

RELEASE IN FULL

Countering Violent Extremism: Needs Assessment Report

I. Introduction and Background

Several SPAS divisions (PD, POL, and SO) have discussed potential CVE training. Representatives from the division collaborated on developing questions and key stakeholders for a needs assessment. In order not to duplicate efforts, SPAS/PD volunteered to carry out the needs assessment on behalf of SPAS to determine:

- a) Whether skills gaps exist for U.S. or overseas-based officers working on CVE issues;
- b) Whether such gaps may be effectively filled through FSI training;
- c) What type(s) of training may be most suitable.

Two major events in 2015 underscored the importance of CVE and its primacy within the United States' foreign policy agenda. First, the White House CVE Summit (February 2015) convened leaders at all levels of local and federal government including leaders from around the world to discuss how to combat this global phenomenon. In a follow-on summit, the United States participated in the Leaders' Summit on Countering ISIL and Violent Extremism held under the auspices of the UN General Assembly in September 2015. Additionally, the *Quadrennial Diplomacy and Development Review* (QDDR) lays out a strong case for focusing on CVE by prioritizing it among only four total objectives.

Currently, modules within *International Terrorism* (PP521) and other courses cover the topic tangentially but do not provide sufficient exposure to the subject and its complexity. Furthermore, some bureaus within the Department have created their own informal training programming, which does not cover the entire spectrum of CVE issues, but rather focuses on those dimensions that relate most closely to their work.

II. Methods

The needs assessment was conducted primarily through a series of phone interviews with:

- Subject matter experts within the Department of State
- Officers serving at Embassies overseas (AF, EAP, NEA, SCA)
- Representatives from the Interagency (USAID, NCTC)

In total, over 20 respondents were asked each of the following questions:

1. How does your office understand CVE? What is its working definition?
2. What kind of CVE-focused programming has your office conducted? Why was it successful/less successful?
3. Are there specific knowledge/skills/attitudes officers need to work CVE portfolios effectively?

4. Have you noticed fundamental gaps in officers' abilities to work successfully on CVE? If so, what are the prime deficiencies?
5. What kind of training would augment officers' ability to do so more effectively?

Follow-up questions, as needed, were used to elicit more detailed responses.

In order to ensure a wide range of opinion, respondents were selected from all levels of responsibility from mid-level desk officers to senior directors and special advisors—both within the Department, across the Interagency, and stationed at overseas posts. Based on the consistency of their responses, SPAS determined that a wider-scale interview process was not necessary.

III. Key Findings

Identification of Skill Gaps

Interview respondents believe that a dedicated training course is essential and that there are key knowledge, skills, and abilities needed to work CVE effectively.

"CVE is a policy priority. We need to equip our diplomats with a solid understanding of what CVE is and infuse it into the fabric of the Department."

"Everyone in the Department needs to become fluent in the language of CVE if we are going to make progress on this front."

Respondents were consistent in identifying three problem areas, which can be summarized as: a) defining the issue; b) creating effective measurable programs; c) honing soft skills.

Defining the issue

Across the board, respondents mentioned the lack of a unified definition of CVE. Although most acknowledged that the mention of CVE in the most recent *Quadrennial Diplomacy and Development Review* in addition to the *White House Summit to Counter Violent Extremism Follow-on Action Plan* had given focus to CVE efforts, many felt that the definition of what constitutes CVE depends heavily on where one sits within the U.S. government.

When pressed on how their office defines CVE, it was common for the respondents to list the activities they are involved in rather than provide a succinct definition. The range of activities included preventive measures (e.g., economic development/job creation) to more active responses such as counterterrorism operations. A representative sampling of comments includes:

"CVE and its definition is very context specific. How we engage in CVE in Norway will be completely different from what we do in Nigeria."

"Diplomacy and government-to-government relations are the foundation of CVE. This is our comparative advantage—not working on economic projects like poverty alleviation."

"There simply is confusion over where CVE ends and CT [counterterrorism] begins."

Creating effective programs and measuring success

How to develop, implement, and monitor CVE programs concerned many of the respondents and each felt that training could help answer this question. Additionally, many surveyed raised the issue of how to differentiate between CVE and non-CVE programs, many of which had common elements. Consensus jelled around the notion that context matters. One respondent said,

"You can design a community policing program in Algeria for the national police—that's a basic INL [International Narcotics and Law Enforcement] program. However, if you begin to drill down and focus on certain villages that have witnessed a rise in extremism linked to abusive police practices and apply a community policing program to that problem set, now you have a CVE program."

Depending on the Embassy, CVE efforts are housed within the Economic, Political, or Public Affairs Sections. Regardless of where they sat in the Embassy, some officers expressed uncertainty regarding their ability to design, coordinate, and monitor a CVE program effectively. One interviewee stated,

"So much of the CVE portfolio is program based and officers seem to spend a large amount of time on program management. Officers are not prepared to do this and it's frustrating to try without training."

Lack of training in program design is not the only factor that has led to frustration in the field. Monitoring and evaluation—perennial challenges for any program manager—weighed on the minds of interviewees. One respondent went so far as to say that *"We shouldn't get bogged down on defining success or effectiveness. Doing so is exceptionally difficult."*

Others took a more optimistic view and are working to develop metrics to gauge CVE efficacy. Until a widely-accepted evaluation tool is developed, officers said they are evaluating what they can even though it might be imperfect. Illustrative of this approach is what one Public Affairs Officer is doing,

"Although evaluating the effectiveness of our programs is tricky, we are measuring output—how many people participated in our programs. This gives us some data although it is not perfect."

Honing soft skills

In addition to the abovementioned knowledge gaps, a deficit in officers' ability to build relationships of trust with others was also cited consistently. One interviewee felt that, "*FSI training teaches us the nuts and bolts of our jobs, but does little to teach persuasion and interpersonal skills.*"

Department officials, officers overseas, and members of the Interagency all echoed the view that interpersonal skills were essential to effective performance in the CVE space. In fact, those who had extensive public outreach experience ascribed much of their effectiveness to being able to win other people's trust.

Several respondents mentioned that gaining these skills is doable but requires training—either formally, or on the job. An interviewee mentioned the need for more senior-level officers to model effective relationship-building skills and to give junior staff opportunities to try them as they develop their own contacts.

IV. Respondents' Recommendations for Training

Interview respondents consistently said training is needed and that it is time the Department addresses this gap.

Typical responses indicating wide-spread support for training include, "*It is high time that FSI develop a course. CVE is a policy priority that is here to stay*" and "*I'm surprised there isn't anything formal. Our office is providing ad hoc training to officers heading out to CVE posts, but they need more than just an hour briefing.*"

Respondents' Ideas for FSI-based CVE training

Many of those surveyed recommended including a literature review on the subject of CVE. Academia, think tanks, and the USG all have conducted extensive research. Exposing students to the latest thinking and how it can be applied to the Department's efforts would round out officers' understanding of the issue and ensure they have a baseline knowledge of the subject before going to post or beginning their job.

Others emphasized a focus on case studies: what worked in the field? What did not? And why? Concrete examples of successful programming would guide officers as they developed their own initiatives and could form the basis of a CVE "best practices" guide.

Understanding the intellectual/ideological/religious frameworks through which extremists view and interpret the world is also an important component to training and would expose students to a variety of ways extremists conceptualize the world and respond to it. By having a familiarity with their worldview, officers would be able to anticipate their arguments and more easily provide counterarguments to them.

In response to the Department's push for Embassies to work with foreign governments to develop CVE strategies, officers felt that further direction was needed in order to do this more effectively. Some stated that they are unsure what a CVE strategy should include and how to ensure the host foreign government is drafting a strategy that truly addresses the roots of the issue.

Respondents also mentioned the need for hands-on training in the art of persuasion and relationship building. Activities designed to allow students to experiment with various techniques would hone skills they already have or allow them to develop new ones to try when conducting outreach.

In addition to Department subject matter experts, an effective course would also draw upon the domestic NGO community as well as local law enforcement agencies—both of which have conducted CVE outreach in the United States and have begun to share their models and best practices with Embassies overseas.

V. Summary of Recommendations for Training

1. FSI should organize a Countering Violent Extremism course.
 - The course should include speakers from within and outside the Department to ensure a multitude of perspectives.
 - The course should highlight effective examples of CVE both domestically and overseas and provide "best practices" for CVE program development.
 - The course should involve hands-on, experiential training opportunities that will allow students to apply what they have learned (e.g., a group project to develop a CVE program; the art of persuasion and negotiation).
2. Additionally, the following topics should be included—each one was mentioned by multiple respondents:
 - a. Defining CVE
 - b. Ideological underpinnings of violent extremism
 - c. Drivers behind violent extremism
 - d. How to respond to and counter commonly-held beliefs by extremists
 - e. Techniques to work with foreign governments to develop CVE strategies
 - f. How to design, implement, and evaluate CVE programs
 - g. How to identify funding for CVE programs

Recommendation Not Requiring Formal Training

On a final note, whether training is used to address these gaps or not, respondents consistently stated that the Department needs to create a unified and coherent definition of CVE. While the recent publication of key documents (e.g., *QDDR*) sheds more light on the subject, respondents felt that it is still not enough to give direction to their work either in Washington or the field. The

development of a course on CVE might serve as a catalyst for USG entities to develop a whole-of-government definition of CVE and key terminology.

Approved: SPAS/PD: CCummins

Drafted: SPAS/PD: CJames

Cleared:	SPAS/POL:	AAllison	(ok)
	SPAS/POL:	VLeBailly	(ok)
	SPAS/PD:	TManson	(ok)
	SPAS/SO:	PMcNerney	(ok)
	SPAS/SO:	DBryant	(ok)
	SPAS/SO:	TSchmidt	(ok)
	SPAS/SO:	DGehrenbeck	(ok)