone who does. Because the environment at this site does not allow sharing, law enforcement lack the "teeth" they need to operate SARs, and it becomes a "hollow initiative." These laws also inhibit sharing ongoing investigation information with local departments.

One investigator spoke about the challenges facing the fusion center in his state and why he does not use it as a source of information. These challenges, which include a limited budget, limited staffing, limited resources, and thus no leverage, have a direct impact on the fusion center's ability to collect and share information. He said that some of the major law enforcement agencies in the state will not share with the fusion center, and other major law enforcement agencies will not use them as a source for information.

Investigators at a few sites also spoke about the "need to have the right contacts" to get information. As one investigator explained, "If your specific liaison is not here, then you end up dialing 20 different numbers to try and find the right person." Another investigator noted similar issues and said that getting information is not a problem, "it's just that you have to know what to ask for—and ask for it." One officer shared that "the media is the most feared aspect of not sharing."

Information Needs

Law enforcement across all levels noted a need for timely information and intelligence that is disseminated regularly and has greater relevance to their specific regions and communities. They asked for products that include case studies, trends, and patterns of violent extremism activity; what is lawful conduct and collection; and how local law enforcement can contribute to CVE. They asked that fire and emergency management communities be involved as well. Others noted that they do not need information, as what they have is sufficient or they "do not know what they do not know."

Final Thoughts and Recommendations

Participants were asked a final question[12] designed to elicit their thoughts on the most critical issues that need to be addressed in order to improve efforts to counter violent extremism. While participants' responses have been incorporated in the report or in the annex, these "final thoughts" also serve as recommendations and those most often mentioned are presented here. These are then followed by the recommendations of the research team based on analysis of the data collected and experiences in the field.

Fusion Centers

Training: Participants recommended that lead agencies involved in CVE provide access to quality training that defines CVE, offers an interactive model, and is locally relevant. They recommended that a comprehensive directory of available CVE training be provided with some indication of how well that training has been received by past participants and the level of difficulty of the training (beginner, intermediate, or advanced).

They also recommended that a train-the-trainer type of program be developed that would enable the provision of training services to be further decentralized. This would improve the subject matter expertise of the centers' staff and create an expanded role for fusion centers beyond their training for TLOs and the other targeted training they provide. Also recommended was the development of a degree program that trains individuals to work in fusion centers as analysts.

Information: Participants recommended that agencies leading CVE efforts improve information sharing and communication at all levels. They recommended that national and local databases on violent extremists be compiled and provided. These would include information on the methods of known groups and individuals and statistics on their operations, much like the gang databases available to many in law enforcement.

CVE Policy: Participants recommended that there be greater clarity about CVE policy and its implementation. A few also requested clarification on the roles and responsibilities of fusion centers in CVE be provided. They recommended that reforms be made in how federal, state, and local agencies coordinate and interact, as well as with security clearance protocols. They also recommended integrating fusion centers into NCTC's outreach to state agencies beyond law enforcement to achieve a more comprehensive approach to CVE and other crimes.

The Public: Participants recommended that efforts to educate the public on CVE and the roles of law enforcement and fusion centers be increased.

Resources, Funding, and Staffing: Participants recommended that more resources be provided to fusion centers so that they can more effectively counter violent extremism. Resources, such as funding, are needed to sustain the current staffing levels in order to maintain operations, increase the number of personnel to expand operations, and provide greater educational and training opportunities for staff.

[12] Participants were asked what thoughts, concerns, or needs they would express to the person in charge of CVE or what they would do if they were in charge of CVE for a day.

Final Thoughts and Recommendations

Law Enforcement

Training: Participants recommended that training on CVE be provided and be provided to all law enforcement officers. They recommended that this training be focused on identifying behaviors, be specific to particular areas of the country, be run by experts and former law enforcement, and offer credits toward POST-certified degrees.

Information: Participants recommended that more information, and more quality information, on CVE be provided and that federal partners facilitate better, more timely information and intelligence sharing. Participants also recommended that the federal government engage in more truthful, transparent, and less politically correct communications about CVE.

Participants recommended that federal partners provide greater clarity about the type of information they are looking for from local law enforcement, and how that information should be reported. They also asked that feedback be provided after information is shared vertically. In addition, participants recommended developing a single system or platform that integrates local, state, and federal databases.

CVE Policy and Implementation: Participants recommended a number of strategies to help successfully implement CVE efforts. These include creating a county-level CVE task force; having a regional CVE representative who visits locations quarterly to encourage dialogue; and mandating that every law enforcement agency have an outreach program, dedicated or collateral, with the salaries of outreach personnel funded by a federal program. Participants also recommended that ongoing attention be paid to CVE in order to understand it, to ensure that the mission and goals are understood by all, and to convince people that violent extremism is serious but that the transition to radicalization can be countered.

Participants also asked that clear leadership for CVE be established and that CVE policy include a prominent role for local law enforcement. Participants recommended that greater weight be given to the changing role of law enforcement in CVE, and to reflect this shift, there be recognition of the need for a cultural shift in how police departments are run.

Cooperation: Participants recommended that better cooperation and collaboration occur among all partners involved in CVE efforts and that focus be kept on those partnerships. They recommended ending federal in-fighting and duplication of efforts and developing federal guidelines that would improve cooperation and information sharing, including in locations that have strict information sharing laws. Participants recommended that those leading CVE efforts provide greater support to local law enforcement institutions and help to bring state and local governments on board in efforts to counter violent extremism. Participants also recommended finding ways to increase the cooperation and outreach between law enforcement and the communities they serve and to improve coordination between locations with similar refugee and immigrant communities.

Resources, Funding, and Staffing: Participants recommended providing resources, consistent funding, and staffing to facilitate efforts to counter violent extremism. Participants also recommended developing a grant that would allow departments to develop CVE-related positions and providing a clearer grant application process for funding CVE-related training.

JBS Recommendations

CVE Training: JBS recommends that training on CVE be developed that is tailored to functional areas and levels of experience and is built on and uses current law enforcement protocols and language. By tailoring training and presenting it in this way, officers can build on experiences and frameworks they already have, allowing for training, and CVE initiatives, to be better incorporated into their jobs. Due to the importance of CVE, such training should be mandatory and be offered by experienced professionals.

CVE Training Program: JBS recommends that a CVE training program be developed that includes a certificate option. This training program should offer a menu of courses at different levels (beginning, intermediate, and advanced). Training on skills related to CVE should be offered as well.

CVE Information: JBS recommends that CVE communications be presented in ways that are appropriate for the target audience and that efforts continue to provide documents with higher tear-lines to law enforcement and others. JBS also recommends that CVE communications be streamlined and that a mechanism is developed to allow law enforcement and fusion center personnel to search multiple databases and secure websites simultaneously.

Annex

Annex 1: Perspectives on Countering Violent Extremism Policy and Implementation

In addition to discussing CVE-related training and information needs, participants in the focus groups and interviews highlighted broader issues related to the implementation of the national strategy for *Empowering Local Partners to Prevent Violent Extremism in the United States* and the role that fusion centers and law enforcement play in it. This annex first presents the perspectives of fusion center personnel and then those of law enforcement.

Fusion Center Perspectives

Fusion Center Senior Staff

Role of Fusion Centers in CVE ***"We're just a cog in the wheel with the prevention of it."***

Most senior staff who spoke of the CVE policy and its implementation acknowledged the importance of bringing local resources to local issues. "To effectively counter violent extremism in the community, it has to be done at the grassroots, local level," noted a senior staff member. While not addressed by most senior staff, several did seek clarification on the role of the fusion center in CVE. One senior staff member explained that the CVE policy and the CVE training initiative "fell out of the sky" and noted that those developing the CVE policy and implementation "assume that everyone [in the field] knows what they've been doing all along." For this senior staff member, there is a "disconnect" between the CVE initiative and what it means for fusion centers, with fusion centers the last to know. Due to this, the senior staff member asked for "clearer direction of the role of the fusion center as it relates to countering violent extremism."

As one senior staff member explained, "The fusion center environment doesn't do community outreach. We provide analytical assessment on the front end, training to law enforcement, and how they engage the community." For them, such involvement is limited to preparing training, presenting indicators, demonstrating reporting mechanisms, and analyzing reported information. Another senior staff member explained that "Without fusion centers, you won't have training to counter violent extremism. There's no other game in town regarding training." Centers that are operational in nature may see a role in conducting operations or developing sources in the communities. Other roles noted by individual participants include serving as a clearinghouse for information or developing counter-narratives.

For one senior leader, the ultimate aim of the CVE policy was unclear, and he was confused as to whether the policy is to prevent extremists from committing crimes or to change their mindsets. As he explained, "I don't understand what the fusion center can do, law enforcement. Any more than the gang situation." Fusion center leaders noted other issues. For example, one leader believed attention and outreach needs to include all communities, as targeting one community is "like a slap in the face for those groups."

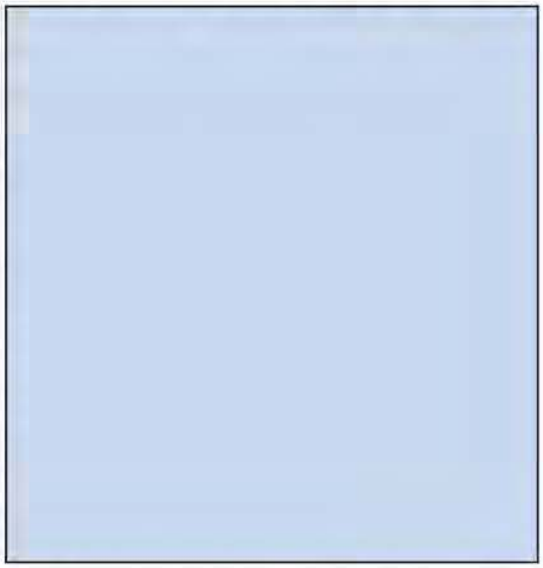
Fusion center senior staff often identified the incompatibilities between fusion centers' critical operating capabilities and CVE. Balancing civil rights protections with receiving, analyzing, disseminating, and gathering data on groups or movements that are not engaged in criminal activities is seen as a challenge by participants; determining what information on which activities and behaviors can be collected, investigated, and retained is an issue. As one senior staff member said, "The issue is under 28 CFR, the legal standards on keeping

information. You can keep certain information, but when do you, when can you, gather, retain, and share it without violating civil liberties? How do you share information on someone, especially when they haven't committed a crime yet?" Senior staff members also noted challenges with receiving reports where activity "only reaches a threshold of being suspicious because of the individual involved."

Another senior staff member explained that the federal government, and the FBI in particular, should be taking the lead in CVE, but "the government writes a paper that enables state and local to take it on." For him, the partnership between state/local and the federal government needed for successful implementation of the policy is not sufficient.

Community Support for Fusion Centers and CVE Initiatives

Senior staff reported that support for fusion centers and CVE is an issue in different communities. At the local level, communities are suspicious, and occasionally antagonistic, about the presence of fusion centers and policies such as the Nationwide SAR Initiative. Fusion center leadership noted a need for assistance with messaging to the public. The leadership at one center spends the majority of their time addressing civil rights and "spying" concerns on the part of the citizenry rather than running the center. At another center, one senior staff member explained that messaging to communities is "something we struggle with the most, describing the value added by the fusion center and getting the message out there." One way in which leadership attempts to ensure positive messaging is by building a center's credibility through protecting civil rights and producing information that is good.



Senior staff also noted that communities may not recognize the dangers of violent extremism or may place a lower priority on it. Moreover, some communities can perceive interaction with law enforcement to be a no-win proposition. For example, communities may think that reporting individuals to law enforcement will automatically lead to jail or criminal prosecution rather than a diversion program (if allowable). One senior staff member also noted divisions between communities and community leaders in CVE. He explained that communities do not want radicalization to occur, but leaders, for example, are insistent that there are no problems in their communities. One participant, describing the challenges of creating an inclusive outreach program, shared that "there's a lot of political poison in this area."

Local law enforcement and leadership at all levels of state politics may provide varying degrees of support for fusion centers and CVE initiatives. In some cases, this affects the willingness of local law enforcement to share case information with the centers, whether at the patrol, investigative, or leadership level. One senior staff member noted that whether law enforcement leadership is elected or appointed—and to whom they are accountable—affects the level of cooperation the fusion center may receive.

Fusion center leadership also explained that CVE is not always a priority for city or state governments. As one fusion center senior staff member explained, fusion centers are governed by the politics of the location. State

offices, such as the state Attorney General, Governor's office, and state legislators, may not be aware of the national and international issues facing their states, and as a result do not recognize the need for centers. Policymakers may also lack an understanding of these communities' cultures and mindsets.

Support for fusion centers at the federal level is marked by inconsistencies, according to some fusion center senior staff. One member of leadership remarked on the various levels of support for different fusion centers from the intelligence community, including the level of support for security clearances. Another noted that the relevance and importance of fusion centers needs to be understood by political leaders as no other entity exists that serves the function of the centers. Yet another senior leader explained that the "need is more for federal partners to recognize the true value of the fusion centers" and leverage them to their advantage.

Fusion Center Resources and Staffing

Senior staff cited issues pertaining to resources and staffing that affect their ability to effectively counter violent extremism. For some centers, high turnover, insufficient staffing levels, and inexperienced staff were noted as concerns. One senior staff member cited a need for "more bodies, more agents, more analysts" and specifically those who possess prior military or intelligence community experience. Local law enforcement agencies do not have an intelligence culture, according to one senior staff member, inhibiting their ability to gather and provide information to analysts, or to conduct their own research. Staffing limitations also affect the amount of research and analysis conducted. For some, primary tasks do not allow for time to conduct open source research. One participant noted gaps in presence of, and proper use of, analytical capabilities in centers.

The perception that violent extremism is not a concern among law enforcement and the public affects funding and staffing levels. As one senior staff member noted, "Grant money is drying up. And we'll see fewer people or fewer centers." The ability to retain its physical location, for one center, relies on DHS funding; most of the staff are donated by partner agencies supportive of the mission.

Defining Violent Extremism and Applying that Definition

Senior staff members at five locations noted challenges around federal government communications related to CVE, and in particular, the different ways in which violent extremism is conceptualized and then applied. Senior staff who spoke of the definition often asked for a consistent message around HVE. They cited disagreements across agencies about what HVE entails and instances in which the same thing is labeled different ways. Another senior staff member noted the addition of a new phrase, "violent fringe extremists." One participant explained that differences of opinion about the definition and the biggest threat lead to confusion and an "either/or" application on the ground: "We might be able to discuss the merits of these disagreements, but for local police, such statements become confusing. How this information gets operationalized is murky."

Fusion Center Analysts

Coordination of Effort *"No one wants to play in a game they are sponsoring."*

Analysts also noted issues with coordination of CVE efforts, whether related to producing training and information products or to receiving federal support at the state level. The production of training and information products around CVE is seen as not systematic. As one analyst explained, "If this [CVE] is really an

important mission, buy in, outreach, and education need to be spoken about at higher levels. The onus and focus needs to be at headquarters." This requires a formal plan that includes intergovernmental coordination and working through state institutions. For him, "*Ad hoc* reports and training don't cut it," and the process needs to be institutionalized.

Analysts noted that giving state/local institutions the responsibility to counter violent extremism also requires providing resources as well. For some centers, it is an uphill battle to get federal representation, leading one analyst to say that "no one wants to play in a game that they are sponsoring." For CVE, one said:

> *We do an OK job of scraping things together. But it's usually from other things, not our products. There is no CVE briefing. Maybe it's a small thing … to [DHS] as a whole, state and local customers are not the highest priority … There are not enough resources … I don't see any huge collaboration on best practices, across the government … It's pretty embarrassing really. No one is thinking, "Let's get together." It seems fractured.*

Definition/Terminology *"Terminology is an issue."*

For analysts, the ambiguity of terminology and the definitions of violent extremism and CVE are seen as a hindrance to CVE. One analyst noted that violent extremism is used to describe extremism linked to Islam or a much broader radicalized violence, sometimes within the same agency. Another analyst explained that "we're still trying to define HVE, autonomous violent extremism." Another analyst, discussing the inherent contradictions in the definition of violent extremism, noted, "I jump in a car and I killed 30 people because I don't like soccer, but if I say I like al-Qa'ida—one is and one isn't [violent extremism]?"

How definitions are used locally is an issue as well. For an analyst in one state, separating a violent act from an act of violent extremism or terrorism is easy for the FBI, which defines terrorism as related to changing political will. State definitions may lack this political component, allowing for any major violent crime to be termed terrorism.

Role of Analysts

Analysts cited issues associated with CVE. These issues include a lack of clarity related to their ability to track extremists who are engaging in protected activity or being required to "walk a fine line." As analysts explained, "[T]here is a fine line between personal freedoms and those who aren't satisfied with protests." Because of First Amendment concerns, fusion centers are not allowed to keep track of or document those who are engaging in free speech until they engage in criminal activity; however, when it comes to CVE, fusion centers and local law enforcement have the "charge of stopping the crime before it occurs." Because of this, the role of law enforcement is shifting as well, but "[p]olicemen have to have a crime to do their job." For another analyst, CVE is just another way to describe intelligence-led policing.

One analyst explained that local populations are not overly familiar with violent extremism, and government messaging may not take this into account. Messaging is seen as inflammatory, and local populations can sometimes see the federal government as a bigger threat than the violent extremists about whom they are warning the community.

The role of the fusion center analyst in CVE, according to participants, is to provide information to local law enforcement. As one analyst explained, "I can't say that me as an analyst, that I would be able to stop something pre-operational on the ground." For another analyst, the fusion center mission is to prepare, but it is the JTTF that will take care of the issue. The "things that would allow us to be more prepared," for one analyst, "would infringe on civil liberties. The monitoring devices for tracking individuals, it would contribute to intolerable living circumstances."

Fusion Center Liaisons

Few liaisons spoke specifically about the CVE policy and implementation. Those who did noted that community outreach is vital, whether through community policing or getting the community to report suspicious activity. Liaisons discussed the challenge of countering violent extremist threats and getting similar application across the country. The lack of clear definitions and the ambiguity that the federal agencies bring to understanding the state and local view are a particular challenge for one liaison. He noted, though, that the focus is getting tighter, leading to better reporting. Other comments about challenges surrounding CVE implementation include:

- "CVE is not black and white. It's gray. It inherently brings challenges. A legal issue could come out anytime and change things."
- "Politics are huge. If politics were out of it, it would be easier … You could identify the issue without being identified as racist."
- "How can you be ready for CVE when you don't know what it is?"

Law Enforcement Perspectives

Law Enforcement Executives

CVE Strategy and Implementation *"There is no silver bullet for this."*

Executives, more than any other functional area, discussed the CVE strategy and tended to have very different views of what that strategy and implementation mean. These different perspectives included: a more narrow community-oriented policing response; a whole-of-the-community response, including law enforcement agencies; and an intelligence-oriented response that includes source development and sophisticated intelligence gathering.

Executives who viewed the policy and implementation through the lens of intensive community-oriented or problem-focused policing noted that such a response, and the underlying premise of the newer CVE term, has been around for decades, if not longer. CVE, for them, is not seen as a new problem nor does it call for a new strategy. For this group it reinforces the need for stronger community policing. Under this approach, frontline officers can mitigate violent extremism by serving as a resource for the community, building relationships and trust. As many executives noted, a by-product of providing resources to communities could be a greater openness from the community to share their concerns about radicalized members or other information. However, even with these relationships, the largest problem—the pre-radicalization piece—would require "a magic wand." As one executive explained, people cannot be "inoculated against extremist views," nor can the government "identify and give a prescription for a healthy, safe community."

A closely related, but much broader, perspective includes community-oriented policing as a core component of a whole-of-the-community approach. Executives who conceptualized the strategy this way tended to focus their remarks on providing resources to alleviate communities' issues through community resource or liaison officers and other public and private entities. As the beginning stages of violent extremism are typically social and not criminal in nature (i.e., involve extremist views rather than violent conduct), community outreach and intervention by religious and other community leaders may be best poised to address it. Such an approach, according to these executives, could decrease drivers of radicalism and violent extremism such as poverty and marginalization, protect American principles and values, and ultimately encourage communities to become pro-active and police themselves.

Some executives also viewed the strategy through an intelligence lens, where law enforcement can mitigate the threat, but countering it must be done by the JTTF and federal agencies. Such an approach would include longer-term investigations, sophisticated intelligence gathering, and the use of technology. It would be applicable to other groups and individuals, such as gangs, who engage in ongoing and difficult-to-prevent activities. For some, this perspective provides only a small role for local law enforcement.

Federal and Local Responsibilities

Executives cited challenges in CVE that stem from overlapping mandates and blending of local CVE and federal CT efforts. Many executives noted a real need for CT—developing and running sources and conducting long-term investigations for intelligence-gathering or prosecution purposes; however, federal CT efforts are often seen as being at cross-purposes with community-oriented CVE efforts. More than one law enforcement

executive expressed frustration with the lack of defined roles and suggested that federal agencies "need to find a way to stay in their own lane."

For example, according to some executives, the FBI's expertise in CT does not translate well into community-based initiatives; these initiatives "are not something that the FBI knows about or cares about, as it is not their responsibility." In some cases, federal involvement in communities for intelligence-gathering purposes has been poorly received and, due to missteps by the federal players, has required apologies from state and local agencies. These different objectives, and the ongoing issues stemming from them, led one executive to recommend rebuilding the CVE policy from "ground zero" to ensure a prominent place for local law enforcement's expertise in community policing, problem solving, and building relationships with community members.

CVE Leadership *"Who is in charge?"*

A few executives wondered who is in charge, or who decides who is in charge, of CVE. From these individuals' perspectives, CVE leadership is either splintered or is not qualified. Executives noted that, depending on which agency is asked, each agency will say it is the "main agency." Since "no defined central person [is] in charge," local law enforcement receives mixed messages from federal agencies. Due to the politics and the frequent turnover of staff, where there should be leadership, those in charge are younger, have less experience, and tend to lack law enforcement experience.

No CVE Training Curriculum

One of the challenges in implementing a CVE program, according to executives, is the lack of a curriculum, which even with current training and pilots, is "virtually non-existent." Executives noted key areas where officers lacked the skills to counter violent extremism adequately and properly:

- Interacting with communities that historically have had very limited positive interaction with law enforcement in their countries of origin;
- Moving past the "community gadflies" and political efforts that only placate vocal members and "greas[e] the squeaky wheel"; and
- Giving officers the authority and the training to move beyond the "is there a crime?" mentality.

Uncertain Parameters *"They try to throw everything in the CVE bucket."*

CVE is associated with a variety of initiatives, from community-oriented policing, to intelligence-gathering, to CT. For many, CVE is not adequately defined from an operational perspective and thus is broadly and variously interpreted. As a result, law enforcement and others "try to throw everything in the CVE bucket." For many executives, a distinction needs to be made for practical reasons between CVE and intelligence, and the program needs to be clearly articulated at the beginning. They note that it is important for their community relations that communities understand the division between resource officers and intelligence collection. Just as critical, field officers may reject a community-oriented outreach program because they see it as too "touchy-feely."

Maintaining Vigilance among Law Enforcement

Executives noted that it is a struggle to maintain the vigilance and energy to detect violent extremist activity. Priorities shift, funding becomes limited, and officers become complacent the further away 9/11 is with no major incidents. While implementing a day-to-day CVE program was perceived to be untenable by most law enforcement units given the priorities of the police, maintaining awareness was considered possible.

Laws Limiting Information Sharing

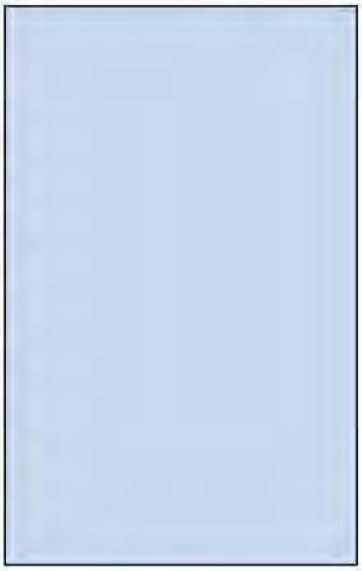
Another challenge mentioned in implementing a CVE policy is the lack of support from state and local political leadership. In at least three locations, laws and policies inhibit the collection, maintenance, and sharing of information, as well as the collection of information on general and specific movements, and this situation reflects disagreement on which groups actually could be considered violent extremists.

Law Enforcement Investigators

A New Type of Policing

Whereas many executives viewed CVE as an extension of community-oriented policing efforts, investigators generally spoke about how their roles in law enforcement would change as a result of the initiative. Investigators often spoke of the need for support for this new role—from advocates, lobbyists, or other non-law enforcement personnel outside of their areas—"to say why this is so important" and to show the importance of the type of work they do. The CVE initiative could receive better support if state leaders, such as the state Attorney General and state institutions for training law enforcement, were brought into the process. Support from the government was also sought to provide education to the public about countering the threat of violent extremism so that "people would recognize that [officers] are not stereotyping," or profiling, but are working to protect the public.

Federal Government Competition and Messaging



Investigators viewed in-fighting between federal government agencies as a major challenge to CVE. Competition between DHS and the DOJ can lead to pressure to support one agency or system over the other, and to duplication of efforts. Battles over which agency receives credit led investigators to note that "[p]eople will be amazed at what gets accomplished when no one gets credit." Local law enforcement noted competition issues with other federal agencies as well.

Investigators, and others, viewed federal government messaging about violent extremism as politically correct, lacking in transparency, and ultimately detracting from efforts to counter violent extremism. As one investigator explained, there is a reluctance to be perceived as insulting a religion or culture, and as a result, political correctness "trumps" providing a complete and accurate accounting of events. As a result, according to another officer, reports are "watered down." Another officer noted that "[t]he whole PC thing is a huge problem. You can't just lay information out. It has to be repackaged in a palatable way." For example, one officer stated that he sees

"'violent extremism' as the politically correct way of saying 'terrorism.'" In another example, many officers saw the decision to characterize Major Nidal Hassan's actions as workplace violence as a lost opportunity for transparency.

Resources *"We can't even take the time to focus on the big picture."*

Participants indicated that most law enforcement agencies face significant hurdles when it comes to resources, staffing, and training. For some agencies, insufficient staffing levels—one urban location employs 649 officers to police a population of 450,000[13]—only allowed officers to deal with the problems immediately facing their communities, preventing them from being able to "focus on the big picture." It was also mentioned that law enforcement agencies lack sufficient numbers of ethnically diverse officers who can liaise with the diverse communities they serve.

Law Enforcement Frontline Officers

Role of the Frontline Officer

Officers, particularly patrol, are trained to deal with crime and stated that CVE is a "new world" that requires a paradigm shift in how officers view situations and process information. However, the implementation of the CVE policy at the local level was seen by officers in one of three ways: as activities that are already undertaken, either through community outreach or community policing; as activities similar to what they currently do, but with other topical areas, such as gang violence; or as activities that are all "new territory" for law enforcement. According to all groups, policy makers are "dramatically changing how law enforcement does business." This changing role may require a similar cultural shift in departmental leadership, their expectations, and how they evaluate their officers. Even officers and departments who do significant outreach saw a difference in the type of outreach needed by the CVE policy. For them, CVE is a long-term commitment to communities and not "just [to] be this week's solution."

Many in local law enforcement stated that CT—which is often used interchangeably with CVE— is not their responsibility. As most officers explained, patrol is response-oriented, and their roles are not geared toward prevention or investigation. One patrol officer discussed the practical challenges of CVE:

> *But then a bigger issue is as a patrol officer stand point, my job is to respond to the call and clear the call. That's it. I got five more calls to get to. I don't have time to worry about if they have writings that look different. I don't have time for that. That's somebody else's job, that's not my job. My job is to get the call and clear it. We just don't have time for it, and if I had to pick up and dial a 1-800 number where I gotta wait forever for the person to answer, and … It's just not worth my time.*

Many officers noted that much of the lead-up activity to violent extremist acts is not illegal and thus does not fall within their scope of work, which focuses only on criminal activities. Some patrol officers have not been

[13] The average ratio of full-time police officers per 1,000 residents for communities larger than 250,000 is 2.5, according to the Bureau for Justice Statistics (http://www.bjs.gov/). That puts this community's law enforcement personnel resources at about half of the average for a jurisdiction of that size.

introduced to or been trained in mitigation techniques, such as CVE, and without such training, it was difficult for them to imagine what their role would be.

Community and Political Challenges to Changes

At a number of locations, frontline officers felt that new CVE-related initiatives face challenges from the community and from political leaders who are concerned about privacy violations. One location has received considerable attention related to training from the federal government, and as a result, adopting a new CVE training initiative may not be practical. Participants in other locations report leadership is unwilling to acknowledge the presence of those who might be considered violent extremists and, in one case, extremist groups were considered the "white elephant in the room."

Additionally, prevention is not visible to the public, who are interested in and want to see results. For departments driven by statistics, spending money on a program that does not produce quantifiable results—how can officers show that they disrupted a future, yet-to-be-planned terrorist attack by building relationships with communities?—is a hard sell to the public, many of whom may only perceive terrorism as overseas phenomena. As one officer said, "How do you prove a negative?" Even typical law enforcement collection techniques put officers on the defensive. As one officer said, society is disillusioned by the Hollywood depiction and people think officers are in the bushes collecting intelligence—"No, we're not in the bushes." Officers, he noted, get information for their cases by "bringing people in and making them tell on others."

Resources and Staffing *"We're doing more with less."*

Frontline officers most often cited resources, funding, and staffing as significant obstacles to CVE. As many officers stated, when resources are limited, officers deal with the major issues that are facing the community, and that typically is not violent extremism. As one officer explained, leaders are proud to say, "We're doing more with less," but what is really happening is poorer quality police work and a faster burn-out of officers.

Annex 2. Focus Group and Interview Guide

State, Local, Tribal and Territorial Law Enforcement Perspectives on Countering Violent Extremism Focus Group Moderator's Guide

Thank you all for coming. My name is _____ and I am with the Aguirre Division of JBS International. We are an independent research firm located in Washington D.C. and we are working with the Department of Homeland Security's Science and Technology Directorate to talk with you today about your training and information needs related to countering violent extremism.

All of your personal information, as well as your opinions and ideas that you share with us today, will be kept strictly confidential. Aguirre/JBS is a wholly independent research firm and we only report information to our clients on an anonymous, aggregate basis. In order to limit distractions during the focus group, could everyone please put their phones on vibrate?

Security Threats in the Community/State

For the first part of our discussion, I would like to find out a little more about the security threats to be in your community/state.

1. What are the primary security threats to your community or state?
    - How are you defining "threat"?
2. Is the threat of violent extremism a concern in your community or state? If so, are there specific groups or movements that are present and of concern?
    - If a colleague were to ask you what violent extremism is, how would you define it?
        - *Note that for this study we will be focusing on groups and individuals inspired by a range of religious, political, or other ideological beliefs that promote and use violence*
3. Do you feel prepared to counter the threat of violent extremism while it is still in its pre-operational stages? What do you believe prepares you, or what do you need in order to be prepared to prevent violent extremism from materializing?
    - Do you view countering violent extremism as different from or similar to countering other types of crime?

Training to Counter Violent Extremism

For the next part of our discussion, I wanted to ask you some questions about the training you have received related to the security threats, and in particular violent extremism, in your community.

1. Have you had any training specifically related to violent extremism or countering violent extremism?

   - How would you rate the quality of that/those training(s)? What did you like or dislike about them? *[Probe on issues related to the accuracy, delivery, and usability of the training]*

2. What type of training related to specific security threats to your community/state have you found useful?

   - Was there anything about the way it was delivered that you found helpful or not helpful? *[For example, the length, the format, the delivery mechanism (online, in-class, hands-on, etc.)?]*

   - How would you rate the quality of that/those training(s)? What did you like or dislike about them? Were there issues related to the accuracy, delivery, and usability of the training?

3. What kind of training do you need (that you may not currently be getting) to counter violent extremism in your community/state effectively?

   - Is there particular content that is needed? Or format? Or how it is delivered?

4. Have you encountered problems trying to incorporate training into your job (or have you noticed that others have had problems)? If so, is there anything that could help you do this?

Sources of Information about Violent Extremism

I want to move the discussion on to sources of information about the threat of violent extremism and how to counter it. *[Listen for and probe on the culture of learning within the participants' organizations, particularly the degree of formality].*

1. What are your best sources of information about the threat of violent extremism and how to counter it?

   - *ONLINE RESOURCES;*
   - *Community sources;*
   - *Fusion centers;*
   - *DHS or other federal agencies;*
   - *Academic research; and*
   - *Informal sources of information.*

2. What kinds of problems have you had trying to get good information on the threat of violent extremism and how to counter it? *[Probe on quality of information, usability of information, frequency of information dissemination]*

3. Have federal communications about the threat of violent extremism and how to counter it been useful or helpful?

   - Are there particular examples of useful communications or products? *[probe on how and why – lines of communication, timeliness, format, etc.]*

4. What additional information do you need about the threat of violent extremism and how to counter it in your community/state? *[Probe on the type of information, the format of the information, the source of information, the frequency of information and the delivery mechanisms.]*

Final Question: If you had 60 seconds to meet with the person in charge of countering violent extremism, what would you say you need? Or, if you were in charge for the day, what you would do?

Moderator:	*Ask if there are any further comments they would like to share with you. Tell them how to contact you if they have any further thoughts, ideas, or suggestions.* *Thank the participants for their time and provide instructions for collecting participation incentives and gathering demographic information.*

MODERATOR INFORMATION

This focus group was composed of: _____ Men _____ Women

Focus Group Moderator: _____

Location: _____

Date: _____