

**U.S.-UK Joint Contact Group Reception
Monday, August 3, 2015**

Overview:

- You are attending a reception for the 20th Joint Contact Group (JCG), hosted by Sir Peter Westmacott, the British Ambassador to the United States.
- The reception will be held at the British Ambassador's Residence. The reception is limited to Her Majesty's Government and DHS guests.
- The reception is from 6:00-7:30pm. Ambassador Westmacott may ask you make brief remarks after his welcoming remarks and toast.

Discussion Points:

- Thank Ambassador Peter Westmacott for hosting the JCG Reception.
- Thank Mark Sedwill and his team for travelling to Washington for the twentieth meeting of the JCG, and the third JCG which Sedwill and you have co-chaired.
- Note that since its inception in 2003, the JCG has advanced the partnership between DHS and the Home Office and provided strategic direction for U.S. – UK homeland security cooperation and collaboration.
- Note that DHS has no closer international partner than the United Kingdom, and has an exceptionally strong relationship with the Home Office. The close relationships developed through the JCG are the heart of this partnership.
-
- Emphasize that our partnership is essential, as we face the many and evolving threats of today.
- Reaffirm that you are privileged to participate in this reception this evening, and in the JCG tomorrow.

Background:

- The British Ambassador, Sir Peter Westmacott is hosting the JCG reception.
 - Ambassador Westmacott became the British Ambassador to the United States in January 2012. Prior to his U.S. posting, he was the British Ambassador to France from 2007-2011, and he has served for over forty years in the British Diplomatic Service.
 - Ambassador Westmacott hosted a reception for the eighteenth JCG in April 2014 in Washington. Elizabeth Dibble, the Deputy Chief of Mission for U.S. Embassy London, hosted the nineteenth JCG reception in November 2014 at her residence, Wychwood House, in London.
- You met UK Home Secretary Theresa May during the G6+1 Ministerial in Dresden, Germany on June 2, 2015. Secretary Johnson previously met the Home Secretary in London in February 2015 at the Five Country Ministerial. She also attended the White House Countering Violent Extremism (CVE) Summit later that month. Home Office Permanent Secretary Mark Sedwill participated in the UN Security Council Ministerial on May 29, 2015, co-chaired by Secretary Johnson and you last met Sedwill in January 2015.
- You co-chaired the last JCG with Sedwill from November 4-5, 2014 in London.

- Prime Minister David Cameron and his Conservative Party won a surprising victory in the UK General Election on May 7th, and the Conservatives have an outright majority for the first time in nearly 20 years, winning 331 of the 650 available seats in the House of Commons. Cameron will face immediate challenges in keeping his fractious party in line, as well as in reconciling right-leaning England and Wales with the Scottish National Party, which won 56 of the 59 available Scottish seats. The Labour Party won fewer than expected seats, and party leader Ed Miliband resigned. The Liberal Democrats retained just eight of their 57 seats, and former Deputy Prime Minister Nick Clegg also resigned as party leader. Overall election turnout in the UK was approximately 66%.
- The British Embassy is one of the largest in Washington, and the statue of Winston Churchill on Massachusetts Avenue has one foot within the grounds of the British Embassy and the other foot within the United States. This symbolizes Churchill's dual Anglo-American heritage, (his father was British and his mother was American), as well as his contributions to the Anglo-American Alliance.

PARTICIPANTS:

UK Participants:

Sir Peter Westmacott, British Ambassador to the United States
Mark Sedwill, Permanent Secretary, Home Office
Paul Lincoln, Director, National Security, Home Office
Christophe Prince, Director Prevent, Home Office
Lucy Bird, Director Border and Aviation Security, Home Office
Peter Storr, Director General, International and Immigration, Home Office
Caroline Dulson, Private Office, Home Office
John Noble, Home Office
Kevin Adams, First Secretary, British Embassy
Emily Slifer, British Embassy
Others TBD

DHS Participants:

Alejandro Mayorkas, Deputy Secretary
Rob Silvers, Senior Counselor to the Deputy Secretary
Francis Taylor, Under Secretary for Intelligence and Analysis
Eugene Gray, Principal Deputy CT Coordinator, Analysis
Joseph Clancy, Director, U.S. Secret Service
Gil Kerlikowske, Commissioner, CBP
Kevin McAleenan, Deputy Commissioner, CBP
Sarah Saldana, Director, ICE
Peter Edge, Executive Associate Director, Homeland Security Investigations,
Peter Neffenger, Administrator, Transportation Security Administration
Paul Fujimura, Assistant Administrator, Office of Global Strategies,
Suzanne Spaulding, Under Secretary, National Protection & Programs Directorate
Reginald Brothers, Under Secretary, Science & Technology
Lori Scialabba, Deputy Director, U.S. Citizenship and Immigration Services
Megan H. Mack, Officer for Civil Rights & Civil Liberties

FOR OFFICIAL USE ONLY

Karen L. Neuman, Chief Privacy Officer
Huban A. Gowadia, Director of the Domestic Nuclear Detection Office
Alan Bersin, Assistant Secretary and Chief Diplomatic Officer, Office of Policy
Matthew King, Deputy Assistant Secretary, Office of Policy
Robert Moczynski, Deputy Assistant Secretary, Office of Policy
Patrick Prisco, Director, European Affairs, Office of Policy
Robert Paschall, DHS Attaché to the United Kingdom
Others TBD

Attachments:

A. Biography

Staff Responsible for Briefing Memo: Patrick Prisco, Director, European Affairs,
PLCY/OIE (b)(6)

**U.S.-UK Joint Contact Group (JCG)
Tuesday, August 4, 2015**

Overview:

- You will co-chair the 20th meeting of the Joint Contact Group (JCG) with Mark Sedwill, the Permanent Secretary of the United Kingdom Home Office.
- The JCG will take place on August 4, 2015, at the NAC (in Building 19 and the Mount Vernon Room) from 09:00-17:00. There will be a JCG reception at the British Embassy on August 3, 2015 from 18:00-19:30.
- The objectives of the JCG are to review DHS's close partnership with the UK Home Office, to deepen cooperation to counter the terrorist threat, and to provide strategic direction to DHS-Home Office collaboration. Specifically, DHS seeks to advance priorities to address the foreign fighter threat, explore expansion of information sharing and the work of the Five Country Ministerial/Five Country Conference, explain the priority of expanding preclearance, focus efforts on countering violent extremism, and discuss the encryption issue. The UK Home Office has also requested to discuss human trafficking and UK migration issues.

Discussion Points:

- Describe DHS leadership areas of focus and priorities.
- Emphasize the importance of improving the detection and prevention of foreign fighter travel and encouraging European partners to enhance screening capabilities.
- Ask for the UK's view on the current international aviation threat and the sustainability of enhanced aviation screening measures at select foreign airports.
- Review key findings of the joint DHS-Home Office counterterrorism exercise.
- Discuss CBP's Automated Targeting System-Global (ATS-G) and proposed Global Travel Assessment System (GTAS), and ask for the UK's view on how best to encourage other countries to develop passenger data collection and analysis systems.
- Discuss the importance of expanding preclearance and the desire to have Heathrow and Manchester airports incorporated into the program as soon as possible.
- Preview DHS's planned introduction of new, higher security criteria for all Visa Waiver Program countries.
- Discuss the UK's experiences with countering extremism and how the Home Office plans to implement the Prime Minister's new proposals.
- Explore the challenges of addressing the encryption issue.
- Discuss information sharing priorities and preparations for the upcoming Five Country Conference meeting in London in September 2015.

Background:

- Since its June 2003 inaugural meeting, the Joint Contact Group has provided strategic direction for U.S. – UK homeland security cooperation and collaboration. The DHS

Deputy Secretary co-chairs the JCG with the UK Permanent Secretary from the Home Office.

- You co-chaired the last JCG with Sedwill from November 4-5, 2014, in London. Primary agenda items included: threat assessments, counterterrorism and foreign fighters, coordinating priorities for the G6+1 Ministerial in November 2014 in Paris, science and technology collaboration, and CBP priorities with the UK. One of the outcomes from the previous JCG was a joint DHS-Home Office counterterrorism exercise, which was conducted on March 13, 2015, in Washington, and which is a sub-agenda item during today's JCG.
- This will be the first JCG since the UK General Election on May 7, 2015. Prime Minister David Cameron and his Conservative Party won a surprising victory in the election, and the Conservatives have an outright majority for the first time in nearly 20 years, winning 331 of the 650 available seats in the House of Commons. Sedwill specifically requested holding this JCG before the end of the summer, rather than waiting until the fall.
- The Home Office oversees immigration, border management, and counterterrorism policy. It is also responsible for Security Service (MI)-5 and the National Crime Agency. Airport security is handled by the Department for Transport and disaster preparedness and cybersecurity are handled by the Cabinet Office.
- DHS has no closer international partner than the United Kingdom, and has an exceptionally strong relationship with the Home Office. The two sides maintain an advanced information sharing relationship, and the UK is also a strong ally in DHS's information sharing and data protection discussions with the EU.
- DHS has 53 permanent personnel in the United Kingdom. DHS, CBP, ICE, TSA, USCIS, USSS and S&T are represented in London. CBP operates its Immigration Advisory Program (IAP) at three UK airports (London Heathrow, London Gatwick and Manchester) and a Container Security Initiative (CSI) port at Felixstowe. CBP also has personnel at the UK's National Border Targeting Center. TSA has an extraordinary relationship with the UK Department for Transport and operates a high volume of Federal Air Marshal (FAMs) missions to the UK. ICE and USSS have excellent working relationships with UK law enforcement agencies. Twelve airports in the UK have last point of departure (LPD) service to the United States. In excess of 900 flights operate from the UK to the United States weekly; London Heathrow is the busiest airport in the UK with approximately 115 flights per day to the U.S. in peak season.
- Cameron has repeatedly stated that his government will hold a referendum on the UK remaining in the European Union by 2017; however, due to elections in France and Germany in 2017, most analysts think the referendum will happen in 2016 to avoid the referendum becoming a political issue in those countries.
 - Cameron has stated that he wants the UK to remain in the EU, but may support renegotiating certain terms with the EU.

- Managing the wishes of the more conservative members of his party and the EU's lack of enthusiasm to make changes to the treaties will be a major challenge for the Conservative government.
- The Conservative government announced its legislative agenda at the Queen's Speech on May 27, 2015. The government is taking a hard stand on extremism and terrorism. In a major speech on July 20, 2015, Prime Minister Cameron discussed the UK's strategy for countering extremism calling it the "struggle of our generation" requiring a major long-term response. He outlined several initiatives including an emphasis on shared UK values and making no distinction on the type of extremist views, challenging all forms of extremism – violent and non-violent.

Participants:

DHS

Entire JCG Plenary:

Deputy Secretary Mayorkas,
Rob Silvers, Senior Counselor to the Deputy Secretary
Alan Bersin, Assistant Secretary and Chief Diplomatic Officer, PLCY
Matthew King, Deputy Assistant Secretary, PLCY (or surrogate)
Frank Taylor, Under Secretary for Intelligence and Analysis
Bob Paschall, DHS Attaché to the United Kingdom
Patrick Prisco, Director, European Affairs, Office of Policy

For relevant sessions:

Gil Kerlikowske, Commissioner or Kevin McAleenan, Deputy Commissioner, CBP (or surrogate – Tom Bush or Troy Miller)
Peter Neffinger, Administrator, TSA (or surrogate – Paul Fujimura)
Peter Edge, Executive Associate Director, Homeland Security Investigations, ICE [where appropriate]
David Gersten, DHS CVE Coordinator
Reginald Brothers, Under Secretary, Science & Technology [where appropriate]
Maria Odom, Blue Campaign [where appropriate]

Home Office

Mark Sedwill, Home Office, Permanent Secretary
Paul Lincoln, Home Office, Director, National Security
Christophe Prince, Home Office, Director Prevent
Lucy Bird, Home Office, Director Border and Aviation Security
Peter Storr Home Office, Director General, International and Immigration
Caroline Dulson, Home Office, Private Office
John Noble, Home Office
Kevin Adams, Embassy, First Secretary
Emily Slifer, Embassy

FOR OFFICIAL USE ONLY

ATTACHMENTS:

- A. Annotated Agenda
- B. Biography

Staff Responsible for Briefing Memo: Matthew King, Deputy Assistant Secretary,
PLCY, ^{(b)(6)}

FOR OFFICIAL USE ONLY

AGENDA
EU – US Justice and Home Affairs Ministerial
November 13, 2014
Washington D.C.

1. Introduction
2. Transnational Organized Crime (EU/US-DOJ)
 - a. Cyber Crime including Global alliance
 - b. Traditional Organized Crime
3. Counter-Terrorism/Foreign Fighters (US-DHS/ EU)
 - a. Border Security Issues (PNR, API, ESTA)
 - b. Prosecution/Legislation Issues
 - c. CVE
4. Data Protection (EU/ US-DOJ)
 - a. Umbrella negotiations
 - b. Safe Harbor (security aspects)
5. Judicial Cooperation
 - a. MLA Review (EU-Just/DOJ)
 - b. Choice Of Court (EU-Just/DOJ)
6. Issues of Ongoing Importance (Italian Presidency, comments by EU and US)
 - a. Visa Waiver/Reciprocity
 - b. Drugs
 - c. Smart Borders
 - d. Hague Convention
 - e. Judgment project
 - f. Victim's Rights
7. Priorities of the Latvian Presidency
8. Any Other Business

Page 01 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1 of 7

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 7

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 7

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 4 of 7

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 5 of 7

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 6 of 7

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 7 of 7

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

MEETING WITH MAJOR CITIES CHIEFS ASSOCIATION

Background Information on Funding for Complex Coordinated Terrorist Attacks (CCTA) Initiative and Countering Violent Extremism Fiscal Year 2016 and DHS Appropriations Act and Joint Explanatory Statement (pertinent parts)

- The Fiscal Year 2016 DHS Appropriations Act provided \$50 million in grant funds to help state and local communities strengthen their counterterrorism efforts. Within that \$50 million, \$39 million is for an initiative to prepare for, prevent, and respond to complex coordinated terrorist attacks, \$10 million is for an initiative to counter violent extremism, and \$1 million is to expand the Joint Counterterrorism Awareness Workshop Series.
- The overarching goal of the \$10 million grant awards is to prevent radicalization to violence. This will be accomplished by enhancing community resilience; developing non-law enforcement off-ramps for individuals being radicalized, recruited, or mobilized to violence; creating or amplifying counter messages to violent extremist narratives; and increasing the capacity of non-traditional partners. Based on the direction Congress provided in the Joint Explanatory Statement accompanying the FY 2016 Appropriations Act, DHS plans to make a wide variety of activities eligible under this initiative.
- As proposed, the complex coordinated terrorist attack program will provide technical assistance and funding to state and local jurisdictions to improve their ability to prepare for complex coordinated attacks like those that occurred in Mumbai, India, and more recently in Brussels, Paris, and San Bernardino. This program will help jurisdictions confront an evolving and dynamic terrorism threat; shifting from symbolic, highly planned Al'Qaeda style attacks, to attacks that could occur in any municipality, at any time.
 - Most of the \$39 million allocated to the program will be provided to state and local jurisdictions through grants/cooperative agreements to help them prepare for complex attacks through planning, training and exercises. Equipment will not be an allowable cost.

Relevant Legislative Text – FY 2016 Consolidated Appropriations Act (P.L. 114-113)

DIVISION F—Department of Homeland Security Appropriations Act, 2016

SEC. 543.

(a) For an additional amount for emergent threats from violent extremism and from complex, coordinated terrorist attacks, \$50,000,000 to remain available until September 30, 2017.

(b) Funds made available in subsection (a) for emergent threats may be transferred by the Secretary of Homeland Security between appropriations for the same purpose, notwithstanding section 503 of this Act.

(c) No transfer described in subsection (b) shall occur until 15 days after the Committees on Appropriations of the Senate and the House of Representatives are notified of such transfer.

1) Joint Explanatory Statement to Legislative Text (Relevant Section)

Responding to Emergent Threats from Violent Extremism

A general provision in title V of this Act provides \$50,000,000 for emergent threats from violent extremism and from complex, coordinated terrorist attacks, and allows the Secretary to transfer such funds between appropriations after notifying the Committees 15 days in advance. Within these funds, not more than \$10,000,000 is for a countering violent extremism (CVE) initiative to help states and local communities prepare for, prevent, and respond to emergent threats from violent extremism; not less than \$39,000,000 is for an initiative to help states and local governments prepare for, prevent, and respond to complex, coordinated terrorist attacks with the potential for mass casualties and infrastructure damage; and not less than \$1,000,000 shall be for expanding or enhancing the Joint Counterterrorism Awareness Workshop Series, which brings together federal, state, and local governments, and the private sector to help regions improve their counterterrorism preparedness posture, including the ability to address the threat of complex terrorist attacks.

All funds under the CVE initiative shall be provided on a competitive basis directly to states, local governments, tribal governments, nonprofit organizations, or institutions of higher education. Eligible activities for the CVE initiative shall include, but not be limited to, planning, developing, implementing, or expanding educational outreach, community engagement, social service programs, training, and exercises, as well as other activities as the Secretary determines appropriate. Existing programs should be utilized wherever practical. Eligible activities for the initiative related to complex coordinated terrorist attacks shall include, but not be limited to, planning, training and exercises to support plans, and other activities the Secretary determines appropriate, consistent with this statement.

Not later than 45 days after the date of enactment of this Act, the Department shall brief the Committees on plans for execution of the initiatives, to include timelines, goals, metrics, and how the Whole of Community will be included.

MEETING WITH MAJOR CITIES CHIEFS ASSOCIATION
Talking Points

Urban Area Security Initiative (UASI) Risk Formula

- Acknowledge that there have been concerns expressed by some major cities chiefs that the formula for determining an urban area's Risk Profile does not adequately assess the vulnerability, threat, and consequences of an UASI jurisdiction.
- Note that you are open to hearing their concerns and explain the criteria and process for calculating risk that ultimately determines the relative risk to UASI jurisdictions.

Law Enforcement Terrorism Prevention Activities (LETPA)

- Stress that DHS is committed to continuing its support to state and local law enforcement through its various grant programs. This includes regularly reviewing all aspects of the programs to ensure effectiveness, including the 25 percent of the Homeland Security Grant Program that is statutorily required to go to law enforcement terrorism prevention activities (LETPA).
- Explain that to enhance States' understanding of LETPA requirements, FEMA will identify the actual amount States' are required to claim as LETPA expenditures and provide that figure separately to each State annually.
- Explain that DHS would like the input of the law enforcement community regarding the list of expenses that they feel should qualify as LETPA under statute and annual funding announcements. The Department has not revisited this list since 2008, and a re-look is appropriate given the evolving threat. FEMA and the Office for State and Local Law Enforcement (OSLLE) will meet with law enforcement to seek this input.
 - Note that this is being done to address concerns that expenditures currently permitted and documented by states as LETPA are not properly focused on terrorism prevention activities that are current priorities of the law enforcement community.
 - Explain that based on the review, FEMA and OSLLE will make a determination on whether to adjust policy guidance for allowable LETPA expenditures (for those not prescribed by statute) and/or whether DHS should request statutory changes (for LETPA allowable expenditures prescribed by law). Any potential changes to the LETPA allowable expenditures that are not prescribed by law would be reflected in the FY 2017 Notice of Funding Opportunity and FY 2017 Grant Guidelines.
- Note that you have been working with FEMA and OSLLE to strengthen and formalize the relationship and role in reviewing LETPA expenditures so that the goals of the law enforcement terrorism prevention program are best addressed.

- Explain that starting with FY 2016 grant reporting and going forward, OSLE, along with FEMA, will review state-submitted expenditure reports and reported LEPTA. Any potential discrepancy between Grant Guidance on LETPA expenditures and actual expenditures will be documented by OSLE and submitted to FEMA for review. OSLE will also work with FEMA to develop an LEPTA Summary Report that will be released to law enforcement annually.

Funding for Complex Coordinated Terrorist Attack (CCTA) Program and Countering Violent Extremism (CVE)

- Explain that in the Fiscal Year 2016 DHS Appropriations Act, Congress provided \$50 million in grant funds to help state and local communities strengthen their counterterrorism efforts.
- Note that within that \$50 million, \$39 million is for an initiative to prepare for, prevent, and respond to complex coordinated terrorist attacks, \$10 million is for an initiative to counter violent extremism, and \$1 million is to expand the Joint Counterterrorism Awareness Workshop Series.
 - Emphasize that these initiatives will enhance local law enforcement's ability to, prepare for, prevent, and respond to acts of terrorism.
- Explain that the overarching goal of the \$10 million grant awards is for a countering violent extremism initiative, to be awarded competitively to law enforcement, states, local governments, tribal governments, non-profit organizations, community based organizations, and institutions of higher education.
- Note that this will be accomplished by enhancing community resilience; developing non-law enforcement off-ramps for individuals being radicalized, recruited, or mobilized to violence; creating or amplifying counter messages to violent extremist narratives; and increasing the capacity of non-traditional partners.
- Explain that the Office for Community Partnerships and FEMA Grants Program Directorate, will jointly administer the competitive program, which will encourage innovation, cost effectiveness, quality performance measures, and whole-of-society partnerships.
 - Indicate that based on the direction Congress provided in the Joint Explanatory Statement accompanying the FY 2016 Appropriations Act, DHS plans to make a wide variety of activities eligible under this initiative.
 - Note that DHS will be issuing a notice of funding opportunity for the grant this Summer.
- Explain that as proposed, the complex coordinated terrorist attack program will provide technical assistance and funding to state and local jurisdictions to improve

their ability to prepare for complex coordinated attacks like those that occurred in Mumbai, India, and more recently in Brussels, Paris, and San Bernardino.

- Explain that at your direction, MCCA, along with other law enforcement associations, have been meeting with DHS and FEMA to provide their input into how they believe the new grant initiative should be structured. Note that these recommendations were relayed to FEMA last week and we look forward to continuing the discussion on how this initiative can best support our state and local partners.
- Note that this program will help jurisdictions confront an evolving and dynamic terrorism threat; shifting from symbolic, highly planned Al'Qaeda style attacks, to attacks that could occur in any municipality, at any time.
- Explain that most of the \$39 million allocated to the program will be provided to state and local jurisdictions through grants/cooperative agreements to help them prepare for complex attacks through planning, training and exercises.

NPPD Reorganization and the Office of Emergency Communications

- Acknowledge the concerns of state and local law enforcement and other first responders about the proposed NPPD reorganization and its effect on the Office of Emergency Communications. Note that you understand the concerns and have been working with NPPD, OEC, and others to address them.

Criminal History Records Information (CHRI)

- Ask that MCCA support DHS's full and unfettered access to criminal history records information, which will help prevent crime and assess security threats.
 - Acknowledge that we have made some progress, but we have more to do and you hope you will support our efforts to expand DHS's access to CHRI for all components with an authorized need for this information.
- Explain that under current interpretation of the National Crime Prevention and Privacy Act ("Compact Act") certain DHS components and activities are considered "non-criminal justice" and, as a result, face restrictions which significantly impact their ability to access and use CHRI that would be relevant and material to conducting full risk assessments.
 - Explain that 11 states (including CA, PA, TX, WA, IL, KY, ND, NE, RI, DE, ME) do not share their records or share minimal information per their state statutes for non-criminal justice purposes. Given the populations involved, this has a substantial impact when conducting background checks on individuals who may have a criminal history in these states and have applied for certain benefits or credentials.

FOR OFFICIAL USE ONLY

- Note that current restrictions do not reflect the new paradigm created in the wake of 9/11, nor the reality that background checks which were previously conducted simply for eligibility purposes are now an essential element of a security threat assessment.
- Explain that since 9/11 the threat has continued to evolve and recent events highlight the importance of having all relevant information available. Note that new challenges keep emerging, as such:
 - The threat of foreign fighters going to Syria and Iraq and returning to our homeland.
 - The largest number of refugees moving to the West since World War II.
 - The need to protect our critical infrastructure and the people who work there from lone wolf attacks.
 - Ensuring all of our Aviation Workers including baggage handlers, and others accessing secure areas are thoroughly cleared
- Explain that current limitations on how we share CHRI with DHS has not kept up. Explain that where Congress has given us many new authorities in the Patriot Act and other legislations, when it comes to CHRI, we are still operating under statutes which pre-date the 9/11 terrorist attacks and are almost 20 years old.
- Highlight that one recent exception was contained in the National Defense Authorization Act (NDAA) of 2016. This language was in response to the 2013 Navy Yard shooting and authorized expanded access to CHRI for DHS and others for the limited purposed federal employee and contractor suitability background investigations (amending §5 USC 9101).
- Emphasize that we need reexamine how we share CHRI within the DHS enterprise and its varied mission requirements, and we are looking for their support.
 - Note that specifically, we need to take another look at what defines criminal justice purpose or criminal justice agency and see where these definitions are impeding appropriate information sharing; . . . [O]r amend other statutes [e.g., the National Security Exception under § 9101] in order to expand DHS access to CHRI for what has traditionally been considered noncriminal justice purposes (i.e., immigration, transportation security, and other).

Staff Responsible for Taking Points: John Iorio, Chief of Staff, OPE/SLLE. (b)(6)

(b)(6)

OGC Reviewer: Kaiya Pontinen, Deputy Chief of Staff, OGC. (b)(6)

**MEETING WITH MAJOR CITIES CHIEFS ASSOCIATION
June 13, 2016**

Overview:

- You will meet with members of the Major Cities Chiefs Association (MCCA) to discuss various homeland security issues including grants, the NPPD reorganization, and the sharing of criminal history records information.
- You will be staffed by Deputy Chief of Staff Jennifer Higgins and OPE/SLLE Assistant Secretary Heather Fong. A full list of participants is below.
- The meeting is **CLOSED PRESS**.

Discussion Points:

- Acknowledge that you are aware there are concerns by some major cities chiefs that the formula for determining an urban area's Risk Profile does not adequately assess the vulnerability, threat, and consequences of an Urban Area Security Initiative (UASI) jurisdiction.
 - Note that you are open to hearing their concerns and explain the criteria and process for calculating risk that ultimately determines the relative risk of Urban Area Security Initiative jurisdictions.
- Explain DHS's plan to address stakeholder concerns regarding funding for Law Enforcement Terrorism Prevention Activities (LEPTA), which includes a comprehensive review of allowable expenditures under the program, strengthening and formalizing OPE/SLLE's role in reviewing Law Enforcement Terrorism Prevention Activity expenditures, and explicitly identifying actual amounts States' are required to claim as Law Enforcement Terrorism Prevention Activity expenditures.
- Explain that in the Fiscal Year 2016 DHS Appropriations Act, Congress provided \$50 million in grant funds to help state and local communities strengthen their counterterrorism efforts. Note that within that \$50 million, \$39 million is for an initiative to prepare for, prevent, and respond to complex coordinated terrorist attacks, \$10 million is for an initiative to counter violent extremism, and \$1 million is to expand the Joint Counterterrorism Awareness Workshop Series. Emphasize that these initiatives will enhance local law enforcement's ability to prevent, prepare for, and respond to acts of terrorism.
 - Explain that at your direction, the Major Cities Chiefs Association, along with other law enforcement associations, have been meeting with DHS and FEMA to provide their input into how they believe the new grant initiative for complex, coordinated attacks should be structured. Note that these recommendations were relayed to FEMA last week and we look forward to continuing the discussion on how this initiative can best support our state and local partners.
- Acknowledge the concerns of state and local law enforcement and other first responders about the proposed NPPD reorganization and its effect on the Office of

Emergency Communications. Note that you understand the concerns and are working with NPPD, OEC, and others to address them.

- Explain that some DHS components (e.g., TSA and USCIS) have limited access to criminal history records information because their use is not currently deemed to be for a criminal justice purpose.
 - Ask that the Association support DHS's full, unfettered access to criminal history records information, which will help prevent crime and assess security threats.
 - Note that current restrictions do not reflect the new paradigm created in the wake of 9/11, nor the reality that background checks which were previously conducted simply for eligibility purposes are now an essential element of a security threat assessment.

Background:

- You last met with Major Cities Chiefs Association members collectively in October 2015 in Chicago, Illinois during the International Association of Chiefs of Police Annual Conference. You discussed immigration enforcement and the Priority Enforcement Program, DHS support for the Criminal Intelligence Enterprise, and interoperable communications.

Participants:

Deputy Secretary Mayorkas

Heather Fong, Assistant Secretary, OPE/SLLE

Chuck DeWitt, Representative, Major Cities Chiefs Association

Tom Manger, Police Chief (Association President), Montgomery County (Maryland) Police Department

Art Acevedo, Police Chief, (Association Vice President), Austin (Texas) Police Department

Joe Lombardo, Sheriff, (Homeland Security Committee Chairman), Las Vegas Metropolitan Police Department

Darrel Stephens, Executive Director, Major Cities Chiefs Association

Shawn Jones, Assistant Chief, Atlanta Police Department

Michael Dvorak, Assistant Chief, Mesa (Arizona) Police Department

Jaime Ayala, Assistant Chief, Arlington (Texas) Police Department

Attachments:

A. Talking Points

B. Letter to Secretary Johnson from Representatives Heck, Modei, and Hardy (January 21, 2016)

C. Response Letter from Assistant Administrator Kamoie to Representatives Heck, Modei, and Hardy (March 1, 2016)

D. Background information on grants for Complex, Coordinated Terrorist Attacks and Countering Violent Extremism and Fiscal Year 2016 DHS Appropriations Act and Joint Explanatory Statement (pertinent parts)

- E. Criminal History Records Information and Operational Impact on DHS Components
- F. Biographies

Staff Responsible for Briefing Memo: John Iorio, Chief of Staff, OPE/SLLE (b)(6)

(b)(6)

OGC Reviewer: Kaiya Pontinen, Deputy Chief of Staff, OGC. (b)(6)

Page 1 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Law Enforcement Terrorism Prevention Program Expenditures

October 13, 2015

Fiscal Year 2015 Report to Congress



Homeland
Security

Federal Emergency Management Agency

DHS-001-425-008044

Message from the Administrator

October 13, 2015

I am pleased to submit the following report, “Law Enforcement Terrorism Prevention Program Expenditures,” prepared by the Federal Emergency Management Agency (FEMA).

This report was compiled in response to Senate Report 113-198 accompanying the *Fiscal Year 2015 Department of Homeland Security Appropriations Act* (P.L. 114-4). This updated report provides details on Law Enforcement Terrorism Prevention Program activities and expenditures to date, and their applicability to prevention. More specifically, the report aims to demonstrate how FEMA homeland security grant dollars currently are, and will continue to be, dedicated toward law enforcement terrorism prevention-oriented planning, organization, training, exercise, and equipment activities. All data are provided by the FEMA Grant Programs Directorate, and are current as of March 31, 2015.



Pursuant to congressional requirements, this report is provided to the following Members of Congress:

The Honorable John R. Carter
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Lucille Roybal-Allard
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable John Hoeven
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable Jeanne Shaheen
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

Inquiries related to this report may be directed to me at (202) 646-3900 or to the Department’s Deputy Under Secretary for Management and Chief Financial Officer, Chip Fulghum, at (202) 447-5751.

Sincerely,

A handwritten signature in blue ink, appearing to read "W. Craig Fugate".

W. Craig Fugate
Administrator
Federal Emergency Management Agency



Law Enforcement Terrorism Prevention Program Expenditures

Table of Contents

| | |
|---|----|
| I. Legislative Language | 1 |
| II. Background | 3 |
| III. Notice of Funding Opportunity Language Addressing the Law Enforcement Terrorism Prevention Program..... | 4 |
| IV. FEMA Funding Directed to the Law Enforcement Terrorism Prevention Program | 7 |
| V. Examples of Law Enforcement Terrorism Prevention Program-Funded Projects .. | 12 |
| VI. Conclusion..... | 25 |

I. Legislative Language

This report was compiled pursuant to Senate Report 113-198 accompanying the *Fiscal Year (FY) 2015 Department of Homeland Security (DHS) Appropriations Act* (P.L. 114-4), directing FEMA to update the current report, which was previously submitted pursuant to Senate Report 113-77, accompanying the *FY 2014 DHS Appropriations Act* (P.L. 113-76).

Senate Report 113-198 states:

Law Enforcement Terrorism Prevention Program

In accordance with section 2006 of the Homeland Security Act of 2002, the Law Enforcement Terrorism Prevention Program [LETPP] is funded through a required set aside of 25 percent of the funds appropriated through the SHSGP¹ and UASI programs. The Committee directs FEMA to provide clear guidance to States and urban areas to ensure that the intent of LETPP is fully realized. FEMA is directed to provide an update of the report on expenditures for prevention activities, as required in Senate Report 113-77, no later than 120 days after the date of enactment of this act.

This report is submitted to the House and Senate Committees on Appropriations in fulfillment of this requirement.

With regard to program expenditures, section 2006(a) of the *Homeland Security Act of 2002*, as amended (P.L. 107-296), includes the following requirement:

(a) Law Enforcement Terrorism Prevention Program

(1) In General.— The Administrator shall ensure that not less than 25 percent of the total combined funds appropriated for grants under sections 2003 and 2004 is used for law enforcement terrorism prevention activities.

¹ The State Homeland Security Program (SHSP) as outlined in the Fiscal Year 2015 Notice of Funding Opportunity is referred to in Senate Report 113-198 as the State Homeland Security Grant Program (SHSGP). These two acronyms can be used interchangeably.

Section 2006(a) of the *Homeland Security Act of 2002*, as amended, also includes the following allowable Law Enforcement Terrorism Prevention Activities:

(2) Law enforcement terrorism prevention activities

Law enforcement terrorism prevention activities include—

- (A) information sharing and analysis;
- (B) target hardening;
- (C) threat recognition;
- (D) terrorist interdiction;
- (E) overtime expenses consistent with a State homeland security plan, including for the provision of enhanced law enforcement operations in support of Federal agencies, including for increased border security and border crossing enforcement;
- (F) establishing, enhancing, and staffing with appropriately qualified personnel State, local, and regional fusion centers that comply with the guidelines established under section 124h (i) of this title;
- (G) paying salaries and benefits for personnel, including individuals employed by the grant recipient on the date of the relevant grant application, to serve as qualified intelligence analysts;
- (H) any other activity permitted under the Fiscal Year 2007 Program Guidance of the Department for the Law Enforcement Terrorism Prevention Program; and
- (I) any other terrorism prevention activity authorized by the Administrator.

II. Background

With the enactment of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (P.L. 110-53) (“9/11 Act”) and the *FY 2008 Consolidated Appropriations Act* (P.L. 110-161), the Law Enforcement Terrorism Prevention Program (LETTP) was no longer recognized or funded as a “stand-alone” preparedness grant program. Instead, section 2006(a) of the *Homeland Security Act of 2002* (P.L. 107-296), as amended by the 9/11 Act, requires the FEMA Administrator to ensure that not less than 25 percent of the total combined funds appropriated under sections 2003 and 2004 of the *Homeland Security Act of 2002*, as amended, are dedicated toward law enforcement terrorism prevention activities. Such activities include planning, organization, training, exercises, and equipment procurement.

Under the current LETTP construct, preparedness grant funds continue to build state, local, and tribal law enforcement capabilities to prevent terrorist attacks and provide law enforcement and public safety communities with funds to support critical prevention activities. FEMA preparedness grant programs funded under sections 2003 and 2004 of the *Homeland Security Act of 2002*, as amended, provide funding to all 56 States, territories, and tribes, as well as to high-risk urban areas, based on a combination of formula, risk, and effectiveness, for LETTP activities.

III. Notice of Funding Opportunity Language Addressing the Law Enforcement Terrorism Prevention Program

Pages 5 and 6 of the FY 2015 Homeland Security Grant Program (HSGP) Notice of Funding Opportunity clearly states the 25 percent LETPP requirement as follows:

- ***Consolidation of Law Enforcement Terrorism Prevention Activities (LETPA)***

Per section 2006 of the Homeland Security Act of 2002, as amended, (6 U.S.C. § 607), DHS/FEMA is required to ensure that at least 25 percent (25%) of grant funding appropriated for the Homeland Security Grant Program and Tribal Homeland Security Grant Program are used for law enforcement terrorism prevention activities. DHS/FEMA meets this requirement, in part, by requiring all SHSP and [Urban Areas Security Initiative (UASI)] recipients to ensure that at least 25 percent (25%) of the combined HSGP funds allocated under SHSP and UASI are dedicated towards law enforcement terrorism prevention activities, as defined in 6 U.S.C. Section 607. The LETPA² allocation can be from SHSP, UASI or both. This requirement does not include awards funds from OPSG. Please refer to Appendix A – FY 2015 Program Allocations [in the 2015 HSGP NOFO] for LETPA minimum allocations for SHSP and UASI by jurisdiction. The 25% LETPA allocation is in addition to the 80% pass through requirement to local governments and Tribes, referenced below.

Further, each year, FEMA works with internal and external stakeholders throughout the homeland security community to ensure that all Notices of Funding Opportunity (NOFO) support the National Preparedness Goal by accurately capturing funding priorities and guiding recipients in closing capability gaps through various planning, organization, training, exercise, and equipment projects.

The following specific language is included within the FY 2015 HSGP NOFO and delineates allowable activities under the LETPP.

From page 6 of the FY 2015 Homeland Security Grant Program NOFO:

The National Prevention Framework describes those activities that should be executed upon the discovery of intelligence or information regarding an imminent threat to the homeland, in order to thwart an initial or follow on terrorist attack,

² Law Enforcement Terrorism Prevention Activities (LETPA) can be used interchangeably with Law Enforcement Prevention Program (LETPP) activities.

and provides guidance to ensure the Nation is prepared to prevent, avoid, or stop a threatened or actual act of terrorism. Activities outlined in the National Prevention Framework are eligible for use of LETPA focused funds. In addition, where capabilities are shared with the protection mission area, the National Protection Framework activities are also eligible. Other terrorism prevention activities proposed for funding under LETPA must be approved by the FEMA Administrator.

Additional allowable LETPP costs and activities are specified beginning on page 54 of the FY 2015 HSGP NOFO to include:

- ***Law Enforcement Terrorism Prevention Allowable Costs (SHSP and UASI)***

Activities eligible for use of LETPA focused funds are outlined in the National Prevention Framework (and where capabilities are shared with the protection mission area, the National Protection Framework) and include but are not limited to:

- *Maturation and enhancement of designated state and major Urban Area fusion centers, including information sharing and analysis, threat recognition, terrorist interdiction, and training/ hiring of intelligence analysts;*
- *Coordination between fusion centers and other analytical and investigative efforts including, but not limited to Joint Terrorism Task Forces (JTTFs), Field Intelligence Groups (FIGs), High Intensity Drug Trafficking Areas (HIDTAs), Regional Information Sharing Systems (RISS) Centers, criminal intelligence units, and real-time crime analysis centers;*
- *Implementation and maintenance of the Nationwide SAR Initiative, including training for front line personnel on identifying and reporting suspicious activities;*
- *Implementation of the “If You See Something, Say Something™” campaign to raise public awareness of indicators of terrorism and terrorism-related crime and associated efforts to increase the sharing of information with public and private sector partners, including nonprofit organizations. Note: DHS/FEMA requires that the Office of Public Affairs be given the opportunity to review and approve any public awareness materials (e.g., videos, posters, tri-folds, etc.) developed using HSGP grant funds for the “If You See Something, Say Something™” campaign to ensure these materials are consistent with the Department’s messaging and strategy for the campaign and the initiative’s trademark;*

- *Training for countering violent extremism; development, implementation, and/or expansion of programs to engage communities that may be targeted by violent extremist radicalization; and the development and implementation of projects to partner with local communities to prevent radicalization to violence, in accordance with the Strategic Implementation Plan (SIP) to the National Strategy on Empowering Local Partners to Prevent Violent Extremism in the United States; and*
- *Increase physical security, through law enforcement personnel and other protective measures by implementing preventive and protective measures at critical infrastructure sites or at-risk nonprofit organizations.*

IV. FEMA Funding Directed to the Law Enforcement Terrorism Prevention Program

A. Total Law Enforcement Terrorism Prevention (LETPP) Expenditures from FY 2008 – FY 2014

Section 2006(a) of the *Homeland Security Act of 2002*, as amended, directs the FEMA Administrator to ensure that not less than 25 percent of the total combined funds appropriated for grants under sections 2003 and 2004 of that Act are used for law enforcement terrorism prevention activities. Preparedness grants funded under the authority of those sections of the Act by annual appropriations acts include the State Homeland Security Program (SHSP), Urban Area Security Initiative (UASI), Operation Stonegarden (OPSG), Tribal Homeland Security Grant Program (THSGP), and UASI Nonprofit Security Grant Program (NSGP). A summary of LETPP expenditures for all of these programs for FY 2008 through FY 2014 is located in Table 1.

Based on the data in Table 1, the minimum amount of funds required to be set aside for the LETPP as required by statute from FY 2008 – FY 2014 was \$2,356,172,785. State Administrative Agencies (SAA) and tribal governments have reported that recipients have dedicated an aggregate of \$3,381,387,094 to LETPP activities from FY 2008 – FY 2014, which is \$1,025,214,309 beyond the statutory minimum required. Overall, LETPP expenditures represent 36 percent of total funding under sections 2003 and 2004 of the *Homeland Security Act of 2002*, as amended.

Table 1- LETPP Expenditures by Program for FY 2008- FY 2014³

| Sections 2003 and 2004 Preparedness Grants LETPP Expenditures for FY 2008- FY 2014 | | | | | | | | | | |
|--|------------------------|------------------------|-----------------------|---------------------|-------------------|---------------------------------|----------------------------------|-------------------------|---------------------------------------|---|
| Grant Award Year | SHSP Expenditures | UASI Expenditures | OPSG Expenditures | THSGP Expenditures | NSGP Expenditures | Total Annual LETPP Expenditures | Total Annual Combined Allocation | LETPP 25% Minimum | LETPP Expenditures Beyond 25% Minimum | LETPP Expenditures as Percentage of Total Combined Allocation |
| FY 2008 | \$240,607,329 | \$223,667,647 | \$ 55,450,000 | \$ 289,261 | * | \$520,014,237 | \$1,719,555,000 | \$ 429,888,750 | \$90,125,487 | 30% |
| FY 2009 | \$287,361,302 | \$231,429,065 | \$ 86,289,114 | \$ 100,250 | * | \$605,179,732 | \$1,766,556,250 | \$ 441,639,063 | \$163,540,669 | 34% |
| FY 2010 | \$276,666,899 | \$220,640,225 | \$ 39,058,199 | \$ 1,556,544 | * | \$537,921,867 | \$1,763,520,000 | \$ 440,880,000 | \$97,041,867 | 31% |
| FY 2011 | \$233,855,785 | \$255,126,549 | \$ 54,720,789 | \$ 1,095,903 | * | \$544,799,026 | \$1,273,348,200 | \$ 318,337,050 | \$226,461,976 | 43% |
| FY 2012 | \$111,992,484 | \$200,062,294 | \$ 46,321,879 | \$ 433,436 | * | \$358,810,091 | \$846,976,000 | \$ 211,744,000 | \$147,066,091 | 42% |
| FY 2013 | \$124,934,544 | \$213,939,326 | \$ 54,119,293 | \$ 728,512 | * | \$393,721,675 | \$988,389,689 | \$ 247,097,422 | \$146,624,253 | 40% |
| FY 2014 | \$165,913,340 | \$201,533,443 | \$ 51,715,744 | \$ 1,777,938 | * | \$420,940,465 | \$1,066,346,000 | \$ 266,586,500 | \$154,353,965 | 39% |
| Grand Total | \$1,441,331,683 | \$1,546,398,549 | \$ 387,675,018 | \$ 5,981,843 | * | \$3,381,387,094 | \$9,424,691,139 | \$ 2,356,172,785 | \$1,025,214,309 | 36% |

³ Table 1 represents LETPP expenditures for each program. For example, "SHSP Expenditures" refers only to LETPP-obligated funds within SHSP. FY 2008 expenditures are final. FY 2009-2014 expenditures reflect obligations reported by recipients and are current as of the December 2014 Biannual Strategy Implementation Report. These figures are subject to change depending on final obligations and reporting by recipients and financial closeout of the underlying grant awards. "Total Annual Combined Allocation" represents the total amount of appropriated funds dedicated to programs authorized under sections 2003 and 2004 of the *Homeland Security Act of 2002*, as amended (SHSP, UASI, OPSG, THSGP, NSGP).

* NSGP recipients currently are not required to distinguish between law enforcement terrorism prevention activities and other allowable expenditures when reporting on activities.

Expenditure reports pulled from FEMA’s Grants Reporting Tool (GRT) capture expenditures at a moment in time and can vary based on project progress, if all projects are reported accurately, disallowed costs, and other factors. This results in the fluctuation of expenditures reported in Tables 1-5 when compared to the data submitted in the 2014 Report to Congress on LETPP Expenditures. FEMA is actively seeking alternatives to current data collection systems that will enable FEMA, SAAs, and recipients to categorize expenditures more precisely and reconcile those numbers with actual expenditures.

B. LETPP Expenditures within SHSP and UASI

Since the enactment of the 9/11 Act, it has been FEMA’s policy to provide guidance to States and urban areas requiring each recipient to ensure that at least 25 percent of their SHSP and UASI awards, exclusive of OPSG, are dedicated toward LETPP. This policy helps FEMA to ensure that it meets the LETPP minimums prescribed by Section 2006(a) of the *Homeland Security Act of 2002*, as amended, and furthers the Congressional intent of the program.

A summary of UASI and SHSP expenditures directed to LETPP activities compared to the LETPP minimums for FY 2008 – FY 2014 can be found in Table 2. Table 2 illustrates how states and urban areas have dedicated anywhere from 28-41 percent of the total combined SHSP and UASI allocations to LETPP. The 7-year LETPP total for SHSP and UASI combined is 34 percent.

Table 2 – SHSP and UASI LETPP Expenditures for FY 2008–FY 2014⁴

| Grant Award Year | SHSP & UASI LETPP Expenditures for FY 2008- FY 2014 | | | | | | | | |
|------------------|---|--------------------|------------------|--------------------|----------------------|-------------------|--------------------------|---------------------------------------|--|
| | SHSP | | UASI | | SHSP & UASI Combined | | | | |
| | Allocation | LETPP Expenditures | Allocation | LETPP Expenditures | Total Allocation | LETPP 25% Minimum | Total LETPP Expenditures | LETPP Expenditures Beyond 25% Minimum | LETPP Expenditures as Percentage of total Allocation |
| FY 2008 | \$ 861,280,000 | \$ 240,607,329 | \$ 781,630,000 | \$ 223,667,647 | \$ 1,642,910,000 | \$ 410,727,500 | \$ 464,274,976 | \$ 53,547,476 | 28% |
| FY 2009 | \$ 861,137,000 | \$ 287,361,302 | \$ 798,631,250 | \$ 231,429,065 | \$ 1,659,768,250 | \$ 414,942,063 | \$ 518,790,368 | \$ 103,848,305 | 31% |
| FY 2010 | \$ 842,000,000 | \$ 276,666,899 | \$ 832,520,000 | \$ 220,640,225 | \$ 1,674,520,000 | \$ 418,630,000 | \$ 497,307,124 | \$ 78,677,124 | 30% |
| FY 2011 | \$ 526,874,100 | \$ 233,855,785 | \$ 662,622,100 | \$ 255,126,549 | \$ 1,189,496,200 | \$ 297,374,050 | \$ 488,982,334 | \$ 191,608,284 | 41% |
| FY 2012 | \$ 294,000,000 | \$ 111,992,484 | \$ 490,376,000 | \$ 200,062,294 | \$ 784,376,000 | \$ 196,094,000 | \$ 312,054,777 | \$ 115,960,777 | 40% |
| FY 2013 | \$ 354,644,123 | \$ 124,934,544 | \$ 558,745,566 | \$ 213,939,326 | \$ 913,389,689 | \$ 228,347,422 | \$ 338,873,870 | \$ 110,526,448 | 37% |
| FY 2014 | \$ 401,346,000 | \$ 165,913,340 | \$ 587,000,000 | \$ 201,533,443 | \$ 988,346,000 | \$ 247,086,500 | \$ 367,446,783 | \$ 120,360,283 | 37% |
| Grand Total | \$ 4,141,281,223 | \$ 1,441,331,683 | \$ 4,711,524,916 | \$ 1,546,398,549 | \$ 8,852,806,139 | \$ 2,213,201,535 | \$ 2,987,730,232 | \$ 774,528,698 | 34% |

Entities that are awarded and accept federal funding must agree to abide by the terms of the grant, including reporting requirements. Recipients are required to submit biannual reports back to FEMA through the Biannual Strategy Implementation Report (BSIR).

⁴ LETPP minimums in Table 2 represent 25 percent of the funding allocated to each respective grant program – SHSP, UASI, or both. References to SHSP in Table 2 do not include OPSG. FY 2008 expenditures are final. FY 2009-2014 expenditures reflect obligations reported by recipients and are current as of the December 2014 BSIR. These figures are subject to change depending on final obligations and reporting by recipients and financial closeout of the underlying grant awards. “Total Annual Combined Allocation” represents the total amount of appropriated funds dedicated to programs authorized under sections 2003 and 2004 of the *Homeland Security Act of 2002*, as amended.

The BSIR is a compilation of data provided directly from the recipients. Recipients are expected to categorize expenditures appropriately when submitting their reports. Because of this limitation, the validity of the report relies heavily on the accuracy of the data provided by recipients.

For Tables 3-5, FY 2008 expenditures are final. FY 2009-2014 expenditures reflect obligations reported by recipients and are current as of the December 2014 BSIR. These figures are subject to change depending on final obligations and reporting by recipients and financial closeout of the underlying grant awards. FY 2015 grants have not yet been awarded; therefore, expenditures have not been incurred and tables within this report do not include data for FY 2015. LETPP activity expenditures are broken out further by the planning, organization, equipment, training, and exercises categories in Tables 3-5 below:

Table 3- SHSP and UASI LETPP Expenditures by Category for FY 2008–FY 2014

| Grant Award Year | Solution Area | SHSP | UASI | Total |
|--------------------------|---------------------|-------------------------|-------------------------|-------------------------|
| FY 2008 | Planning | \$20,979,797.55 | \$16,209,780.73 | \$37,189,578.28 |
| | Organization | \$6,676,407.70 | \$15,201,528.05 | \$21,877,935.75 |
| | Equipment | \$195,577,144.63 | \$178,152,898.99 | \$373,730,043.62 |
| | Training | \$15,980,036.51 | \$13,323,972.99 | \$29,304,009.50 |
| | Exercises | \$1,393,942.47 | \$779,466.36 | \$2,173,408.83 |
| Total for FY 2008 | | \$240,607,328.86 | \$223,667,647.12 | \$464,274,975.98 |
| FY 2009 | Planning | \$37,935,941.95 | \$39,563,922.61 | \$77,499,864.56 |
| | Organization | \$9,928,876.04 | \$22,476,261.03 | \$32,405,137.07 |
| | Equipment | \$213,722,210.73 | \$155,603,004.36 | \$369,325,215.09 |
| | Training | \$22,045,793.85 | \$9,031,890.58 | \$31,077,684.43 |
| | Exercises | \$3,728,479.85 | \$4,753,986.50 | \$8,482,466.35 |
| Total for FY 2009 | | \$287,361,302.42 | \$231,429,065.08 | \$518,790,367.50 |
| FY 2010 | Planning | \$37,885,380.64 | \$27,090,231.92 | \$64,975,612.56 |
| | Organization | \$11,740,778.77 | \$46,337,756.80 | \$58,078,535.57 |
| | Equipment | \$210,071,467.02 | \$132,624,361.26 | \$342,695,828.28 |
| | Training | \$14,945,006.05 | \$9,987,361.60 | \$24,932,367.65 |
| | Exercises | \$2,024,266.76 | \$4,600,513.29 | \$6,624,780.05 |
| Total for FY 2010 | | \$276,666,899.24 | \$220,640,224.87 | \$497,307,124.11 |
| FY 2011 | Planning | \$33,757,146.42 | \$35,474,186.95 | \$69,231,333.37 |
| | Organization | \$11,848,415.40 | \$31,275,665.99 | \$43,124,081.39 |
| | Equipment | \$147,012,676.62 | \$173,963,274.70 | \$320,975,951.32 |
| | Training | \$36,549,044.66 | \$11,661,262.14 | \$48,210,306.80 |
| | Exercises | \$4,688,502.08 | \$2,752,159.21 | \$7,440,661.29 |
| Total for FY 2011 | | \$233,855,785.18 | \$255,126,548.99 | \$488,982,334.17 |
| FY 2012 | Planning | \$14,519,687.58 | \$22,221,547.58 | \$36,741,235.16 |
| | Organization | \$8,759,042.32 | \$40,339,396.49 | \$49,098,438.81 |
| | Equipment | \$80,157,072.14 | \$118,353,078.69 | \$198,510,150.83 |
| | Training | \$7,347,907.57 | \$15,329,257.62 | \$22,677,165.19 |

| Grant Award Year | Solution Area | SHSP | UASI | Total |
|--------------------------|---------------|---------------------------|---------------------------|---------------------------|
| | Exercises | \$1,208,773.92 | \$3,819,013.24 | \$5,027,787.16 |
| Total for FY 2012 | | \$111,992,483.53 | \$200,062,293.62 | \$312,054,777.15 |
| FY 2013 | Planning | \$18,192,857.54 | \$23,950,900.59 | \$42,143,758.13 |
| | Organization | \$11,745,499.76 | \$55,404,649.57 | \$67,150,149.33 |
| | Equipment | \$78,420,692.74 | \$112,611,220.96 | \$191,031,913.70 |
| | Training | \$14,133,876.62 | \$19,731,789.18 | \$33,865,665.80 |
| | Exercises | \$2,441,617.54 | \$2,240,765.95 | \$4,682,383.49 |
| Total for FY 2013 | | \$124,934,544.20 | \$213,939,326.25 | \$338,873,870.45 |
| FY 2014 | Planning | \$19,405,200.30 | \$45,106,686.90 | \$64,511,887.20 |
| | Organization | \$8,816,624.27 | \$19,393,233.33 | \$28,209,857.60 |
| | Equipment | \$114,120,686.70 | \$118,479,470.34 | \$232,600,157.04 |
| | Training | \$20,312,966.84 | \$17,434,739.11 | \$37,747,705.95 |
| | Exercises | \$3,257,861.60 | \$1,119,313.70 | \$4,377,175.30 |
| Total for FY 2014 | | \$165,913,339.71 | \$201,533,443.38 | \$367,446,783.09 |
| Grand Total | | \$1,441,331,683.14 | \$1,546,398,549.31 | \$2,987,730,232.45 |

Table 4- OPSG LETPP Expenditures
by Category for FY 2008–FY 2014

| Grant Award Year | Solution Area | Total |
|--------------------------|---------------|--------------------------|
| FY 2008 | Planning | \$ 33,997,918.70 |
| | Equipment | \$ 21,452,081.30 |
| Total for FY 2008 | | \$ 55,450,000.00 |
| FY 2009 | Organization | \$ 26,595,499.14 |
| | Equipment | \$ 59,693,614.86 |
| Total for FY 2009 | | \$ 86,289,114.00 |
| FY 2010 | Organization | \$ 21,381,296.86 |
| | Equipment | \$ 17,676,902.14 |
| Total for FY 2010 | | \$ 39,058,199.00 |
| FY 2011 | Organization | \$ 23,818,527.67 |
| | Equipment | \$ 30,902,261.58 |
| Total for FY 2011 | | \$ 54,720,789.25 |
| FY 2012 | Organization | \$ 23,753,646.42 |
| | Equipment | \$ 22,568,232.27 |
| Total for FY 2012 | | \$ 46,321,878.69 |
| FY 2013 | Organization | \$ 38,391,476.90 |
| | Equipment | \$ 15,727,816.13 |
| Total for FY 2013 | | \$ 54,119,293.03 |
| FY 2014 | Organization | \$ 23,947,173.62 |
| | Equipment | \$ 27,768,570.53 |
| Total for FY 2014 | | \$ 51,715,744.15 |
| Grand Total | | \$ 387,675,018.12 |

Table 5- THSGP LETPP Expenditures
by Category for FY 2008–FY 2014

| Grant Award Year | Solution Area | Total |
|--------------------------|--------------------------|------------------------|
| FY 2008 | Equipment | \$ 265,261.08 |
| | Training | \$ 24,000.00 |
| Total for FY 2008 | | \$ 289,261.08 |
| FY 2009 | Planning | \$ 100,250.00 |
| | Total for FY 2009 | \$ 100,250.00 |
| FY 2010 | Planning | \$ 14,875.00 |
| | Equipment | \$ 1,513,489.00 |
| | Training | \$ 28,180.00 |
| Total for FY 2010 | | \$ 1,556,544.00 |
| FY 2011 | Planning | \$ 15,000.00 |
| | Organization | \$ 35,000.00 |
| | Equipment | \$ 1,026,981.00 |
| | Training | \$ 13,922.00 |
| | Exercises | \$ 5,000.00 |
| Total for FY 2011 | | \$ 1,095,903.00 |
| FY 2012 | Planning | \$ 7,000.00 |
| | Equipment | \$ 375,599.77 |
| | Training | \$ 44,162.86 |
| | Exercises | \$ 6,673.01 |
| Total for FY 2012 | | \$ 433,435.64 |
| FY 2013 | Equipment | \$ 728,511.50 |
| | Total for FY 2013 | \$ 728,511.50 |
| FY 2014 | Planning | \$ 27,000.00 |
| | Organization | \$ 4,204.00 |
| | Equipment | \$ 1,485,160.00 |
| | Training | \$ 247,773.00 |
| | Exercises | \$ 13,801.00 |
| Total for FY 2014 | | \$ 1,777,938.00 |
| Grand Total | | \$ 5,981,843.22 |

V. Examples of Law Enforcement Terrorism Prevention Program-Funded Projects

Law Enforcement Terrorism Prevention Program (LETPP)-funded projects build and sustain law enforcement capabilities related to the prevention of terrorism. The list below includes descriptions of some of the activities funded by the LETPP with FY 2013 – FY 2014 funding through which grant recipients have increased their prevention, protection, and response capabilities.

Alabama

In FY 2014, the Alabama Law Enforcement Agency (ALEA) awarded its Fusion Center \$550,000 for multiple projects, including communications equipment, software, and training for intelligence analysts. As a result of the technology, ALEA was able to provide information to another jurisdiction that resulted in the arrest of an individual suspected of involvement with a terrorist organization.

Alaska

The Municipality of Anchorage, Alaska, used \$234,592 of 2013 LETPP funds from the State Homeland Security Program to purchase an enhanced multi-mission robotic platform as well as ballistic armor for its Special Weapons and Tactics (SWAT) team. This investment allows for screening, search, and detection, and enhances law enforcement's capabilities to respond to all-hazards events.

American Samoa

American Samoa used LETPP funding to conduct critical law enforcement weapons training and to purchase equipment to support the Local Area Network Mobile Radio project for law enforcement communications.

Arizona

Arizona used \$36,638 of LETPP funds from the 2013 Urban Area Security Initiative to the Goodyear Police Department in order to provide for the continuation and enhancement of the Phoenix Urban Area Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Response Team strategy. This project will further enhance the Goodyear Police Department's capability to mitigate incidents from an all-hazards approach. Funding will increase the protection of officers and allow for multiple shifts by responding personnel. The enhancements improve the CBRNE response capabilities of Goodyear Police to support regional and statewide response.

Arkansas

In FY 2014, the Fort Smith Bomb Squad used \$189,000 of LETPP funds from the State Homeland Security Program to upgrade its existing bomb detection robot. Upgrades to the robot include wireless control and increased maneuverability. The safety of technicians is increased because the robot can be utilized in more situations, keeping the technicians out of the danger zone. In addition, the Squad will add radiation detection monitors, personal radiation dosimeters, and a Grid Aim X-ray system. This system will give the capability to perform precision disruption on an improvised nuclear device or radio detonation device. The squad will acquire additional personal protective equipment and a portable X-ray source & X-ray system that will support the Tactical Bomb Tech mission that is driven by the increasing number of active shooter incidents.

California

The Anaheim/Santa Ana urban area (ASAUA) used \$750,400 in LETPP funds from its 2014 Urban Area Security Initiative (UASI) grant award to sustain a countywide automated license plate reader (ALPR) system that allows data to be shared at a centralized server where all agencies have the ability to analyze and arrange data for their specific needs. This project is designed to fund the integration of multiple local data sources into the existing regional, state, and federal information systems. Through this data enrichment, the ASAUA will enhance its interdiction and disruption capabilities along with improving its intelligence and information sharing capabilities.

Colorado

In FY 2013, the Southwest Colorado Council of Government used \$19,938 of LETPP funds from the State Homeland Security Program grant to purchase body-worn video cameras to increase responder safety.

Connecticut

The Connecticut Department of Emergency Services and Public Protection used \$300,000 in LETPP funds from the 2014 State Homeland Security Program to assign multiple municipal law enforcement representatives to serve as Regional Intelligence Liaison Officers for 2-year periods as part of the Regional Intelligence Liaison Program (RILP). RILP enhances information sharing and collaboration with each of the municipal intelligence liaisons and lends critical support to the Connecticut Fusion Center mission.

Delaware

The State of Delaware is using \$65,850 in LETPP funds from the FY 2014 State Homeland Security Program to conduct a statewide facial recognition cleanup of the driver's license/identification card photo database. This process is essential in order to identify and investigate individuals who may have successfully obtained

multiple identities within the DMV database. This system scan will run a one-to-many random image data base sweep that will identify fraudulent applicants or Delaware driver's license and identification card holders with multiple identities. Evidence, once investigated, will be turned over to appropriate law enforcement officials.

District of Columbia

As part of the District of Columbia urban area, the Montgomery County Office of Emergency Management and Homeland Security used \$60,000 of LETPP funds from the 2013 UASI grant award to purchase composite sketch software to provide investigators tools to document suspect descriptions and transmit suspect information to other investigators. This is a new capability for the county and it is used to assist in identification and arrest by law enforcement of criminal suspects.

Florida

In October 2014, Polk County Emergency Management, in conjunction with the Polk County Sheriff's Office and School Board, conducted an active shooter exercise at Lake Gibson High School in Lakeland using \$20,000 in LETPP funding. The exercise served as a national training forum for active shooter incidents. It was transmitted via closed circuit television and hand-held cameras from Polk County Government TV to an audience of 500 school administrators and school resources officers from around the country who observed the event in the school auditorium.

Georgia

The Gwinnett County Police Department (Gwinnett PD) received \$3,996,188 in federal homeland security grant funding for equipment and training to support explosive ordnance disposal, SWAT, and CBRNE response capabilities. During a hostage incident, Gwinnett PD executed a rescue plan and successfully rescued the hostage victims. Gwinnett PD credits the use of grant funding for equipment and training as key to the success of this operation.

Guam

Using LETPP funds from FY 2013 and 2014 State Homeland Security Program grant awards, the Guam Office of Homeland Security matured and enhanced the Mariana Regional Fusion Center (Guam). Enhancements include increasing the capability for information sharing and analysis, target hardening, threat recognition, and terrorist interdiction. Additionally, funds were used for the hiring and training of intelligence analysts.

Hawaii

Hawaii utilized \$300,000 in LETPP funds to upgrade the Automated Fingerprint Identification System (AFIS) in all county police departments. The AFIS upgrade

includes fingerprint and facial recognition capabilities. Additionally, Hawaii will spend approximately \$500,000 in LETPP funds to upgrade all counties' law enforcement radio systems to enhance interoperable communications.

Idaho

The Fremont County Sherriff's Office used \$17,635 of LETPP funds from the 2014 State Homeland Security Program to purchase a digital fingerprint scanner.

Illinois

The Illinois Law Enforcement Training and Standards Board is using \$339,865 in LETPP funds from the 2014 State Homeland Security Program to continue to offer law enforcement intelligence sharing planning workshops. The workshops are delivered through the 16 Mobile Team Units, to more than 37,000 local law enforcement officers throughout the State of Illinois to: strengthen information-sharing and dissemination capabilities, counterterrorism investigations, and law enforcement capabilities. This project aligns with the State of Illinois' Homeland Security Strategic Plan, addressing Vision 2020 Priorities #1, as the various workshops offered will ensure that state and local public safety officials have access to the most current and comprehensive training and education available to prepare them for any realized emerging threats posing a risk or vulnerability to the state and for facilitation of standardized and safe implementation of response and recovery duties.

Operation Virtual Shield (OVS) is a program implemented in the City of Chicago, Illinois, that created the most extensive video surveillance network in the United States by linking more than 3,000 surveillance cameras to a centralized monitoring system that captures and processes camera feeds in real time. It is able to detect suspicious or dangerous activity and identify its location, and now incorporates facial recognition. OVS also is used to record activity at a potential crime scene before police arrive at a call. To date \$27,142,191 of LETPP funding from the Homeland Security Grant Program has been provided to support the OVS program, with more funding planned for future grant years.

Indiana

The Clinton County Emergency Management Agency is purchasing SWAT equipment for its law enforcement SWAT teams to help ensure their safety while performing many assigned responsibilities. In addition, Clinton County currently has mutual aid agreements signed with other counties, and the equipment will be available for those officers as needed. Equipment includes an outside public address system and push-to-talk tactical D switches that work on any communications device, including gas masks. This equipment, funded with \$7,408 of Homeland Security Grant Program dollars, will help to keep the SWAT members and citizens of Clinton County safe.

Iowa

The City of Des Moines used \$233,922 of LETPP funds from the 2014 State Homeland Security Program to sustain capabilities of Iowa's Weapons of Mass Destruction Tactical Task Force, in accordance with the National Incident Management System (NIMS) resource typing for Type-II tactical teams for counterterror investigation, law enforcement operations, and emergency public safety and security response.

Kansas

The Kansas City Highway Patrol (KHP) used \$66,218 in LETPP funds from the State Homeland Security Program to procure a truck for the KHP Hazardous Devices Unit (HDU). The KHP HDU's primary area of operation for improvised explosive device (IED) response covers 55 counties and a population of 447,012. The HDU is also the backup bomb squad for the Wichita Police Department and an additional 20 counties. The truck allows bomb and HazMat technicians to establish a command post in the working zone, house equipment, and work in a climate controlled environment. This equipment allows diagnostics, planning, and offensive operations rehearsals prior to deployment. It will be used to assist/augment other bomb squads at large events and crime scenes. The KHP bomb squad supported by this project meets standards for a NIMS Type-I team.

Kentucky

In FY 2014, the Newport Police Department used \$23,000 in LETPP funds to enhance special team response through the purchase of cybersecurity equipment and related items. This project develops a new capability for the Newport Police Department.

Louisiana

The West Feliciana Parish Sheriff's Office (WFPSO) used \$7,514 of LETPP funds from the 2014 State Homeland Security Program for the implementation of and connectivity to network-based systems to enhance intelligence and information-sharing capabilities. This was accomplished through the purchase of computers to enable compatibility with upgraded law enforcement systems. These computers will provide operating upgrades for WFPSO to utilize the same software in order to share information, reports, arrests, logs, calls, suspect information, and pending investigations as well as certain administrative functions.

Maine

Maine used \$255,000 in FY 2014 LETPP funds to support the Maine Information and Analysis Center (MIAC). As Maine's designated fusion center, the MIAC's mission is to collect, analyze and share intelligence. LETPP funds three analysts, one of whom focuses on Critical Infrastructure Protection. These three funded

positions ensure that the MIAC functions above the minimum staffing levels needed to fulfil its mandate under Gubernatorial Executive Order 24. As well as being the primary focal point for the State's intelligence and information-sharing capability, the MIAC, using LETPP funding, serves as the focal point for the State's cybersecurity program to ensure the capability to detect, respond to, and recover from cyber-attacks.

Maryland

The City of Baltimore Police Department was awarded \$345,000 of LETPP funds from the 2014 Urban Area Security Initiative to assess the vulnerability of and/or harden/protect critical infrastructure and key assets by investing in new and sustaining current fixed and portable CCTV systems. Additionally, the Baltimore Police Department was awarded with \$124,000 of the 2014 Urban Area Security Initiative grant for the sustainment and investment toward other law enforcement projects including K9 teams and bomb squads.

Massachusetts

The Massachusetts State Police used \$164,700 in LETPP funds from the 2014 State Homeland Security Program to procure a small unmanned aerial system for Air Wing tactical operations. This unmanned aerial system increases the Massachusetts State Police's capability to interdict and disrupt criminal activity.

Michigan

Michigan's Emergency Management Region 5 established tactical response team capabilities through a multi-year project. The Region used grant funding for procuring equipment and training to build a NIMS Type-II SWAT team. Ongoing sustainment of this project has been built into subsequent grant budgets with \$100,000 budgeted under the 2014 Homeland Security Grant Program and with future funding focused on supporting regionalized training needs. Since its inception, approximately \$891,000 has been spent on this multi-year project.

Minnesota

The Metropolitan Airports Commission used \$90,000 in LETPP funds from the 2014 State Homeland Security Program to support increased law enforcement presence at select Minnesota airports. The purchase of protective equipment for responders will maintain/sustain health and safety capabilities. Implementation of the "See Something, Say Something" program will increase public awareness of terrorism behaviors and substantially increase the reporting of those behaviors. Additionally, part of the funds will be used to train investigators to vet cases and share this information with analysts who specialize in terrorism analysis.

Mississippi

During the past 2 years, the Mississippi Office of Homeland Security has been building out a statewide ALPR system for information sharing. Currently the system consists of 10 camera locations throughout the state that collect license plate information on each vehicle as it passes the camera. The ALPR system then conducts an automated inquiry on the license plate to see if the vehicle may be stolen, or if the driver may be a wanted felon or a missing person/amber alert individual, or if the individual is on the terrorism watch list. A reply is generated and returned to local law enforcement in approximately 3 seconds from the time the vehicle passes the camera site. The Mississippi Office of Homeland Security was awarded \$200,000 in LETPP funds from the State's 2014 State Homeland Security Program award to further this capability.

Missouri

The Missouri Sheriff's Association used \$265,300 in LETPP funds from the State's 2014 State Homeland Security Program grant for planning, equipment sustainment, and enhancement for the Iris-Scan and Facial Recognition (IFR) project, which provides identity verification technology to collect unique identifiers of an individual. The IFR provides that information to intelligence networks and criminal databases to enhance law enforcement data collection.

Montana

The Montana Department of Justice is using \$383,298 on interactive law enforcement training equipment and a simulator. The simulator allows officers from across the state to engage in training events on a wide variety of scenarios. These simulators have been proven to enhance an officer's ability to recognize and respond to situations more quickly and effectively, and are in use by several federal and state law enforcement agencies, including the Federal Bureau of Investigation (FBI), the U.S. Marshals Service, and the Federal Law Enforcement Training Center.

Nebraska

Nebraska used \$172,968 in LETPP funds from its 2014 State Homeland Security Program grant to establish and maintain the baseline capabilities of the Nebraska Information and Analysis Center and for the integration of Nebraska State Patrol functions in support of coordination among state, local, regional, federal, Joint Terrorism Task Forces, and interstate partners in law enforcement and terrorism prevention as described in the Nebraska Homeland Security Strategy.

Nevada

Nevada used \$205,238 in LETPP funds from its 2014 State Homeland Security Program award to build and enhance its cybercrime detection capability through the Washoe County Sherriff's Office. Specific areas addressed in this project

include cyber forensics, cyber intrusion prevention, configuration management of cyber protection devices, and capabilities to interrupt and prevent malicious events in near-real time. By developing regional cyber capabilities in a standardized manner, metrics, information, and expert resources will be shared for maximum benefit.

New Hampshire

The New Hampshire State Police Explosives Operation Disposal (EOD) Unit is the only FBI-accredited EOD unit in the state and is complemented by the Nashua Police Department bomb unit, which has slightly less resource-typed capability. From FY 2012–FY 2014, \$567,950 in LETPP funds allowed for the purchase of equipment that was interoperable between these two teams. Funds also were invested to support joint training between these two teams. Without these funds, these opportunities for planning, training, and equipping would not have existed between these specialty units that must cover the entire state for EOD-related responses.

New Jersey

Middlesex County is using \$120,605 in LETPP funding to procure interactive visual collection and survey tools at the seven largest malls within the UASI region. Each mall operation will be provided a finished visual project that can be used for visual awareness and training for mall staff and security personnel. The completed project will also be provided to area first-response agencies to increase their visual awareness of the facility and to enhance their response capabilities. It will provide visual awareness to responders who may have never actually visited the facility. The project spans multiple locations within the UASI region. The project location listed is the procuring agency.

Morris County is using \$250,000 in LETPP funds from the State's 2014 UASI award to procure additional cameras and lighting to outfit the existing 20 MobilePro portable surveillance trailers previously funded in FY 2011 so that they can be easily deployed at any of the Critical Infrastructure/Key Resource (CI/KR) sites located in the region. This project will allow for the integration into existing software and allow portability and visibility within the UASI region. This equipment will enhance existing purchases and build out the capabilities. These trailers can be deployed at CI/KR locations on a routine/random basis or during heightened threat levels. They also can be deployed at special events when large crowds are expected to gather.

New Mexico

The City of Clovis in Curry County, New Mexico, is using \$40,000 in LETPP funds from the State's 2014 State Homeland Security Program award to purchase

Apollo Thermal Imaging System digital optics (night vision optics) for their Type III SWAT unit. This unit provides a regional response capability.

New York

The New York City Police Department (NYPD) is using \$19,619,852 in 2014 UASI LETPP funding for its Domain Awareness System (DAS). The DAS consists of an extensive network that has been built to support the transfer of video from the license plate readers and cameras to a dedicated law enforcement coordination center called the Lower Manhattan Security Coordination Center (LMSCC). The LMSCC is staffed by NYPD personnel and private-sector stakeholders from key sectors who work together to analyze video and data streams and to share information with key personnel at the Emergency Operations Center at Police Headquarters. The program is now operational in Lower and Midtown Manhattan with more than 5,300 cameras and 300 license plate readers connected to the network, including more than 700 Metropolitan Transit Authority cameras from high-density transit hubs. Each day, these surveillance assets monitor entry and egress points in Manhattan. The Operational Dashboard gives law enforcement personnel the capability to run video analytics on each camera and to flag and search for suspicious behavior and activities. With FY 2014 funding, NYPD will expand the video and sensor network and enhance the ability to correlate multiple data streams to manage incidents and provide extended analytic capabilities. The expanded DAS will be able to support up to 6,000 cameras, plus hundreds of fixed-site and mobile chemical, radiation, and biological sensors deployed by the NYPD and its regional Securing The City partners.

The Wayne County Interoperable Mobile Data Terminal Project is a previously established project in Wayne County involving all law enforcement agencies, the 911 Center, and the Emergency Management Office. The program involves the use of Mobile Data Terminals in each patrol vehicle to communicate secure police information, including terrorist-related information, between all the police agencies vehicles and the County 911 Center, along with the various federal law enforcement agencies and the U.S. Border Patrol. This project will use \$42,500 in LETPP funds from New York's State Homeland Security Program award.

North Carolina

In 2014, North Carolina Emergency Management Agency invested \$4 million in LETPP funding to support several projects. The most notable project is the Voice Interoperability Plan system. The system is operational statewide, with P25 upgrades completed. This project provides interoperable communications with federal, state, and local entities, which is essential to supporting response activities and providing assistance across jurisdictional boundaries.

North Dakota

North Dakota is using \$203,607 in LETPP funds from the State's 2014 State Homeland Security Program to provide personal protective equipment, explosive device mitigation and remediation equipment, CBRNE operational and search and rescue equipment, information technology equipment, interoperable communications equipment, detection equipment, CBRNE incident response vehicle, and CBRNE logistical support equipment to the Grand Forks Police Department's Regional Bomb/SWAT Team.

Northern Mariana Islands

The Commonwealth of the Northern Mariana Islands (CMNI), in conjunction with state police, first response agencies, and the U.S. Army Pacific Area Command, annually planned and executed 36-hour, all-hazards, and full-scale exercises for the past 4 years to test existing capabilities within the CNMI and validate agency and state plans. Over the course of 3 days, Homeland Security Emergency Management staff and its other stakeholders executed a series of simulated events (e.g. HazMat spills, active shooter events, terrorist activities, IEDs).

Ohio

The Ohio Emergency Management Agency has purchased early identification equipment (including ALPRs), automated fingerprint identification, mobile data terminals, and other biometric equipment) with LETPP funds from its FY 2013 and 2014 Homeland Security Grant Program award in the amount of more than \$1.1 million. These acquisitions and required maintenance are designed to assist local law enforcement in identifying suspicious persons and vehicles quickly in order to gather and report appropriate information to the fusion center network. ALPRs continue to be the primary area of spending, allowing for the tracking of potential terrorist activity throughout the state.

Oklahoma

Oklahoma used \$866,125 in LETPP funds from its State Homeland Security Program award to support staffing, training, and equipping Fusion Center analysts. Additionally, a portion of the funds were used to establish an information-sharing network (OASIS) for federal, state, tribal and local law enforcement; to create a state information search network (OKLEX) for federal, state, tribal, and local law enforcement; and to develop appropriate procedures and plans for the Fusion Center. The Oklahoma Information Fusion Center has become an integral part of the state's homeland security efforts.

Oregon

Active shooter scenario training for law enforcement through the Advanced Law Enforcement Rapid Response Training was funded through the LETPP. Four such exercises were conducted in 2013, and six in 2014. Additionally, the fusion center

has been working on active shooter presentations from private businesses, providing this information to the public to help educate them in the event of such an incident.

Pennsylvania

Pennsylvania's South Central Counter Terrorism Task Force used \$90,000 in LETPP funds from the State's 2014 State Homeland Security Program award to sustain the interdiction, disruption, and on-scene security and protection core capabilities that are provided through six Law Enforcement Strike Teams and five county-based tactical teams.

Puerto Rico

Puerto Rico used LETPP funds to purchase interoperable communications equipment for the Commonwealth's municipal police departments as well as for the Puerto Rico Police Department. Through LETPP funds, Puerto Rico also has been able to purchase computer-aided dispatch systems for many of the Commonwealth's larger police departments.

Rhode Island

In FY 2014, the Rhode Island Emergency Management Agency obligated approximately \$972,100 to law enforcement terrorism prevention activities. Homeland Security Grant Program funds were vital to improving the capability of the Rhode Island State Bomb Squad, including optic enhancement to the CBRNE robot platform, critical transportation for deployment, and training for explosives-detecting canines.

South Carolina

In FY 2014, South Carolina used \$90,000 of LETPP funds to conduct five active shooter instructor certification courses. One hundred and seventy-seven instructors were certified during these courses.

South Dakota

With FY 2014 State Homeland Security Program LETPP funds, the County of Minnehaha procured interoperable radios for the Sherriff's Office and Police Department.

Tennessee

Tennessee's Homeland Security District 7 (Montgomery, Cheatham, Stewart, Robertson, Dickson, Humphries, and Houston counties) procured tactical communications equipment for tactical squad members throughout the district in order to enhance tactical team communications capabilities using \$37,000 in State Homeland Security Program funds. This equipment ensures more effective operations and significantly improves command and control.

Texas

Using 2014 LETPP funds, the North Central Texas Council of Governments (NCTCOG) will assist in building and sustaining NIMS-typed resources, SWAT teams throughout the NCTCOG region. A survey of all North Central Texas SWAT teams that participated in the 2013 Urban Shield Exercise identified a number of areas needing additional training. The survey and 2013 Urban Shield After-Action Review (AAR) also identified a continued need for SWAT teams to conduct joint training. This project will enhance terrorism and criminal activity response for SWAT teams throughout the region by funding joint training in the areas of hostage rescue, joint team search techniques, and close-Quarter battle techniques. The training will also provide continued training with tactical robot systems as force multipliers and intelligence collection assets.

Utah

The Utah Bomb Squad Committee is using \$325,000 of LETPP funds from the State's 2014 State Homeland Security Program award to maintain current robot units used for disposal of explosive ordnance. The funds also will assist in purchasing and updating to newer robots.

Vermont

Using FY 2014 Homeland Security Grant Program funds, the Vermont Department of Public Safety funded five departments to purchase \$109,760 in tablets and accessories to move from outdated mobile data terminals. Officers are able to receive intelligence information much more easily via the tablet, regardless of where they are during their day. Tablets have reduced the amount of hardware necessary in the patrol cruiser, thus increasing officer safety. Vermont plans to continue funding these projects with FY 2015 funding.

Virgin Islands

Using LETPP funds, the U.S. Virgin Islands was able to build a basic explosive device disposal capability by acquiring equipment and training for members of the Virgin Islands Police Department's Bomb Squad Unit. The Bomb Squad is able to provide a capability that did not previously exist within the territory.

Virginia

LETTPP funds were used to expand and sustain surveillance of waterways within Portsmouth city. This project allowed the Portsmouth Police Department to expand its long-range day/night surveillance system that overlooks the Norfolk/Portsmouth Harbor and its shoreline, greatly improving Maritime Domain Awareness, IED, and CBRNE prevention, protection, response, and recovery capabilities. The project was developed with consideration of and alignment with core capabilities in both the State Preparedness Report and the State Homeland Security Strategy.

Washington

The King County Office of Emergency Management is using \$125,000 in LETPP funds from the State's 2014 State Homeland Security Program award for planning. Planning under this project addresses regional coordination, mass care, cybersecurity, resource management, and hazardous materials. Efforts include capabilities assessment, analysis, prioritization, and reporting; planning facilitation including engagement of whole community; development of plans, policies, and procedures to address and support mitigation, response, and recovery activities and emergency coordination center roles and responsibilities; development of regional detection, interdiction, disruption, and on-scene security, and protection and response concepts of operation and standard operating procedures.

West Virginia

The West Virginia Department of Military Affairs and Public Safety (WVDMAPS) made several law enforcement awards in 2014. These included awards for radios, cameras, SWAT equipment, and dive team equipment. One of the most notable procurements was made for the purchase of a throw phone. During a barricade incident at the federal courthouse in Wheeling, West Virginia, local law enforcement did not have the throw phone equipment needed to communicate with the offender. Following the incident, WVDMAPS used \$23,000 in 2014 to purchase the equipment (which includes video capability) for the Wheeling Police Department, which maintains jurisdiction at the courthouse.

Wisconsin

The Dane County Sheriff's Office is using \$10,000 in LETPP funds to procure lightweight, ballistic protective helmets that will greatly enhance the ability of the Tactical Response Team (TRT) to respond to and mitigate hazardous situations more efficiently and safely. In addition, the Sheriff's Office will procure five sets of ballistic facial protection that attach to the new helmets, in order to provide additional ballistic protection to the members of the TRT that perform breaches.

Wyoming

The State of Wyoming used a combined \$42,526 of LETPP funds from the 2014 State Homeland Security Program to outfit police officers in Mills, New Castle, Rock Springs, and Torrington with body cameras.

VI. Conclusion

From FY 2008 – FY 2014, states, tribes, territories, and urban areas have collectively spent 36 percent of State Homeland Security Program, Urban Area Security Initiative, Operation Stonegarden, Tribal Homeland Security Grant Program, and Nonprofit Security Grant Program funds on Law Enforcement Terrorism Prevention Program (LETPP) activities. This percent reflects more than \$1 billion beyond the 25 percent required set-aside for LETPP. The examples provided herein showcase the wide variety of prevention and protection core capabilities obtained, maintained, and enhanced through dedicated funding to the LETPP.

Law enforcement personnel continue to face unique hazards, threats, and challenges. Through the FY 2015 preparedness grants, FEMA will continue to support the LETPP activities that build state and local law enforcement capabilities to prevent terrorist attacks and to provide law enforcement and public safety communities with funds to support critical prevention activities.

Page 01 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1 of 5

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 5

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 5

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 4 of 5

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 5 of 5

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

THURSDAY, APRIL 21, 2016

BANQUETING HOUSE

6:00 – 7:00 PM

The Complexities of Today's Security Challenges

The Director of the FBI has said that the bureau has counterterrorism investigations underway in all 50 states, underscoring the gravity of the “insider” terrorism threat in the United States. Simultaneously, terrorists from abroad, especially “foreign fighters” from among ISIL’s ranks in Iraq/Syria, are seeking to enter Western countries, including the United States, to carry out attacks. Complicating matters further, technology innovation is advancing so quickly that terrorists are leveraging these advancements, making it easier for them to plot and plan undetected by counterterrorism professionals. Director Comey will address the complexity of today’s security challenges and how and the FBI is working both at home and with global partners to confront them.

James Comey, Director, Federal Bureau of Investigation, United States

Moderator: Brooke Masters, Companies Editor, Financial Times

7:00 – 8:00 PM

Opening Reception to Follow

FRIDAY, APRIL 22, 2016

LANCASTER HOUSE

8:00 – 9:00 AM

Registration & Breakfast

Attendees may pick up their registration packets prior to our first session at Lancaster House. Packets will contain a master program, as well as a Forum badge, which will be required to enter any Forum event. Registration packets will be available for pick-up through April 23rd.

9:00 – 9:05 AM

Welcome & Opening Remarks

Clark Ervin, Executive Director, Aspen Security Forum: Global; Former Inspector General, Department of State and Department of Homeland Security, United States

9:05 – 9:50 AM

NATO/Russia: Cold War Redux?

Putin's Russia is acting much like the Soviet Union – invading and annexing its weaker neighbors; probing NATO's defenses in the air and at sea for vulnerabilities; building up its military; and violating arms control treaties. Are we in a new “Cold War,” and, if so, is the alliance up to the challenge? America's Ambassador to NATO, a warrior-diplomat, and two veteran Russia watchers, will attempt to divine Russia's intentions, assess its capabilities, and analyze NATO's strengths and weaknesses in this time of unsettling uncertainty.

Douglas Lute, Ambassador of the United States to the North Atlantic Treaty Organization

Samuel Greene, Director, Russia Institute, King's College London, United Kingdom

Roderic Lyne, Deputy Chairman, Chatham House; Former Ambassador of the United Kingdom to the Russian Federation, United Kingdom

Moderator: John Gearson, Director, Centre for Defence Studies, King's College London, United Kingdom

9:50 – 10:00 AM

Break

10:00 – 10:45 AM

Countering Violent Extremism: The Security Challenge of our Time

How does a person become radicalized? Once radicalized, what leads someone from radical thinking to violent action? What works to counter extremism? Three noted experts grapple with these elemental questions that lie at the heart of an effective counterterrorism strategy.

Richard Barrett, Senior Vice President, The Soufan Group; Former Chairman, United Nations Counter Terrorism Implementation Task Force, United Kingdom

Gilles de Kerchove, Counterterrorism Coordinator, European Union

Mark Simmonds, Chief Operating Officer, Counter-Extremism Project, United Kingdom

Moderator: Ciarán Devane, CEO, British Council, United Kingdom

10:45 – 11:00 AM

Break

11:00 – 11:45 AM

Reflections from the Intelligence World

President Obama famously dismissed ISIL a couple of years ago as a “JV team,” and now it is at the very top of the lengthening list of American, and Western, security concerns. In retrospect, the Administration’s mistranslation of the Russian word for “reset” can be taken as a metaphor for a fundamental misunderstanding of Putin’s intentions and Russia’s capabilities. While the invasion of Iraq in search of WMD is the most infamous, there are numerous examples of “getting it wrong” on fundamental questions of intelligence and, thus, policy. Two noted intelligence experts discuss the challenges facing analysts in today’s ever more complicated security environment.

John Scarlett, Former Chief, Secret Intelligence Service, United Kingdom

John McLaughlin, Former Acting and Deputy Director, Central Intelligence Agency, United States

Moderator: Gordon Corera, Security Correspondent, BBC

11:45 AM – 12:00 PM

Break

12:00 – 12:45 PM

Bright Spots and Dark Clouds: Promise and Peril in Latin America

After decades of civil war and descent into the abyss of narco-trafficking, Colombia is stable and prosperous. Meanwhile, Venezuela is in political and economic chaos, and Mexico is riven by corruption and lawlessness. Three experts will discuss the challenges in these countries in particular and in the region as a whole.

Juan Carlos Pinzón, Ambassador of Colombia to the United States; Former Minister of Defense, Colombia

Daniel Lansberg-Rodriguez, Director for Latin America, Greenmantle LLC, United States

Eduardo Medina-Mora, Justice, Supreme Court of Justice of the Nation, Mexico

Moderator: Vinicius Mariano de Carvalho, Lecturer, King’s Brazil Institute, King’s College London, United Kingdom

12:45 – 1:45 PM

Lunch

1:45 – 2:30 PM

Rethinking Europe

Europe is at a crossroads. As discussed earlier, the continent’s security is being tested by an increasingly aggressive and assertive Russia to a degree not seen since the Cold War. As the attacks in Paris and Brussels underscore, ISIL has Europe in its sights. The civil war in Syria and the establishment there of the capital of the “Islamic State” has spawned a human and economic crisis that has serious political, economic, and social consequences for Europe. And, this is not to mention the continuing economic strains of the Eurozone and the challenges of continued political integration. These Euro-experts will explore the dimensions of these challenges in detail.

Robin Niblett, Director, Chatham House, United Kingdom

Peter Ammon, Ambassador of Germany to the United Kingdom

Rob Wainwright, Director, Europol

Moderator: Matthew Kaminski, Executive Editor, POLITICO Europe

2:30 – 2:45 PM

Break

2:45 – 3:30 PM

The Continuing Struggle for Afghanistan and Indo/Pakistan Relations

The Long War in Afghanistan continues, more than a decade after the 9/11 attacks and the subsequent American invasion to dislodge the Taliban and Al Qaeda. Yet, in the wake of America's withdrawal and NATO's refocus on its core mission of deterring Russian aggression, the Taliban is back with a vengeance. Meanwhile, both the Taliban and Al Qaeda are still active in Pakistan, posing, respectively, a local and global security threat. This session will explore these challenges, as well as the prospect of a further rapprochement between India and Pakistan and the degree to which the Afghanistan/Pakistan dynamic complicates that rapprochement.

Hina Rabbani Khar, Former Foreign Minister, Pakistan

Moderator: TBD

3:30 – 3:45 PM

Break

3:45 – 4:30 PM

Homeland INsecurity

In the age of terrorism and Twitter, the “homeland” is inherently unsafe. In free societies, there are unlimited targets, and limited means of foiling plots before it's too late. Making bad matters still worse, the “viral” nature of social media and the anonymity of the Internet make recruiting terrorists all too easy, and stopping them much, much harder. What, then, are those whose job it is to protect the “homeland” to do?

Pauline Neville-Jones, Member, House of Lords; Former National Security Advisor, Minister of State for Security and Counterterrorism, and Special Representative to Business for Cyber Security, United Kingdom

Charles Farr, Chairman, Joint Intelligence Council, United Kingdom

Alejandro Mayorkas, Deputy Secretary, Department of Homeland Security, United States

Moderator: Frank Gardner, Security Correspondent, BBC

4:30 – 4:45 PM

Break

4:45 – 5:30 PM

Cybersecurity: The New Frontier

Cyber is the new security frontier. There is cyberwarfare; cyberterrorism; cyberespionage; and cybercrime. There are state actors; non-state actors; and “blokes in their basements.” Though cyber threats have been with us for some time, and they are growing in intensity and severity, we still lack clear rules of the road to govern how best to confront them. And, the line between offensive and defensive is blurry. This panel will attempt to make sense of this muddle.

Shami Chakrabarti, Director, Liberty, United Kingdom

Stewart Baker, Partner, Steptoe & Johnson LLP; Former Assistant Secretary for Policy, Department of Homeland Security, United States

Moderator: David Sanger, Chief Washington Correspondent, *The New York Times*

TBD PM

Reception

- 8:30 – 9:00 AM **Breakfast**
- 9:00 – 9:45 AM **Defeating ISIL**
 The Obama Administration's Envoy for the Global Coalition to Counter ISIL and France's National Intelligence Coordinator discuss the strategy and progress made in degrading and ultimately defeating this global scourge.
- Brett McGurk**, Special Presidential Envoy for the Global Coalition to Counter ISIL, United States
Didier Le Bret, National Intelligence Coordinator, France
Moderator: Mark Urban, Diplomatic and Defense Editor, BBC
- 9:45 – 9:50 AM **Break**
- 9:50 – 10:35 PM **Shadows Across Africa**
 From Boko Haram in the West to Al Shabab in East, Africa is plagued by terrorism, endangering not only the continent's security, but the progress it has made in recent years in terms of political and economic development and social cohesion. This session will explore Africa's security challenges and the prospects for successfully confronting them.
- Mohamed Abdullahi Mohamed**, Founder and Secretary-General, Tayo Political Party;
 Former Prime Minister, Somalia
Alexander Rondos, Special Representative for the Horn of Africa, European Union
Moderator: Karin von Hippel, Director-General, Royal United Services Institute
- 10:35 – 10:45 AM **Break**
- 10:45 – 11:30 AM **The Nuclear Deal with Iran: The Beginning of a Fundamental Change in the Relationship with the West?**
 Does the nuclear deal with Iran presage a fundamental change in the relationship with the West, with the eventual cessation of support for terrorism and regional meddling as its supporters fervently hope, or is a discrete thing that will ultimately only enrich the country and empower it to be more of a security threat in the future, as its detractors predict? This session will discuss and debate this key question with global geopolitical implications.
- Sara Bazoobandi**, Associate Fellow, Middle East and North Africa Program, Chatham House,
 United Kingdom
Peter Westmacott, Former Ambassador of the United Kingdom to the United States
Moderator: Deborah Haynes, Defense Editor, *The Times of London*
- 11:30 – 11:35 AM **Break**

- 11:35 AM – 12:20 PM** **Saber Rattling in East Asia: The Challenge that China and North Korea Pose to Regional Stability and Security**
 Much like Russia with NATO, China is building up its maritime and air capabilities in the South China Sea and testing the strength of the alliance between the United States and our key partners in the Asia Pacific. Meanwhile, North Korea continues to conduct missile tests and to threaten not only South Korea in particular and regional stability overall, but also the United States. What more must be done to confront these challenges, and is the alliance up to it?
- Gordon Chang**, Contributor, Forbes.com; Author, *The Coming Collapse of China* and *Nuclear Showdown: North Korea Takes on the World*, United States
Bonnie Glaser, Director, China Power Project, and Senior Adviser for Asia, Center for Strategic and International Studies, United States
Sung-Yoon Lee, Kim Koo-Korea Foundation Professor in Korean Studies and Assistant Professor, The Fletcher School, Tufts University, United States
Moderator: TBD
- 12:20 – 1:00 PM** **Lunch**
- 1:00 – 1:45 PM** **The View from the Oval Office and 10 Downing Street**
 President Obama's top adviser on homeland security and counterterrorism takes us inside the Oval Office to give a sense of the kind of advice she gives to the U.S. Commander-in-Chief each day as to the various security challenges facing the United States and the world. And, the Prime Minister's deputy advisor for national security gives us his perspective on these issues.
- Lisa Monaco**, Assistant to the President for Homeland Security and Counterterrorism
Paddy McGuinness, Deputy National Security Advisor, United Kingdom
Moderator: Nic Robertson, International Diplomatic Editor, CNN
- 2:00 – 3:00 PM** **A Conversation with the Defence Secretary**
 The Secretary will give us his perspective on how the Strategic Defence and Security Review will inform Britain's response to security risks, including the terrorist threat from ISIL/Daesh and other groups; the challenges facing NATO ahead of Warsaw, including its relationship with Russia; the geopolitical challenges facing Asia-Pacific; and other issues including cyber.
- Michael Fallon**, Defence Secretary, United Kingdom
Moderator: James Harding, Director of News and Current Affairs, BBC
- TBD PM** **Closing Reception**

Page 1 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act



Home Office



JOINT CONTACT GROUP AGENDA

@ The Home Office, (b)(6) 20-21 April 2016

* * * * *

Wednesday 20 April

| | | |
|------------------|-------------------------------------|--|
| 1200 | Arrival | <i>The Permanent Secretary will greet Deputy Secretary Mayorkas and escort the delegation to Conference Room 2 (6th Floor)</i> |
| 1200-1300 | Working Lunch | <ul style="list-style-type: none"> • RICU Presentation on Strategic Communications |
| 1300-1330 | Intelligence Briefing | <ul style="list-style-type: none"> • Overview of the Threat Picture • Emerging Trends • EU Migrant Crisis • JTAC-DHS Paper on Citizens of the Caliphate Paper |
| 1330-1500 * | Counterterrorism & Foreign Fighters | <ul style="list-style-type: none"> • Enhancing Cooperation: Four-Way Mapping (Capacity Building) Update • Priority Countries for Engagement (Inside Europe) • Priority Countries Engagement (Outside Europe) • Aviation Security & Capacity Building |
| * 5 minute pause | | |
| 1500-1530 | Break | <i>Tea & coffee provided</i> |
| 1530-1630 | Countering Violent Extremism | <ul style="list-style-type: none"> • UK Extremism Strategy • Changes to the US CVE architecture • Engaging CSPs and Industry on Tackling Extremist and Terrorist Use of the Internet • Strengthening Partnerships on CVE communications • Returnees / Exit Programmes |
| 1630-1715 | Cyber & Encryption | <ul style="list-style-type: none"> • Access to Data • Encryption • Cyber Paper / Bilateral Activities |
| 1715-1800 | Close | <ul style="list-style-type: none"> • <i>Transfer to Reception</i> |
| 1800-1930 | JCG Reception | <ul style="list-style-type: none"> • <i>Hosted @ the Deputy Chief of Mission's Residence</i> |
| 2000-2200 | Dinner | <ul style="list-style-type: none"> • <i>Hosted @ The Special Forces Club</i> |

OFFICIAL

Thursday 21 April

0830-0845 Arrival *Home Office representatives will greet Deputy Secretary Mayorkas and escort the delegation to Conference Room 2 (6th Floor)*

Tea & coffee provided

0845-1045 *
* 15 minute
pause Information Sharing & Border Security

- Working with Interpol and Europol
- Implementing Five Country Conference, Five Country Ministerial (FCM) & Attorney-General Quintet actions
- Preventing and Combatting Serious Crime (PCSC): Agreement and Implementation
- Secure Real-Time Platform (SRTP)
- Extending Use of Advanced Passenger Information (tbc)
- Preclearance
- Global Entry / Registered Traveller
- Visa Waiver Program

1045-1100 Break *Tea & coffee provided*

1100-1230 Migration & Refugees

- Updating International Frameworks on Refugees
- Biometric Returns & Refugee Screening
- Turkey
- Organised Immigration Crime Strategic Action Plan
- People Smuggling Routes and Trends

1230-1300 Conclusion

- JCG Governance & Next JCG Topics
- Update on JCG Action Items & Accomplishments
- Strengthening DHS-HO Communication & Relations

1300-1315 Transfer to Permanent Secretary's Office

- *Signing of JCG Governance Principles & SRTP Statement of Intent*

* * * * *

| | |
|------------------|---|
| From: | Ulloa, Isabella (b)(6) (b)(6) |
| To: | "Blumenthal, Nathan (b)(6) (b)(6) "Manfra, Jeanette </O (b)(6) (b)(6) |
| CC: | (b)(6) |
| Subject: | [Counselor Clearance Request] S2 BB - Topline Messaging for Trip to Berlin & London - 4.18.16 |
| Date: | 2016/04/13 13:39:48 |
| Priority: | Normal |
| Type: | Note |

Nate and Jeanette,

Please find attached topline messaging for S2's trip to London and Berlin. This document will be included with his materials for the Aspen Security Forum given the substantial amount of press that will attend the event. The toplines include information on Brussels, CVE, and cyber (as it relates to recent legislation and China).

OPA was lead.

We're requesting your review and clearance by 4:30 pm today. Thank you!

Best,
Isa

Isabella Ulloa
Office of the Executive Secretary
U.S. Department of Homeland Security
Desk (b)(6)
Cell: (b)(6)

| | |
|-------------------|---|
| Sender: | Ulloa, Isabella (b)(6) (b)(6) |
| Recipient: | "Blumenthal, Nathan (b)(6) (b)(6) "Manfra, Jeanette </O (b)(6) (b)(6) |

| | | |
|------------------------|---------------------|--|
| | (b)(6) | |
| Sent Date: | 2016/04/13 13:39:46 | |
| Delivered Date: | 2016/04/13 13:39:48 | |

ASPEN SECURITY FORUM
Topline Messaging

Attacks in Brussels, Belgium

As the President has said, we stand in solidarity with the Belgian people in condemning the terrorist attacks that occurred in Brussels; we mourn the loss of those killed, and we will do what we can to help Belgian authorities bring to justice those responsible for the attacks.

At present, we have no specific, credible intelligence of any plot to conduct similar attacks here in the United States.

We remain very focused on the threat posed by lone terrorist actors who may lack direct connection to a foreign terrorist organization; we are concerned that such radicalized individuals or small groups could carry out an attack in the Homeland with little warning.

We also remain very engaged in the effort to identify and disrupt foreign terrorist fighters who may seek to travel to or from the United States.

The Department of Homeland Security, along with our partners in federal law enforcement and the intelligence community, are doing a number of things to monitor events in Brussels, work with the authorities there, and continue to secure our Homeland.

Public awareness and vigilance are vital to our homeland security efforts, and have in fact prevented terrorist or criminal acts in the past. In today's environment, we urge the public to continue to travel, visit public events and places, and continue with their daily lives, but at all times be aware and vigilant.

Q: How is the Department working with law enforcement authorities to investigate these attacks?

- **DHS personnel have an excellent working relationship with Belgian authorities, and we continually receive information about the attacks and those who may have been involved.**
- **Since the Paris attacks in November, we have enhanced information sharing about potential terrorist threats with both Belgian and French authorities, and we will continue this effort.**
- **The Department has also been in communication with the FBI, state and local law enforcement, to share the latest about what we know of these attacks in Belgium.**

State and local law enforcement are themselves enhancing their security posture as they deem appropriate.

- We are also in regular communication with organizations representing the private sector to share with them what we know.

Q: Are there concerns about foreign terrorist travel between the United States and Belgium? What measures are in place to guard against this?

- Though we do not require Belgian citizens to have a visa to travel here for business or tourism purposes, both TSA and CBP have procedures in place to identify and prevent suspicious individuals from traveling to the United States from Belgium.
- All travelers arriving in the United States are vetted against the U.S. Terrorist Screening Database, regardless of whether they arrive with a visa or an Electronic System for Travel Authorization (ESTA).
- We continually evaluate whether more screening is necessary, particularly in light of these attacks.

Q: What's the link between these perpetrators and the Paris network?

- It is early in the investigation and there still is much to be learned.
- That said, it appears that there are in fact clear connections between the November attacks in Paris and this week's attacks in Brussels. Attackers in both cities were enabled by support and facilitation networks and there appears to be overlap between those networks.
- For additional comment, we'd refer you to the Belgian authorities as the investigation remains underway.

Q: Was this an intelligence failure?

- The terrorism threat that we face today, at home and abroad, is in many ways more complex, more challenging, and less predictable than at any point in the last 15 years.
- The ISIL threat does not stop at national borders, and we're accordingly increasing our intelligence cooperation with international partners to stop ISIL from carrying out these kinds of attacks. Given the increasing level of threat we are seeing across Europe, cooperation and collaboration among partners is more essential than ever. It is this collaboration and strength in unity that will ultimately lead to degrading and disrupting ISIL and other violent extremists.

Q: Was this attack related to, or accelerated because of, Abdeslam's arrest?

- While the investigation is ongoing, the complexity of this attack indicates that it had likely been planned prior to Salah Abdeslam's arrest. As the investigation is ongoing, I'll decline to speculate further.

Q: What is the threat to homeland?

- At present, we have no specific, credible intelligence of any plot to conduct similar attacks here in the United States. That said, we remain very focused on the threat posed by lone terrorist actors who may lack direct connection to a foreign terrorist organization; we are concerned that such radicalized individuals or small groups could carry out an attack in the Homeland with little warning. We also remain very engaged in the effort to identify and disrupt foreign terrorist fighters who may seek to travel to or from the United States.
- We continue to work closely with our international law enforcement, counterterrorism and intelligence partners to monitor events in Brussels and continue to secure our homeland.

Q: Is it true that you are deploying enhanced airport security in the wake of this attack?

- As a precautionary measure, TSA is deploying additional security to major city airports, and at various rail and transit stations around the country. TSA is also calling upon state and local law enforcement to augment that security.
- State and local law enforcement are themselves enhancing their security posture as they deem appropriate. We are also in regular communication with organizations representing the private sector to share with them what we know.

Q: What assistance are you providing Belgium? How are they coping?

- Belgium faces significant challenges associated with violent extremism, and Belgian intelligence and law enforcement services are working together to capably respond to a significant volume of threats. We stand ready to assist them in any way we can.
- Given the increasing level of threat we are seeing across Europe, cooperation and collaboration among partners is more essential than ever. It is this collaboration and strength in unity that will ultimately lead to degrading and disrupting ISIL and other violent extremists.
- We will continue to assist and support our Belgian counterparts in tracking down and dismantling those who helped perpetrate these horrific attacks. Belgium does not stand alone in facing the menace of violent extremism.
- We also commend statements from Belgian Prime Minister Michel that now is the time to be calm and show solidarity, and from the Belgian Ambassador to the United States expressing the resilience of the Belgian people.

Q: Can you share any details on attack – suitcase? Suicide bomber? Gunfire?

- ISIL has claimed responsibility for these terrorist attacks. As there is an ongoing Belgian investigation, I'm not going to comment or speculate further.

Q: Can you comment on reports Belgian nuclear power plants sent home non-essential staff?

- We are aware of reports that Belgium has tightened security at nuclear plants across the country, but understand that this response is standard procedure based on the country's current threat level.
- There is no indication that any incident has occurred or a threat exists at either nuclear power plant.
- We refer you to Belgian authorities for additional detail about their nuclear power plant operations or procedures.

Q. Should terrorists succeed in gaining access to a nuclear facility, what is the risk level?

- We are not going to speculate on this specific case. We take any potential threat to a nuclear facility very seriously.

Q. What additional measures are being taken to improve nuclear security in Belgium?

- I would refer you to the Belgian authorities. We understand that the Belgian government has decided to deploy on-site military quick response teams at nuclear plants and research centers while it determines what other actions may be necessary.
- It is important that we all learn from the recent events and the United States would like to engage with Belgium in expert discussions on facility and material security.

Countering Violent Extremism

In the current threat environment, countering violent extremism has been a key focus of DHS's work to secure the homeland. Through this effort, we have been working to build relationships and promote trust with communities across the country.

Last year, I announced the creation of the DHS Office for Community Partnerships to take the Department's CVE efforts to the next level. Its focus is to support and enhance efforts by communities to counter violent extremism and promote community resilience.

As we engage in these vital efforts to secure the homeland, we remain committed to protecting civil rights and civil liberties.

Q: What has DHS done in the past year to further and maintain its role and responsibility in the interagency CVE effort?

- In January 2016, the CVE Task Force was formed to integrate and harmonize domestic CVE efforts here at home. Advancing these efforts means working as effectively as possible across the U.S. Government, which is why we formed the CVE Task Force.
- The CVE Task Force is a permanent, interagency task force hosted by DHS with overall leadership provided by DHS and the DOJ. Additional staffing is provided by the FBI, the National Counterterrorism Center, and other supporting departments and agencies.

Q: Was this Department priority a reaction to Paris and San Bernardino? Are we as a public safe on a day-to-day basis?

- Both of these initiatives were undertaken following extensive, months-long reviews of our domestic and international CVE efforts. These reviews have roots in the February 2015 White House CVE Summit.
- The horrific attacks in Paris and San Bernardino last year were a stark reminder of the importance of this work, and of how important it is to harmonize our domestic and international efforts.
- Representatives from 11 departments and agencies have reviewed our current structure, strategy, and programs for domestic CVE efforts and have offered concrete recommendations as we work to further strengthen our efforts.

Q: What is DHS doing to counter violent extremism online?

- The Office for Community Partnerships is actively exploring how we can best support efforts to challenge violent extremist use of the Internet and counter

narratives that are used to recruit, radicalize, and mobilize individuals and groups to violence.

- For example, the Office for Community Partnerships, along with interagency partners, is working closely with the State Department to support the domestic portion of the Peer to Peer Challenging Extremism (P2P) competition. The goal of the Peer to Peer Challenging Extremism program is to engage university students, here at home and abroad, to create and activate their own social media campaigns to challenge recruitment messaging propagated by ISIL and other violent extremist groups online.

Q: How will the Department be using funds allocated for CVE in the 2016 omnibus spending bill?

- The Office for Community Partnerships is working with FEMA to issue a notice of funding opportunity in the near future.
- This is the first time federal funding has been provided, on a competitive basis, specifically to support local CVE efforts.
- This funding is critical, but as I have said before: \$10 million is not enough, and we will continue to explore what options are available to reprogram Fiscal Year 2016 funding in support of our CVE efforts.

Cybersecurity

Cybersecurity is one of the Department of Homeland Security's highest priorities, and we've recently made significant progress increasing the cybersecurity posture of our Government, our citizens, and our critical infrastructure.

In December 2015, Congress passed and the President signed into law the Cybersecurity Information Sharing Act of 2015. This established the department's National Cybersecurity and Communications Integration Center, or NCCIC, as the Federal Government's hub for cyber threat indicator sharing.

Now, with the help of Congress, we will be able to continue our work to protect the cybersecurity of the American public, American businesses large and small, and the Federal Government, and take that work to the next level.

Q: What impact will the Department's FY 2017 budget request have on the Department's cybersecurity efforts?

- The Budget provides \$471.1 million for the National Cybersecurity Protection System that will maintain currently deployed EINSTEIN capabilities, and invest in new capabilities for analytics, information sharing, and intrusion prevention.
- Also included in the Budget is \$274.8 million for the Continuous Diagnostics and Mitigation program which provides hardware, software, and services designed to support activities that strengthen the operational security of federal ".gov" networks.
- DHS is also continuing to work with the Congress to reorganize and transition NPPD to become an operational component.

Q: What are you doing to enhance critical infrastructure security and resilience?

- The Department of Homeland Security, the Department of Commerce, and the Department of Energy are establishing a National Center for Cybersecurity Resilience where companies and sector wide organizations can test the security of systems in a contained environment, such as by subjecting a replica electric grid to cyber-attack.
- The Department of Homeland Security will double the number of cybersecurity advisors available to assist private sector organizations with in-person, customized cybersecurity assessments and implementing best practices.
- The Department of Homeland Security is partnering with Underwriters Laboratory to develop a Cybersecurity Assurance Program to test and certify networked devices within the "Internet of Things," whether they be refrigerators or pacemakers, so that when you buy a new product, you can be sure that it has been certified as secure.
- As mandated by Congress, the Department of Homeland Security has successfully launched a system to exchange cyber threat indicators with the private sector. DHS will increase the breadth and speed of cyber threat indicator sharing while protecting American's privacy and civil liberties.

Q: What is the status of U.S. relations with China in cyberspace?

- As part of Chinese President Xi Jinping’s state visit in September 2015, we received several key commitments from China on cyber issues. These focus on concrete actions and arrangements that will allow us to hold Beijing accountable to the commitments they have made.
- These commitments do not resolve all our challenges with China on cyber issues. However, they do represent a step forward in our efforts to address one of the sharpest areas of disagreement in the U.S.-China bilateral relationship.
- Those commitments are:
 - China will provide timely responses to requests for assistance from the United States regarding malicious cyber activity emanating from China;
 - Neither government will conduct or knowingly support cyber-enabled economic espionage for commercial gain;
 - Our governments will work together to further identify and promote appropriate norms of state behavior in cyberspace and hold a senior experts group on international security issues in cyberspace; and
 - Our governments will establish a Ministerial-level joint dialogue mechanism on fighting cybercrime and related issues.
- The United States and China held the first ministerial level dialogue on cybercrime and other related issues in Washington on December 1, 2015.

Q: Is China adhering to these commitments?

- Holding the first ministerial level dialogue on cybercrime and other issues was a positive step.
- We are monitoring China’s cyber activities closely, to make sure they are complying, but we cannot comment further on our intelligence activities.
- As the President said in September 2015, “the question now is, are words followed by actions. And we will be watching carefully to make an assessment as to whether progress has been made in this area.”

Page 1 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 3

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 01 of 13

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 13

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 13

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 13

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 13

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 13

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 13

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 13

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 13

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 13

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 13

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 13

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 13

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1 of 4

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 4

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 4

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 4 of 4

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1 of 4

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 4

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 4

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 4 of 4

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1 of 5

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 5

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3 of 5

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 4 of 5

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 5 of 5

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

**CHRISTIAN SCIENCE MONITOR BREAKFAST
Topline Messaging**

Countering Violent Extremism (CVE)

Last year, I announced the creation of the DHS Office for Community Partnerships to take the Department's Countering Violent Extremism efforts to the next level.

OCP's focus is to support and enhance community efforts to counter violent extremism and promote community resilience.

There is definitely a role for the public to play in this environment. It is almost always the case, if not always the case, that when someone self-radicalizes and acquires weapons of mass violence, somebody sees the warning signs. And so building bridges, encouraging people to, if they see something, say something, is in my judgement as important as any other homeland security mission in this existing environment.

In our efforts to build these bridges, what I consistently hear is that ISIL has hijacked their religion, and they do not represent Islam. They are a terrorist organization claiming the banner of Islam and to refer to the Islamic State or al-Qaeda as "Islamic extremism," suggests the notion that they occupy an aspect of their religion.

Moving forward, building bridges with Muslim communities and integrating them into the fabric of our society is crucial to our homeland security efforts.

As we engage in these vital efforts to secure the homeland, we remain committed to protecting civil rights and civil liberties.

Q: In this evolving threat environment, how can we look to prevent future attacks?

- In this evolving threat environment, we have to anticipate the next terrorist attack, not the last one. We see not only the rise of ISIL but the rise of the terrorist inspired attacks where the operative may not have met a single other member of the terrorist organization that he is inspired by; may never have trained with the organization; may never have been to Iraq or Syria; or may not have ever received a direct order from a terrorist leader. Instead, the operative may be inspired by something in social media or on the internet to go commit an attack.

Q: What has DHS done in the past year to further and maintain its role and responsibility in the interagency countering violent extremism effort?

- In January 2016, the CVE Task Force was formed to integrate and harmonize domestic efforts to counter violent extremism.

- The CVE Task Force is a permanent, interagency task force hosted by DHS and led by DHS and DOJ. Additional staffing is provided by FBI, the National Counterterrorism Center, and other supporting departments and agencies.
- The Department has also recently announced the Fiscal Year (FY) 2016 CVE Grant Program, with \$10 million in available funds. This is the first federal assistance program devoted exclusively to providing local communities with the resources to counter violent extremism in the Homeland.
 - These grants will empower local communities to provide resources to friends, families, and peers who may know someone on the path toward violent extremism, encouraging community-based solutions to deter an individual well before criminal or terrorist action, which would require the attention of law enforcement.
- The Department's efforts to partner with local communities are a central part of its CVE mission.

Q: Was this Department priority a reaction to Paris and San Bernardino?

- No. Both of these initiatives were started well before these attacks and followed comprehensive reviews of our established domestic and international CVE efforts. The reviews have roots in the February 2015 White House Countering Violent Extremism Summit and were intended to improve the implementation of the 2011 Strategy, Empowering Local Partners to Prevent Violent Extremism in the United States.
- The horrific attacks in Paris and San Bernardino last year were a stark reminder of the importance of this work.
- The Department has worked to counter violent extremism since its inception. As the threat environment has changed, DHS has increased its efforts to prioritize and coordinate CVE initiatives, including community engagement and research on the causes of and best methods to counter violent extremism.
- In recent years, DHS has employed new tools to raise awareness of the threat and encourage communities to do more with the Department, local government, and law enforcement. For example, DHS has led Community Awareness Briefings and Community Resilience Exercises in multiple cities across the country

Q: What is DHS doing to counter violent extremism online?

- OCP is actively exploring how to best support efforts to challenge violent extremists' influence online and counter narratives used to recruit, radicalize, and mobilize individuals to violence.
- OCP is working closely with DOS and other interagency partners to support the Peer-to-Peer Challenging Extremism (P2P) competition. The competition aims to engage university students at home and abroad to create and activate their own social media campaigns to challenge recruitment messaging propagated by ISIL and other violent extremist groups online.

- DHS is also working with the technology and marketing sectors to amplify non-violent, credible voices. Facebook, for example, is a key sponsor of the Peer-to-Peer program. In Los Angeles, YouTube has helped the Department start a similar high-school content creation contest.

Syrian Refugee Vetting and Resettlement

The United States remains deeply committed to safeguarding the American public from terrorists, just as we are committed to providing refuge to some of the world's most vulnerable people. We do not believe these goals are mutually exclusive, or that either has to be pursued at the expense of the other.

The refugee security screening and vetting process has been significantly enhanced over the past few years. Today, all refugees undergo the highest level of security checks of any category of traveler to the United States. All refugees, including Syrians, are admitted only after successful completion of a comprehensive and stringent security screening.

Q: How many Syrian refugees have been resettled in the United States?

- With increased referrals from UNHCR, Syrian refugee admissions rose to 105 in FY 2014, and 1,682 in FY 2015. To date this fiscal year, we have resettled 5,186 Syrian refugees, while another 6,482 have been approved for resettlement, and 4,128 have been conditionally approved pending security checks. DOS estimates at least 10,000 Syrian refugees will be admitted to the United States by the end of FY 2016.

Q: Does DHS feel comfortable that existing refugee security screening practices are sufficient to identify Syria-based extremists?

- Security checks are an integral part of the U.S. Refugee Admissions Program (USRAP) for applicants of all nationalities. The refugee vetting process in place today employs the highest security measures of any immigrant or non-immigrant travel program to protect against risks to our national security, and USCIS continues to engage with law enforcement agencies to ensure that refugee vetting for Syrian applicants is as stringent as possible.

Q: Do intelligence and vetting gaps in the refugee process still exist? If so, what is being done to fix them?

- Refugees are subject to the highest level of security checks of any category of traveler to the United States. Screening procedures have been expanded over time to include a broader range of checks and applicants. Screening partners include the National Counterterrorism Center (NCTC), the FBI, DHS, DOD, and other Intelligence Community and law enforcement members.
- We are deeply committed to safeguarding the American public, just as we are committed to providing refuge to some of the world's most vulnerable people. We do not believe these goals are mutually exclusive, or that either has to be pursued at the expense of the other. We have admitted three million refugees since 1975,

and have a great deal of experience in safely admitting vulnerable refugees from around the world.

Q: Has DHS identified any opportunities for enhancing current security screening practices?

- DHS and USCIS have been working with Intelligence Community members to identify additional screening opportunities leveraging unique holdings and capabilities. Security screening continuously evolves, and new enhancements to security screening practices have come on line and been refined as recently as this fiscal year. USCIS has operationalized manual Facebook checks for Syrian refugee enhanced review cases.

Q: Where in the United States have Syrian refugees been resettled?

- DOS works with a network of domestic resettlement agencies to make initial placement decisions for newly arriving refugees. In some instances, this is driven by the location of relatives already residing in the United States or by particularized medical needs.
- In FY 2015, the largest placement states were Texas, California, and Illinois.

Q: There have been varying data reports on the ratio of men to women and children coming into our borders. Most of the statistics I have come across indicate that the majority of Syrian refugees are predominately males while a small percentage remains women and children. Is this true? And if so, what is the correct ratio of Syrian refugee men to women and children?

- The overwhelming majority of Syrian refugees we have accepted and will accept are families, children, and other especially vulnerable refugees, such as victims of torture and those with medical needs or disabilities. We have prioritized the most vulnerable of Syrian refugees for resettlement—which include those who are victims of the violence perpetrated by both the Assad regime and ISIL in Syria.

Q: As we welcome an additional 10,000 Syrian refugees in FY 2016 alone, how are you and your partner agencies planning to monitor admitted refugees to ensure violent extremists have not infiltrated their ranks?

- Refugees undergo a rigorous screening process prior to their admission into the United States. The process is the most stringent for any category of individuals seeking admission into the United States. The process is multi-layered and intensive. It involves multiple law enforcement, national security, and intelligence agencies across the Federal Government. Only those satisfying these rigorous requirements are admitted into the United States as refugees.

Southwest Border Security

The Department of Homeland Security and its interagency partners continue to closely monitor the humanitarian situation in Central America and current migration trends.

We are working aggressively to address the underlying causes of this migration, to deter future increases and support broader regional efforts to provide avenues for protection of vulnerable populations in Central America.

While CBP has registered an increase in the number of apprehensions of unaccompanied children (UAC) and families over the past several months, this upward rise is not incongruous with seasonal trends. Furthermore, the number of FY 2016 apprehensions are significantly less than the number of apprehensions in FY 2014. Total apprehensions across our entire Southwest border remain at near-historic lows.

El Salvador, Honduras, and Guatemala make up the majority of unaccompanied children and family unit apprehensions, and general conditions related to the economy and violence in these countries continue to serve as push factors leading to migration northward.

As I have said repeatedly, our borders are not open to illegal migration, and we will continue to enforce the immigration laws and secure our borders consistent with our priorities and values. At the same time, we will work to protect vulnerable populations in Central America, in accordance with our legal and humanitarian obligations.

Q: Can you comment on the latest apprehension numbers?

- In June 2016, apprehensions by the Border Patrol on our southwest border—an indicator of total attempts to cross the border illegally—decreased in May and April 2016.
- Of the overall 34,463 total Border Patrol apprehensions on the southwest border reported in June 2016, 4,809 apprehensions were unaccompanied children and 6,633 apprehensions were members of family units traveling together.

Q: What are the criteria for migrants targeted for removal?

- Our borders are not open to illegal migration, and we will continue to enforce the immigration laws and secure our borders consistent with our priorities and values.
- Recent enforcement actions, which focus on those apprehended at the border on or after January 1, 2014, continue.

- With respect to family units, the focus of our current enforcement and removal priorities are adults and their children who:
 - Were apprehended after January 1, 2014;
 - Have been issued final orders of removal by an immigration court; and
 - Have exhausted appropriate legal remedies, and have no outstanding appeal or claim for asylum or other humanitarian relief under our laws.
- With respect to unaccompanied children, the focus of our current enforcement and removal priorities are unaccompanied children who:
 - Entered the United States illegally as unaccompanied children after January 1, 2014;
 - Are now over 18 year of age;
 - Have been ordered removed by an immigration court, and;
 - Have no pending appeal or claim of asylum or other relief.

Q: How will the Department continue to strategize on this issue?

- We recognize that we must offer alternatives to those who are fleeing violence and persecution in Central America. More border security and removals, by themselves, will not overcome the underlying conditions that currently exist in Central America.
- In the meantime, DHS and DOS are accelerating the development of new mechanisms to process and screen Central American refugees in the region.
- We are expanding access to the U.S. Refugee Admissions Program in the region and developing more legal alternatives to the dangerous and unlawful journey many are currently taking in the hands of human smugglers.
- With DOJ, we are also doubling down on our efforts to apprehend and prosecute smugglers through initiatives like Operation Coyote.
- We support DOJ's efforts to ensure that as many unaccompanied children as possible have appropriate representation.
 - To support improving the process for all those in immigration proceedings, the Administration has requested over \$17 million as part of the President's FY 2017 budget request to support long-standing critical initiatives that provide legal assistance services and information to vulnerable immigrants.
 - This includes over \$1 million for Justice AmeriCorps—a program that specifically provides legal representation to unaccompanied minors.

Q: The President of the National Border Patrol Council said that agents are being told to “stand down” and let immigrants go. Is that true?

- The assertion that there exists some Department policy requiring U.S. Border Patrol agents to release undocumented immigrants apprehended at the border and not provide an effective response to an attempted illegal entry simply has no basis in fact. This assertion is also wholly inconsistent with the actual direction and training agents have received.

- The U.S. Border Patrol continues to enforce immigration laws consistent with the Department's enforcement priorities, which are focused on border security, national security, and public safety. As I have said many times, our border is not open to illegal migration, and those who cross the border illegally will be sent back.
- The Border Patrol's resources are most effectively focused on the border—prioritizing the apprehension and removal of individuals attempting to unlawfully enter the United States. Our removal numbers reflect that. Border Patrol Agents are issuing Notices to Appear, consistent with law, regulation, and the Department's enforcement priorities.

TSA Summer Travel Wait Times

We will not compromise safety for convenience.

TSA is taking every step possible to protect the American people while managing the amount of time spent awaiting security screening at U.S. airports.

First, TSA is increasing the number of its Transportation Security Officers, so passengers can move through the checkpoint process more securely and quickly without compromising security.

Second, TSA has added more canine teams to help screen passengers at the Nation's busiest seven airports.

Third, TSA is collaborating with airports and airlines to support non-security screening operations that are personnel-intensive—for example, returning personal property bins, and reminding travelers of checkpoint policies, like three ounce containers for liquids. TSA is also working with airports and airlines to help TSA manage checkpoint lines, passenger flows, and communication with the traveling public.

Fourth, TSA is expanding enrollment efforts for TSA Pre✓[®], which provides a more streamlined screening experience.

This is not a short-term fix. TSA is focused on enhancing security and screening in the long-term, not just for the summer, but for the busy summer travel season and into the future.

The traveling public can help, too, by enrolling in DHS's Trusted Traveler programs, like TSA Pre✓[®] and Global Entry; leaving prohibited items at home; and checking luggage, or packing an uncluttered carry-on.

Q: Why are we seeing longer lines now?

- The increase in wait times is fueled, in part, by the rapid growth in travel volume, with the number of travelers up significantly over the last year. TSA is screening 125,000 more people per day over last year and is on pace to screen over 740 million passengers and crew. This is 45 million more people than last year. Further, more people are choosing to travel with carry-on bags, which still must be screened to ensure safe flights.

Q: Are wait times improving? Have the wait times changed since the beginning of the busier summer travel season?

- TSA works hard to keep passengers moving through security checkpoints, and keep them safe. From June 30 to July 4, 2016, TSA screened 10.7 million travelers. June 30 and July 1, 2016, were the highest-volume travel days we have seen since 2007. During this period, however, the average wait time nationwide in standard security lines was less than ten minutes, while those in TSA Pre-Check lines waited less than five minutes.

Q: Do you feel that security will be compromised if your focus is on processing more travelers more quickly?

- Traveler security is TSA's first priority, and we will remain intensely focused on this important mission. With that said, we are working to alleviate the stress of long lines on travelers, while ensuring our security mission is not compromised.

Q: What is your advice to the traveling public for smooth traveling?

- Every traveler, frequent flier or not, also plays a critical role in security. Just one prohibited item in a carry-on bag can significantly delay movement in a checkpoint line. Passengers can make a positive impact on the security process by packing responsibly, being prepared for checkpoint screening, and arriving at the airport with plenty of time before departure.
- TSA strongly encourages travelers to arrive at the airport early enough (up to two hours prior to domestic departure) to allow for effective screening.
- Most of all, we encourage travelers to enroll in TSA Pre✓® or other Department of Homeland Security trusted traveler programs such as Global Entry, Nexus, or Sentry. These programs help improve security, but they also reduce wait times. The more people who enroll, the more efficient and pleasant screening is for everybody.

Cybersecurity

Cybersecurity is one of the Department of Homeland Security's highest priorities, and we've recently made significant progress increasing the cybersecurity posture of our government, our citizens, and our critical infrastructure.

In December 2015, Congress passed and the President signed into law the Cybersecurity Information Sharing Act of 2015. This established the Department's National Cybersecurity and Communications Integration Center, or NCCIC, as the Federal Government's hub for cyber threat indicator sharing.

Now, with the help of Congress, we will be able to continue our work to protect the cybersecurity of the American public, American businesses large and small, and the Federal Government. We will be able to take this work to the next level.

Q: What impact will the Department's Fiscal Year 2017 budget request have on the Department's cybersecurity efforts?

- The budget provides \$471.1 million for the National Cybersecurity Protection System that will maintain currently deployed EINSTEIN capabilities, and invest in new capabilities for analytics, information sharing, and intrusion prevention.
- Also included in the budget is \$274.8 million for the Continuous Diagnostics and Mitigation program which provides hardware, software, and services designed to support activities that strengthen the operational security of federal ".gov" networks.
- DHS is also continuing to work with Congress to reorganize and transition NPPD into a Component focused on cyber and infrastructure protection.

Q: What is the status of U.S. relations with China in cyberspace?

- As part of Chinese President Xi Jinping's state visit in September 2015, we received several key commitments from China on cyber issues. These focus on concrete actions and arrangements that will allow us to hold Beijing accountable to the commitments made.
- These commitments do not resolve all our challenges with China on cyber issues. However, they do represent a step forward in our efforts to address one of the sharpest areas of disagreement in the U.S.-China bilateral relationship.
- Four notable commitments were secured during Chinese President's Xi Jinping's state visit:
 - China will provide timely responses to requests for assistance from the United States regarding malicious cyber activity emanating from China;
 - Neither government will conduct or knowingly support cyber-enabled economic espionage for commercial gain;

- Our governments will work together to further identify and promote appropriate norms of state behavior in cyberspace and hold a senior experts group on international security issues in cyberspace; and
- Our governments will establish a Ministerial-level joint dialogue mechanism on fighting cybercrime and related issues.
- The United States and China held the first ministerial level dialogue on cybercrime and other related issues in Washington on December 1, 2015.

Q: Is China adhering to these commitments?

- Holding the first ministerial level dialogue on cybercrime and other issues was a positive step.
- We are monitoring China's cyber activities closely, to make sure they are complying, but we cannot comment further on our intelligence activities.
- As the President said in September 2015, "the question now is, are words followed by actions. And we will be watching carefully to make an assessment as to whether progress has been made in this area."

DHS Cybersecurity Workforce Initiative

Protecting the Nation from cyber-attacks will require a trained and mentally-agile workforce. One of the Department's highest priorities is to acquire, grow, and sustain the most talented people in cybersecurity.

Through the DHS Cybersecurity Workforce Initiative, the Department is hiring a diverse group of cybersecurity professionals to secure the Nation's digital assets and critical infrastructure. That includes computer engineers, scientists, analysts, and Information Technology (IT) specialists.

DHS is also building strong cybersecurity career paths within the Department and in partnership with other government agencies. To accomplish this critical task, we have created a number of very competitive scholarship, fellowship, and internship programs to attract top talent.

Q: How is DHS's effort to hire cyber professionals progressing?

- We are focused on attracting, training, and retaining quality Information Technology professionals. We do this in part by supporting the CyberSkills Management Support Initiative (CMSI) to develop and execute programs that will create, enhance, and support a top-notch cyber workforce.
- We have also developed and leveraged the National Workforce Framework to identify the critical skills needed to create an agile cyber workforce.

Need for Cyber and Infrastructure Protection Agency

Cybersecurity has emerged as one of our country's most important national security priorities, as a range of range of traditional crimes are now perpetrated through cyberspace including threats to the Nation's critical infrastructure.

Over the last few years, our cyber operations have become more unified, agile, and effective in the face of a growing and evolving threat environment. Now, we believe we need a Component focused on cybersecurity and infrastructure protection, and so our vision is to reform, rebuild the National Protection and Programs Directorate, which is a directorate, into a Cyber and Infrastructure Protection Component.

These efforts are being closely coordinated with internal and external stakeholders. The proposed structure would realign the Component's programs and functions, allowing for enhanced operations and performance of its critical mission while implementing efficiencies.

Q: What is the status of the transition from NPPD to CIP?

- We continue to work with our partners in Congress, as completing these transition efforts will require congressional action.
- We provided a report to Congress with specifics regarding the organization and additional capabilities of the new CIP structure. We continue to listen to feedback from internal and external stakeholders, as well as members of Congress.

Staff Responsible: Todd Brasseale, Assistant Secretary, OPA,



Page 01 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 18 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 19 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 20 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21 of 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Renewed EU-U.S. Statement
Enhancing transatlantic cooperation in the area of Justice, Freedom and Security

The European Union and the United States of America recall their joint statement on enhancing transatlantic cooperation in the area of Justice, Freedom and Security adopted in Washington D.C. on 28 October 2009. Building on that statement and the commitments therein as well as on our joint efforts, our good cooperation, and the progress we have achieved since its adoption, and noting that our cooperation has expanded since to encompass a wider range of topics and methods than we had initially foreseen, including through cooperation of our agencies, we the European Union and its Member States, on the one side, and the United States of America on the other side, renew our commitment to cooperate further for the benefit of our citizens.

We share strong values and face many similar challenges. We agree to strengthen our cooperation both bilaterally and in international fora to strengthen our partnership and to address these challenges even more effectively.

Recognizing the successful cooperation achieved so far in the areas of Mobility and Migration, Security and criminal and civil justice, we agree that this work should be pursued on the basis of reciprocity and in view of a stronger and balanced partnership.

To this end, we commit to undertake the following concrete actions:

- I. PERSONAL DATA PROTECTION
 1. Conclude the review of the Safe Harbor Framework and negotiations of the “Umbrella” Agreement concerning law enforcement transfers of personal information between the European Union and the United States, in order to ensure effective protection of such information when transferred across the Atlantic
- II. COUNTERTERRORISM AND COUNTERING VIOLENT EXTREMISM
 1. Enhance the cooperation in the area of countering terrorism and violent extremism including preventing people from being drawn into terrorism, building the capacity of civil society and other sectors to support those at risk of radicalization to violence, and challenging terrorist and violent extremist narratives
 2. Increase all aspects of engagement and cooperation with the Communication Service Providers to tackle violent extremists’ and terrorists’ abuse of the internet, including exchange of best practices and experiences, while also protecting fundamental freedoms
 3. Promote the use of multi-national platforms, such as INTERPOL’s Stolen and Lost Travel Documents (SLTD) database, INTERPOL’s 24/7 network for

notices, and the INTERPOL Foreign Fighter Cell to address and combat terrorist activity in all countries

4. Enhance bilateral information sharing between the EU Member States and the U.S. Terrorist Screening Centre
5. Continue and further expand the engagement on borders and aviation security including in high-risk third countries, following risk and threat based principles, including through collaboration in the areas of science and technology to detect and screen for current and future terrorist threats

III. MIGRATION AND BORDER CONTROL

1. Promote dialogue on voluntary and forced return and readmission, in accordance with the international protection standards including cooperation with third countries
2. Expand the U.S.-EU dialogue on the growing phenomenon of mixed migration and discuss organization of common joint initiatives to provide increased protection to persons most in need
3. Discuss the feasibility of developing cooperation on future entry/exit systems and solutions accelerating border control processes including through trusted traveler programs as well as continue the reflection on the feasibility of the U.S. preclearance in the EU Member States
4. Without prejudice to the necessary U.S. legislative efforts, continue tripartite meetings with the aim of achieving full visa reciprocity as soon as possible in a secure environment
5. Carry out joint research and/or best practices exchange on fighting financial crimes, money laundering and organised crime structures linked to migrant smuggling and human trafficking
6. Enhance EU-U.S. dialogue and cooperation on international protection and voluntary resettlement in particular in response to the continuing crisis in Syria

IV. MONEY LAUNDERING AND TERRORISM FINANCING

1. Engage with our international partners to combat money laundering and the financing of terrorism and support compliance with international standards, including the Financial Action Task Force Recommendations.
2. Exchange best legal and technical practices to combat money laundering and terrorist financing (in particular to address current and emerging risks such as value movements via the internet and new payment methods)

V. FIREARMS AND EXPLOSIVES

1. Improve firearms tracing in coordination with U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives
2. Organize joint actions and training for U.S./EU law enforcement, including:
 - a. The EU-U.S. Explosives Experts Seminar to share information on IED techniques, harmonize C-IED research and

development efforts, coordinate training and equipping of personnel, and limit the diversion of IED precursor materials.

- b. EU-U.S. Explosive Detection Canine Group and EU-U.S. Explosive Detection Dog Canine Handler Seminar
- c. Detecting illegal or trafficked firearms sent through express delivery services

VI. CYBERCRIME

1. Facilitate law enforcement exchanges including but not limited to those pertinent to child sexual abuse offenses, travelling child sexual offenders and network intrusion
2. Collaborate in fighting and disrupting cybercrimes and enhancing cyber security including through joint research
3. Promote adoption of the Budapest Convention, and train practitioners on its provisions

VII. DRUGS

1. Pursue and enhance our cooperation on all aspects of the drugs phenomenon in a balanced approach and promoting it in international fora

VIII. INFORMATION EXCHANGE AND CRIMINAL JUSTICE COOPERATION

1. Enhance the implementation of the U.S.-EU Mutual Legal Assistance Agreement (including in relation to transmission of financial information), conclude its review as foreseen by the Agreement and conduct workshops (including through Eurojust) to discuss such issues with national competent authorities
2. Joint training for Central Authorities on internet technology to improve both cybercrime initiatives and MLAT practice
3. Explore the possibilities for enhancing reciprocal law enforcement authorities' access to the criminal records systems of their partners
4. Complete the Joint Review of the U.S.- EU PNR Agreement
5. Exchange information on victim's assistance programs

IX. OUTREACH

1. Support coordinated capacity building in third countries, including through UNODC, in the areas of drug supply and drug demand reduction, cybercrime, combatting transnational organized crime, promoting judicial reforms and strengthening the justice sector institutions with a particular focus to strengthen central authorities
2. Engage with international Partners and assist authorities in certain third countries to recover stolen and fraudulently obtained assets
3. Promote reinforced coordination in multilateral fora for judicial cooperation, such as the Hague Conference
4. Promote increased implementation of the international anti-crime legal instruments, including the United Nations Convention against Transnational

Organized Crime (UNTOC), the United Nations Convention against Corruption (UNCAC)

We recognize that priorities that are not included in the above non-exhaustive list of actions may develop in the coming five years and we envision our ministerial and senior officials and expert/operational level meetings as a mechanism: (a) to monitor the current trends and challenges; (b) to identify new ones in the area of Justice, Freedom and Security; and (c) to establish concrete actions designed to meet those challenges. We further reaffirm our commitment to cooperate in order to accomplish those actions, responsive to and consistent with our values, to secure justice and freedom for our citizens.

| | |
|------------------|--|
| From: | Wall, Joel (b)(6) (FYDIBOHF) |
| To: | (b)(6) |
| CC: | (b)(6) |
| Subject: | Counter ISIL Messaging Speaker Series 25 Feb 1300 ET |
| Date: | 2016/02/23 14:27:35 |
| Due Date: | 2016/02/25 19:00:00 |
| Priority: | Normal |
| Type: | Note |

Forwarded on behalf of SMA... Dr. Jacob Olidort, Washington Institute for Near East Policy, will speak about his article "The Game Theory of Terrorism: How ISIS Radicalizes Others"

Please dial into (b)(6)

Joel D Wall
DHS, S&T, OCS

(b)(6) (U/STE)
(b)(6) (ICS)
(b)(6) (SIPR)

CLASSIFICATION: UNCLASSIFIED

All,

Please join us on Thursday 25 Feb at 1300 ET when we will hear from Dr. Jacob Olidort, Washington Institute for Near East Policy, who will speak about his article "The Game Theory of Terrorism: How ISIS Radicalizes Others" Please dial into (b)(6) passcode (b)(6)

I've attached the slides, the article they are based on and Dr. Olidort's bio. If your email server stripped them out you can download them at this URL:

(b)(4),(b)(5)

v/r

Sam

Sam Rhem
J39, DDGO

CLASSIFICATION: UNCLASSIFIED

| | | |
|------------------------|-------------------------------|--|
| Sender: | Wall, Joel (b)(6) (FYDIBOH | |
| Recipient: | (b)(6) | |
| Sent Date: | 2016/02/23 14:27:32 | |
| Delivered Date: | 2016/02/23 14:27:35 | |

Page 03 of 18

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 18

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 18

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 18

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 18

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 18

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 18

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 18

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 18

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 18

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 18

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 18

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

The Game Theory of Terrorism: How ISIS Radicalizes Others

[Jacob Ollidort](#)

Foreign Affairs

December 10, 2015

Washington has an abundance of information about the group's ideology, targets, and media campaigns, but the challenge lies in figuring out what to do with all the data, both strategically and militarily.

At what point does an extremist become a violent extremist? As the world -- wakened by the recent terrorist attacks in Baghdad, Beirut, Paris, and now in California and London, too -- struggles to defeat the Islamic State (also called ISIS), the answer is more important than ever.

For his part, U.S. President Barack Obama has tried to solve the puzzle by introducing a new ingredient to the counterterrorism recipe. In February 2015, he gathered the world's top experts for a summit on countering violent extremism, a new strategy designed to address the process of radicalization -- in particular, ISIS' apparently unmatched ability to recruit across linguistic, cultural, and geographic boundaries through social media.

Countering violent extremism is different in approach from the one that analysts and policymakers took with al Qaeda. Where they once hunted down operatives and leaders in the top echelons of terrorist organizations, they now also look for so-called influencers and study how, precisely, they incite individuals to violence. Consequently, U.S. counterterrorism has moved from a purely operations-centered strategy -- for example, assassinating al Qaeda leaders or what the media calls "cutting off the snake's head" -- to analyzing what the Department of Homeland Security describes as "the dynamics of radicalization to violence" or the reasons why some individuals associated with violent extremism commit violence and others do not. This new perspective has roped in government bodies, activists, and data scientists who not only analyze terrorist social networks and messaging patterns, but also transmit counter-extremist narratives.

As a result, Washington certainly has an abundance of information about ISIS' ideology, targets, messages, and media campaigns. But the challenge, it seems, is figuring out what to do with all the data. The *Washington Post* recently revealed that the U.S. State Department's Center for Strategic Counterterrorism Communications is rethinking its counter-messaging strategy after an outside panel gave it poor marks on effectiveness. Although the White House's summit on countering violent extremism in February admirably paved the way for the U.S. State Department and other agencies to begin collaborating with regional partners to tackle locally bred extremism -- cultivating grassroots knowledge and empowering local, moderate voices -- the local focus risks overlooking the possibility of more salient transregional ideologies that radicalize to violence. Similarly, although they deserve much credit for building partnerships with local communities, domestically oriented programs for countering violent extremism tend to focus disproportionately on mental health and economic factors. These may account for some degree of social estrangement, but they too overlook the exceptional nature of ISIS' ideological radicalization to violence. In short, our countering violent extremism policies do little, if anything, to address the very root cause and means of ISIS' radicalization to violence -- its ideology.

To enhance the countering violent extremism project and stop ISIS recruitment, Washington should look to game theory.

THE SCHELLING POINTS OF RADICALIZATION

In 1960, at the height of the Cold War, Nobel Prize-winning American economist Thomas Schelling introduced the world to his "theory of strategy," an adaptation of game theory to the world of international relations. In his book *The Strategy of Conflict*, Schelling coined the concept of a "focal point" (now known as a "Schelling point") to describe how individuals and nations reach an agreement when bargaining with each other. The process involves anticipating what the other person or country might do. To demonstrate, in the 1950s, Schelling asked a group of students to pick a place in New York City where they could meet a stranger without having coordinated a place and time beforehand. Without knowing what any of the other students said, most of them not only picked the information booths at Grand Central Station, but nearly all chose to arrive at noon.

Schelling later conducted a second experiment. He gave a group of people sheets of paper with 16 squares. He promised a prize if they all checked the same box. Statistically speaking, only six percent should have checked the same one. In reality, 60 percent checked the top left square. This means that people can reach the same conclusion when properly motivated without having even spoken to one another.

Although Schelling certainly could not have foreseen the application of this idea to defeating ISIS, it is eerily appropriate. If we apply the 16 squares scenario with radicalization, what we are trying to prevent is, in effect, this "psychic moment," as Schelling calls it, when likeminded individuals all come to check the same box: engage in terrorism. Around 20,000 plus foreign fighters, many of whom grew up in prosperous, democratic countries, have already done so.

In Schelling's theory, these individuals would have made their decision through "rational behavior...based on an explicit and internally consistent value system." For jihadists, that value system is Salafism. Given the fact that most of the world's Salafis are not violent, however, it cannot be the Salafi ideology alone that encourages violence. Moreover, given that ISIS disseminates a good deal of nonviolent messaging -- it recently released its own set of textbooks on geography, history, and Arabic poetry for a course to "educate" future jihadists -- it is not violence alone that attracts individuals to its worldview.

It is, rather, ISIS' ability to sell and validate its worldview in light of distinct circumstances that Muslim communities either experience or observe. Specifically, for both those socially and economically disenfranchised by life in the developed world, as well as for those experiencing or witnessing the violent unrest in Syria, ISIS offers the promise of a tranquil and authentic Islamic state, full of opportunity for those who accept its authority. The brutality and sectarian nature of the Shiite-Alawite regime of Syrian President Bashar al-Assad further buttresses ISIS' cause because it validates its claims that only its Sunni worldview is just and fair. Indeed, the group's carefully curated magazine, *Dabiq*, consistently juxtaposes pictures and stories of ISIS providing for its people (i.e., medical care to children, repairing bridges and roads, etc.) with profiles of fighters who were killed, allegedly in defense of such projects.

Essentially, those who buy into ISIS' worldview opt for terrorism not as an ends, but rather as a means for joining a cause in which they can find both physical and spiritual fulfillment. Schelling himself noted in 1980 that "terrorism is contagiously suggestive and furthermore looks easier the more there is of it." In addition, as terrorism grows locally, Schelling asserts, "the easier it is to get away with it because counterterrorist forces are overextended and 'saturated.'"

DECONSTRUCTING THE RADICAL FRAME

But ideology alone doesn't draw recruits to Syria. If the West is serious about preventing a "focal point of radicalization" from ever being created, it will not be enough to counter the ISIS narrative. That is because theoretically, focal points need a foundation -- after all, to check the same box among 16, there first needs to be a grid, or what British economist Michael Bacharach calls a "frame." He has contributed greatly to game theory by explaining how frames lead to the creation of Schelling points. He defines a frame as "the set of concepts or predicates an agent uses in thinking about the world." In the case of ISIS recruitment, then, the task at hand is not simply to refute ISIS propaganda, but to prevent a potential recruit from setting up this frame.

ISIS helps construct this frame in two ways. It offers material enticements (concubines, money) and ideological ones -- the promise of a society based on a highly rigid strand of Sunnism whose principal appeal is its claim of truly representing the vision of the Prophet Muhammad. It has shown it can deliver on both. It has quickly overtaken large swaths of territory in Iraq and Syria and enacted its version of sharia. It has earned hundreds of millions of dollars through oil sales, ransoms, the selling of looted artifacts, and taxes, just to name a few of the group's methods.

However, when this frame fails, it also becomes the principal catalyst for driving potential recruits away from ISIS. Indeed, the *New York Times* recently revealed in an article titled "Promise of Statehood Falling Far Short" that former "citizens" of the Islamic State were disgruntled by the group's excessive taxes, inability to pay its fighters, and the closure of hospitals and schools since they were "stresses [that] could provide opportunities for the group's many enemies." If we consider the promise of a functioning and fair Islamic state to be a frame for recruits to arrive at the focal point of terrorism, then the West could chip away at this frame by further crippling ISIS' governance abilities. From the perspective of countering violent extremism, this objective can be achieved operationally rather than rhetorically, by stopping cash flow and disrupting access to natural resources. Essentially, these tactics increase the "stresses" on the functions of the state and prevent the realities on the ground from validating their narrative.

But the Western world also helps in erecting frames. In 2013, Obama put a red line on Syrian President Bashar al-Assad's use of chemical weapons. When it was discovered a few months later in August that Assad had, in fact, used chemical weapons, the United States decided not to do anything. Salafi-jihadists perceived the move as tacit approval of Assad's oppression of Syrian Sunnis. In the fourth issue of *Dabiq*, released in September 2014, the group featured a lengthy story on Washington's support for the Shiite-majority Iran titled "The crusade serving Iran and Russia." The article also cited how the Assad regime has "managed to 'hide' chemical weapons from the West and use them without a deterrent." Thus, the president's inaction indirectly served as a powerful call to arms that further escalated ISIS' cause. In a July 2014 op-ed in the *New York Times*, scholars Chams Eddine Zaougui and Pieter Van Ostaeyen noted that after interviewing foreign fighters who had returned home, they realized that these recruits were motivated by Assad's "industrial-scale torture, barrel bombs, and chemical attacks." Zaougui and Ostaeyen explained that Assad's ruthlessness "evokes a strong desire to defend fellow Muslims" and criticize the West "for, as they see it, standing idly by over Syria." Zaougui and Van Ostaeyen also observe that of a small contingent of the nearly 350 Belgian fighters in Syria (as of July 2014) "most started as idealists." More recently, last Saturday's knife attacker on the London tube affirmed this view when he reportedly shouted, "This is for Syria."

As Bacharach explains this "is a story of the progressive internalization of these externalities." This internalization, as Bacharach explains, could involve "a tendency to feel shame at failing to do the acts in question, especially when the failure is observed by others." When the Assad regime used chemical weapons against its own people, this may have led potential jihadists in internalizing this situation. When ISIS entered the scene, it provided a Sunni call to arms and enabled potential recruits to externalize their frustrations.

A policy of striking at the heart of ISIS recruitment should involve not only countering the ideology, but rather, rewriting the narrative of events. The aim in doing so should be preventing two "psychic moments" from taking place among would-be jihadists: first, the framing of regional conflicts in sectarian terms and, second, the perception that ISIS is the solution to these conflicts. To accomplish both, the West must form a strategy that empowers local actors who want to rebuild stable, inter-sectarian states (and these voices do still exist) and, simultaneously, continue to destroy ISIS' infrastructure and state capabilities. Doing both would show not only that ISIS' narrative is inauthentic, but also that in practice, it is unrealistic. While no partnerships should be made unconditionally, and while no effective strategy on the ground will definitively eliminate the threat of terrorism, an inclusionary approach -- one that engages local groups committed to defeating ISIS -- may be the most vivid, if not realistic way to eliminate ISIS' focal points of radicalization.

Jacob Olidort is a Soref Fellow at The Washington Institute. All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or views of the U.S. government.

This article was originally published on the [Foreign Affairs website](#).

Dr. Jacob Olidort is a Soref Fellow at the Washington Institute for Near East Policy, where he focuses on Salafism and Political Islam, and is an adjunct professor at the Elliott School of International Affairs at George Washington University. He received his BA in Middle Eastern Studies from Brandeis University, his AM in Near Eastern Languages and Civilizations from Harvard University, and his MA and Ph.D. in Near Eastern Studies from Princeton University, where his work focused on the intersection between Islamic law, theology and modern politics. Dr. Olidort has spent nearly two years in the Middle East, including a Fulbright Scholarship in the UAE and a field work studying Salafism in Jordan. He has given presentations and has consulted on Salafism and on countering violent extremism to audiences in academia, government and policy. His writings have appeared in Foreign Affairs, the Washington Post, Lawfare, and War on the Rocks, among other publications.

| | |
|------------------|--|
| From: | Wall, Joel (b)(6) |
| To: | (b)(6) |
| CC: | (b)(6) |
| Subject: | Counter ISIL Messaging Speaker Series 28 Jan 1000 ET |
| Date: | 2016/01/27 11:20:22 |
| Priority: | Normal |
| Type: | Note |

Forwarded FYI on behalf of SMA.

Joel D Wall
DHS, S&T, Special Projects Office

(b)(6) U/STE)
BB)
ic.gov (JWICS)
sgov.gov (SIPR)

Subject: Counter ISIL Messaging Speaker Series 28 Jan 1000 ET
CLASSIFICATION: UNCLASSIFIED

All,

Please join us tomorrow, **Thursday 28 Jan 1000 ET**, when we continue our Counter-ISIL messaging speaker series and will hear from Dr. Jytte Klausen, Brandeis University, will discuss "**A New Approach To Understanding The Dynamics Of Homegrown Radicalization**"

Please dial into (b)(6) passcode (b)(6)

Attached are the slides and Bio. If your email server stripped them out you can download them at this URL:

<https://drive.google.com/folderview?id=0Bz3bazlO0zAEeVVCam5DMkd3OTQ&usp=sharing>

v/r

Sam

Sam Rhem
J39, DDGO
Program Manager - SRC
SMA Management Team

(b)(6)

NIPR - (b)(6) mail.mil
SIPR - (b)(6) mail.smil.mil
JWICS (b)(6) .ic.gov

CLASSIFICATION: UNCLASSIFIED

| | |
|------------------------|---------------------|
| Sender: | Wall, Joel (b)(6) |
| Recipient: | (b)(6) |
| Sent Date: | 2016/01/27 11:20:16 |
| Delivered Date: | 2016/01/27 11:20:22 |

Jytte Klausen

- Dr. Klausen founded the Western Jihadism Project in 2006 with the aim of providing an integrated approach to demographic research and network analysis of Western violent extremists associated with Al Qaeda and the study of extremist Islamist ideology. The project has produced an archive of jihadist publications—virtual and print—linked to a database containing records related to 5,000 Western citizens and permanent residents who have been convicted in connection with actions related to Al Qaeda and associated violent extremist organizations. She leads a team at Brandeis University who are studying Islamist terrorist networks, funded initially by the UK Home Office, and now by an award from the National Institute of Justice at the U.S. Department of Justice



A NEW APPROACH TO UNDERSTANDING THE DYNAMICS OF HOMEGROWN RADICALIZATION

Professor Jytte Klausen
Brandeis University

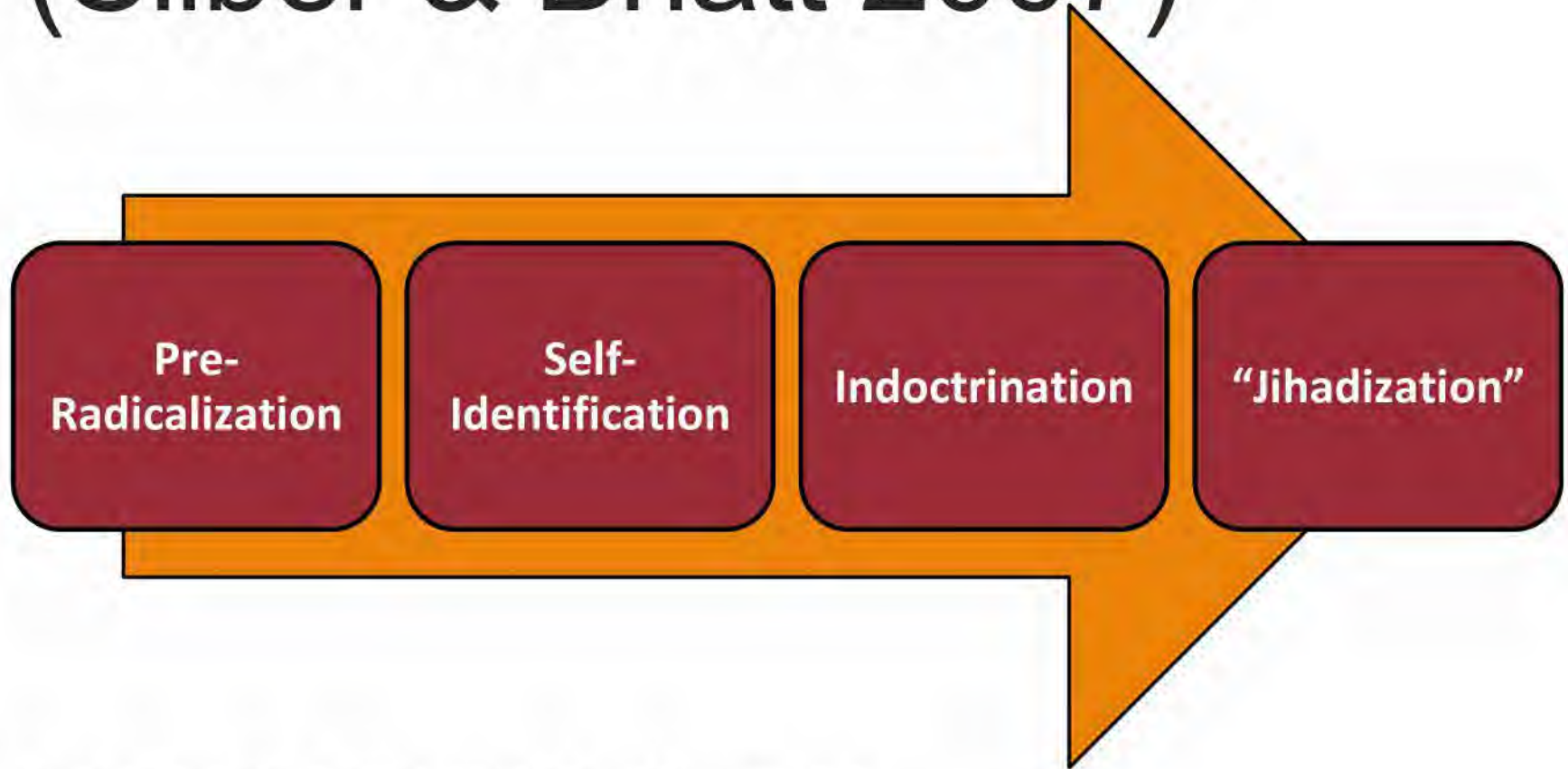
Purpose of Study

- The study presents a dynamic evidence-based assessment model for analyzing the radicalization trajectories of homegrown militants inspired by the Salafi-Jihadist ideology. The questions that concern us are how best to measure the timeline for the increasing commitments that accompany the radicalization process, and how to identify patterns of behavior that reliably signal a deepening commitment to violent extremism. The methodology and preliminary findings were presented at a meeting of researchers and law enforcement officials from Canada, the United Kingdom, and the United States held in Washington D.C. July 28-30, 2015. The research for this paper was supported by a grant from the U.S Department of Justice, Office of Justice Programs, the National Institute of Justice. (Award #2013-ZA-BX-0005). Jytte Klausen (PI), “A Behavioral Study of the Radicalization Trajectories of American “Homegrown” Al Qaeda-Inspired Terrorist Offenders.” Opinions or points of view expressed in this paper are those of the author and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

Data & Methodology

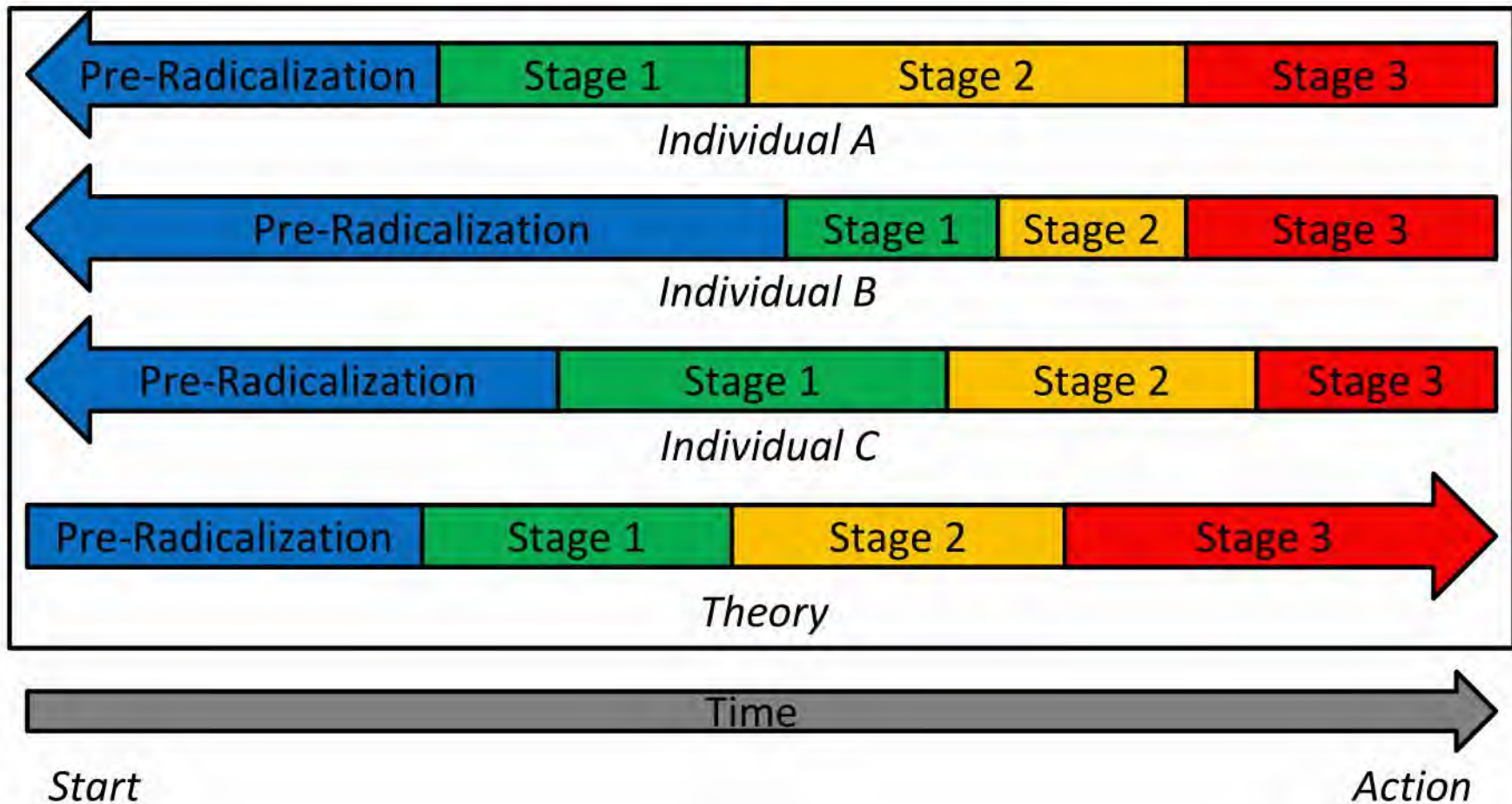
- Subjects were considered eligible as for inclusion in the study based on four conditions: The individual must have spent some or all of their formative years in the United States. The individual's radicalization must have taken place primarily within the United States. The individual's first instance of illicit terrorist activity must have taken place subsequent to September 11, 2001. It was possible to assess the year of their first overt act indicating jihadist militancy from the public record. 331 individuals met the above criteria (Study Group A). From this group, 135 individuals were selected for a more detailed study (Study Group B) that charted the radicalization timelines of the offenders by means of information collated from court records and other public sources. Although unable to ascertain greater details about their paths to carrying out action, we were able to use Study Group A as a control group against which we could compare the smaller focus group.

NYPD Model (Silber & Bhatt 2007)



Randy Borum, "Radicalization into Violent Extremism II: A Review", *Journal of Strategic Security*, no. 4, Winter 2011.

Methodology for Estimating Radicalization Trajectories



Behavioral Indicators of Stage Progression

| Stage: | Pre-Radicalization | Stage 1: Detachment | Stage 2: Peer-Immersion and Training | Stage 3: Planning and Execution of Violent Action |
|---------------------|---|--|--|---|
| Description: | Searching behavior indicative of cognitive opening. | Detaching from previous life; e.g. by spending inordinate amounts of time with online extremist peers | Leaving home to become closer to like-minded individuals. | Enacting violent action or joining a terrorist group abroad, or attempting to do either. |
| This could include: | Expressing disillusionment with world affairs or with religious or political authorities. | Actively seeking to get closer to new authority figures, or engaging in Da'wah online or in real-life. | Attempting to find an organization or a network to “live” as prescribed by the ideology. | Actively supporting another person carrying out violent action on behalf of the ideology. |
| | Behavior indicative of a personal crisis in response to personal events; e.g. family crisis, drug addiction, incarceration, being arrested. | Experiencing a revelation or making changes to lifestyle such as dropping out of school or work. | Behavior indicative of a desire to permanently join the militant community; e.g. by finding a spouse (or spouses) through the extremist community. | Issuing threats online or in real-life, or in other ways supporting immediate violent action; e.g. by engaging in online fraud. |
| | Seeking information in venues outside the individuals’ established social milieu—either online or in real-life, from new authority figures. | Picking fights with local mosque, teachers, colleagues, or family, or otherwise trying to convince others to change by starting a blog or a website. | Seeking out ways to demonstrate commitment to the new ideology and its mission; e.g. by acquiring practical training in the use of firearms or other skills considered important to the extremist mission. | Joining a foreign terrorist organization or taking practical steps to carry out an attack; e.g. by acquiring materials needed to fabricate a bomb or purchasing firearms. |

Sample Coding of Expressions of Behavioral Indicators of Radicalization

| | | | | | | | | | |
|---|---------------------|---------------------|---------------------|---------------------|-------------------|-------------------|------------------------|--------------------|-------------------|
| A | Dropout Date | Disillusioned | Seeking Information | Rebellion | Lifestyle Changes | Training | Peer Immersion | Desire for Action | Steps to Violence |
| B | Seeking Information | Authority Figures | Peer Immersion | Training | Lifestyle Changes | Da'wah- Real Life | Desire for Action | Steps to Violence | |
| C | Dropout Date | Seeking Information | Authority Figures | Lifestyle Changes | Peer Immersion | Da'wah- Virtual | Desire for Action | Foreign Org. | |
| D | Authority Figures | Peer Immersion | Disillusioned | Lifestyle Changes | Desire for Action | Steps to Violence | Training | | |
| E | Seeking Information | Disillusioned | Lifestyle Changes | Da'wah- Virtual | Authority Figures | Peer Immersion | Desire for Action | Training | Steps to Violence |
| F | Seeking Information | Authority Figures | Peer Immersion | Societal Withdrawal | Da'wah- Virtual | Steps to Violence | Nonviolent Support | | |
| G | Disillusioned | Authority Figures | Lifestyle Changes | Peer Immersion | Desire for Action | Foreign Org. | Nonviolent Support | Steps to Violence | |
| H | Dropout Date | Personal Crisis | Seeking Information | Lifestyle Changes | Marriage Seeking | Peer Immersion | Da'wah- Virtual | Nonviolent Support | Steps to Violence |
| J | Seeking Information | Authority Figures | Desire for Action | Peer Immersion | Da'wah- Virtual | Training | Educational Withdrawal | Steps to Violence | |
| K | Disillusioned | Authority Figures | Dropout Date | Seeking Information | Lifestyle Changes | Desire for Action | Societal Withdrawal | Steps to Violence | Foreign Org. |
| L | Personal Crisis | Seeking Information | Authority Figures | Lifestyle Changes | Da'wah- Virtual | Desire for Action | Peer Immersion | Steps to Violence | |
| M | Disillusioned | Authority Figures | Seeking Information | Lifestyle Changes | Peer Immersion | Training | Marriage Seeking | Foreign Org. | |

- by Sequence and Date (dates not shown)

Case Study –

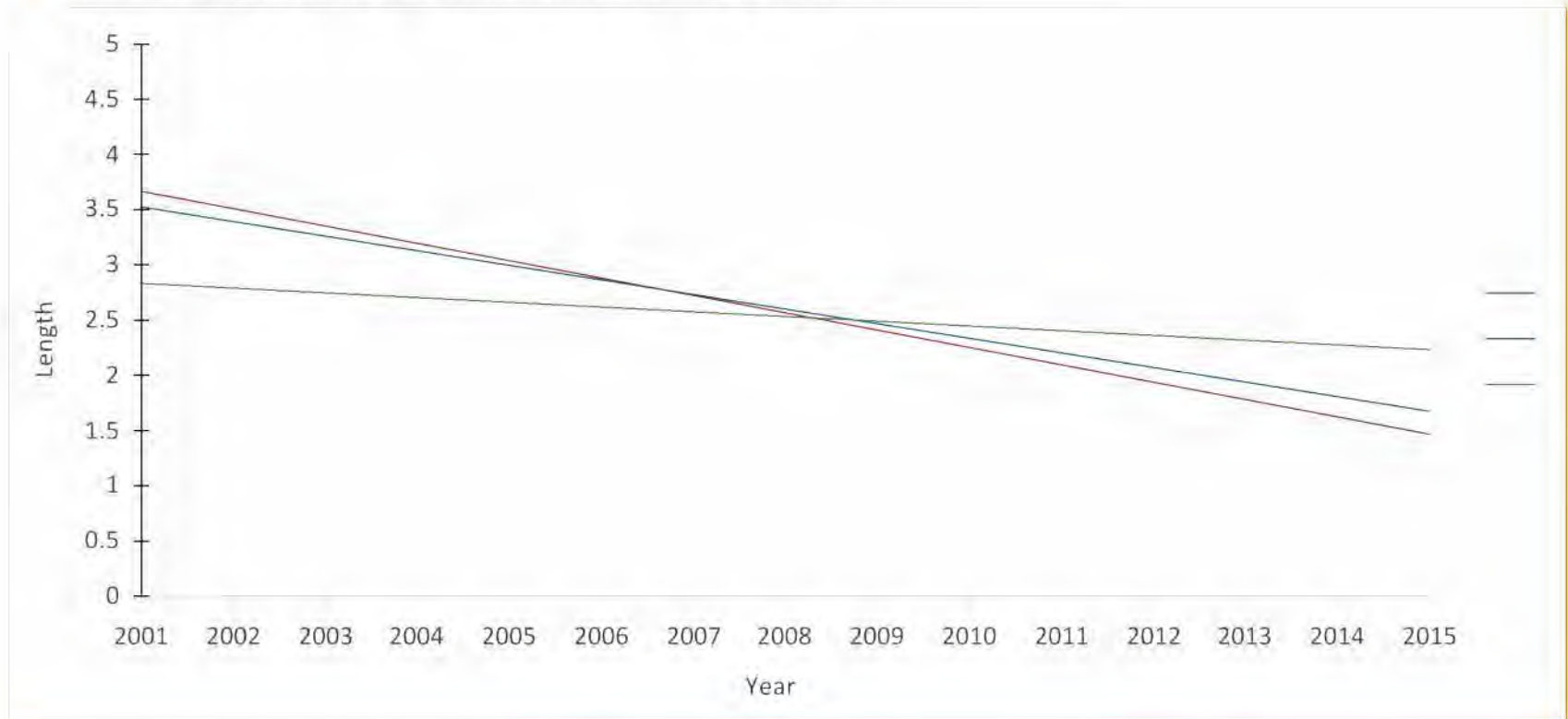
(b)(6)

(b)(6)

| | | | | | | | | | | | | |
|-------------|---------------------|------------------|-----------------------|-------------------|-------------------|----------------|-----------|---------------------|-------------------|------------------------|--------------------------|--------------|
| Spring 2011 | June 2011 | September 2011 | January 2012 | January 2012 | May 2012 | May 2012 | June 2012 | July 2012 | July 2012 | July 2012 | September 2012 | January 2013 |
| Dropout | Seeking Information | Da'wah Real Life | New Authority Figures | Lifestyle Changes | Desire for Action | Peer Immersion | Rebellion | Societal Withdrawal | Physical Training | Steps Towards Violence | Joins Foreign Insurgency | Arrest |

Comparison with Larger Study Group

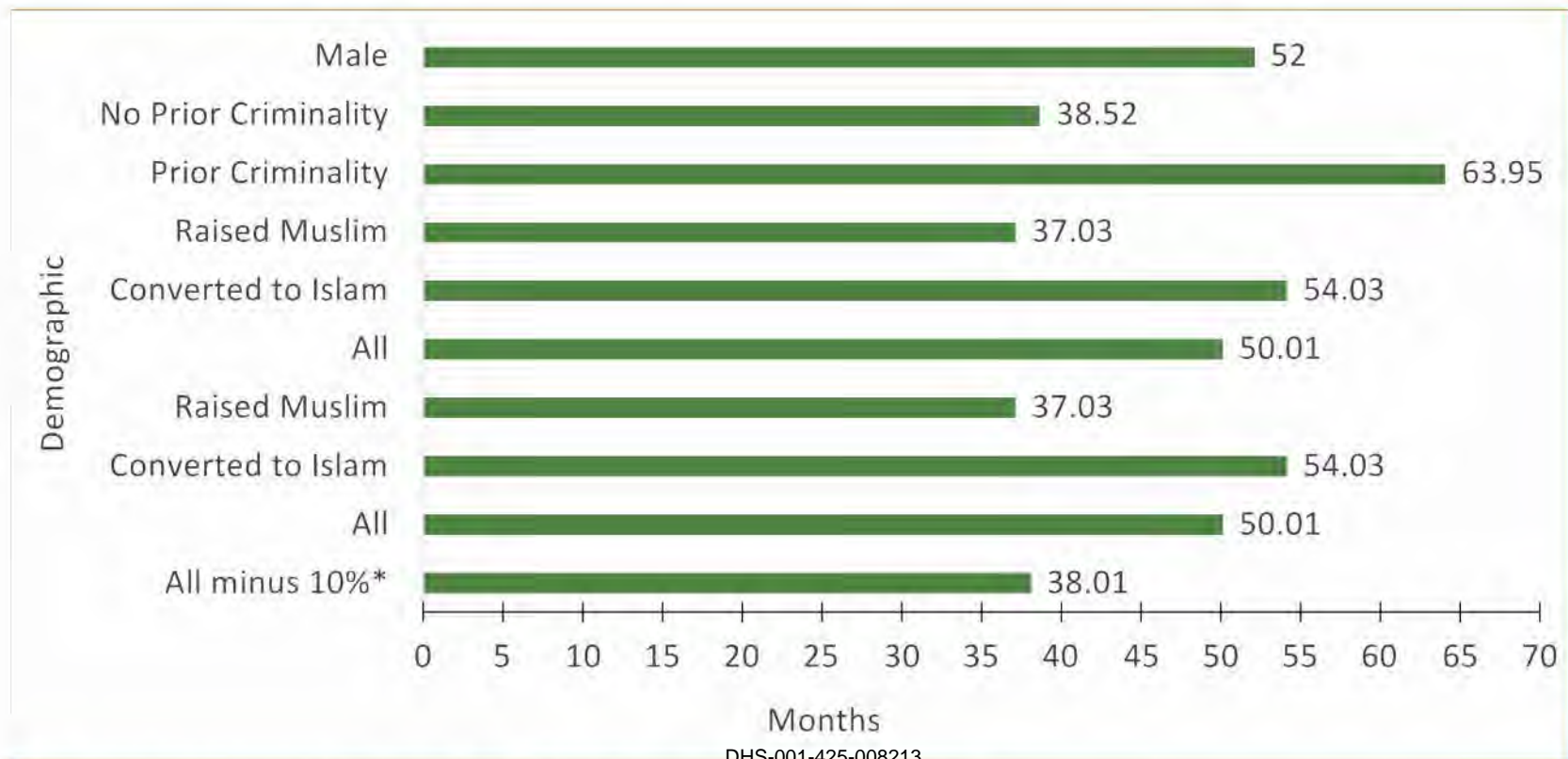
- Median years from radicalization to action



- ANOVA showed no significant difference between Groups B and C $F(1, 315) = 3.17, p > 0.08$ Group C is Group A ($n=331$) minus Group B ($n=135$)

Trajectory Length

- Time from initial cognitive opening to end of terrorist action—all stages. Months; median values; n = 125 10 missing pre-radicalization stage

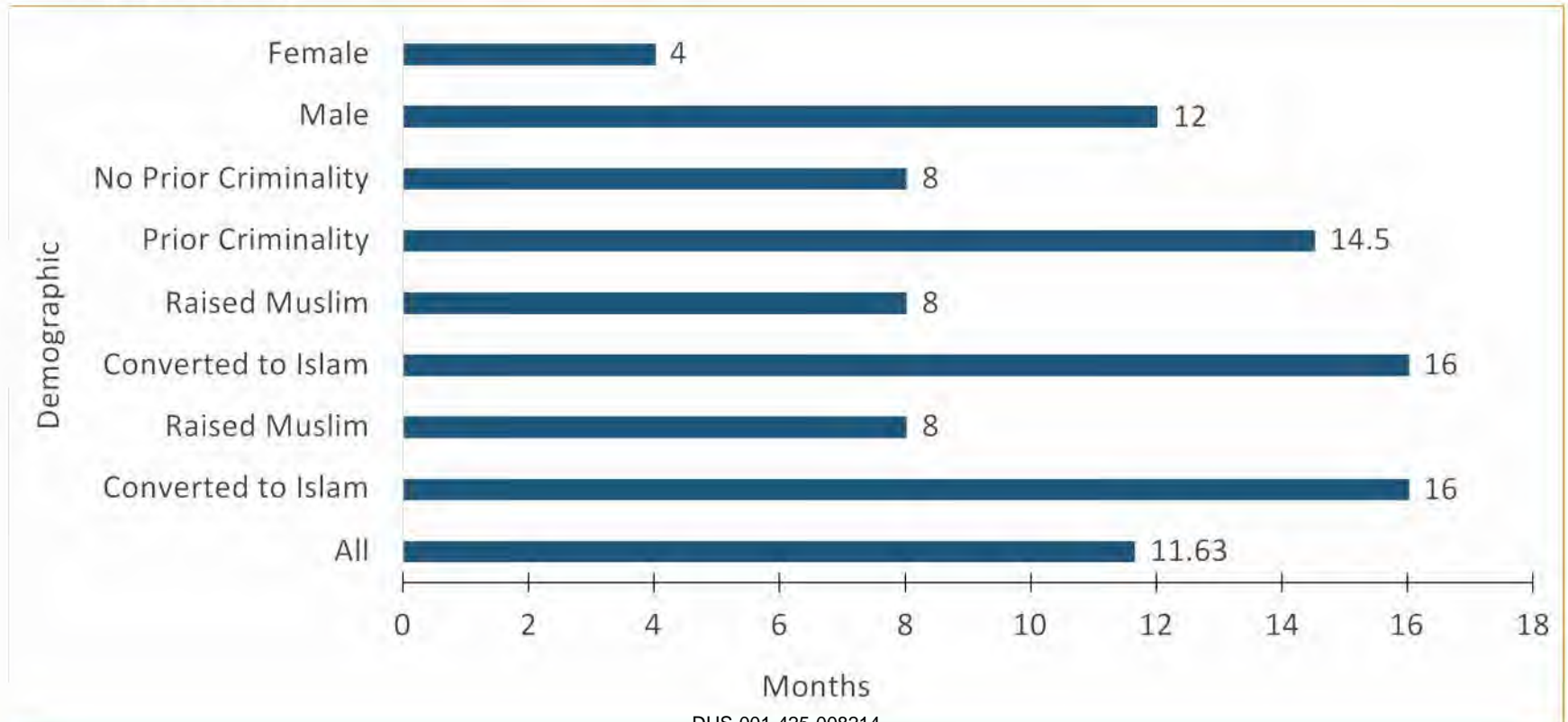


DHS-001-425-008213

*10% outliers removed from upper end of distribution (long-tail removed).

Length from Stage 1 to Stage 2

- Time from start of detachment to end of peer immersion/training— stages 1 and 2. Months; median values; n = 123 (10% Outliers removed from upper end of distribution)



Incidence Rates of Indicators

| | Indicators | Total Occurrences | Percentage of Occurrences in All Cases (135) | Times Placed as Expected | Percentage Placed as Expected |
|----|---------------------------------|-------------------|--|--------------------------|-------------------------------|
| 1 | Disillusionment | 57 | 42.22% | 45 | 78.9% |
| 2 | Personal Crisis | 37 | 27.41% | 28 | 75.7% |
| 3 | Seeking Information | 74 | 54.81% | 62 | 83.8% |
| 4 | Trauma | 26 | 19.26% | 22 | 84.6% |
| 5 | New Authority Figures | 76 | 56.30% | 54 | 71.1% |
| 6 | Rebellion | 16 | 11.85% | 5 | 31.3% |
| 7 | Edu./Occupational Disengagement | 25 | 18.52% | 12 | 48.0% |
| 8 | Lifestyle Changes | 73 | 54.07% | 58 | 79.5% |
| 9 | Drop-Out Date | 51 | 37.78% | 26 | 51.0% |
| 10 | Dawa- Virtual | 46 | 34.07% | 26 | 56.5% |
| 11 | Dawa-Real Life | 32 | 23.70% | 18 | 56.3% |
| 12 | Underemployment | 23 | 17.04% | 15 | 65.2% |
| 13 | Peer-Immersion | 93 | 68.89% | 90 | 96.8% |
| 14 | Desire for Action | 115 | 85.19% | 111 | 96.5% |
| 15 | Physical/Domestic Training | 46 | 34.07% | 42 | 91.3% |
| 16 | Societal Disengagement | 20 | 14.81% | 17 | 85.0% |
| 17 | Marriage Seeking | 28 | 20.74% | 25 | 89.3% |
| 18 | Joins Foreign Insurgency/Org. | 62 | 45.93% | 62 | 100.0% |
| 19 | Steps towards Violence | 87 | 64.44% | 87 | 100.0% |
| 20 | Passive Support | 21 | 15.56% | 19 | 90.5% |
| 21 | Issues Threats | 16 | 11.85% | 16 | 100.0% |

Triads

- Triads of behaviors from pre-radicalization, stage I, and stage II are highly prevalent in cases of known terrorist offenders. On their own behavioral changes are not indicative of radicalization, but, in conjunction with one another, may propel an individual towards illegal terrorist action. A triad is a set of three sequential cues that span at least two stages in the radicalization process.

Triads

- The most common triad included peer immersion (here understood as real-life rather than online peers) followed by expressions of desire for action—preceded by any pre-radicalization indicator. This triad appears in 50% of timelines (Figure X). The most common pre-radicalization behavior leading to criminal actions later was efforts to seek out new religious authority. This particular combination of sequential factors occurred in 24.44% (33) of cases.



Triads

- Behaviors associated with early radicalization reliably anticipated subsequent terrorist action when followed by real-life peer immersion and public expressions of desire for action. This triad was observed in 38% of the offenders' trajectories when preceded by any stage 1 indicator (Figure Y). It is more common that an individual verbalizes interest in carrying out violence after having become immersed in a radical peer-group-- an individual is generally not fully radicalized until he or she seeks out contact with like-minded peers.



Works Published from Study

Jytte Klausen, Selene Champion, Nathan Needle, Giang Nguyen & Rosanne Libretti (2016) Toward a Behavioral Model of “Homegrown” Radicalization Trajectories, *Studies in Conflict & Terrorism*, 39:1, 67-83. Available at: <http://dx.doi.org/10.1080/1057610X.2015.1099995>

Jytte Klausen

Jytte Klausen is the Lawrence A. Wien Professor of International Cooperation at Brandeis University and an Affiliate at the Center for European Studies at Harvard University. Her most recent books are *The Cartoons That Shook the World* (Yale University Press 2009), which is about the worldwide protests against the Danish cartoons of the Muslim Prophet, and *The Islamic Challenge: Politics and Religion in Western Europe* (Oxford University Press 2005, pb. 2007 (translated into German and Turkish; Arabic translation in progress)). In 2006, Klausen founded the Western Jihadism Project, which studies Western violent extremists associated with Al Qaeda. She is currently writing a book about the Western adherents to Bin Laden's movement. Klausen is a commentator on international terrorism on national and international television and radio. She has written, among other journals and newspapers, for *Foreign Affairs*, *The Wall Street Journal*, *TIME*, and *The Boston Globe*.

| | |
|------------------|--|
| From: | Wall, Joel (b)(6) (FYDIBOH) |
| To: | (b)(6) |
| Subject: | Counter ISIL Messaging Speaker Series 31 March 0900 ET |
| Date: | 2016/03/28 15:01:47 |
| Due Date: | 2016/03/27 20:00:00 |
| Type: | Note.EnterpriseVault.Shortcut |

FYSA. Black Swan Author - Professor Nassim Taleb, will discuss his articles "What are the chances of War" and "statistical properties and tail risk of violent conflicts" on 31 March 0900 ET for the SMA Counter ISIL Messaging Speaker Series.

Dial into (b)(6) passcode (b)(6) to participate.

If your email server stripped out the attachments you can download them here:

<https://drive.google.com/open?id=0Bz3bazlO0zAERkxhT2c3S3p3NIU>

Joel D Wall
DHS, ST, OCS

(b)(6) (U/STE)
(b)(6) (BB)
(b)(6) c.gov (JWICS)
(b)(6) gov.gov (SIPR)

CLASSIFICATION: UNCLASSIFIED

| | |
|-------------------|-----------------------------|
| Sender: | Wall, Joel (b)(6) (b)(6) |
| Recipient: | (b)(6) |
| Sent Date: | 2016/03/28 15:01:31 |

| |
|--|
| Delivered Date: 2016/03/28 15:01:47 |
|--|

April 18, 2012

TO: Michael Frias

FROM: John Leyden

RE: Think Tanks with Interest in Countering Violent Extremism

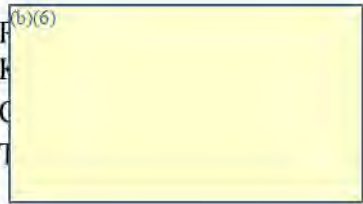
ORGANIZATION:

CSIS – Center for Strategic International Studies

LITERATURE:

- ***Overcoming Extremism: Protecting Civilians from Terrorist Violence***
http://csis.org/files/media/csis/pubs/080321_overcomingextremismconfreport.pdf
- ***Confronting and Uncertain Threat: The Future of Al Qaeda and Associated Movements***
http://csis.org/files/publication/110826_Nelson_%20ConfrontingAnUncertainThreat_Web.pdf
- ***A Growing Terrorist Threat? Assessing “Homegrown” Extremism in the United States***
http://csis.org/files/publication/100304_Nelson_GrowingTerroristThreat_Web.pdf
- ***Countering Terrorism and Radicalization in 2010 and Beyond: A New Terrorist Threat? Assessing “Homegrown Extremism***
http://csis.org/files/publication/100121_countering_terrorism_n_radicalization.pdf

POC:

-  (b)(6)

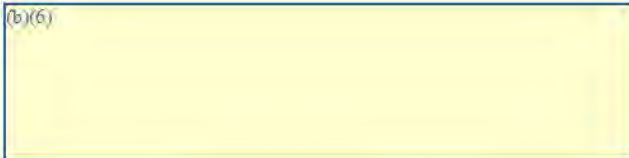
ORGANIZATION:

Council on Foreign Relations

LITERATURE:

- ***Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States, 2011***
<http://www.cfr.org/terrorism/strategic-implementation-plan-empowering-local-partners-prevent-violent-extremism-united-states-2011/p26739>
- ***Low Bar Set in U.S. Counterradicalization Strategy***
<http://www.cfr.org/terrorism/low-bar-set-us-counterradicalization-strategy/p25593>

POC:

-  (b)(6)

ORGANIZATION:

The German Marshall Fund of the United States

LITERATURE:

- ***Democracy under pressure***
<http://blog.gmfus.org/2010/05/democracy-under-pressure/>

POC:

-  (b)(6)

ORGANIZATION:

New America Foundation

LITERATURE:

- ***Right- and Left-Wing Terrorism Since 9/11***
http://homegrown.newamerica.net/overview_nonjihadists
- ***Countering Domestic Radicalization
Lessons for Intelligence Collection and Community Outreach***
http://www.newamerica.net/sites/newamerica.net/files/profiles/attachments/Fishman_Lebovich_Domestic_Radicalization.pdf

POC:

-  (b)(6)

ORGANIZATION:

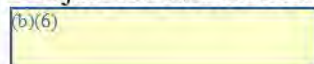
Pew Research Center

LITERATURE:

- ***Political Extremism (at Home and Abroad) Dominates the Blogosphere***
<http://pewresearch.org/pubs/1258/new-media-index-extremism-holocaust-museum-britain-letterman-palin>
- ***Religion in Prisons: A 50-State Survey of Prison Chaplains***
<http://pewresearch.org/pubs/2226/prison-chaplains-prisoners-proselytizing-extremism-rehabilitation>
- ***Muslim Americans: No Signs of Growth in Alienation or Support for Extremism
Mainstream and Moderate Attitudes***
<http://pewresearch.org/pubs/2087/muslim-americans-islamic-extremism-911-attacks-mosques>

POC:

- Project for Excellence in Journalism

 (b)(6)

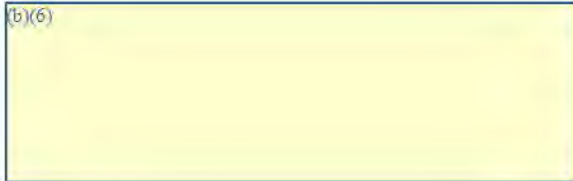
ORGANIZATION:

Quilliam Foundation

LITERATURE:

- ***Cheering for Osama: How jihadists use internet discussion forums***
http://www.quilliamfoundation.org/images/stories/pdfs/cheering-for-osama.pdf?dm_i=JI3,AEVL,3031IN,SI26,1
- ***Radicalisation on British University Campuses: a case study***
http://www.quilliamfoundation.org/images/stories/pdfs/radicalisation-on-british-university-campuses.pdf?dm_i=JI3,AEVL,3031IN,SI26,1

POC:

- (b)(6) 

ORGANIZATION:

Triangle Center on Terrorism and Homeland Security

LITERATURE:

- ***Muslim-American Terrorism Since 9/11: An Accounting***
http://sanford.duke.edu/centers/tcths/about/documents/Kurzman_Muslim-American_Terrorism_Since_911_An_Accounting.pdf

POC:

- (b)(6) 

ORGANIZATION:

American Enterprise Institute

LITERATURE:

- *Safety, Liberty, and Islamist Terrorism*
<http://www.aei.org/book/foreign-and-defense-policy/safety-liberty-and-islamist-terrorism/>

POC:

- (b)(6)

ORGANIZATION:

Homeland Security Policy Institute

LITERATURE:

- ***THE TRAGEDY IN TOULOUSE:
WHEN KINETIC COUNTERTERRORISM TACTICS AREN'T ENOUGH***
http://www.gwumc.edu/hspi/policy/commentary026_Toulouse.pdf

POC:

- (b)(6)

LIST OF REVIEWED THINK TANKS:

- Center for American Progress
- Center for National Policy
- Center for Strategic & International Studies
- Center for International and Security Studies
- CLSA
- Council on Foreign Relations
- The German Marshall Fund of the United States
- HSPI Homeland Security Policy Institute
- New America Foundation
- Peter G. Peterson Foundation
- Pew Research Center
- Quilliam Foundation
- RAND
- Royal United Services Institute
- School for Advanced International Studies
- The Brookings Institution

- The Heritage Foundation
- Triangle Center on Terrorism and Homeland Security
- American Enterprise Institute
- Woodrow Wilson International Center for Scholars



Countering Violent Extremism

Imam Mohamed Magid

Understanding Recruitment

- ◆ Social Vulnerability Isolation from the Mosque Parent-Children Relationship Seeking understanding of religion online Emotional and psychological vulnerability

Community Response

- ◆ Conducting internet safety workshop
Hiring professionals to address youth issues
Create platforms for youth to express their concerns regarding international issues
Counseling parents who notice signs of extremism or radicalization of their children
Establishment of Muslim Compassionate Corps

Counseling People Exposed to Radicalization

- ◆ Deconstructing the narrative that is based on a false sense of “dignity, opportunity and religiosity” Reestablishing the trust between young people and their parents by empowering parents and teaching them how to engage with their children who are now speaking a different language in terms of religiosity Counseling young people on the importance of family and the priorities from the Islamic perspective Reestablishing trust between young people and their communities by showing them various programs that they can engage with in their communities that help them to make a difference

Relationship Between the Community and Law Enforcement

- ◆ Establish a relationship with communities that is broader than Violent Extremism Prevention. I.e. Engage the community on ways to protect the general safety of the community and provide information on what services law enforcement offers. Train on how to deal with active shootings, emergency preparedness, and other crisis situations. Establish mechanisms and ways in which communities are able to report any suspicious behavior without the fear of backlash. Protection of civil rights and civil liberties by building trust that the community is not being monitored as a suspect. Impact of Islamophobia on the community and law enforcement leadership Training Law Enforcement about Islam

Page 01 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16 of 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

| | |
|-----------------|------------------------------------|
| From: | Seaman, Matthew <(b)(6)> (b)(6) |
| To: | (b)(6) |
| CC: | |
| Subject: | Countering Violent Extremism - SOF |
| Date: | 2012/07/27 10:10:26 |
| Type: | Note.EnterpriseVault.Shortcut |

(b)(6)

Please see the attached statement of facts for the priority 1 GAO engagement "Training to Address Violent Extremism" (441015). We are shooting to have the exit conference on August 8th or 9th.

Password will follow.

Thanks,

Matt

Matthew G. Seaman
 Departmental GAO-OIG Audit Liaison
 Office of the Chief Financial Officer
 U.S. Department of Homeland Security

Desk: (b)(6)

BB (b)(6)

(b)(6).dhs.gov <mailto:(b)(6)dhs.gov>

(b)(6)gov.gov <mailto:(b)(6)gov.gov>

| | |
|------------------------|------------------------------------|
| Sender: | Seaman, Matthew <(b)(6)> (b)(6) |
| Recipient: | (b)(6) |
| Sent Date: | 2012/07/27 10:10:12 |
| Delivered Date: | 2012/07/27 10:10:26 |

Page 01 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 05 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 06 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 07 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 08 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 10 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 13 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17 of 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

| DEPARTMENT OF HOMELAND SECURITY | | | | |
|--|--|-----------------------|----------|------------|
| CVE Program Funding Levels | | FY16 Enacted | | |
| | | Insert Component Name | | |
| [Insert Mission Here] | | # of FTE | FTE \$ | Program \$ |
| Encourage and Enable Our Partners To Counter Violent Extremism | | | | |
| Enhance community understanding of the threat and effective measures to counter violent extremism. | | | | |
| Enhance training for federal, state, local, tribal, and territorial law enforcement | | | | |
| Develop and share intelligence assessments with state, local, tribal, territorial, and community partners. | | | | |
| Evaluate DHS progress in meeting targets in the 2011 White House Strategic Implementation Plan. | | | | |
| Enhance DHS collaboration with the technology and philanthropic sectors on CVE. | | | | |
| Provide tools to our partners. | | | | |
| Enhance DHS mechanisms for providing financial assistance to CVE programs. | | | | |
| Expand the DHS presence in the pilot cities (Boston, Los Angeles, and Minneapolis). | | | | |
| Total | | 0 | 0 | 0 |
| Build Trust and Partnerships Between Government Entities and Communities | | | | |
| Build trusted relationships to support community-based efforts. | | | | |
| Facilitate rapid response in the wake of an event. | | | | |
| Launch the "Your Homeland Security" campaign | | | | |
| Initiate the "Every Interaction Counts" campaign | | | | |
| Total | | 0 | 0 | 0 |
| Understand the Threat of Violent Extremism and Effective Efforts to Counter the Threat | | | | |
| Conduct focused research and analysis | | | | |
| Engage communities and SLTT entities to identify effective actions | | | | |
| Leverage insights from international partners | | | | |
| Support the comprehensive evaluation of current CVE programs. | | | | |
| Encourage the identification and testing of new ideas for CVE | | | | |
| Ensure that research investments are prioritized to address critical CVE gaps. | | | | |
| Ensure that DHS CVE efforts are directly informed by our understanding of the violent extremist threat. | | | | |
| Total | | 0 | 0 | 0 |
| Improve coordination and direction of DHS effort to counter violent extremism | | | | |
| Establish the Office of Countering Violent Extremism. | | | | |
| Measure program impacts and effectiveness of DHS CVE programs and share this data with senior leaders | | | | |
| Leverage outside expertise through the Homeland Security Advisory Council. | | | | |
| Total | | 0 | 0 | 0 |
| TOTAL | | 0 | 0 | 0 |



Homeland Security Advisory Council

Countering Violent Extremism Subcommittee

| Name | Title, Organization |
|-------------------------------------|---|
| Farah Pandith (Chair) | Adjunct Senior Fellow at the Council on Foreign Relations, Senior Fellow at the Kennedy School of Government at Harvard University, Former Special Representative to Muslim Communities, U.S. Department of State |
| Adnan Kifayat (Chair) | Senior Resident Fellow, German Marshall Fund of the United States |
| Laila Alawa | Chief Executive Officer & Founder, Coming of Faith |
| John Allen | Retired U.S. Marine Corps. General and Former Special Presidential Envoy for the Global Coalition against ISIL |
| Russ Deyo | Under Secretary for Management, Department of Homeland Security |
| Paul Goldenberg | President and Chief Executive Officer, Cardinal Point Strategies |
| Jane Harman | President and Chief Executive Officer, Woodrow Wilson Center |
| Seamus Hughes | Deputy Director, Program on Extremism at George Washington University |
| Joel Meyer | Senior Vice President, Public Sector at Dataminr |
| Jeffrey Miller | Senior Vice President and Chief Security Officer, National Football League |
| Michael Nutter | Former Mayor, Philadelphia, Pennsylvania |
| Matthew Olsen | President of Consulting and Co-Founder, IronNet Cybersecurity |
| Ali Soufan | Chairman and Chief Executive Officer, The Soufan Group LLC |
| Juan Zarate | Senior Adviser at the Center for Strategic and International Studies |
| William Webster (Ex-officio) | Retired Partner, Milbank, Tweed, Hadley & McCloy LLP |

| | |
|------------------|--|
| From: | Miron, Mike (b)(6) |
| To: | "Miron, Mike (b)(6) |
| Subject: | Countering Violent Extremism Training Grants - June 30 note from the Office of Intergovernmental Affairs |
| Date: | 2014/07/01 08:18:54 |
| Priority: | Normal |
| Type: | Note |

Good morning FBAC members,

Please see the below note sent yesterday regarding FEMA's 2014 Continuing Training Grant Funding Opportunity Announcement (FOA) via grants.gov. This year's FOA includes Countering Violent Extremism as a training focus area for 2014.

More information can be found at: <http://www.grants.gov/web/grants/search-grants.html?keywords=cve>

I have also attached:

- FY 2014 Homeland Security National Training Program (HSNTP) Continuing Training Grants (CTG) Program
- Fiscal Year (FY) 2014 Continuing Training Grants (CTG) Program Frequently Asked Questions (FAQs)
- The Department of Homeland Security Funding Opportunity Announcement

Thank you,

Mike

Mike Miron
 Director,
 Homeland Security Advisory Council
 U.S. Department of Homeland Security

(b)(6)

For information about the Homeland Security Advisory Council, go to www.dhs.gov/homeland-security-advisory-council-hsac

From: DHS.IGA
Sent: Monday, June 30, 2014 10:05 AM
To: DHS.IGA
Subject: Countering Violent Extremism Training Grants

Dear Colleagues,

The Department of Homeland Security's Office of Intergovernmental Affairs would like to share with you information from the Department's Federal Emergency Management Agency (FEMA) about their 2014 Continuing Training Grant (CTG) Funding Opportunity Announcement (FOA) via grants.gov. This year's FOA includes Countering Violent Extremism (CVE) as a training focus area for 2014. ***The FOA will be open for 30 days and close on July 16, 2014.***

Eligible applicants include: State governments; Public and State controlled institutions of higher education; County governments; Private institutions of higher education; **Nonprofits** (including community organizations) having a 501(c)(3) status with the IRS, other than institutions of higher education; City or township governments; and Native American tribal governments (Federally recognized).

Here is the link to the FOA: <http://www.grants.gov/web/grants/search-grants.html?keywords=cve>

Regards,

DHS Office of Intergovernmental Affairs
U.S. Department of Homeland Security
DHS.IGA@hq.dhs.gov



cid:image001.gif@01CB1EA8.7DF6B3D0

| | | |
|------------------------|---------------------|--|
| Sender: | Miron, Mike (b)(6) | |
| Recipient: | "Miron, Mike (b)(6) | |
| Sent Date: | 2014/07/01 08:18:52 | |
| Delivered Date: | 2014/07/01 08:18:54 | |



Fiscal Year (FY) 2014 Continuing Training Grants (CTG) Program Frequently Asked Questions (FAQs)

1. What is the purpose of the FY 2014 Continuing Training Grants (CTG) Program?

The purpose of the FY 2014 CTG program is to develop and deliver a national training program that provides tailored, specialized training to first responders, homeland security/emergency management officials, and/or citizens to meet emerging training needs in our nation's communities to help prevent, mitigate, protect against, respond to, and recover from disasters. The training must address the requirement that all courses be accessible, complying with section 504 and 508 of the Rehabilitation Act http://www.hhs.gov/web/508/resources/508_508.html.

Funding for this year's Funding Opportunity Announcement (FOA) is authorized by The Consolidated Appropriations Act, 2014 (Public Law No: 113-76).

2. What areas will the FY 2014 CTG Program focus on to address training requirements?

Program Objectives

- Hazardous Materials (HazMat)/Weapons of Mass Destruction (WMD)
- Cybersecurity
- Countering Violent Extremism (CVE)
- Maturing Public-Private Partnerships
- Medical Readiness/Immediate Victim Care at Mass Casualty Events
- Rural Training

3. How were the six focus areas selected for CTG funding?

The focus areas were selected based on the FY 2014 Consolidated Appropriations Act and the findings in the National Preparedness Report (NPR), the State Preparedness Reports (SPR), and the Threat and Hazard Identification and Risk Assessment (THIRA) reports.

4. How much funding is available under the FY 2014 CTG program?

In FY 2014, a total of \$11,000,000 is available.

5. Who is eligible to apply for FY 2014 CTG funds?

Eligible applicants for the FY 2014 CTG include entities with existing programs or demonstrable expertise relevant to the focus areas in the funding opportunity announcement to include: State, local, tribal, and territorial entities, nonprofit national associations and organizations; non-profit higher education institutions; and non-profits, including community and faith-based organizations. Applicants for the Rural Training focus areas must have

demonstrable experience and expertise in rural training as well as in developing and delivering FEMA-certified courses to rural communities across the Nation.

6. How are multi-State/multi-jurisdictional applications being defined?

Applications that are submitted on behalf of more than one state or local jurisdiction are strongly encouraged to apply for the FY 2014 CTG. Single states and single jurisdictions remain eligible to apply. Multi-state, multi-jurisdiction applications are meant to encourage collaboration between states and jurisdictions with similar homeland security strategies and approaches. Under a multi-State / multi-jurisdiction submission, one State or local jurisdiction will need to be the applicant on behalf of the other parties. The application should reference the other parties associated with the application.

7. What are the major differences between the FY 2013 and the FY 2014 CTG Funding Opportunity Announcements?

- The focus areas for the competitive pool within CTG are different:
 - In FY13, the focus areas included:
 - Medical Readiness/Immediate Emergency Victim Care at Mass Casualty Events,
 - Countering Violent Extremism, Hazardous Materials/Weapons of Mass Destruction,
 - Emergency Management Leadership,
 - Cybersecurity; and
 - Rural training competitive pool: (1) Isolation and Quarantine and (2) Environmental Health.
 - The FY14 focus areas are:
 - Hazardous Materials /Weapons of Mass Destruction ;
 - Cybersecurity;
 - Countering Violent Extremism;
 - Maturing Public-Private Partnerships;
 - Medical Readiness/Immediate Victim Care at Mass Casualty Events; and
 - Rural Training which include six new training topics;
 - Hazardous Materials;
 - Mass Fatality Planning and Response;
 - Crisis Management for School Based Incidents;
 - Development of Emergency Operations Plans;
 - Bioterrorism Awareness; and
 - Media Engagement Strategies for First Responders.
- The amount of funding available for the competitive portion of the CTG has increased in FY14:
 - In FY13, the available funding was \$7,811,256.
 - In FY14, the total funding available is \$11,000,000.

8. Who will administer the CTG? Is FEMA involved in developing the training programs?

The FY 2014 CTG will be administered by DHS-FEMA's National Training and Education Division. CTG training programs are not administered by the states. The CTG FOA is announced directly to eligible applicants through grants.gov.

FEMA requires substantial federal involvement with the programs awarded within the CTG training programs because they are cooperative agreements. The CTG training supports the core capabilities of the five mission areas of FEMA: Prevention, Protection, Response, Recovery, and Mitigation. FEMA collaborates and reviews the curricula of the training as it is developed to assure that the material appropriately reflects FEMA's mission and the National Preparedness Goal. FEMA also evaluates whether the trainers have sufficient credentials to carry out the training, and whether sufficient state, tribal, and local personnel are attending the trainings. FEMA also collaborates and assures that the training provided is sufficiently national in scope, so all areas of the nation are included.

9. Is this a competitive grant program?

Yes, the FY 2014 CTG is an open and competitive training program.

10. Does funding for the FY 2014 CTG go through the State Administrative Agency?

No. All eligible applicants may apply directly through Grants.gov for the FY 2014 CTG.

11. What are some of the specific training needs to be addressed in the focus area

Hazardous Materials (HazMat)/Weapons of Mass Destruction (WMD)? Training developed in the HazMat/WMD focus area should bring together members of the response community within various jurisdictions for training that uses the resources and protocols required to respond to HazMat/WMD incidents—incidents that are complex in nature as they require members of multiple agencies and disciplines to work together to control threats to responders, the public, infrastructure (e.g., transportation, public works and communication systems), property, and the environment. Applicants should consider the following training objectives:

- Support Executive Order 13650: Improving Chemical Facility Safety and Security. <http://www.whitehouse.gov/the-press-office/2013/08/01/executive-order-improving-chemical-facility-safety-and-security>
- Achieve compliance with current competencies identified in the National Fire Protection Association (NFPA) 472 Standard for Competence of Responders to Hazardous Materials/Weapons of Mass Destruction Incidents;
- Deliver training which addresses planning, response, mitigation strategies and actions for transportation incidents. Training on this topic should cover, at a minimum, combustible and flammable petroleum hazards and response.
- Increase knowledge, skills, and abilities to achieve the core capabilities of interdiction and disruption, on-scene security and protection, operational communications, and operational coordination to enhance a jurisdiction's capability to prepare for, mitigate, and respond to hazardous materials and WMD complex incidents through awareness of other first responders' roles and responsibilities and practical applications;
- Address preparedness and response capability for acts of terrorism; and

- Create curriculum which utilizes standardized terminology to describe concepts and actions, and comply with the National Incident Management System.

12. What are some of the specific training needs to be addressed in the focus area of Cybersecurity?

The training should include goals and objectives that meet criteria to include, but not limited to, the following:

- **Cybersecurity Policy** – Training to develop and refine policies, plans, and procedures, which are related but serve distinctly different purposes. A policy is the highest level document that states what a company, group, or department will and will not do during a cyber emergency. A plan is the organizational document that describes a methodology for how to achieve the policy’s goals. A procedure is the step-by-step instructions to the operator for exactly how a task is to be done. All are essential to a comprehensive approach to cybersecurity.
- **Cybersecurity Awareness and Training** – The most vulnerable aspect of a system is the human component. Users who have been granted access to a system need to be instructed in how to keep that access information confidential. Along with access credentials, users possess other knowledge of an organization that can be valuable to someone with malicious intent. In addition to logical controls, physical controls, a comprehensive company policy, and other important security measures, training should be performed regularly in order to maximize the effectiveness of existing security measures and to reduce the risk of social engineering. Security training and reinforcement of that training through ongoing awareness information sessions has been shown to lower the risks associated with the human component of a security strategy.
- **Monitoring and Incident Response** – In the event of an emergency that involves a system failure, a detected or active intrusion, detection or suspected involvement of malware, or Advanced Persistent Threat (APT) action, having an established protocol and response team is critical to timely incident mitigation and response to limit the extent and degree of the damage. Monitoring and incident response address the need for a proactive approach to system incidents. Rather than waiting for incidents to occur and attempting to shape a response when time and resources are not at optimal levels, preparation ahead of time to include continuous monitoring and information sharing, and maintenance of situational awareness can greatly reduce the damage, as well as the time needed to recover from an adverse event. Recognizing security events for what they are and making management aware of the incidents and their potential for harm is a critical element, not only to limit the damage from cyber attacks, but also to obtain the appropriate support and resources to effectively manage cybersecurity.
- **Disaster Recovery and Business Continuity** – Information Technology (IT) systems are known to be vulnerable to a variety of adverse events, any of which has the potential to impact normal business operations and compromise the confidentiality, integrity, and availability of data. Although planning and mitigation strategies are known to reduce the risks posed by these events, it is impossible to fully eliminate the risks, and the potential damage posed by them. Because of this, due care should be taken to plan what steps an organization will take in the event of a system disruption, no matter the size. By making and testing effective plans ahead of time, the potential damage and loss of productivity, revenue, and sensitive information can be greatly reduced.

- Risk (and Vulnerability) Management – Cyber risk methodologies usually include various processes to identify and measure risk to a system or group of systems and provide a repeatable method for conducting and monitoring risk. Most common to all methodologies are processes for conducting risk assessments performing system testing including observation, data analysis, and electronic testing (e.g., vulnerability scanning, penetration testing); and tracking and monitoring system weaknesses and mitigation activities (e.g., Plan of Action). The risk identification methodology should be standardized and approved by senior management to ensure results are consistent with one another and throughout the organization.

13. What are some of the specific training needs to be addressed in the focus area of Countering Violent Extremism (CVE)

CVE Training should:

- Raise awareness and understanding of violent extremism based on analysis and research, case studies on behaviors and indicators associated with violent extremists, and radicalization to violence
- Counter the “us-versus-them” mentality propagated by terrorist organizations and others, including using a more inclusive method of outreach and trust-building between law enforcement and community partners
- Increasing cultural competency and identify the difference between constitutionally protected, cultural, and religious behavior versus indicators of criminal behavior or radicalization to violence
- Promote and support best practices in community-oriented policing, and community engagement, in order to strengthen partnerships between communities and the Government and promote information-driven, community-based solutions to prevent violent extremism and build community resilience. As an example, training efforts improving the internal community support derived from its network of families and friends in order to improve resistance to the emergence of radicalized violent extremism efforts or in countering the effects of radicalization to violence within individuals. These programs also serve to change perceptions of mistrust for external community partners, such as law enforcement and other agencies.
- Use existing resources located on the Homeland Security Information Network (HSIN) joint DHS and FBI Countering Violent Extremism and Active Shooter (CVE-AS) Web Portal.

14. What are some of the specific training needs to be addressed in the focus area of Maturing Public-Private Partnerships?

Training in this focus area should address and support the following goals for public-private partnerships:

- Provide lessons learned and training tools for building strong public-private partnerships that can strengthen state, local, tribal and territorial Emergency Operation Centers (EOC) plans;
- Promote collaboration, coordination, and communication efforts between government and private sector partners to create more resilient communities and increase jurisdictional capacity to prevent, protect against, respond to, and recover from major incidents;

- Increase the effectiveness of emergency management and homeland security efforts in the public and private sectors by increasing all partners' understanding of each other's capabilities and preparedness efforts;
- Build strong teams (pre-incident) based on mutual understanding that result in faster, more effective response and recovery efforts;
- Share situational awareness during disasters, such as through structured situation reports between a public and private emergency operations centers, or through social media exchanges, as an example. The private sector, too, relies on timely information from the government to make sound business decisions related to operations, customer and employee safety, and supporting communications; and
- Leverage public and private sector communication channels to expand reach and access to timely, vital information.

15. What are some of the specific training needs to be addressed in the focus area of Medical Readiness/Immediate Victim Care at Mass Casualty Events?

Training developed should include the following elements:

- Mass casualty planning, training, and exercises oriented specifically with law enforcement, fire, and EMS providers to rapidly deploy in a coordinated effort into areas that have been cleared, but not secured, in order to initiate treatment at or near the point of injury and effect rescue of survivors.
- Develop and exercise plans, which ensure the health and safety of first responders and citizen responders; and training focused on the prevention and detection of secondary attacks.
- Enhancing coordination between law enforcement, fire, first responder agencies, EMS systems, local healthcare delivery and trauma systems that provide victim triage, treatment, and transport to ensure patients are distributed to appropriate levels of definitive emergency care.
- Establishing protocols that incorporate the guidelines on the medical principles of Tactical Emergency Casualty Care and conduct training for responders.
- Empowering community members through public education and training, such as Community Emergency Response Teams (CERTs), about life sustaining actions, including aggressive hemorrhage control measures for severe bleeding and use of tourniquets to support survivors and providers in a mass casualty event.

16. What are some of the specific training needs to be addressed in the focus area of Rural Training?

Training should be developed to address the following topics:

- Hazardous Materials (HazMat) – This topic includes training in the areas of HazMat planning and response at plants and fixed sites, HazMat transportation incident response, HazMat pipeline incident response, and HazMat port (waterways) incident response for rural first responders. Training should be appropriate to accommodate volunteer emergency responders with an understanding of the challenges faced by volunteer forces. Training should support Executive Order 13650: Improving Chemical Safety and Security. <http://www.whitehouse.gov/the-press-office/2013/08/01/executive-order-improving-chemical-facility-safety-and-security>. Training should address compliance with current competencies identified in the

National Fire Protection Association (NFPA) 472 Standard for Competence of Responders to Hazardous Materials/Weapons of Mass Destruction Incidents; and address planning, response, and mitigation strategies and actions for transportation incidents. Training for transportation incidents should cover, at a minimum, combustible and flammable petroleum hazards and response.

- Mass Fatality Planning and Response– This topic includes training in the areas of planning and response for rural emergency managers and first responders, and courses for rural morticians and funeral directors.
- Crisis Management for School Based Incidents– This topic includes training on all significant school-based incidents to include bomb threats, active shooter, severe weather, structural/mechanical failures, student demonstrations, and HazMat releases. Training should be targeted for rural law enforcement officials, fire and EMS professionals/volunteers, and school system administrators and staff.
- Development of Emergency Operations Plans (EOP) – This topic includes training on plan development and testing of EOPs in rural jurisdictions. Training should target rural emergency managers, incident commanders, Emergency Operations Center (EOC) staffs and any personnel or agencies serving or supporting an Incident Command System (ICS) structure.
- Bioterrorism Awareness– This topic includes training in the areas of biological threats and the adverse effects of biological contamination; this training should also focus on agro-terrorism and food system disasters. Training should target emergency managers, law enforcement, fire, and EMS professionals/volunteers, hospital providers and staff, agriculture community professionals and associations, and other appropriate emergency planners and responders in rural communities.
- Media Engagement Strategies for First Responders–Training in this topic should focus on dealing with the media in a variety of disaster situations. Training should target rural government officials, emergency managers, public information officers, incident commanders, and others as appropriate within rural communities.

17. How can I access the FY 2014 CTG funding opportunity announcement?

Applications can be found via www.grants.gov. Eligible grantees must apply for funding through www.grants.gov. The application must be completed and submitted through the ND Grants system located at <https://portal.fema.gov>. Training for submitting the applications via ND Grants can be found at <http://www.fema.gov/government/grant/ndgms.shtm>. The www.grants.gov customer support hotline is (800) 518-4726.

18. What is the Catalog of Federal Domestic Assistance (CFDA) Number and Title for this Program?

The CFDA number is 97.005 and the title is State and Local Homeland Security National Training Program.

19. Is one of the goals of the FY 2014 CTG to develop national training programs that are national in scope?

Yes, the delivery of training programs should incorporate geographic diversity when offering the courses, including training at the state, local, tribal, and territorial levels across the 56 states and territories. All applicants will be evaluated on their ability to develop and deliver

training programs to participants on a national level. Applicants should describe their course delivery methods and demonstrate their ability to reach a national audience, such as instructor led mobile deliveries, resident, or on-line training.

20. What is the period of performance for the FY 2014 CTG?

The period of performance for the FY 2014 Continuing Training Grants is 36 months. The projected award start date is October 1, 2014 and the projected end date is September 30, 2017.

21. Can eligible applicants apply for funding in more than one identified Focus Area?

Yes, an eligible applicant can apply for funding in more than one identified focus area.

22. What are SAM Accounts?

The acronym "SAM" stands for System for Award Management. All recipients of federal funds must have an account in SAM. Applicants must ensure that their SAM account is active and will not expire prior to September 30, 2014. Applicants will not be able to complete their grant application without an active SAM account. **Establishing a SAM account can take up to 15 business days.** Failure to do so prior to the application period may result in major complications during the application period and you may not receive your award.

23. How are awards determined?

FEMA's National Preparedness Directorate will facilitate the review and evaluation of each application to ensure the applicants clearly demonstrate their ability to design, develop, and deliver a national training program that provides tailored, specialized training to first responders and/or citizens. FEMA's administrative, independent peer review process will determine that all applications meet the requirements of the CTG before moving eligible applicants to the full application review process.

FEMA's National Preparedness Directorate (NPD) will facilitate peer panels of subject-matter experts to review each proposal. The purpose of the peer review process is to ensure objective and unbiased subject-matter expert input into the strengths and weaknesses of proposals submitted under the CTG. Peer reviewers are selected based on their technical expertise and/or knowledge and experience in the development of training curriculum. The panels will discuss each proposal in detail, resolve disparate scoring issues among panel members, and reach a consensus on which proposals should be recommended for funding. There is no predetermined number of proposals that will be funded. The panel may recommend all, some, or none of the proposals for funding with proper justification. NPD will review each report to analyze the justifications and determine the final list of training programs to recommend to FEMA leadership for approval of funding.

24. When will all the awards be announced?

Awards will be announced by the end of the current fiscal year, September 30, 2014.

25. How will information be shared with applicants between the application and award phases?

During the month of August 2014, FEMA will post an update message on www.grants.gov in the same location as the FY 2014 CTG Funding Opportunity Announcement.

26. Who can I contact if I have questions about the FY 2014 CTG?

For questions, contact the Grant Programs Directorate (GPD). FEMA GPD's Grants Management Division will provide fiscal support, including pre- and post-award administration and technical assistance, to the grant programs included in this funding opportunity announcement. Additional guidance and information can be obtained by contacting the FEMA Call Center at (866) 927-5646 or via e-mail to ASK-GMD@dhs.gov.

National Preparedness Directorate (NPD) / National Training and Education Division (NTED). NPD/NTED has the programmatic responsibility for this FOA and will also maintain the program management function and responsibilities throughout the life-cycle of the awarded grant. Additional guidance and information can be obtained by contacting the NPD/NTED point of contact Mr. Patrick Cowhey at (202) 786-0905 or via e-mail to patrick.cowhey@fema.dhs.gov or Mr. Terry Pruitt at (202) 786-9565 or via email at terry.pruitt@fema.dhs.gov.

Centralized Scheduling and Information Desk (CSID). CSID is a non-emergency comprehensive management and information resource developed by DHS for grants stakeholders. CSID provides general information on all FEMA grant programs and maintains a comprehensive database containing key personnel contact information at the Federal, State and local levels. CSID can be reached by phone at (800) 368-6498 or via e-mail to ASKCsid@fema.dhs.gov. The Grants.gov customer support hotline is (800) 518-4726.



Homeland Security

FY 2014 Homeland Security National Training Program (HSNTP) Continuing Training Grants (CTG) Program

Overview

As appropriated by the *Department of Homeland Security Appropriations Act, 2014* (Public Law 113-76); and authorized by the Implementing Recommendations of the 9/11 Commission Act of 2007 (Public Law 110-53) (hereafter “9/11 Act”) and the *Homeland Security Act of 2002* (6 U.S.C. § 101 et seq.); the Fiscal Year (FY) 2014 Homeland Security National Training Program Continuing Training Grants (CTG) program provides funding via cooperative agreements to training partners to develop and deliver training to prepare whole communities to prevent, protect against, mitigate, respond to, and recover from acts of terrorism, and natural, man-made, and technological hazards.

In Fiscal Year 2013, DHS awarded \$7,811,256 through the CTG to enhance the ability of whole communities and responders to prevent, protect against, mitigate, respond to, and recover from potential terrorist acts and other hazards

The FY 2014 CTG plays an important role in the implementation of the National Preparedness System by supporting the building, sustainment, and delivery of core capabilities essential to achieving the National Preparedness Goal of a secure and resilient Nation. FY 2014 CTG focus areas support Presidential, Legislative, and Departmental priorities for improving security and resilience.

Funding

For FY 2014, the total amount of HSNTP funds available under the CTG program is \$11,000,000, to be used for training in the following focus areas:

- Hazardous Materials (HazMat)/Weapons of Mass Destruction (WMD)
 - Cybersecurity
 - Countering Violent Extremism (CVE)
 - Maturing the Role of Private-Public Partnerships
 - Medical Readiness/Immediate Victim Care
 - Rural Training
-

Eligibility

The FY 2014 CTG is an open and competitive funding opportunity, available to entities with existing programs or demonstrable expertise relevant to the focus areas in the funding opportunity announcement to include: State, local, tribal, and territorial entities, nonprofit national associations

and organizations; non-profit higher education institutions; and non-profits, including community and faith-based organizations. Multi-State/multi-jurisdictional applicants are strongly encouraged to apply.

Funding Guidelines

DHS grant funds may only be used for the purpose set forth in the grant and must be consistent with the statutory authority for the award. Grant funds may not be used for matching funds for other Federal grants/cooperative agreements, lobbying, or intervention in Federal regulatory or adjudicatory proceedings. In addition, Federal funds may not be used to sue the Federal government or any other government entity.

Federal employees are prohibited from serving in any capacity (paid or unpaid) on any proposal submitted under this program. Federal employees may not receive funds under this award.

Key Changes

The FY 2013 FOA contained the following focus areas:

- Hazardous Materials/Weapons of Mass Destruction
- Cybersecurity
- Rural Training
- Medical Readiness/Immediate Victim Care at Mass Casualty Events
- Countering Violent Extremism
- Emergency Management Leadership

The FY 2014 FOA contains the following focus areas:

- Hazardous Materials/Weapons of Mass Destruction
- Cybersecurity
- Rural Training
- Medical Readiness/Immediate Victim Care at Mass Casualty Events
- Countering Violent Extremism
- Maturing the Role of Public-Private Partnerships

The key change between FY 2013 and FY 2014 is the addition of *Maturing the Role of Public-Private Partnerships* and moving *Emergency Management Leadership* off the 2014 CTG focus area list. Emergency Management Leadership was determined to be a relative priority but analysis concluded that T&E requirements for this focus area are satisfied through other FEMA training programs at the Naval Postgraduate School Center for Homeland Defense and Security and through FEMA's Emergency Management Institute.

The key changes regarding the topic of *Rural Training* are as follows:

In FY 2013 rural training topics included:

- Isolation and Quarantine
- Environmental Health

The FY 2014 rural training topics include:

- Hazardous Materials
 - Mass Fatality Planning and Response
 - Crisis Management for School Based Incidents
 - Development of Emergency Operations Plans
 - Bioterrorism Awareness
 - Media Engagement Strategies for First Responders
-

Application Process and Evaluation Criteria

Applicants are restricted to one application per focus area but may apply for more than one focus area. Applications are evaluated in the following three areas:

Eligibility check: Applications will be evaluated based on the Eligibility Criteria in the FOA. Applicants that do not meet eligibility requirements will be removed from consideration.

Subject Matter Expert (SME) Review and Scoring: Applications will be scored by SMEs from Federal, State, Local, Tribal, and Territorial sectors using requirements contained in the FOA. Results of this process will be used to inform a Federal Review.

Federal Review. Federal program offices with responsibility for each focus areas, along with FEMA, will review, evaluate, and score all applications.

Complete applications must clearly demonstrate the applicant's ability to design, develop, and deliver training programs of national scope which provides tailored, specialized training to whole communities with appropriate emphasis on first responders where suitable. The CTG funds must enhance the nation's capability to prevent, protect against, mitigate, respond to, or recover from risks posed by incidents of national significance, including acts of terrorism and/or catastrophic events in accordance with program guidelines, and guidance from DHS/FEMA.

HSNTP CTG Resources

There are a variety of resources available to address programmatic, technical, and financial questions which can assist with CTG.

- The FY 2014 CTG FOA is located online at: <http://www.fema.gov/grants> as well as on <http://www.grants.gov>. CFDA 97.005
- For additional program-specific information, please contact the Centralized Scheduling and Information Desk (CSID) help line at (800) 368-6498 or AskCSID@dhs.gov. CSID hours of operation are from 9:00 a.m. to 5:30 p.m. EST, Monday through Friday.
- For financial-related questions, including pre-and post-award administration and technical assistance, applicants may contact the FEMA Grant Programs Directorate Call Center at (866) 927-5646 or via e-mail to ASK-GMD@dhs.gov.

**The Department of Homeland Security
Funding Opportunity Announcement**

OVERVIEW INFORMATION

Issued By

U.S. Department of Homeland Security (DHS): Federal Emergency Management Agency (FEMA), National Preparedness Directorate, National Training and Education Division

Catalog of Federal Domestic Assistance Number

97.005

CFDA Title

State and Local Homeland Security National Training Program

Funding Opportunity Announcement Title

FY 2014 Continuing Training Grants (CTG)

Authorizing Authority for Program

The Department of Homeland Security Appropriations Act, 2014 (Pub. L. 113-76)

Appropriation Authority for Program

The Department of Homeland Security Appropriations Act, 2014 (Pub. L.113-76)

FOA Number

DHS-XX-XXX-XXX-XXX-XX

Key Dates and Time

| | |
|---------------------------------------|------------------------|
| Application Start Date: | 6/16/14 |
| Application Submission Deadline Date: | 7/16/14 at 11:59:59 ET |
| Anticipated Funding Selection Date: | 8/15/14 |
| Anticipated Award Date: | 8/29/14 |

Other Key Dates

Not Applicable

Intergovernmental Review

Pursuant to Executive Order 12372, an intergovernmental review may be required by applicable State law or regulation. Applicants must contact their state's Single Point of Contact (SPOC) to find out about and comply with the state's process under Executive Order 12372. Name and addresses of the SPOCs are maintained at the Office of Management and Budget's home page at http://www.whitehouse.gov/omb/grants_spsc to ensure currency.

FOA EXECUTIVE SUMMARY

Program Type

Select the applicable program type: New Continuation One-time

Date of origin for Program:
2002

Funding Opportunity Category

Select the applicable opportunity category:

- Discretionary Mandatory
 Competitive Non-competitive
 Sole Source

Application Process

DHS makes all funding opportunities available through the common electronic “storefront” grants.gov, accessible on the Internet at <http://www.grants.gov>. If you experience difficulties accessing information or have any questions please call the grants.gov customer support hotline at (800) 518-4726.

Application forms and instructions are available at Grants.gov. To access these materials, go to <http://www.grants.gov>, select “Apply for Grants,” and then select “Download Application Package.” Enter the CFDA and/or the funding opportunity number located on the cover of this announcement. Select “Download Application Package,” and then follow the prompts to download the application package. To download the instructions, go to “Download Application Package” and select “Instructions.”

Eligible Applicants

The FY 2014 CTG is available to entities with existing programs or demonstrable expertise relevant to the focus areas herein to include; state, local, tribal, and territorial entities, nonprofit national associations and organizations; non-profit higher education institutions; and non-profits, including community and faith-based organizations.

Type of Funding Instrument

Select the applicable funding instrument: Cooperative Agreement Grant

Program authority and responsibility under this cooperative agreement resides with FEMA. Accordingly, FEMA will be substantially involved in the activities of the recipient beyond the level involved with typical award administration activities.

Specifically, FEMA will work with the recipient to review and refine work plans to ensure program goals and objectives can be effectively accomplished. The recipient shall not develop or engage in the development of tasks not approved in recipient's application without post-award approval from the program office, and the issuance of a Grant Amendment from FEMA.

In addition, FEMA will monitor the project on a continual basis by maintaining ongoing contact with the recipient and will provide input to the program's direction, in consultation with the recipient, as needed.

Cost Share or Match

There is no Cost Match or Cost Share requirement for this program.

Maintenance of Effort

Is there a Maintenance of Effort (MOE) requirement? Yes No

Management and Administration

Management and Administration (M&A) activities are those directly relating to the administration of the award, such as financial management and monitoring. Grantees may use up to 5% of the amount of the award for their M&A.

Indirect Cost

Indirect costs are allowable only if the applicant has an approved indirect cost rate agreement with the cognizant Federal agency. A copy of the approved rate (a fully executed, agreement negotiated with the applicant's cognizant Federal agency) is required at the time of application. Indirect costs will be evaluated as part of the application for Federal funds to determine if allowable and reasonable.

Specifically, grantees should apply the training indirect cost rate (when it is available) or the "offsite" indirect cost rate (when a training rate is not available). The full organized research negotiated rate should not be applied to these training awards. Written exceptions will be made in rare cases upon request and with adequate justification. FEMA will work closely with the grantee to determine the appropriateness of indirect costs for the type of activity and location proposed in the application, in accordance with the negotiated indirect cost rates approved by the grantee's cognizant Federal agency.

FULL ANNOUNCEMENT

I. Funding Opportunity Description

Program Overview and Priorities

The Continuing Training Grant (CTG) program develops and delivers innovative training programs that are national in scope and have an important role in the implementation of the National Preparedness System by supporting the building, sustainment, and delivery of core capabilities essential to achieving the National Preparedness Goal (NPG) of a secure and resilient Nation (<http://www.fema.gov/national-preparedness-goal>).

Delivering core capabilities requires the combined effort of the whole community, rather than the exclusive effort of any single organization or level of government. The FY 2014 CTG program supports efforts to build and sustain core capabilities across the Prevention, Protection, Mitigation, Response, and Recovery mission areas.

Program Objectives

The objectives of the CTG program in FY 2014 are for the development and delivery of training in the following focus areas:

- Hazardous Materials (HazMat)/Weapons of Mass Destruction (WMD)
- Cybersecurity
- Countering Violent Extremism (CVE)
- Maturing Public-Private Partnerships
- Medical Readiness/Immediate Victim Care at Mass Casualty Events
- Rural Training

Focus Area 1:

Hazardous Materials (HazMat)/Weapons of Mass Destruction (WMD)

FEMA's HazMat/WMD training programs are designed to complement the programs within the state, local, tribal, territorial, and private sectors, while maximizing training resources and facilities owned by FEMA or operated by FEMA's partners, resulting in increased national preparedness. FEMA-certified HazMat/WMD programs maximize the use of world-class training facilities capable of recreating simulated tanker car incidents; detection, monitoring and sampling of toxic chemical agents, biological materials, radiation sources, and explosive materials; medical treatment and patient management in a fully operational hospital; and functional emergency operations centers supported by state-of-the-art simulations and robust communications platforms. These institutions include faculty from the emergency response community that serve as nationally recognized subject-matter experts who hail from the community of practice at the state, local, tribal, and territorial levels of government.

Training developed in the HazMat/WMD focus area should bring together members of the response community within various jurisdictions for training that uses the resources

and protocols required to respond to HazMat/WMD incidents—incidents that are complex in nature as they require members of multiple agencies and disciplines to work together to control threats to responders, the public, infrastructure (e.g., transportation, public works and communication systems), property, and the environment.

Training should be tailored to address the hazards facing responders, agencies, and jurisdictions during a complex HazMat/WMD incident or attack. Training recipients should include career and volunteer firefighters, emergency medical technicians, law enforcement, specialized emergency response teams (e.g., hazardous materials, search and rescue, and explosive ordnance disposal), emergency managers, skilled support personnel (e.g., public works, private industry, and health departments), and private sector organizations. Training should be appropriate for volunteer emergency responders with an understanding of the challenges faced by volunteer forces.

Training should be national in scope, while distinct from other, national training programs. Multi-jurisdictional training may be conducted at local fire academies or other training facilities, and should include the core capabilities of interdiction and disruption, on-scene security and protection, operational communications, and operational coordination.

Applicants should consider the following training objectives:

- Support Executive Order 13650: Improving Chemical Facility Safety and Security. <http://www.whitehouse.gov/the-press-office/2013/08/01/executive-order-improving-chemical-facility-safety-and-security>;
- Achieve compliance with current competencies identified in the National Fire Protection Association (NFPA) 472 Standard for Competence of Responders to Hazardous Materials/Weapons of Mass Destruction Incidents;
- Deliver training which addresses planning, response, mitigation strategies and actions for transportation incidents. Training on this topic should cover, at a minimum, combustible and flammable petroleum hazards and response;
- Increase knowledge, skills, and abilities to achieve the core capabilities of interdiction and disruption, on-scene security and protection, operational communications, and operational coordination to enhance a jurisdiction's capability to prepare for, mitigate, and respond to hazardous materials and weapons of mass destruction (WMD) complex incidents through awareness of other first responders' roles and responsibilities and practical applications;
- Address preparedness and response capability for acts of terrorism; and
- Create curriculum which utilizes standardized terminology to describe concepts and actions, and comply with the National Incident Management System.

Focus Area 2:

Cybersecurity

Our Nation's increasing reliance on computer networks and information systems has made cybersecurity a national priority. Cyber incidents have increased in number and

complexity and the ability to manage the risks and consequences associated with these incidents must keep pace, especially where there is the potential for physical impact and cascading consequences. Cybersecurity supports Executive Order 13636, Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive 21, Critical Infrastructure Security and Resilience. Training in this Focus Area will support mitigation of the cyber threat to critical infrastructure, and will help to achieve improvement goals described in the 2013 National Preparedness Report. (<http://www.fema.gov/national-preparedness-report>). The 2013 State Preparedness Report indicates that cybersecurity is the lowest-rated core capability.

In February 2014, the National Institute of Standards and Technology released the Framework for Improving Critical Infrastructure Cybersecurity, (<http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>) providing voluntary guidelines based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure. The Framework suggests that organizations categorize and assess all activities related to cybersecurity into five basic functions: identification, protection, detection, response, and recovery. The Framework can be used to identify and prioritize actions for reducing cybersecurity risk, and is a tool for aligning policy, business, and technological approaches to managing that risk. As directed by Executive Order (EO) 13636, the Department of Homeland Security (DHS) is partnering with the critical infrastructure community to establish a voluntary program to support increased security and resilience of the Nation's cyber infrastructure, through use of the Framework. The Critical Infrastructure Cyber Community (C3) Voluntary Program will be the coordination point within the federal government for critical infrastructure owners and operators interested in improving their cyber risk management processes.

In 2011, the Department of Homeland Security, in coordination with the Multi-State Information Sharing and Analysis Center and the National Association of State Chief Information Officers, developed the Nationwide Cyber Security Review (NCSR). The NCSR was developed to identify the level of maturity and risk awareness of State and local government information security programs. Among other things, the results showed that state and local governments are at substantial risk because of the growing number of cyber threats.

The NCSR revealed that cybersecurity training should be a top priority and that participants should be prepared to identify, prevent, protect against, respond to, and recover from cyber incidents at the state and local levels. Another finding was that training programs in this focus area should be directed to network managers and operators tasked with the creation and maintenance of computer and information systems.

The training should include goals and objectives that meet criteria to include, but not limited to, the following:

- Cybersecurity Policy – Training to develop and refine policies, plans, and procedures, which are related but serve distinctly different purposes. A policy is the highest level document that states what a company, group, or department will

and will not do during a cyber emergency. A plan is the organizational document that describes a methodology for how to achieve the policy's goals. A procedure is the step-by-step instructions to the operator for exactly how a task is to be done. All are essential to a comprehensive approach to cybersecurity.

- **Cybersecurity Awareness and Training** – The most vulnerable aspect of a system is the human component. Users who have been granted access to a system need to be instructed in how to keep that access information confidential. Along with access credentials, users possess other knowledge of an organization that can be valuable to someone with malicious intent. In addition to logical controls, physical controls, a comprehensive company policy, and other important security measures, training should be performed regularly in order to maximize the effectiveness of existing security measures and to reduce the risk of social engineering. Security training and reinforcement of that training through ongoing awareness information sessions has been shown to lower the risks associated with the human component of a security strategy.
- **Monitoring and Incident Response** – In the event of an emergency that involves a system failure, a detected or active intrusion, detection or suspected involvement of malware, or Advanced Persistent Threat (APT) action, having an established protocol and response team is critical to timely incident mitigation and response to limit the extent and degree of the damage. Monitoring and incident response address the need for a proactive approach to system incidents. Rather than waiting for incidents to occur and attempting to shape a response when time and resources are not at optimal levels, preparation ahead of time to include continuous monitoring and information sharing, and maintenance of situational awareness can greatly reduce the damage, as well as the time needed to recover from an adverse event. Recognizing security events for what they are and making management aware of the incidents and their potential for harm is a critical element, not only to limit the damage from cyber attacks, but also to obtain the appropriate support and resources to effectively manage cybersecurity.
- **Disaster Recovery and Business Continuity** – Information Technology (IT) systems are known to be vulnerable to a variety of adverse events, any of which has the potential to impact normal business operations and compromise the confidentiality, integrity, and availability of data. Although planning and mitigation strategies are known to reduce the risks posed by these events, it is impossible to fully eliminate the risks, and the potential damage posed by them. Because of this, due care should be taken to plan what steps an organization will take in the event of a system disruption, no matter the size. By making and testing effective plans ahead of time, the potential damage and loss of productivity, revenue, and sensitive information can be greatly reduced.
- **Risk (and Vulnerability) Management** – Cyber risk methodologies usually include various processes to identify and measure risk to a system or group of systems and provide a repeatable method for conducting and monitoring risk. Most common to all methodologies are processes for conducting risk assessments performing system testing including observation, data analysis, and electronic testing (e.g., vulnerability scanning, penetration testing); and tracking and monitoring system weaknesses and mitigation activities (e.g., Plan of Action).

The risk identification methodology should be standardized and approved by senior management to ensure results are consistent with one another and throughout the organization.

Finally, the NCSR stipulated that training programs should be developed with enough flexibility so they can apply to results from the Threat and Hazard Identification and Risk Assessment (THIRA) and be implemented at the state and local levels to manage risk, including identification of mitigation opportunities and other supporting preparedness activities.

The target audience for this training is information technology professionals responsible for creating and maintaining computer networks and information systems for state, local, tribal, and territorial emergency responders, along with government managers administering these systems and jurisdictions, and law enforcement investigators of cyber crimes. This focus area is aligned with the cybersecurity core capability within the Protection Mission Area as described in the National Preparedness Goal, September 2011.

Focus Area 3:

Countering Violent Extremism (CVE)

According to the White House Strategic Implementation Plan (SIP) For Empowering Local Partners to Prevent Violent Extremism in the United States, “Protecting our Nation’s communities from violent extremist recruitment and radicalization is a top national security priority. It is an effort that requires creativity, diligence, and commitment to our fundamental rights and principles.”

CVE is vital to the public safety and to homeland security. The SIP identifies the Federal Government’s focus 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 our ideals.

In addition, the Department of Homeland Security (DHS) has laid out three broad objectives concerning its CVE efforts:

- Support and coordinate efforts to better understand the phenomenon of violent extremism, including assessing the threat it poses to the Nation as a whole and within specific communities;
- Bolster efforts to innovate and support non-governmental, community-based programs, and strengthen relationships with communities that may be targeted for recruitment by violent extremists; and
- Disrupt and deter recruitment or individual mobilization through support for local law enforcement programs, including information-driven, community-oriented policing efforts that for decades have proven effective in preventing violent crime.

Based on focus group studies with state, local, and tribal law enforcement officers at fusion centers and in surrounding communities, DHS has identified a need to develop

additional training for state, local, and tribal law enforcement relevant to CVE. The primary training audience for this focus area is the Nation's more than 800,000 state, local, territorial, and tribal law enforcement officers and fusion center analysts, who work to protect communities from a range of threats including, but not limited to, violent extremism.

The award recipient will coordinate with the DHS/FEMA leadership, program staff, and operational staff to prioritize the emerging training requirements related to identifying and countering violent extremism. The applicant is expected to use a combination of readily available resources and their working knowledge of the subject matter to refine the focus area and to shape the overall training program in keeping with current national policies, doctrines, and priorities, to include the CVE Training Guidance and Best Practices, published by the DHS Office of Civil Rights and Civil Liberties, that can be found at <http://www.dhs.gov/xlibrary/assets/cve-training-guidance.pdf>

The protection of individuals' privacy, civil liberties, and civil rights is paramount within CVE training materials. As noted in the White House National Strategy, "protecting our fundamental rights and liberties is an important end in itself, and also helps counter violent extremism by ensuring nonviolent means for addressing policy concerns; safeguarding equal and fair treatment; and making it more difficult for violent extremists to divide our communities."

CVE Training should:

- Raise awareness and understanding of violent extremism based on analysis and research, case studies on behaviors and indicators associated with violent extremists, and radicalization to violence;
- Counter the "us-versus-them" mentality propagated by terrorist organizations and others, including using a more inclusive method of outreach and trust-building between law enforcement and community partners;
- Increasing cultural competency and identifying the difference between constitutionally protected, cultural, and religious behavior versus indicators of criminal behavior or radicalization to violence;
- Promote and support best practices in community-oriented policing, and community engagement, in order to strengthen partnerships between communities and the Government and promote information-driven, community-based solutions to prevent violent extremism and build community resilience. As an example, training efforts improving the internal community support derived from its network of families and friends in order to improve resistance to the emergence of radicalized violent extremism efforts or in countering the effects of radicalization to violence within individuals. These programs also serve to change perceptions of mistrust for external community partners, such as law enforcement and other agencies; and

All resources developed, to include training, support materials, and/or outreach guides, will be added to the respective CVE-AS Web Portal site through the CVE-AS Program Manager to further awareness and enhance existing information and outreach networks. In addition, the CVE training may address gaps identified through additional research and

analysis and must be guided by the five priority areas as identified in the Strategic Implementation Plan (SIP) For Empowering Local Partners to Prevent Violent Extremism in the United States, to include:

- The role of the Internet in radicalization to violence and how virtual space can help counter violent extremism;
- Single-actor terrorism (so called “lone wolves”), including lessons learned from similar phenomena, such as active shooters;
- Counter radicalization and disengagement from terrorism and violent extremism;
- Non-al-Qa’ida related radicalization to violence and anticipated future violent extremist threats; and
- Pre-operational indicators and analysis of known case studies of extremist violence in the United States.

The applicant should ensure that the training aligns with the Federal approach to CVE, including prioritizing civil rights and civil liberties and building partnerships with communities. (See the White House Approach to Countering Violent Extremism. http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf.)

Further, the applicant must address community engagement to ensure that those communities that may be targeted by violent extremists or recruitment by violent extremists are aware of these efforts. This should follow two tracks:

- Community and faith-based engagement related to the threat of violent extremism to raise awareness, build broad partnerships, and promote empowerment; and,
- Community and faith-based engagement to promote the sharing of information, and participation in multi-disciplinary prevention efforts.

Focus Area 4:

Maturing Public-Private Partnerships

FEMA believes that every community benefits from public-private collaboration in emergency management. This philosophy is central to everything we do. We are better able to serve our neighbors, fellow citizens, and our nation's disaster survivors in particular, when public sector and private sector representatives are both active members of the same team. FEMA believes in the value of public-private partnerships and has worked steadily to provide tools, models, and resources designed to inspire their creation and nurture their success.

Through public-private partnerships both government and the private sector can:

- Enhance situational awareness
- Improve decision making
- Access more resources
- Expand reach and access for communication efforts
- Improve coordination with other efforts by segments of the private sector
- Increase the effectiveness of emergency management efforts
- Maintain strong relationships, built on mutual understanding

- Create more resilient communities

Public and private sector partnerships, used during joint planning, response, and recovery efforts can yield benefits for the whole community. One of the major benefits of this partnership is that it allows each partner (public and private) to focus on gaps which the other does not address and aids in the coordination of mutual support. By doing this, the private sector benefits from minimal business interruption and the government benefits by using its resources more effectively. Working together, the public and private sectors can ensure effective prevention, protection, mitigation, response, and recovery.

As disaster relief operations become more complex, there is also an increasing need for societies to become resilient in the face of disasters. And while in recent years there has been excellent progress toward this objective, we remain a far stretch from fully achieving societal resilience. But public-private partnerships, if properly defined, implemented, and regulated, adapt disaster management practices to the increasing complexity of today's large-scale emergencies. In this way, public-private partnerships bolster societal resilience. Training in this focus area should address and support the following goals for public-private partnerships:

- Provide lessons learned and training tools for building strong public-private partnerships that can strengthen state, local, tribal and territorial Emergency Operation Centers (EOC);
- Promote collaboration, coordination, and communication efforts between government and private sector partners to create more resilient communities and increase jurisdictional capacity to prevent, protect against, respond to, and recover from major incidents;
- Increase the effectiveness of emergency management and homeland security efforts in the public and private sectors by increasing all partners' understanding of each other's capabilities and preparedness efforts;
- Navigate the legal structures involved in establishing non-contractual relationships with the private sector;
- Build strong teams (pre-incident) based on mutual understanding that result in faster, more effective response and recovery efforts;
- Share situational awareness during disasters, such as through structured situation reports between a public and private emergency operations centers, or through social media exchanges, as an example. The private sector, too, relies on timely information from the government to make sound business decisions related to operations, customer and employee safety, and supporting communications; and
- Leverage public and private sector communication channels to expand reach and access to timely, vital information.

The audience for this training should include personnel from Federal departments and agencies, including Sector-Specific Agencies (SSAs); state, local, tribal, and territorial (SLTT) governments who have a likelihood (based on position and assigned duties) of collaborating on public-private partnership efforts.

Focus Area 5:

Medical Readiness/Immediate Victim Care at Mass Casualty Events

The immediate impacts of mass casualty events upon victims and the whole community demand a prepared force of professionals, trained to effectively respond and act to save lives, mitigate suffering, and prevent further injury, illness, or death. Responders in the law enforcement, fire, and EMS communities are the primary targets for this focus area. Training developed should include the following elements:

- Mass casualty planning, training, and exercises oriented specifically with law enforcement, fire, and EMS providers to rapidly deploy in a coordinated effort into areas that have been cleared, but not secured, in order to initiate treatment at or near the point of injury and effect rescue of survivors.
- Develop and exercise plans, which ensure the health and safety of first responders and citizen responders; and training focused on the prevention and detection of secondary attacks.
- Enhancing coordination between law enforcement, fire, first responder agencies, EMS systems, local healthcare delivery and trauma systems that provide victim triage, treatment, and transport to ensure patients are distributed to appropriate levels of definitive emergency care.
- Establishing protocols that incorporate the guidelines on the medical principles of Tactical Emergency Casualty Care and conduct training for responders.
- Empowering community members through public education and training, such as Community Emergency Response Teams (CERTs), about life sustaining actions, including aggressive hemorrhage control measures for severe bleeding and use of tourniquets to support survivors and providers in a mass casualty event.

Applicants are strongly encouraged to utilize existing relationships with law enforcement, fire, and EMS agencies at the local, State, private, and Federal levels to emphasize collaboration strategies that substantially reduce and mitigate the impact of mass casualty events.

Focus Area 6:

Rural Training

Ensuring that emergency responders in small, rural, and remote communities are properly trained to deal with all-hazards events is essential. Competition in this focus area is restricted to applicants that have demonstrable experience and expertise in rural training

as well as in developing and delivering FEMA-certified courses to rural communities across the Nation.

Funding is available for the development and delivery of training in the following topics:

- Hazardous Materials (HazMat) – This topic includes training in the areas of HazMat planning and response at plants and fixed sites, HazMat transportation incident response, HazMat pipeline incident response, and HazMat port (waterways) incident response for rural first responders. Training should be appropriate to accommodate volunteer emergency responders with an understanding of the challenges faced by volunteer forces. Training should support Executive Order 13650: Improving Chemical Safety and Security. <http://www.whitehouse.gov/the-press-office/2013/08/01/executive-order-improving-chemical-facility-safety-and-security>. Training should address compliance with current competencies identified in the National Fire Protection Association (NFPA) 472 Standard for Competence of Responders to Hazardous Materials/Weapons of Mass Destruction Incidents; and address planning, response, and mitigation strategies and actions for transportation incidents. Training for transportation incidents should cover, at a minimum, combustible and flammable petroleum hazards and response.
- Mass Fatality Planning and Response– This topic includes training in the areas of planning and response for rural emergency managers and first responders, and courses for rural morticians and funeral directors.
- Crisis Management for School Based Incidents– This topic includes training on all significant school-based incidents to include bomb threats, active shooter, severe weather, structural/mechanical failures, student demonstrations, and HazMat releases. Training should be targeted for rural law enforcement officials, fire and EMS professionals/volunteers, and school system administrators and staff.
- Development of Emergency Operations Plans (EOP) – This topic includes training on plan development and testing of EOPs in rural jurisdictions. Training should target rural emergency managers, incident commanders, Emergency Operations Center (EOC) staffs and any personnel or agencies serving or supporting an Incident Command System (ICS) structure.
- Bioterrorism Awareness– This topic includes training in the areas of biological threats and the adverse effects of biological contamination; this training should also focus on agro-terrorism and food system disasters. Training should target emergency managers, law enforcement, fire, and EMS professionals/volunteers, hospital providers and staff, agriculture community professionals and associations, and other appropriate emergency planners and responders in rural communities.
- Media Engagement Strategies for First Responders–Training in this topic should focus on dealing with the media in a variety of disaster situations. Training should target rural government officials, emergency managers, public information

officers, incident commanders, and others as appropriate within rural communities.

Other Training Requirements

Use Existing Training Mechanisms

CTG-developed training must not duplicate training provided by Federal, state, local, tribal, or territorial agencies. Additionally, application and use of existing standards and media (e.g. on-line, computer based) is recommended to ensure that training delivery adapts to meet evolving needs of students.

Link Training and Exercises to Align Resources

Linking training and exercises is imperative for ensuring that course participants are adequately trained to perform the tasks of each exercise and in real life events. Training must be linked to relevant core capabilities.

Incorporate the National Incident Management System

The National Incident Management System (NIMS) (http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf) identifies concepts and principles that answer how to manage emergencies from preparedness to recovery regardless of their cause, size, location or complexity. NIMS provides a consistent, nationwide approach and vocabulary for multiple agencies or jurisdictions to work together to build, sustain and deliver the core capabilities needed to achieve a secure and resilient Nation. Training programs must be consistent with NIMS in order to provide a solid foundation across jurisdictions and disciplines to ensure effective and integrated preparedness, planning and response.

National Preparedness System

The National Preparedness System is the instrument the Nation will employ to build, sustain, and improve core capabilities in order to achieve the National Preparedness Goal (Goal) of a secure and resilient Nation. The objective of the National Preparedness System is to facilitate an integrated, all-of-Nation, risk informed, capabilities-based approach to preparedness. The guidance, programs, processes, and systems that support each component of the National Preparedness System enable a collaborative, whole community approach to national preparedness that engages individuals, families, communities, private and nonprofit sectors, faith-based organizations, and all levels of government (<http://www.fema.gov/whole-community>).

National preparedness is a shared responsibility of the whole community. Every member must be given the opportunity to contribute. To that end, the National Preparedness Goal defines success as a secure and resilient Nation with the capabilities required by the whole community – including individuals and citizens – to prevent, protect against, mitigate, respond to, and recover from disasters.

FY 2014 CTG plays an important role in the implementation of the National Preparedness System by supporting the building, sustainment, and delivery of core

capabilities. Core capabilities are essential for the execution of critical tasks for each of the five mission areas outlined in the Goal. Delivering core capabilities requires the combined effort of the whole community, rather than the exclusive effort of any single organization or level of government. CTG supports all core capabilities in the Prevention, Protection, Mitigation, Response, and Recovery mission areas based on the focus areas of each award and their allowable costs.

The highest priority of CTG is to build and sustain the core capabilities identified in the Goal. Particular emphasis will be placed on capabilities that address the greatest risks to the security and resilience of the United States, and the greatest risks along the Nation's borders. Funding will support training that can be utilized anywhere in the Nation.

The FY 2014 CTG supports core capabilities in the five mission areas:

- Prevention. Prevent, avoid or stop an imminent, threatened or actual act of terrorism.
- Protection. Protect our citizens, residents, visitors, and assets against the greatest threats and hazards in a manner that allows our interests, aspirations, and way of life to thrive.
- Mitigation. Reduce the loss of life and property by lessening the impact of future disasters.
- Response. Respond quickly to save lives, protect property and the environment, and meet basic human needs in the aftermath of a catastrophic incident.
- Recovery. Recover through a focus on the timely restoration, strengthening and revitalization of infrastructure, housing and a sustainable economy, as well as the health, social, cultural, historic and environmental fabric of communities affected by a catastrophic incident.

The core capabilities contained in the Goal are highly interdependent and require the use of existing preparedness networks and activities to improve training and exercise programs, promote innovation, and ensure that the appropriate administrative, finance, and logistics systems are in place and functioning.

Use an Adult Learning Approach

Training programs that support the Nation's preparedness efforts have long relied on classroom instruction and practical exercises; however, CTG training programs must be innovative and distinct in comparison to current training offered by other Federal, State, and local training academies. To ensure that CTG training courses are accessible to as many key public and private officials with homeland security responsibilities throughout the Nation as possible, training partners must leverage technology, when appropriate, to reduce student travel and maximize learning outcomes. The adult learning approach encourages traditional classroom instruction with creative uses of interactive web-based and computer-based training, simulations, toolkits, job aids, and/or other leave behind materials.

Training Should Be National in Scope

Delivery of training programs will incorporate geographic diversity when offering courses, including providing training at the State, local, tribal, and territorial levels. All applicants will be evaluated on their ability to develop and deliver training programs to participants on a national level. Applicants should describe their course delivery methods and demonstrate their ability to reach a national audience, such as instructor led mobile deliveries, resident, or on-line training.

Whole Community Approach to Emergency Management

A community-centric approach for emergency management that focuses on strengthening and leveraging what works well in communities on a daily basis offers an effective path to building societal security and resilience. By focusing on core elements of successful, connected, and committed communities, emergency management can collectively achieve better outcomes in times of crisis, while enhancing the resilience of our communities and the Nation. The three core principles of whole community—understanding and meeting the actual needs of the whole community, engaging and empowering all parts of the community, and strengthening what works well in communities on a daily basis—provide a foundation for pursuing a whole community approach to emergency management through which security and resiliency can be attained.

Truly enhancing our Nation’s resilience to all threats and hazards will require the emergency management community to transform the way the emergency management team thinks about, plans for, and responds to incidents in such a way to support community resilience. It takes all aspects of a community to effectively prevent, protect against, mitigate, respond to, and recover from threats and hazards. It is critical that individuals take responsibility for their own self-preparedness efforts and that community members work together to develop the collective capacity needed to enhance their community’s security and resilience.

Building community resilience in this manner requires emergency management practitioners to effectively engage with and holistically plan for the needs of the whole community. This includes but is not limited to accommodating people who speak languages other than English, those from diverse cultures or economic backgrounds, people of all ages (i.e., from children and youth to seniors), people with disabilities and others with access and functional needs, and populations traditionally underrepresented in civic governance. At the same time, it is important to realign emergency management practices to support local needs and work to strengthen the institutions, assets, and networks that work well in communities on a daily basis. (Ref: A Whole Community Approach to Emergency Management: Principles, Themes, and Pathways for Action, December 2011).

II. Funding Information

Award Amounts, Important Dates, and Extensions

Available Funding for the FOA: \$11,000,000
Projected number of Awards: 8
Projected Award Start Date(s): 10/1/14
Projected Award End Date(s): 9/30/17
Period of Performance: 36 Months

Period of Performance

Is an extension to the period of performance permitted? Yes No

No-cost extensions to the Period of Performance for this program are allowed on a case-by-case basis. Only no-cost extensions to the initial period of performance identified in the award will be considered only through formal, written requests to FEMA/National Training and Education Division (NTED) and must contain specific and compelling justifications as to why an extension is required. Grantees are advised to coordinate with NTED as needed, when preparing an extension. All extension requests must address the following:

1. Grant Program, Fiscal Year, and award number;
2. Reason for delay – this must include details of the legal, policy, or operational challenges being experienced that prevent the final outlay of awarded funds by the applicable deadline;
3. Current status of the activity/activities;
4. Approved period of performance termination date and new project completion date;
5. Amount of funds drawn down to date;
6. Remaining available funds, both Federal and non-Federal;
7. Budget outlining how remaining Federal and non-Federal funds will be expended;
8. Plan for completion including milestones and timeframes for achieving each milestone and the position/person responsible for implementing the plan for completion; and
9. Certification that the activity/activities will be completed within the extended period of performance without any modification to the original Statement of Work approved by FEMA.

Extension requests will not exceed 12 months.

III. Eligibility Information

Eligibility Criteria

The FY 2014 CTG is a competitive program, which is available to entities with existing training programs or demonstrable expertise relevant to the focus areas in the funding opportunity announcement to include; State, local, tribal, and territorial entities, nonprofit national associations and organizations; non-profit higher education institutions; and non-profits, including community and faith-based organizations. Multi-State/multi-jurisdictional applicants are strongly encouraged to apply.

IV. Funding Restrictions

Restrictions on Use of Award Funds

Federal funds made available through this award may only be used for the purpose set forth in this award and must be consistent with the statutory authority for the award.

Award funds may not be used for matching funds for any other Federal grants/cooperative agreements, lobbying, or intervention in Federal regulatory or adjudicatory proceedings. In addition, federal funds may not be used to sue the federal government or any other government entity.

Construction Costs: Construction costs are not allowable under this funding opportunity announcement.

Equipment: Applicants should analyze the cost benefits of purchasing versus leasing equipment, especially high cost items and those subject to rapid technical advances. Large equipment purchases must be identified and explained. For more information regarding property management standards for equipment, please reference 2 CFR Part 215, located at http://www.whitehouse.gov/omb/fedreg/2004/040511_grants.pdf.

Fringe Benefits: Fringe benefits should be based on actual known costs or an established formula. Fringe benefits on overtime hours are limited to FICA, Workman's Compensation, and Unemployment Compensation.

Foreign Travel: Foreign travel is not an allowable cost under this funding opportunity announcement unless approved otherwise by the managing Federal agency.

i. Other Cost Requirements

Environmental Planning and Historic Preservation (EHP) Compliance

As a Federal agency, FEMA is required to consider the effects of its actions on the environment and/or historic properties to ensure that all activities and programs funded by the agency, including grants-funded projects, comply with Federal EHP regulations, laws and Executive Orders as applicable. Grantees and sub-grantees proposing projects that have the potential to impact the environment, including but not limited to construction of communication towers, modification or renovation of existing buildings, structures and facilities, or new construction including replacement of facilities, must participate in the FEMA EHP review process. The EHP review process involves the submission of a detailed project description that explains the goals and objectives of the proposed project along with supporting documentation so that FEMA may determine whether the proposed project has the potential to impact environmental resources and/or historic properties. In some cases, FEMA is also required to consult with other regulatory agencies and the public in order to complete the review process. The EHP review process must be completed before funds are released to carry out the proposed project.

V. Application Review Information and Selection Process

Applicants are restricted to one application per focus area but may apply for more than one focus area. Applications will be evaluated in the following four areas:

i. Eligibility

Applications will be evaluated based on the Eligibility Criteria in Section II of this FOA. Applicants that do not meet eligibility requirements will be removed from consideration. Multi-State/multi-jurisdictional applicants are strongly encouraged to apply.

ii. Completeness of Application

Complete applications must clearly demonstrate the applicant's ability to design, develop, and deliver a training program of national scope which provides tailored, specialized training to first responders and/or citizens. The CTG funds must enhance the Nation's capability to prevent, protect against, mitigate, respond to, or recover from risks posed by incidents of national significance, including acts of terrorism and/or catastrophic events in accordance with program guidelines, and guidance from DHS/FEMA. See Section X Application Submission Information on the requirements for submitting an application.

iii. Subject Matter Expert (SME) Review

Subject Matter Experts evaluate the following:

- All sections included in the application
- Each application's content for compliance with guidance and technical merit
- The applicant's ability to deliver training that is national in scope, and
- Analyzes relevance to training objectives outlined in focus area descriptions within the funding opportunity announcement

iv. FEMA Review

FEMA Staff then performs the following:

- Adjudicate context to correlate related programs, services, and activities to determine where the greatest opportunity is to magnify the effect of the CTG program
- Judge relevance to priority initiatives such as the White House School Safety Initiative, the Quadrennial Homeland Security Review (QHSR), the NIPP, and the Framework for Improving Critical Infrastructure Cybersecurity
- Assess correlation to the FEMA Administrator's Intent
- Validate history of past performance
- Confirm relevancy to national standards (e.g., NFPA) where applicable
- Certify alignment with Homeland Security Grant Program priorities, and
- Supports Whole Community Approach to Training

The full application will be evaluated and scored for each required criteria element. The elements are listed in each required section.

Application Selection Process

Award recommendations are based on results from the SME and FEMA Review.

VI. Post-Selection and Pre-Award Guidelines

Notice of Award

Notification of award approval is made through the Non Disaster (ND) Grants system through an automatic e-mail to the awardee point of contact (the “authorized official”) listed in the initial application. The date the approval of award is the “award date.” The awardee should follow the directions in the notification to accept the award.

Grantees must accept their awards no later than 90 days from the award date. The grantee shall notify the awarding agency of its intent to accept and proceed with work under the award, or provide a written notice of intent to decline. Funds will remain on hold until the grantee accepts the award through official correspondence (e.g., written, electronic signature, signed letter or fax to the Programs Office) and all other conditions of award have been satisfied, or the award is otherwise rescinded. Failure to accept the grant award within the 90 day timeframe may result in a loss of funds.

Administrative and Federal Financial Requirements

Before accepting the award the authorized official should carefully read the award package for instructions on administering the grant award and the terms and conditions associated with responsibilities under Federal awards. Grantees must accept all conditions in this FOA as well as any Special Terms and Conditions in the Award notice to receive an award under this program.

i. Standard Terms and Conditions

A complete list of Federal Financial Requirements is available at:

http://www.whitehouse.gov/omb/grants_forms. All successful applicants for all DHS grant and cooperative agreements are required to comply with DHS Standard Administrative Terms and Conditions, which are enumerated in the DHS Chief Financial Officer *Financial Management Policy Manual* and are available online at: <http://www.dhs.gov/sites/default/files/publications/Proposed%20FY%2014%20Standard%20TC%202013-12-04.pdf>

ii. Payment

FEMA utilizes the Payment and Reporting System (PARS) for financial reporting, invoicing and tracking payments. Additional information can be obtained at <https://isource.fema.gov/sf269/execute/LogIn?sawContentMessage=true>.

DHS/FEMA uses the Direct Deposit/Electronic Funds Transfer (DD/EFT) method of payment to Recipients. To enroll in the DD/EFT, the Recipient must complete a Standard Form 1199A, Direct Deposit Form.

VII. Program Performance Reporting Requirements

Awardees are required to submit various financial and programmatic reports as a condition of their award acceptance. Future awards and fund drawdowns may be withheld if these reports are delinquent.

i. Financial and Compliance Audit Report:

For audits of fiscal years beginning on or after December 26, 2014, recipients that expend \$750,000 or more from all Federal funding sources during their fiscal year are required to submit an organization-wide financial and compliance audit report. The audit must be performed in accordance with the requirements of GAO’s Government Auditing Standards, located at <http://www.gao.gov/govaud/ybk01.htm>, and the requirements of Subpart F of 2 C.F.R. Part 200, located at <http://www.ecfr.gov/cgi-bin/text-idx?SID=55e12eead565605b4d529d82d276105c&node=2:1.1.2.1.1.6&rgn=div6>.

For audits of fiscal years beginning prior to December 26, 2014, recipients that expend \$500,000 or more from all federal funding sources during their fiscal year are required to submit an organization-wide financial and compliance audit report. The audit must be performed in accordance with GAO’s Government Auditing Standards, located at <http://www.gao.gov/govaud/ybk01.htm>, and OMB Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations, located at http://www.whitehouse.gov/omb/circulars/a133_compliance_supplement_2012. Audit reports are currently due to the Federal Audit Clearinghouse no later than nine months after the end of the recipient’s fiscal year.

ii. Financial and Program Reporting Periods and Due Dates

The following reporting periods and due dates apply:

| Reporting Period | Report Due Date |
|-------------------------|-----------------|
| October 1 – December 31 | January 30 |
| January 1 – March 31 | April 30 |
| April 1 – June 30 | July 30 |
| July 1 – September 30 | October 30 |

iii. Federal Financial Report (FFR)

Obligations and expenditures must be reported on a quarterly basis through the FFR (SF-425) and must be filed electronically using PARS. The SF-425 form is available at http://www.whitehouse.gov/sites/default/files/omb/assets/grants_forms/SF-425.pdf. An FFR report must be submitted for quarterly throughout the period of performance, including partial calendar quarters, as well as for periods where no grant award activity occurs. Future awards and fund drawdowns may be withheld if these reports are delinquent, demonstrate lack of progress, or are insufficient in detail.

iv. Program Performance Reporting Requirements

Performance Progress Report (SF-PPR). Awardees are responsible for providing updated performance reports using the SF-PPR on a semi-annual basis. The SF-PPR

is due within 30 days after the end of the reporting period Grantees must complete the cover page of the SF-PPR and submit it as an attachment to the ND Grants system. The SF-PPR can be accessed online at http://www.na.fs.fed.us/fap/SF-PPR_Cover%20Sheet.pdf.

v. Monitoring

Grant Award recipients will be monitored programmatically and financially on an annual and as needed basis by FEMA staff to ensure that the activities and project goals, objectives, performance requirements, timelines, milestone completion, budgets, and other related program criteria are being met.

Monitoring may be accomplished through either a desk-based review or on-site monitoring visits, or both. Monitoring will involve the review and analysis of the financial, programmatic, performance, compliance and administrative processes, policies, activities, and other attributes of each Federal assistance award and will identify areas where technical assistance, corrective actions and other support may be needed.

vi. Close Out

Within 90 days after the end of the period of performance, or after an amendment has been issued to close out a grant, whichever comes first, grantees must submit a final FFR and final progress report detailing all accomplishments and a qualitative summary of the impact of those accomplishments throughout the period of performance. As part of the final report, grantees must also submit the Tangible Personal Property Report (SF-428), available at http://www.whitehouse.gov/sites/default/files/omb/grants/approved_forms/sf-428.pdf, to provide an inventory of all tangible personal property acquired using CTG funds.

After these reports have been reviewed and approved by FEMA a close-out notice will be completed to close out the grant. The notice will indicate the period of performance as closed, list any remaining funds that will be deobligated, and address the requirement of maintaining the grant records for three years from the date of the final FFR.

The grantee is responsible for returning any funds that have been drawn down, but remain as unliquidated on grantee financial records.

**VIII. DHS – FEMA - Contact Information
Contact and Resource Information**

For Program Questions About Applying for an Award

The Centralized Services Information Desk (CSID) is a non-emergency comprehensive management and information resource developed by DHS for grants stakeholders. CSID provides general information on all FEMA grant programs and maintains a comprehensive database containing key personnel contact information at the Federal, state, and local levels. When necessary, grantees will be directed to a Federal point of contact who can answer specific programmatic questions or concerns. CSID can be

reached by phone at (800) 368-6498 or by e-mail at askcsid@dhs.gov, Monday through Friday, 8:00 a.m. – 5:30 p.m. EST.

For Financial and Administrative Questions About Applying for an Award

GPD’s Grant Operations Division Business Office provides financial support and technical assistance, such as for password resets and registration requests, questions regarding Form 1199A, payment status, amendments, closeouts, and tracking de-obligation and award amounts. Additional guidance and information can be obtained by contacting the FEMA Call Center at (866) 927-5646 or via e-mail to ASK-GMD@dhs.gov.

FEMA National Training and Education Division (NTED)

Contact the National Preparedness Directorate (NPD)/National Training and Education (NTE)/ National Training and Education Division (NTED). NTED has the programmatic responsibility for the CTG program and will also maintain the program management function and responsibilities throughout the life-cycle of the awarded grant. Additional guidance and information can be obtained by contacting the NTED point of contact Mr. Patrick Cowhey at (202) 786-0905 or via e-mail to patrick.cowhey@fema.dhs.gov.

Office of Environmental Planning and Historic Preservation (OEHP)

OEHP provides guidance and information about the EHP review process to FEMA programs and its grantees and sub-grantees. All inquiries and communications about EHP compliance for FEMA grant projects or the EHP review process should be sent to emily.blanton@fema.dhs.gov.

**IX. Other Critical Information
Additional Information**

Not Applicable

**X. How to Apply
Application Instructions**

Applying for an award under this program is a multi-step process and requires time to complete. To ensure that an application is submitted on time applicants are advised to start the required steps well in advance of their submission. **Applicants should allow at least 15 business days (three weeks) to complete the five steps of applying listed below.** Failure of an applicant to comply with any of the required steps before the deadline for submitting their application will automatically disqualify their application from funding.

The steps involved in applying for an award under this program are:

1. Applying for, updating or verifying their DUNS Number
2. Applying for, updating or verifying their EIN Number
3. Updating or verifying their SAM Number
4. Submitting an initial application in grants.gov, and
5. Submitting the complete application in ND Grants

1. Obtain a Dun and Bradstreet Data Universal Numbering System (DUNS) Number

The applicant must provide a DUNS number with their application. This number is a required field for all subsequent steps in the application submission. Applicants should verify they have a DUNS number, or take the steps necessary to obtain one.

Applicants can receive a DUNS number at no cost by calling DUNS number request line at (866) 705-5711. FEMA cannot assist applicants with questions related to obtaining a current DUNS number.

2. Obtain an Employer Identification Number (EIN)

FEMA requires both the EIN and a DUNS number prior to the issuance of a funding award and for grant award payment; both are also required to register with SAM (see below). The EIN base for an organization is the IRS Tax ID number, for individuals it is their social security number, both of which are nine-digit numbers. Organizations and individuals submitting their applications must correctly identify the EIN from the DUNS since both are 9-digit numbers. If these numbers are not correctly identified in the application, this may result in a delay in the issuance of the funding award and/or incorrect payment to a grantee organization.

Organization applicants applying for an EIN should plan on a minimum of 2 full weeks to obtain an EIN.

If you need assistance registering an EIN, please go to [http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Apply-for-an-Employer-Identification-Number-\(EIN\)-Online](http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Apply-for-an-Employer-Identification-Number-(EIN)-Online). FEMA cannot assist applicants with questions related to obtaining a current EIN.

3. Register with the System for Award Management (SAM)

Payments are contingent on the information provided in SAM and must be completed by the applicant at <http://www.sam.gov>. It is imperative that the information provided by the applicant is correct and current. Please ensure that your organization's name, address, DUNS number and EIN are up to date in SAM and that the DUNS number used in SAM is the same one used to apply for all other FEMA awards.

SAM registration is a multi-step process including validating your EIN with the Internal review Service (IRS) to obtain a Commercial and Government Entity (CAGE) code. The CAGE code is only valid for one year after issuance and must be current at the time of application. If you need assistance registering with SAM, please go to <https://www.fsd.gov/> or call 866-606-8220. FEMA cannot assist applicants with questions related to obtaining a current CAGE code.

4. Initial Application Submission in Grants.gov.

All applicants submit their initial application through Grants.gov. Applicants may need to first create a grants.gov user profile by visiting the Get Registered section of the grants.gov website. Successful completion of this step is necessary for FEMA to determine eligibility of the applicant. Applicants should complete this step at <http://www.grants.gov>. The initial on-line application in grants.gov requires completing

- Standard Form 424 (SF424), Application for Federal Assistance, and
 - grants.gov (GG) Form Certification Regarding Lobbying Form.
- Both forms are available in the Forms tab under SF-424 Family. The initial application cannot be started or submitted in Grants.gov unless the applicants registration in SAM is confirmed.

Application forms and instructions are available at grants.gov. To access these materials, go to <http://www.grants.gov>, select *Apply for Grants*, enter the CFDA number or the Opportunity ID Number noted in this FOA, select *Download Application Package*, and follow the prompts to download the application package. The information submitted in grants.gov will be retrieved by ND Grants, which will allow FEMA to determine if an applicant is eligible. Applicants are encouraged to submit their initial application in grants.gov at least ten days before the application deadline.

If you need assistance applying through grants.gov, please go to <http://www.grants.gov/web/grants/applicants/grant-application-process.html>, contact support@grants.gov, or call 800-518-4726. FEMA cannot assist applicants with questions related to registering with grants.gov.

5. Final Application Submission in Non Disaster Grants System (ND Grants).

Eligible applicants will be notified by FEMA and asked to proceed with submitting their complete application package in ND Grants located <https://portal.fema.gov>. Applicants can register early with ND Grants and are encouraged to begin their ND Grants registration at the time of this announcement. Early registration will allow applicants to have adequate time to start and complete their application.

If you need assistance registering for the ND Grants system, please contact ndgrants@fema.gov or (800) 865-4076.

XI. Application and Submission Information

In ND Grants applicants will be prompted to submit all of the information contained in the following forms. Applicants should review these forms before applying to ensure they have all the information required.

- Standard Form 424A, Budget Information (Non-construction);
- Standard Form 424B, Standard Assurances (Non-construction);
- Standard Form LLL, Disclosure of Lobbying Activities (if the grantee has engaged or intends to engage in lobbying activities).

In addition applicants must submit copies of the following in ND Grants:

Application Format

Applications submitted must meet certain format and content requirements. In order to receive full credit for this section, applications must meet the following criteria in the application:

- Doubled spaced
- Times New Roman, 12 point font
- One inch margins
- All required sections: Executive Summary, Description of Training, Analysis of Need, Training that is National in Scope, Capacity to Deliver Training that is National in Scope, Timeline, and Budget
- Application not to exceed 15 pages. If the application contains more than 15 pages the application runs the risk that the excess pages may not be reviewed.

Applications must be created in Microsoft Word (.docx) or text (.txt) and:

- Include an Executive Summary not to exceed two (2) pages confirming the application's intent for applying for an award.
- Executive Summary must include a description of the training program being proposed and the focus area that the training addresses.
- Executive Summary must include a description of the application's qualifying factors (i.e., application is in partnership with a multi-state, multi-jurisdiction, tribal, or territorial government; non-profit association or organization; community or faith-based organization; or non-profit higher education institution).
- Executive Summary must also include a confirmation that the application is not listed on a debarment list.

Application Content

At a minimum, the application must include the following sections:

1. Description of Training

- 3 pages maximum
- Application provides a clear description of the 3-year proposed national training program and describes how the training addresses the identified focus area.
- Application describes the number of courses to be developed, and if more than one course, describes how the courses interrelate or build upon each other.
- Application describes the length of time of each course(s), including the number of times it proposes to deliver each.
- Application explains the course(s) goals and learning objectives.
- Application clearly identifies and describes the target audience (disciplines) and discusses its strategy for reaching out to large numbers of these participants across the nation.
- Application specifies how it will identify and recruit individuals to attend training including the sources it will tap into to recruit individuals for training courses and what will be done to ensure that it can reach a national audience.
- Application describes the course prerequisites, specifically the general skills and knowledge required for maximum learning.
- Application describes the training level to which its course(s) is/are geared among the following:
 - ♦ Awareness - Designed for responders who require the skills necessary to recognize and report a potential catastrophic incident or who are likely to

witness or investigate an event involving the use of hazardous/explosive devices.

- ♦ Performance - Designed for first responders who perform tasks during the initial response to a catastrophic event, such as safeguarding the at-risk public, rescuing victims, decontaminating victims, etc.
 - ♦ Management/Planning – Designed for managers who build plans and coordinate the response to a mass consequence man-made or natural event.
 - ♦ Other: Application could not accurately fit its course(s) into one of the existing categories, but described its course(s) in enough detail for review panel to understand the training level.
- Application realistically identifies the number of people it will train during the three years of the project and specifies how many will be trained in each delivery method (i.e., classroom, web, etc.).
 - Application describes the intended impact the training will have to assist participants in preventing, protecting, responding, and/or recovering from acts of terrorism and/or catastrophic events, and what the potential measurable outcomes will be.
 - Application describes a performance-based evaluation plan that includes program performance measures that will assess the attainment of goals, objectives, and outcomes and details a data collection plan including how data will be analyzed.
 - Application describes what instructional methods it will use in its blended learning strategy (classroom, web-based, etc.) and why.
 - Application describes the sequence and how different methods will be combined to form a cohesive training program for the target audience.

2. Analysis of Need

- 2 pages maximum
- If a needs analysis was conducted, application describes the sources analyzed and reviewed to identify the need for this particular training.
- Application describes results of the analysis; including the gaps identified that point to a need for this particular training.
- If a needs analysis was not conducted, the application describes how they arrived at the need for the proposed training, and what analysis they will do to verify the need for it.
- Application describes training that currently exists that addresses the training they are proposing or includes a statement that none exists.

3. Training Program that is National in Scope

- 1 page maximum
- Application identifies an overall approach that will be taken to develop and deliver its training program to participants on a national level.
- Application describes how its program will translate to participants nationally (e.g., a participant in Kansas could utilize the same information as a participant in Maine).
- Application describes the delivery method of course (i.e., mobile, residential, or on-line) and, if not on-line, describes the number of sites and site locations.

4. Capacity to Deliver Training that is National in Scope

- 1 page maximum
- Application provides an overview of past successes in similar efforts.
- Application describes the technical expertise of each proposed staff member relevant to the focus area.
- Application describes a staffing plan that demonstrates its capacity to support a large scale training effort.
- Application describes the efforts it proposes to sustain the training program beyond the Federal funding it receives for the development and delivery of this program during this period of performance.
- Application describes any partnerships it will enter into and how it will strengthen the program.

5. Timeline

- 2 pages maximum
- Application presents a timeline, going from 1-36 months and includes at a minimum, the following major milestones:
 - ♦ Hiring of key staff
 - ♦ Analysis phase, if applicable
 - ♦ Design phase
 - ♦ Development phase
 - ♦ Course pilots
 - ♦ Implementation phase (course delivery)
- Application provides justification for course development lasting longer than 18 months.

6. Budget Narrative and detailed budget

- 3 pages maximum
- Application provides a budget justification to include the following areas:
 - ♦ Divides the budget between development and delivery costs and explains how those separate budgets support the other (Development includes everything prior to the delivery of the courses.)
 - ♦ Explains what percentage is devoted to development versus delivery
- Application explains the cost per student for delivery (the portion of the budget devoted to delivery divided by the number of students in the project to be trained.)
- Application ensures:
 - ♦ The budget is directly related to and supports the activities described in the proposal. Detailed budget utilizes required budget categories included in the proposal (personnel, fringe benefits, travel, equipment, supplies, consultants/contractors, etc.)
 - ♦ The budget is complete, allowable, and cost effective in accomplishing the tasks in the proposal.
 - ♦ The budget supports the total cost of the development and delivery of training, including numbers to be trained, that are reflected in the proposal.

7. Indirect Cost Rate Agreement

- 1 page maximum
- Include a copy of an “Indirect Cost Rate Agreement” between the applicant and a cognizant Federal Agency.

Applicants will also be prompted to assure compliance with all Standard and Special Terms and Conditions before being eligible to receive an award under this program.

If you need assistance registering for the ND Grants system, please contact ndgrants@fema.gov or (800) 865-4076.

Hard copies of the FOA

Hard copies of the FOA can be downloaded from the common electronic “storefront” grants.gov or via email from <mailto:patrick.cowhey@fema.dhs.gov>.

Telephone Device for the Deaf (TDD)

The Telephone Device for the Deaf (TDD) and/or Federal Information Relay Service (FIRS) number available for this Announcement is: (800) 462-7585.

Countering Violent Extremism (CVE) Working Group

**Homeland Security Advisory Council
Spring 2010**

Secretary's Tasking of HSAC

Recognizing that there have been many successful cases of local law enforcement working with communities to fight violent crime, at the February 2010 HSAC Meeting Secretary Napolitano tasked the HSAC to “...work with state and local law enforcement as well as relevant community groups to develop and provide to me recommendations regarding how the Department can better support community-based efforts to combat violent extremism domestically – focusing in particular on the issues of training, information sharing, and the adoption of community-oriented law enforcement approaches to this issue.”

Secretary's Tasking (Con't.)

Specifically, the initial recommendations will focus on the following issue areas:

- **Best Practices:** What are some best practices that demonstrate how information driven, community-based efforts can be effective in reducing violent crime within a community?
- **Information Sharing:** What type of information and intelligence should DHS be providing state and local authorities so that they are better able to leverage existing community-oriented policing efforts to identify and address ideologically-motivated violent crime?
- **Training and Other Support:** What type of training, technical assistance and funding support is required so that local authorities are better able to integrate information driven, community-oriented policing activities into overall efforts to establish safe and secure communities?

Development of Recommendations

- Recommendations were developed through a series of telephonic and face to face meetings that included working group members, state, county and local government officials, and representatives from community organizations.
- Discussions of the Working Group were organized around four major themes:
 - Every day, across the Nation, local, state, and tribal law enforcement agencies work with community members to prevent violent crime – what are some of the best examples of how police/community partnership can lead to significant reductions in violent crime?
 - Does this approach lend itself to preventing violent crime that is motivated by extreme ideological beliefs – and how does this effort to counter violent extremism impact the police-community partnership?
 - If local law enforcement were to incorporate efforts to counter violent extremism into pre-existing, community-oriented violent crime reduction efforts – what information would these local entities need from the Federal Government – specifically DHS.
 - If local law enforcement were to incorporate efforts to counter violent extremism into pre-existing, community-oriented violent crime reduction efforts, what type of training would front line officers, investigators and management personnel require?

General Findings

- **Community-Oriented Policing works in preventing violent crime** – The Working Group found that information-driven, community-oriented policing efforts have proven effective in reducing and/or preventing violent crime in numerous jurisdictions across the Nation.
- **Emphasis should be on building safe, secure, resilient, and crime resistant communities** – In working with community members, law enforcement seeks to understand and proactively address factors which enable violent criminal activity to occur.
 - Effective public –private partnerships, designed to enable civic engagement, problem-solving, and violent crime mitigation provide the foundation for efforts to prevent, protect against and respond to violent criminal activity – including that which may be motivated by ideological objectives.
 - While acknowledging that information-driven, community-based law enforcement efforts hold great promise in preventing violent crime that is terrorism-related, that promise will be best realized when local authorities work with community members to understand and mitigate all threats facing local communities.
 - The current level of understanding regarding the sociology of “radicalization” and “extremism” is still immature. Accordingly, Working Group members believe that the concept of building safe, secure, resilient and crime resistant communities should be the priority and operationally, efforts should focus on stopping violent behavior regardless of the motivation.
 - Working Group members felt that discussions regarding how to improve local law enforcement crime reduction efforts should be delinked from the current academic and policy discussions on “radicalization” and “countering violent extremism” until such time that the understanding of these phenomena matures.

General Findings (Cont.)

- **All violent crime is local** – While there may be some common indicators of ideologically-motivated violence, each circumstance is unique, needs to be viewed individually, and viewed within the context of the specific community in which the suspect lives, works, and operates.
- **There can be tension between those involved in law enforcement investigations and those collaborating to establish local partnerships to stop violent crime** – Community policing can be impeded if other enforcement tactics involving a community are perceived as conflicting with community partnership efforts. Crime control efforts at the local level involve a variety of operational activities that can be – if properly coordinated – supportive and complementary. Roles and responsibilities of federal, state, local and tribal law enforcement, and the community need to be clearly defined and articulated. Law enforcement should be sensitive to the fact that perceptions regarding enforcement actions and intelligence gathering can impact community-oriented policing goals.

Best Practices of Local Law Enforcement/Community Partnerships Are Leading to Significant Reductions in Violent Crime

- Multiple examples exist of effective community/local government partnerships which have led to significant reductions in violent crime including:
 - **Los Angeles, California**
Law enforcement joins communities and government agencies to improve quality of life issues and reduce violent crime.
 - **Cincinnati, Ohio**
College professors collaborate with law enforcement and communities to lower crime.
 - **Austin, Texas**
Law enforcement works with community on rapid response teams to mitigate tough issues and work in partnership to reduce violent crime.
 - **Las Vegas, Nevada**
Grassroots community effort led by faith based organizations that assist in reducing violent crimes and gangs.
 - **Dearborn, Michigan**
Collaborative effort to engage the community in the identification and resolution of community issues to include combating violent crime.
 - **State of Maryland**
Established an executive level coordinating office within the Governor's Office to work with community groups, ethnic groups, and faith based organizations to address quality of life and other issues of concern.
 - **State of Ohio**
Established a community engagement office which built a collaborative and cooperative relationship with the communities based on trust and mutual respect.
 - **Minneapolis, Minnesota**
Designated crime professional specialists who are liaisons between the community and local law enforcement and have safety centers that are funded by the neighborhoods.

The Working Group recognized that these are only a few examples of best practices by community-oriented policing efforts across the country. The Working Group also noted that it should be a continuing priority to identify best practices as well as to document instances where partnerships have not worked well in order to identify and compile lessons learned.

Community-Oriented Policing

Community-oriented policing is a viable strategy to address crimes of violence if the approach involves:

- Developing meaningful partnerships between the government and communities in which all partners contribute to the identification of community issues and needs;
- Collaborative problem solving; and
- Law enforcement and other government agencies implement institutional and organizational changes to support the effort.

Key Elements of Community-Oriented Policing to Reduce Violent Crime

- **Partnerships** – Establishing advisory councils/focus groups to include civic and community organizations, faith based and education entities, private sector security, and the media. Encourage participation through these partnerships to draw involvement from all segments of the community.
- **Leadership** – Executive Leadership/Guidance of local law enforcement heads in taking the lead in outreach to communities.
- **Multidisciplinary** – Leverage all available public and private resources within a local environment including social services, medical, mental health and family/school counseling professionals to help build bridges to communities; an excellent example has been the outreach/athletic programs for community youth spearheaded by some local police departments as well as outreach programs for community youth to include enrichment, education, and participatory programs like Police Explorers and Internships, and other self esteem building initiatives.
- **Training** – Continuous training is key to both law enforcement and the community and should focus on:
 - Improving capacity of law enforcement and other government personnel to communicate and collaborate with individuals from diverse religious, ethnic and racial communities; and
 - Better understanding the threats facing a local community and recognizing behavior and indicators associated with those threats.

Key Elements of Community-Oriented Policing to Reduce Violent Crime (Cont.)

- **Consistency** – Maintaining a presence at community events year-round including religious events. Law enforcement is partnering with religious and community activists, community leaders and business leaders to hold community events (i.e. barbecues, park events, and rallies), where ideas to reduce or eliminate violence are discussed and relationships are established or enhanced.
- **Broad approach** – Work with community and government partners to reduce violence in all forms. Help design interventions to be included in a community or city anti-violence program.
- **Trust** – Effective partnership requires a relationship built on trust and two-way communication between government personnel and community members.
- **Collaboration/coordination** – Efforts should be proactive and designed to prevent crime, reduce fear, and improve the quality of life within a community.
- **Minimize harmful outside influences** – Local crime reduction efforts can be affected by events occurring outside the community.
 - Some localities have established “rapid response” teams to work with communities to better understand and place into context international, national, and local incidents that “raise the temperature” in terms of targeting the community may face (either for hate crimes or by ideologically-motivated recruiters).

Key Elements of Community-Oriented Policing to Reduce Violent Crime (Cont.)

- **Conduct research** – A “best lesson learned,” is to ensure the up-front effort of proper research and the identification and inclusion of important under-represented communities is a foundational part of any Community Policing initiative. To that end, the inclusion of all representative sections of a community will lead to a safer and more secure country.
- **Remember the past** – An important facet to supporting and implementing Community Policing initiatives is to recognize that those who cannot remember the past are condemned to repeat it. In analysis of previous major crimes and critical incidents, dating back to the 1960’s, a common theme can be developed. Law enforcement entities that properly researched all segments of the community and developed relationships based on elicited input and free exchange of information did much better in the detection, investigation, and mitigation of these situations.
- **Law enforcement personnel should come from the communities they serve** – Law enforcement should make a concerted effort to hire more individuals representative of the communities served by that agency.

Recommendations to DHS on Community Policing

- **Document and make available best practices** – DHS should work with external groups to (a) identify and document those information-driven, community based violent crime reduction efforts that represent “best practices” AND making “best practices” resources available online for other law enforcement agencies and the community to be able to have access; and (b) identify challenges and unsuccessful practices so that best practices can be strengthened.
- Information-driven, community based violent crime reduction efforts should be recognized as a critical element of national efforts to protect the homeland from terrorism and other threats.
- DHS should work closely with the Office of Community Oriented Policing Services (COPS) at the Department of Justice (DOJ) to better incorporate the concept of community-oriented policing into programmatic and policy efforts associated with homeland security preparedness.
 - Increased resources should be made available (funding, training, technical assistance) to state and local authorities.
 - Establishing information-driven community-based violent crime reduction capabilities should be considered a preparedness priority by DHS.
 - Community-oriented policing costs should be included as an allowable expense within DHS grant programs.

Key Elements of Applying Violent Crime Prevention to Stopping Ideological-Motivated Crime

- Emphasis should be placed on supporting local efforts to establish safe and secure communities – this could mean securing them against all types of threats from outside as well as from within.
- Dealing with ideologically-motivated crime is done best when there is a pre-existing relationship between communities and local law enforcement and needs to be done in the broader context of dealing with all crimes.
- Information-driven, community based violent crime reduction efforts should emphasize stopping violent behavior regardless of the motivation.
 - Communities may be hesitant to enter in relationships with local, state, tribal or federal law enforcement if they perceive that they are viewed as incubators of violent extremism.

Key Elements of Applying Violent Crime Prevention to Stopping Ideological-Motivated Crime (Cont.)

- Information regarding specific threats should be shared with local law enforcement, who in turn should share with the community, so there is a shared understanding of the threat:
 - Work together to develop a plan to mitigate the threat;
 - Place police actions into context;
 - Be more aware of indicators and behavior associated with a specific threat; and
 - Define roles and responsibilities associated with threat mitigation. The federal government should ensure adequate safeguards for basic rights in cases of individuals about whom information is provided by communities. This is extremely important to maintain trust and cooperation among communities and local authorities.
- Offer the community a separate clear point of contact to open a regular channel of communication and gain information from the government to learn about new programs, initiatives and policies (Protective Security Advisors in the states).

Recommendations to DHS

- **Develop and use common terminology** – Use of various terms to describe ideologically-motivated violent crime (radicalization, violent extremism, etc...) causes confusion. DHS should work with the federal government, and state and local partners to establish common use lexicon and consistent use of terminology. This product should be made available to the public via the internet.
- **Expand CRCL engagement efforts separate from support of community-oriented policing** – Recognizing that policies implemented by DHS can affect local community partnerships, DHS Civil Rights Civil Liberties (CRCL) and other relevant DHS offices should continue and expand their engagement and grievance resolution efforts at DHS. DHS should also work with other federal agencies to come up with a verification process for groups it interacts with. This in turn will help establish a national environment conducive to the establishment of local partnerships.

Recommendations to DHS (Cont.)

- **Incorporate information-driven, community-based violent crime reduction into local preparedness efforts** – Efforts to increase support to local, community-based violent crime reduction should be viewed as a core element of preparedness programs as opposed to being part of national efforts to understand the phenomena of domestic violent extremism.
- **Support efforts to establish local dispute resolution capabilities** – DHS should provide resources and guidance to support local partnerships efforts to address community issues and grievances. These resources can be an empowering tool that generate a greater role for communities to extend themselves to law enforcement and have greater input in addressing violence and violent extremists. Moreover, it serves the long term objective of engaging the communities to view violence not only as a law enforcement concern but as society's concern.
- **Through Policy, DHS should utilize the philosophies based on communication, trust, and mutual respect to develop relationships with local law enforcement** – These are the same principles local law enforcement is using through Community Policing to build relationships in their respective communities. Relationships between local law enforcement and DHS must be broader than just communication at the executive level. Individual Agents and Individual Officers must form relationships at the “grassroots” level to effectively communicate and achieve mutual goals.

Information Partnerships Need from DHS

- To be effective, efforts to combat violent crime should be information-driven, which requires that local partnerships have a shared understanding of:
 - Specific threats facing an individual community;
 - Groups and/or individuals associated with a threat; and
 - Behavior and indicators associated with a threat.
- State and major urban area fusion centers play a critical role in local crime prevention efforts in that they receive intelligence/information from federal authorities regarding threats to the homeland and evaluate those threats from a local context. These fusion centers must share that knowledge with local law enforcement so that it can inform the community on violent crime reduction efforts.
- Knowledge regarding specific threats should be blended with awareness of societal and religious practices so that local authorities can place reported and observed behavior into context, thereby allowing them to distinguish legal behavior from criminal activity.
- The timely sharing of accurate threat-related information is an essential component of community-based efforts to combat violent crime.
- There can be an inherent tension between federal law enforcement investigations and local partnerships to stop violent crime. While this tension can be healthy or unhealthy, it must be managed by senior officials.

Recommendations to DHS on Information-Sharing

- **Generate threat-related information products** – DHS should increase the availability to local authorities of accurate, threat-related information in a format that allows broader sharing with community members. DHS should work with fusion centers to demystify the process for the community. This information should include:
 - Trends observed internationally regarding types of attacks and recruitment efforts;
 - Specific threats to the community; and
 - Behavior and indicators associated with such threats.
- **Establish communication platform to share threat-related information directly with faith-based or other communities** – DHS should explore expanding the Secure Community Network concept to other faith-based communities and put together a task force to look at best practices for faith-based communities.
- DHS should publicly welcome organized community-based engagement efforts on CVE policy development and best practices promotion around the country.

Recommendations to DHS on Information-Sharing (Cont.)

- **Increase public awareness regarding terrorism and other homeland security related trends so that they can be demystified and incorporated into local violent crime reduction efforts** – DHS should explore ways in which it can provide the public, particularly the more youthful segments of the population, with a better understanding of terrorism-related trends, and training so that communities are better able to recognize behavior associated with terror-related criminal acts, the variety of government offices that could play a role in a response, and the relationship between these offices. This process should also include education to communities on law enforcement processes and procedures to help demystify law enforcement.
 - DHS should consider building a website that “speaks to” parents, caregivers, educators, counselors, etc.. The website should take a holistic approach and include tools for schools and parents to keep an eye on behavioral traits, as well as the use of internet social networking sites, reporting hate crimes, human trafficking, child predators, and other security issues.
 - DHS should also work with the American Ad Council on public service announcements, which could be for awareness messages that indicate characteristics of individuals who engage in dangerous and anti-social behavior.

Recommendations to DHS on Information-Sharing (Cont.)

- **Develop case studies** – DHS, in partnership with other federal law enforcement agencies and community representatives, should package and release analytical reviews of major events of domestic violent extremism (Zazi, Holocaust museum shooting, Ft. Hood shooting, etc.) and develop case studies that can be used by local authorities as a learning tool for law enforcement personnel. The use of real life examples of the threats will better illustrate the dangers faced by specific local communities as well as the Nation. Involving community representatives in the development process will help build trust and engage the community in dialogue and greater cooperation that serves the common good.
- DHS should work with its federal partners to increase collaboration to ensure community partnerships and intelligence community (IC) are not undermined by each other but instead work in a complementarily effective manner.

Recommendations to DHS on Information-Sharing (Cont.)

- **Continue efforts to ensure that fusion centers have the capacity to receive and understand threat-related information and to share that knowledge with local authorities.** DHS should work with fusion centers so that fusion centers have a greater capacity to understand (a) the threat posed by ideologically-motivated criminal activity and share that knowledge with local law enforcement, and (b) cultural, societal, and religious customs so that intelligence is placed in context and legal behavior is distinguished from criminal activity.

Findings on Training

- Continuous training of government personnel is a key element of successful community-oriented policing efforts. Law enforcement officers must have the ability to have honest conversations with people in their community and must recognize the value that comes from effective, proactive problem solving.
- The capacity to interact with members of the public in order to address crime and quality of life issues needs to be a fundamental skill set of front line and management personnel. Effective and open communication by law enforcement officials provides the foundation for effective collaboration and partnership at both the organizational and individual levels.

Findings on Training (Cont.)

- Training should focus on:
 - Improving capacity of law enforcement and other government personnel to communicate, collaborate, and partner with individuals from diverse religious, ethnic, and racial communities; and
 - Better understand the threats facing a local community and recognizing behavior and indicators associated with those threats.
- Training should be provided to community members so they better understand how government, and in particularly law enforcement, operates. This will demystify and minimize tensions due to misperceptions.
- Members of the community should be invited to provide training to government personnel.
- Training is needed for school officials and parents on a variety of issues including: how to recognize behaviors consistent with criminal activity or specific threats; the use of internet social networking sites by sexual predators and extremist recruiters; recognizing hate crimes; human trafficking; child predators; gangs; and other security issues.

Findings on Training (Cont.)

- Current training programs should be re-evaluated and priority given to supporting those programs that introduce or support the community policing model. Good training is essential as bad training not only is ineffective – but can serve to escalate tensions between law enforcement and the community.
- Enforcing hate crimes is one way for law enforcement to build trust with minority communities.
 - Law enforcement and communities rarely reported hate crimes before they received hate crime training. Law enforcement personnel generally respond to crime rather than report it.
- Local law enforcement should train communities on what constitutes a hate crime and encourage them to report hate crimes. This will help strengthen the community-police relationship.

Recommendations to DHS on Training

- **Expand availability of training and technical assistance focused on the understanding, identifying and mitigating threats through community-oriented policing** – DHS, working in partnership with the COPS office, should explore how best to expand the training and technical assistance provided to state, tribal, and local personnel so that they are better able to:
 - Understand and mitigate threats facing their communities;
 - Identify behavior and indicators associated with ideologically-motivated crime;
 - Engage more effectively with communities; and
 - DHS and DOJ’s COPS should consider providing additional support for efforts that trains law enforcement on community policing such as the Regional Community Policing Institutes and the National Counter-Terrorism Academy for State and Local Law Enforcement in Los Angeles.
- **Improve quality of training** – DHS should institute quality control processes to ensure that training provided through DHS, or paid for by DHS provided grant funding, meets minimum quality control.
- Training should seek to instill greater understanding regarding the “us versus them” perspective that many cultures have toward law enforcement and government and enable law enforcement personnel to better understand and address unrest or anger within the community (whether it be ideologically-based or not) in order to prevent violent activities.

Recommendations to DHS on Training (Cont.)

- **Expand availability of training for state, local and tribal law enforcement and DHS components** – Operational and law enforcement personnel including corrections personnel, should possess an understanding of cultural and religious practices so that they are better able to distinguish between criminal activity and lawful behavior. A collaborative effort comprised of community, academia, and law enforcement professionals should be involved in helping develop these trainings.
- DHS should fund efforts to expand Federal Law Enforcement Training Center's hate crime training.
- DHS should explore expanding FLETC's role to include training in the building of community capacity, partnerships, cultural knowledge awareness and development of specialized training modules for community leaders and non-governmental organizations.
- DHS should reassess its hate crime training to include understanding extremism and ideological violence.
- DHS should work with state and local partners to provide training for schools and parents on a variety of issues including: how to keep an eye on behavioral traits, the use of internet social networking sites, reporting hate crimes, human trafficking, child predators, gangs, and other security issues.

Members of the Countering Violent Extremism Working Group

| | |
|-------------------------|---|
| Martin O'Malley | Governor, State of Maryland, (Working Group Chair) |
| Art Acevedo | Chief of Police, Austin Police Department |
| Nimco Ahmed | Policy Aide, Vice-President of the Minneapolis City Council |
| Omar Alomari | Community Engagement Officer, Ohio Homeland Security |
| Asli Bali | Acting Professor of Law, UCLA School of Law |
| Richard Cañas | Former Director, New Jersey Office of Homeland Security and Preparedness |
| Richard Cohen | President and CEO, Southern Poverty Law Center |
| Michael Downing | Deputy Chief, Commanding Officer, Counter Terrorism and Criminal Intelligence Bureau, Los Angeles Police Department |
| Mohamed Elibiary | President and CEO, The Freedom and Justice Foundation |
| Clark Ervin | Director, Homeland Security Program, The Aspen Institute |

Members of the Countering Violent Extremism Working Group (Cont.)

Paul Goldenberg

National Director, Secure Community Network

Doug Gillespie

Sheriff, Las Vegas Metropolitan Police Department

Ellen Gordon

Associate Director, Naval Postgraduate School Center for
Homeland Defense and Security

Ronald Haddad

Chief of Police, Dearborn Police Department

Amin Kosseim

Deputy Inspector, New York City Police Department

Cathy Lanier

Chief, Washington DC Metropolitan Police Department

Imam Mohamed Magid

Executive Director, All Dulles Area Muslim Society (ADAMS
Center)

Mary Marr

President, Christian Emergency Network

Dalia Mogahed

Senior Analyst and Executive Director, Gallup Center for Muslim
Studies

Jeff Moss

Director, Black Hat/Techweb

Dan Rosenblatt

Executive Director, International Association of Chiefs of Police

Asim Rehman

President, Muslim Bar Association of New York

Members of the Countering Violent Extremism Working Group (Cont.)

Nadia Roumani

Director, American Muslim Civic Leadership Institute

Frances Townsend

Partner, Baker Botts, L.L.P.

Chuck Wexler

Executive Director, Police Executive Research Forum

Skip Williams

Provost and Vice President for Health Affairs, The George Washington University

Subject Matter Experts

Arif Alikhan

Assistant Secretary, Policy Development, DHS

John Cohen

Special Advisor to the Secretary on Information Sharing, DHS

Bart Johnson

Principal Deputy Under Secretary, Intelligence and Analysis, DHS

David Schanzer

Associate Professor of the Practice for Public Policy and Director, Triangle Center of Terrorism and Homeland Security, Sanford School of Public Policy, Duke University

Bob Wasserman

Chairman, Strategic Policy Partnership

Laurie Wood

Analyst, Southern Poverty Law Center/Instructor, Federal Law Enforcement Training Center



COUNTERING VIOLENT EXTREMISM SUBCOMMITTEE AGENDA

DHS HQ

3801 Nebraska Ave NW DC

Thursday, April 14th, 2016 – 9:00 a.m. to 4:00 p.m.

- 9:00-10:00 a.m. **Classified Intelligence Briefing (Building 19)**
Chad Reifer, Office of Intelligence and Analysis, DHS
Stephanie Maniglia, Office of Intelligence and Analysis, DHS
Conley Hefley, Office of Intelligence and Analysis, DHS
- 10:10 a.m. **Welcome and Introductions (Building 1, Room 01-044)**
Sarah E. Morgenthau
Executive Director, Homeland Security Advisory Council
- 10:15-11:30 a.m. **Focus Area Progress Reports by Subcommittee Members**
Ali Soufan (Communications/Messaging)
Seamus Hughes (Funding and Resourcing)
Joel Meyer (Engaging with Tech and Social Media Companies)
Paul Goldenberg (Incorporating the Education and Mental Health Sectors)
Laila Alawa (Pop Culture/Millennials)
- 11:30-12:00 p.m. **Leadership Remarks**
- 12:00-1:00 p.m. **Working Lunch (EDF Private Dining Room)**
Russ Deyo, Under Secretary for Management, DHS
George Selim, Director, Office for Community Partnerships, DHS
- 1:00 -2:00 p.m. **Discussion on Partnering with Industry**
Christopher Graves, Global Chair, Ogilvy Public Relations
- 2:00-2:15 p.m. **Break**
- 2:15-3:00 p.m. **S&T Briefing on CVE Metrics and Assessments**
Kathleen Deloughery, Science and Technology Directorate, DHS
- 3:00-4:00 p.m. **Continued Focus Area Read Outs and Discussion on Building out the Framework for the Final Report**
Farah Pandith, Chair, CVE Subcommittee
Adnan Kifayat, Chair, CVE Subcommittee
- 4:00 p.m. **Meeting Adjourns**

Page 1 of 1

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1 of 1

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

**Homeland Security Advisory Council
Countering Violent Extremism Subcommittee Meeting
April 14, 2016**

Overview:

- You will meet with the Homeland Security Advisory Council's (HSAC) Countering Violent Extremism (CVE) Subcommittee.
- The Subcommittee is chaired by Farah Pandith, Adjunct Senior Fellow at the Council on Foreign Relations and Senior Fellow at the Kennedy School of Government at Harvard University, and Adnan Kifayat, Senior Resident Fellow, German Marshall Fund of the United States.
- During the meeting, the Subcommittee will hear from various subject matter experts and discuss how the Department can best collaborate with technology and social media companies, philanthropic organizations, and education and mental health sectors to help counter violent extremism.
- Your participation is as follows:
 - 11:30 a.m.: You will arrive during the meeting and greet the Subcommittee members.
 - 11:35 a.m.: You will receive a progress report from the co-chairs.
 - 11:45 a.m.: You will make remarks and provide feedback to the group.
 - 12:00 p.m.: You will depart.

Discussion Points:

- You will have thirty minutes to meet with the CVE Subcommittee, hear about the progress they have made to date, and receive an overview of the final report they will issue in June 2016.
- The Subcommittee is focused on six key areas regarding CVE efforts:
 - Communications and Messaging
 - Research and Analysis
 - Engaging with Technology and Social Media Companies
 - Funding and Resourcing Efforts
 - Incorporating the Education and Mental Health Sectors
 - Pop Culture and Millennials
- You should provide candid feedback and guidance to the group, specifically on their approach and overall direction of the report. The meeting is not open to the public, allowing you to speak freely and to fully leverage the expertise in the room.

Background:

- On January 21, 2016, the CVE Subcommittee co-chairs briefed you during the HSAC meeting at the Wilson Center.

- The CVE Subcommittee was stood up in December 2015 to act as an incubator of ideas for the Office for Community Partnerships, and to leverage outside expertise and new thinking to allow the Department to go beyond how it has conventionally framed and envisioned CVE efforts.
- The CVE Subcommittee is comprised of members of the HSAC as well as a number of selected subject matter experts and key thought leaders from private industry, academia, and non-governmental organizations.

Participants:

Secretary Johnson

George Selim, Director, Office for Community Partnerships

Sarah Morgenthau, Executive Director, Homeland Security Advisory Council

Homeland Security Advisory Council CVE Subcommittee Members

Attachments:

A. Meeting Agenda

B. CVE Subcommittee Membership List

C. Biographies

D. CVE Subcommittee Tasking Memo

E. CVE Subcommittee Federal Register Notice

Staff Responsible for Briefing Memo: Sarah Morgenthau, Executive Director, Homeland Security Advisory Council, OPE, (b)(6)

OGC Reviewer: Attorney in Component Counsel or HQ, Title, Phone Number.



HSAC CVE SUBCOMITEE MEETING

Attendance List April 14, 2016

Yes (12)

Farah Pandith (Chair)

Adjunct Senior Fellow at the Council on Foreign Relations,
Senior Fellow at the Kennedy School of Government at
Harvard University, Former Special Representative to
Muslim Communities, U.S. Department of State

Adnan Kifayat (Chair)

Senior Resident Fellow, German Marshall Fund of the
United States

Russ Deyo

Under Secretary for Management, Department of
Homeland Security

Paul Goldenberg

President and Chief Executive Officer, Cardinal Point
Strategies

Seamus Hughes

Deputy Director, Program on Extremism at George
Washington University

Joel Meyer

Senior Vice President, Public Sector at Dataminr

Michael Masters (proxy)

Senior Vice President, The Soufan Group LLC

Michael Nutter

Former Mayor, Philadelphia, Pennsylvania

Juan Zarate

Senior Adviser at the Center for Strategic and International
Studies

William Webster (Ex-officio)

Retired Partner, Milbank, Tweed, Hadley & McCloy LLP

Joining via conference call

Laila Alawa

Chief Executive Officer & Founder, The Tempest

Ali Soufan

Chairman and Chief Executive Officer, The Soufan Group
LLC

No (4)

John Allen

Retired U.S. Marine Corps. General and Former Special
Presidential Envoy for the Global Coalition against ISIL

Jane Harman

President and Chief Executive Officer, Woodrow Wilson
Center

Jeffrey Miller

Senior Vice President and Chief Security Officer, National
Football League

Matthew Olsen

President of Consulting and Co-Founder, IronNet
Cybersecurity

Page 1 of 1

Withheld pursuant to exemption

(b)(6)

of the Freedom of Information and Privacy Act

HSAC Countering Violent Extremism (CVE) Meeting April 14, 2016

Action items

- General Action Items
 - Focus areas need to provide more granularity on recommendations to move towards a “just add water” product.
 - This means recommendation need to come with specific groups, people, programs, and process that should be engaged and provide plans for how to engage them.
 - Judge Webster’s letter to the Secretary should be publicized on the website, perhaps directly posted.
 - May 10th is when the interim report from DHS Science and Tech will come out. Send report to Subcommittee.
- Communications/Messaging
 - Ruling on whether DHS can do counter messaging targeted towards Americans? Is that an option on the table and can we investigate that?
 - Need to create a framework explaining what CVE is and how CVE programs should be addressing problems. Needed to educate groups like Congress, law enforcement, and others.
- Funding/Resources
 - Office of General Council should provide Secretary a memo on if/how he can reach out to philanthropic community to help petition funding for CVE issues and partner organizations.
 - Need to find out how much additional funding the Secretary might be able to ask Congress for, to support CVE.
 - Need a hard number on what it would cost to do CVE successfully in the US.
 - Need to create a game-plan that could be given to the Secretary when he goes to philanthropies so he can explain what exactly their money would go to and how CVE programs would use it.

Recommendations

- Communication/Messaging
 - Secretary should convene a round table of private sector funders and business groups and then bring CVE community partners in to make a pitch and get additional funds.
 - DHS could help facilitate ISAC (Information Sharing and Analysis Centers) type interactions for CVE issues.
 - Congress, law enforcement, and general public need to be given a framework explaining what CVE is and how CVE funds should be spent.
 - Compstat: A program that receives situational reports from on the ground agencies to their superiors on a regular basis. Secretary should develop a similar program and ask for a situational report from components.
- Funding/Resources
 - DHS should create a FACA type committee.
 - Secretary should seek greater funding for CVE from Congress given existence interests to do so within the legislative body.
 - During the next grant funding budget cycle, DHS should ask applicants to explain how much of their current funding is going towards CVE activities, how much of the new

HSAC Countering Violent Extremism (CVE) Meeting April 14, 2016

funding they intend to allocate to CVE, what their current funding is, and what CVE programs they have in place.

- Engaging with Tech and Social Media Companies
 - DHS should seek to create some kind of platform to support and allow for the organic development of CVE messaging. Need to catalyze others to organically impact this problem. Something like an In-Q-Tel type public/private partnership.
- Incorporating the Education and Mental Health Sectors
 - Resilience building through closer bonds and trust should be a primary objective of government programs within the CVE space.
 - DHS should expand current CVE pilot program to more than three cities (Minneapolis, LA, and Boston).

Timeline

- May 10th have a draft from all sub-components and the recommendations they would like to offer.
- June 2, next council meeting with Secretary
 - CVE report needs to be ready to be considered by the broader committee.
 - CVE report needs to go through a transmittal memo to the Secretary before it becomes official.
- Report Framework
 - Framework
 - Judge Webster – Be sure everyone reads through the charging by the Secretary for our committees' work and make sure we are giving recommendations that touch on what he tasked us to hit
 - Would be good for Michael, Joel, and Laila to meet up and have a strategic conversation on their parts and potential synergy
 - **Report should also have some new products, maps, and visuals on what CVE looks like in the US**
 - **Something to really show how CVE exists and especially showing how CVE looks like as the recommendations are implemented over time.** Very similar to some of the good data graphics like in the foreign fighters report
 - Employee task force report gives a good example of concise recommendations model
 - Things to include in the report

HSAC Countering Violent Extremism (CVE) Meeting April 14, 2016

- Who you interviewed
- Broad themes and insights gained about CVE during your research and work
- “just add water” recommendation and advice for the Secretary
- Argument and reasons why those recommendation will work and accomplish what we say they will accomplish
- Include also a timeline for how these recommendations will be rolled out and implemented.
 - Example: Within 90 days the Secretary should do X,Y, and Z.
 - This is meant to provide as specific of an action plan as possible.
 - Frame this process as a “road map” for what the timetable of completion looks like for these recommendations.
- Agree on a font and font size before people start drafting full report.

Focus Areas

- Michael Masters (Proxy for Ali Soufan) (Communication/Messaging)
 - IS Insights
 - Ability to engage vary different youths throughout the world in many different cultures and many different life circumstances.
 - **Similar communication tactics and underlying motivations similar to those employed by white supremacists and school shooting individuals.**
 - Why are they effective
 - Messages
 - Play on identity crisis and social issues of youth which are left uncovered by other youth.
 - These messages have appeal across socio-economic paths.
 - Messengers
 - Deploy a narrative with a space for inclusion and a virtual support structure.
 - Media
 - Much of this online engagement structure is through peer to peer messaging systems
Most interaction are meant to start online and then move offline.
 - Why US and other ineffective to counter

HSAC Countering Violent Extremism (CVE) Meeting
April 14, 2016

- **USG and other governments lack authority and legitimacy to effectively deploy counter messaging.**
 - USG messaging doesn't create dialogue, it is just a one way communication process.
 - Due to the self-selecting nature of media and social media it is very difficult to reach the most vulnerable individuals through traditional challenges.
- Law enforcement is engaging both sides of the argument but the message is still not getting to underdeveloped communities and youth.
- Lessons learned
 - Credible voices
 - Using influencers with existing credibility within susceptible communities to directly engage in dialogue with individuals who might radicalize.
 - Comedians, sports players, actors, celebrities could all be potential speakers to delegitimize and denounce extremism.
 - Offer alternative
 - Should stop trying to counter the narrative and should instead focus on providing a totally separate alternative narrative to offer susceptible persons.
 - Target audience
 - Need to develop strategies that do not alienate vulnerable populations.
 - Governments role
 - USG must empower and engage voices outside the institution to drown out the voices of extremists.
 - **USG need to convene, coordinate, and empower other voices to counter extremist dialogues.**
- Comment and Questions
 - Pandith - Need to go deeper in the analysis for the final report. Needs specifics on who should be the messengers, radio stations to be used, and specific dialogues to be engaged.
 - Pandith - What was your groups ahh haa moment?
 - **Michael response – Stories of what draws people towards extremism seem very similar.**

HSAC Countering Violent Extremism (CVE) Meeting
April 14, 2016

- **Disenfranchisement and disillusionment.**
They seek a place to belong and a group to identify with and feel cared for by.
 - Pandith – We need more granularity on this info for the eventual report. I want to see specific structures and issues we can bring to the secretary to provide a “just add water” recommendation.
 - Hughes – Could we get a ruling on whether DHS can do counter messaging targeted towards Americans? Is that an option on the table and can we investigate that?
 - Messages should be tailored to fit the phase of radicalization a person may be in.
 - Messaging needs to attract youth proactively by offering other forms of intervention
 - Acts of CVE heroism, social service programs
 - Michael Masters – Need a proactive message that resonates with millennials.
 - Goldenberg – We also need to make sure the messages are tailored to the right people. Some messages need to be sent to kids and young people, but some messages also need to be sent to community leaders and even more critical would be parents who want to know what to look for if their kid is radicalizing.
 - Parents can be concerned that their kids are influenced by more than just terrorism, like community violence.
 - Nutter – With the rise of hate groups again, tactics attracting people to go overseas to fight are some of the same things which draw hate group persons to engage in disruptive actions. **There is a synergy and dual purpose to this discussion to also be repurposed to focus on engaging hate group messaging and communication here at home.**
 - Joel Meyer – On the tech side we see the ability to micro-target select audiences to avoid us having to do blanket messaging. We should take advantage of that but we must first think about who creates the message and how we target for those specific offices.
 - Juan Zarate – If we are going to reframe this we should also think about reframing the thematic of this process.
-
- Seamus Hughes (Funding and Resourcing)
 - Resource
 - Outside resources

HSAC Countering Violent Extremism (CVE) Meeting
April 14, 2016

- **Office of general council should provide sec aid memo on how he can engage aid groups and appeal for funding from outside groups for CVE issues.**
- **Secretary should convene round table of funders that HSAC could pitch CVE ideas towards. This would be a business round table where community partners pitch for funding from business (not government pitchers)**
 - FACA report would be needed.
- Inside Resources
 - **Secretary would have receptive audience for greater DHS funding. Secretary should go to the hill and ask for more money for CVE.**
 - Will need to ask and find out how much additional funding might be able to be added.
 - (Juan Zarate) – CVE was big part of the discussion when I testified to congress.
 - Paul Goldenberg – Does Congress understand that CVE funding isn't enforcement and door kicking. They need to be given a clear idea of what CVE activities would look like and that it is prevention centric.
 - CVE pilot program should be expanded to more than three cities (Minneapolis, LA, Boston).
 - Secretary should advocate for increase in CVE officers operating in areas like larger city areas.
- **Redirection of FEMA grants. Money left over should be considered for re-appropriations.**
- Comments and questions
 - Pandith - We need to get a hard number on the exact money we need to successfully engage in CVE in the US.
 - Should work to allow philanthropists to raise money and get leadership involved outside of the government.
 - Nutter – Strongly encourage that law enforcement be roped in to discussion of CVE funding and where it all goes. Really need law enforcement to voice what exactly they would do with additional CVE funding they get.

HSAC Countering Violent Extremism (CVE) Meeting
April 14, 2016

- US Mayors created a resolution and engaged the International Association of Chiefs of Police (IACP).
 - Michael Masters – We should make sure we provide law enforcement a framework for how to appropriately spend CVE money and guide their investments.
 - Law enforcement tend to think tactics and equipment type solutions. We want to create a clear sense of what the CVE program objective should be to focus on the CVE strategies laid out by HSAC and the Secretary.
 - Many people have a different idea of what CVE is so we should create a framework to give to the Secretary.
 - Sarah Morgenthau – Want Shameus and Joel to send plans on how she can leverage Private Sector Office towards these goals.
 - Juan Zarate – I would recommend that DHS look at ISAC type interactions.
-
- Joel Meyer (Engaging with Tech and Social Media Companies)
 - **We need to create some kind of platform to allow “a thousand flowers bloom”. We need to catalyze others to organically impact this problem. Something like an In-Q-Tel type public/private partnership.**
 - **We are trying to target a very small number of people with a diverse background and a diverse set of motivations.**
 - Private sector skill sets should be adopted in making messaging more effective, more pointed and targeted, and more proficient in actually having an impact.
 - What works may not be directly applicable to CVE issues but may be more about engagement and how to motivate persons towards other actions.
 - Out counter narrative doesn’t have to be against violent extremism.
 - We need to think of what content will fire people up and move them towards positive action.
 - How can we create an entity that can feed this process and engage in it. This is where we want to create a platform to obtain funding to do this type of work.
 - Comments and Questions
 - Pandith – Can you give us a short list of orgs that the Secretary can go to and seek out these practices? We all need to work to provide

HSAC Countering Violent Extremism (CVE) Meeting
April 14, 2016

immediate partners and actions that the Secretary can take on to engage with these issues.

- Adnan K. – **When we seek out these partners we need to make sure we find partners that have a desire to work with us and are ready to engage with us. We need to really bore down on the few actors that would be interested in partnering with the Secretary in the near future.**
 - Qualitative partner selection not quantitative partner selection.

Secretary Enters into the Conversation -----

- Pandith – Our recommendation is that we engage leaders in the field of philanthropy to engage CVE issues.
 - Good example is the Jane-Zuckerberg Initiative and utilizing them to build and inoculate new generation against extremist ideology.
 - We recommend that the secretary goes out and talks to philanthropies and advocates for them to fund CVE groups and projects.
- S1 - Put Judge Webster's letter out on the website.
 - Engage philanthropies
 - Need to go to the Jane-Zuckerberg Initiative or the New York Community trust with a clear plan on what DHS CVE would do with their funds.
 - Flag prohibited content
 - Look at examples of things working elsewhere. **There is a Middle Eastern Law Enforcement Office that lives in the community of Detroit and serves as a model for other communities.**

Secretary Exits Conversation -----

- Paul Goldenberg (Incorporating the Education and Mental Health Sectors)
 - Mental health is a wide range of disorders. Many terrorists and radicalized individuals are rarely able to be medically diagnosed with any mental health analysis.
 - Not all mental health disorders pose any kind of risk of violence. Additionally, only a small part of violence in society can be attributed to mental health issues. Mental health thus should not be identified as a marker for those likely to be radicalized into violent groups.
 - Mentally ill shouldn't be seen as a pool of potential terrorists.
 - Such stigmatization of mental health can only agitate the community and not improve its rehabilitation.

HSAC Countering Violent Extremism (CVE) Meeting
April 14, 2016

- Health and behavior has many roots including biological, genetic, social, family, online behavior, community engagement, feelings of belonging, social bonds, constructive civic and political engagement.
- Social ecological approach
 - This model highlights the notion that the range of social contexts a person exists in (family, friends, school etc.) effects there overall mental health and acts within these certain contexts can affect other areas either positively or negatively.
- Other violent extremism attributes: Social bonds, identity, delinquency, trauma, individual resilience, violent community activities, in or outgroup activities, online behavior/health. To determine these factors, we looked at what, why and how they view things.
 - Also, we looked at how they perceive risk and what plays into the intervention strategies as to what works and what doesn't.
 - Constructive violent civic engagement- emerged highly as an indicator of radicalization.
 - Data on attitudes of certain communities towards violent activities has been largely absent and recent data has been difficult to obtain due to lacking community trust in such actions.
 - **Researchers found five distinct samples within groups**
 - **The largest group are politically engaged and anti-violent.**
 - **The second largest group are also politically engaged but expressed feelings of being disconnect to the American community and see violence as an acceptable means of action and engagement for things they believe in.**
 - Changing approaches to CVE issues are seen through many best practices in the world sphere.
 - Programs in Britain and Dutch have worked to bring law enforcement, social services, mental health professionals.
 - Singapore has also brought local Muslim communities into the fold with these other groups to form unified strategies in dealing with CVE issues.

Comments and Questions:

HSAC Countering Violent Extremism (CVE) Meeting
April 14, 2016

- Adnan Kifayat – Is it appropriate to view CVE as an addiction or filling that type of space? Could we recommend to deepen research of whether extremism has any backing as being an addiction of sorts?
 - Answer (Goldenberg): For 35 years we have seen young people engaged in violence. Not much has changed other than the fact that the message can get out quicker and in a much more dangerous manner and embodiment.

- Laila Alawa (Pop Culture/Millennials)
 - Will have the comprehensive list of big movers and shakers in social media and millennial centric communications channels later this week.
 - **CVE focused groups have largely been met with disinterests and discouragement with most millennials.**
 - People who have influence with millennials
 - Fouseytube
 - Date Malaik (one direction guy)
 - Lupa Fiasko
 - Dina Tokyo
 - Laila Ali (Boxer)
 - And many others
 - Cause related marketing incidences
 - Gram cracker commercial based on hatred and lack of community and had a women in a headscarf advocating for acceptance and happy feeling.
 - Got a lot of chatter, shares, and comments.
 - Peace House commercial
 - Responding to recent slew of hate speech. Video focused on showing the similarities between trump supporters and the rest of the community.
 - **Millennial influencers will be most effective if they can speak to their audiences on issues that mean something to them.**
 - I will be creating a pilot program to engage with diversity issues and bringing in Muslim American influencer and youth that can create positive diversity content to help lower barriers to engage with.

- Michael Nutter
 - We need greater accountability within the CVE landscape both on the federal level but also going all the way down to state and local government.
 - ARCI – Accountability Resources Cooperation Intel

HSAC Countering Violent Extremism (CVE) Meeting
April 14, 2016

- **The on the ground agencies need to report what their local level engagement is and that regular engagement and activities on the ground need to be apart of the review process and information pipeline.**
 - Compstat: A program that receives situational reports from on the ground agencies to their superiors on a regular basis.
 - Recommend for the Secretary to develop a similar program and ask for a situational report from components.
 -
- Resources
 - Very excited in reaching out philanthropic funding but we can't forget other funding option on the table.
 - I would suggest that the secretary should convene local leaders on a fairly regular basis to really drive home a CVE relationship and partnership.
- Cooperation
 - No one is going to have all the resources they need so partnership can multiple resources and allow for project fulfillment.
 - The secretary can do a lot to bridge barriers between groups and get them to want to cooperate.
 - Incentivize cooperation through having funding tied to such cooperation.
- Intelligence
 - Need to see better intelligence transfer between organizations so persons of risk can be better identified and engaged in an appropriate manner.

Discussion on Partnering with Industry

- Christopher Graves
 - Framework for communication strategies
 - Audience analysis
 - We find there is merit in looking at sub segmenting audiences.
 - Any communication strategy requires a layers of analysis.
 - *Righteous Minds* – a book about motivation for people not to change their minds and changing their view.
 - Cultural cognition, Yale Researcher, Kahan, is a model of a world view of communication strategies.

HSAC Countering Violent Extremism (CVE) Meeting
April 14, 2016

- Social Systems Analysis
 - Most people seek out likeminded persons who confirm the way they see the world. Understanding these systems can help us isolate at-risk groups.
- Motivated reasoning
 - **Notion that you can change minds through factual or evidence based approach is often impossible and such attempts will often consolidate persons point of view more towards their original perspective**
- Narrative transportation theory
 - Narratives labeled as fiction and with the correct immersion for the reader can be just as effective at changing minds as non-fiction approaches.
 - **Identifiable victim**
 - Human empathy is quickly depleted when applied on a large scale. Narratives focused on a single individual is much more convincing than narratives focused on the masses
 - The human brain better processes concrete, easily imagined language, it is more readily understood and more believable than language that gravitates towards abstractions.
 - Emotionally bound arguments are more important than a strong rational cogent argument.
 - Decision making is largely done with emotional parts of the brain.
 - These are our innate heuristic form of thinking (system 1 thinking)
 - Explaining why you did things is based on your rational side.
 - This requires more focused and rational thinking (system 2 thinking).
 - People don't want to change their minds due to a fear of being exiled from their community. This decision is not often based in evidence or fact based narratives.

HSAC Countering Violent Extremism (CVE) Meeting
April 14, 2016

- **To change minds you need a narrative that takes advantage of these elements and fact based/evidence based arguments are just not effective for changing minds.**
- Comments and Questions
 - Juan Zarate- How do we animate innovative messaging to provide the motivational ecosystem you described? What is the mechanics that can animate this type of communication and activity?
 - Answer (Graves) – People can sense when they are being messaged and this can lead to a big resistance to any packaged narrative. **The best solution is an organic peer-to-peer system where the message and narrative comes from organic influencers already in the community.**
 - These influencers need to have an organic desire to join your narrative and cannot be coopted by money or any other potentially corrupting issue.
 - Popularity is not what you want but instead you want influence. Popularity is someone who is known by many. Influence is someone who can motivate and produce real change and movement on an issue.
 - Nutter – What is an example or sample of a good message narrative within society today and what is an example of an ideal message platform and deliverer?
 - Answer (Grave) – The best message is not one that you seed but instead a message that grows from a community you are targeting.
 - Don't try to masquerade when you enter a community because if you do you will get unmasked and then lose all credibility.
 - Anything that feels like government working through a person is very unlikely to result in mass change. The more peer-to-peer messaging the better the messaging will likely be.
 - Learn as much as you can about the in-group. Learn their humor, norms, assumptions, etc, and then from that base you can build a palpable narrative and communication strategy.
 - Pandith – How does the government partner to create these solutions.
 - Answer (Graves) – Government should seek out partners that want to help and contribute to CVE. Government should empower those persons but be careful not to risk their legitimacy by making them look like government propagandists.

HSAC Countering Violent Extremism (CVE) Meeting
April 14, 2016

- Michael – What is an effective way to listen into different communities to gain the groundwork to make an alternative messaging package.
 - Answer (Graves) – Lookalike modeling is where you identify your ideal profile for your influencers and search for similar individuals.
 - We use “Social Labs” to engage in this data collection. We use social media to seek out patterns of behavior for how certain groups react to certain appeals. “Pattern recognition through meta-data approach”.
- Pandith – Where can we go to find out what Muslim millennials like, want, are buying, and what messages might resonate with them.
 - Answer (Graves) – Ogglve Noor does work in this space.

S&T Briefing on CVE Metrics and Assessments

Kathleen Deloughery

- CVE is a collection of problems, varying stakeholders, and thus requires multifaceted solutions.
 - Four mission areas for where researched is needed on CVE
 - Diversion
 - Diverting individuals off of radicalization at the earliest point possible.
 - Prevention
 - Through criminology studies how do we prevent and disrupt CVE recruitment and actions.
 - Mitigation
 - Changing the vulnerabilities and risk that communities face in CVE.
 - Resilience
 - Building communities against attacks and more importantly against recruitment.
 - Impacts whether people get radicalized in the future and if done right can create a positive feedback mechanism.
- S&T’s objective
 - Developing a CVE success matrix

HSAC Countering Violent Extremism (CVE) Meeting
April 14, 2016

- Identifying indicators for success
- Create knowledge
 - Research briefs
 - Increase community capacity to resist extremist activities.
- **CVE should not reinvent the wheel. Many groups aren't interested in CVE issues so the challenge isn't creating CVE approaches but instead incorporating CVE elements into existing structures which do related practices to what CVE attempts to target.**
 - Big part of our work is to gather information that is already out there and tap into the existing programs.
- CVE Pilot cities
 - Operational framework: 12 month project and was kicked off Oct. 2015.
 - Developed initial set of process and output metrics important to determine success.
 - In stage of starting to see if stakeholders are willing to participate with data collections and assess if the program is able to reach the desired end.
 - **Interviews with cities: Reached out to the US attorneys then leveraged Brian Murphy from the FBI to use the FBI field offices to assist with obtaining contacts in each of the cities.**
 - Boston – US Attorney's office, LA – DHS CVE office, ultimately was on S&T to determine who was engaged after that.
 - **Identifying individuals and organizations who are involved in the framework, who were not involved in the framework, and individuals that should be involved.**
 - **We interviewed police departments, some faith-based/NGO organizations, Imam/mosques, etc.**
 - When asked, where do you think you are? Two scenarios: CVE is the largest problem, level 0. Level 10: CVE is not an issue.
 - Average response is 3, what would be needed to see to transition from a 3 to a 5? Trying to find how to measure achievement.
 - Metrics on slide 13:
 - Both also
 - Identified mental health measures: number of referrals
 - Law enforcement: trust in law enforcement, use of force, etc
 - Suggestions are done by aggregating the suggestions across all stakeholders interviewed.

HSAC Countering Violent Extremism (CVE) Meeting
April 14, 2016

- Asking communities during discovery phase - Was is that you need? Was is it that you don't know? What will you need to be successful?
- Not much out there in terms best practices from mental health and CVE preventative measures.
- Final Project
 - Decision support for CVE practitioners
 - Stakeholders need validated assessments for identifying persons that need intervention from extremist behavior, and might succeed from alternatives to incarceration programs.

Comments and Questions:

- Nutter – In next funding round, DHS should ask how much of grant funding is going to go to CVE activities to make sure we find the programs that will have the largest CVE impact.

Page 1 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 1 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 2 of 2

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

**Homeland Security Advisory Council
Countering Violent Extremism Subcommittee Meeting
April 14, 2016**

Overview:

- You will be meeting with the Homeland Security Advisory Council's (HSAC) Countering Violent Extremism (CVE) Subcommittee.
- Your participation is as follows :
 - 11:30 a.m.: You arrive during the meeting and greet the Subcommittee.
 - 11:35 a.m.: You receive an in depth progress report from the co-chairs.
 - 11:45 a.m.: You make remarks and provide feedback to the group.
 - 12:00 p.m.: You depart.
- During the meeting, the CVE Subcommittee will hear from subject matter experts to discuss how the Department can best collaborate with technology and social media companies, philanthropic organizations, and education and mental health sectors to help counter violent extremism.
- The subcommittee is chaired by Farah Pandith, Adjunct Senior Fellow at the Council on Foreign Relations and Senior Fellow at the Kennedy School of Government at Harvard University, and Adnan Kifayat, Senior Resident Fellow, German Marshall Fund of the United States.

Discussion Points:

- You will have thirty minutes to meet with the CVE Subcommittee, hear their progress report, and receive an overview of the final report they will issue in June 2016.
- The Subcommittee is focused on six key areas regarding CVE efforts:
 - Research and Analysis
 - Communications and Messaging
 - Engaging with Technology and Social Media Companies
 - Funding and Resourcing Efforts
 - Incorporating the Education Sector
 - Incorporating the Mental Health Sector
- You should provide candid feedback and guidance to the group, specifically on their approach and overall direction of the report. The meeting is not open to the public, allowing you to speak freely and to fully leverage the expertise in the room.

Background:

- On January 21, 2016, you were briefed by the CVE Subcommittee co-chairs during the HSAC meeting at the Wilson Center.
- The CVE Subcommittee was established in December 2015 to act as an incubator of ideas for the Office for Community Partnerships, and to leverage outside expertise

and new thinking to allow the Department to go beyond how it has conventionally framed and envisioned CVE efforts.

- The CVE Subcommittee is comprised of members of the HSAC as well as a number of selected subject matter experts and key thought leaders from private industry, academia, and non-governmental organizations.

Participants:

Secretary Johnson

George Selim, Director, OCP

Sarah Morgenthau, Executive Director, Homeland Security Advisory Council, IGA/OPE

HSAC CVE Subcommittee Members

Attachments:

A. Agenda

B. Biographies

C. CVE Subcommittee Tasking Memo

D. CVE Subcommittee Federal Register Notice

Staff Responsible for Briefing Memo: Sarah Morgenthau, Executive Director, Homeland Security Advisory Council, IGA/OPE (b)(6)

OGC Reviewer: Attorney in Component Counsel or HQ, Title, Phone Number.

Developing Effective Counter-Narrative Frameworks for Countering Violent Extremism

Meeting Note
September 2014



Table of Contents

| | |
|-------------------------------|----|
| Introduction | 1 |
| Types of Narratives | 2 |
| Identifying the Right Message | 3 |
| Messenger | 4 |
| Target Audience | 6 |
| Conclusion | 10 |

Introduction

With the violent attacks of the Islamic State of Iraq and al-Sham (ISIS) gaining traction in Iraq and Syria and a media campaign that is nearly as aggressive, the need for effective counter-narrative strategies to prevent the spread of violent extremism and terrorism is more relevant than ever. While ISIS has since broken away from mainstream Al-Qaeda leadership, its origins in relation to Al-Qaeda have helped it quickly establish some legitimacy and authority among those they wish to radicalize and recruit. ISIS has also benefited from roots in Al-Qaeda in terms of inheriting a developed communications strategy, which ISIS has altered and improved to better fit their needs. This can be seen in the release of two online issues of Dabiq magazine during Ramadan (July 2014) and the press attention given to ISIS-related hashtags on Twitter such as #AllEyesOnISIS or #CalamityWillBeFallUS. In fact, recent discussions of Dabiq attribute a significant number of the magazine's messages to narratives from the former leader of the Al-Qaeda in Iraq, Abu Mus'ab al-Zarqawi.¹ In other words, the narrative of the self-proclaimed "Islamic State" relies in part on the narratives of Al-Qaeda. Thus, any analysis of the media strategy of ISIS, or attempts to counter its narrative, should also include an analysis of the organization that preceded it.

In an attempt to address some of the past and present concerns regarding counter-narratives against Al-Qaeda and related organizations, Hedayah (the International Center of Excellence for Countering Violent Extremism (CVE)) and the International Centre for Counter-Terrorism — The Hague (ICCT) organized a one and a half day roundtable expert meeting on "Developing Effective Counter-Narrative Frameworks for Countering Violent Extremism" in June 2014. The meeting brought together approximately 25 leading experts in the field that work in Afghanistan, Australia, Bangladesh, Canada, Georgia, Indonesia, Malaysia, the Netherlands, the United Kingdom and the United States. The discussions at the meeting built on a recently published background paper written by ICCT Research Fellow, Dr. Alex P. Schmid, in order to provide a starting point to identify the challenges with existing governmental and non-governmental counter-narrative frameworks against the violent extremist narrative espoused by Al-Qaeda, and to propose a number of ways forward.² The general outcomes of the expert meeting and recommendations for ways forward are described in the remainder of this meeting note.³

1 "Hot Issue: Dabiq: What Islamic State's New Magazine Tells Us about Their Strategic Direction, Recruitment Patterns and Guerrilla Doctrine." The Jamestown Foundation. http://www.jamestown.org/programs/tm/single/?tx_ttnews%5Btt_ne%20ws%5D=42702&cHash=0efbd71af77fb92c064b9403dc8ea838#.U-iv6E3lrIU (accessed September 16, 2014).

2 Schmid, Alex. "Al-Qaeda's "Single Narrative" and Attempts to Develop Counter-Narratives: The State of Knowledge." ICCT. <http://www.icct.nl/download/file/AP-Schmid-Al-Qaedas-Single-Narrative-January-2014.pdf> (accessed September 16, 2014).

3 The recommendations in this meeting note are based on discussions at the expert meeting and analysis by the author, and do not necessarily reflect the viewpoints of Hedayah or ICCT.

TYPES OF NARRATIVES

Before discussing the message, messenger, target audience and medium of counter-narratives, the participants established a baseline of the different types of counter-narratives relevant to Al-Qaeda and related organizations.

Positive/Alternative Narratives

Experts at the meetings discussed the terminology being used with regards to countering violent extremist narratives, noting that counter-narratives imply responding and reacting to these narratives. Participants warned that by only focusing on counter-narratives, Al-Qaeda has the upper hand, and that only reacting is doing too little, too late. It was recommended that so-called counter-narrative efforts should focus more on creating proactive, positive and alternative narratives.

Strategic Counter-Narratives

Strategic counter-narratives for broad audiences may be useful for governments or large, multi-lateral organizations wishing to condemn violent extremists and their efforts. However, participants also noted that, while strategic counter-narratives are often a necessary response to a crisis or an attack, these narratives are not necessarily intended on reaching the individuals that are already supporting Al-Qaeda and similar organizations.

Ethical Counter-Narratives

These types of narratives point out that violent action is not a moral way of achieving aims. They may be useful if the messenger has ethical or moral influence over the target audience. These arguments may not be religious in nature, but rather point out the commonalities between all humans, and call for a better cooperation between all nations and peoples.

Ideological and Religious Counter-Narratives

This type of counter-narratives may be useful if the messenger has religious authority in the target community. In the case of Al-Qaeda, this includes Islamic scholars, imams and community-based religious leaders. Participants noted that governments making religious arguments, especially Western governments, can be counter-productive, and the (credibility of the) messenger is especially important in this case.

Tactical Counter-Narratives

Tactical counter-narratives are those that emphasize that violence in the long run is often less effective when compared to more peaceful methods, and not useful to an organizations' overall reputation and objectives. This type of narrative can be used by a variety of messengers, including governments and community-based organizations. The main obstacle to success for this type of narratives is in providing an alternative that still allows for the individual, group or organization to potentially achieve their goals in a non-violent way.

Humor and Sarcasm

Participants noted that humor and sarcasm may be useful in de-legitimizing the narrative of violent extremists in certain instances. Participants gave the example of the film *Four Lions* as a pop-culture way of delegitimizing the violent extremist narrative through humor. However, it was also mentioned that there had been little work done in terms of assessing the impact of that film or how it was received by the public through a CVE lens. It was also suggested that using humor may not reach the intended target audience, and only reinforce the absurdity of terrorism to the general public that already does not support Al-Qaeda and similar organizations.

IDENTIFYING THE RIGHT MESSAGE

Setting Clear Objectives

Participants noted that one of the most essential components of designing a counter-narrative is to start with defining the objective. This was said to be important for both determining the content of the narrative, and also for measuring whether or not the narrative is effective. Participants identified several possible objectives of counter-narratives, including:

- Preventing violent extremism (changing behavior, namely violence and incitement)
- Preventing extremism (changing minds)
- Protecting one's country or region from violent extremist influence
- Preventing the violent extremist narrative from spreading

Learning from Al-Qaeda's narrative

Participants also discussed the need to learn from the Al-Qaeda narrative, and start with a clear understanding of the multi-layered messaging of Al-Qaeda before entering the counter-narrative development process. It was recommended that the content of counter-narratives should systematically and directly address the different components of the Al-Qaeda narrative. Discussions mentioned several key components of the Al-Qaeda narrative, including:

1. That a cherished world is under threat;
2. It is obligatory to defend that world from contamination;
3. That the treat has reached a critical point or crisis;
4. That violence is the only way to overcome the threat/contamination;
5. That action is obligatory according to Islam;
6. And that those fighting for the cherished world will receive a heavenly reward for doing so.

Participants agreed that some of these could be potential entry points in terms of counter-narratives, depending on the local context and

messenger.

Participants discussed some elements of the Al-Qaeda narrative that should also be incorporated into the counter-narrative, where relevant. The Al-Qaeda narrative is easy to understand, adaptable, and has a strong emotional and religious appeal. Al-Qaeda is also quick to respond to current events, and counter-narratives should be just as quick. Participants noted that if there is not a response within 24 hours to an event or action, this is perceived by the public and target audience as a non-response. Al-Qaeda's narrative also provides a clear solution (violence against the "enemy" to achieve its aims) to a real or perceived problem, which is often lacking in current counter-narratives. In other words, a call to action is an important component of any counter-narrative or positive/alternative narrative against Al-Qaeda.

Participants also noted that a clear, simple message is often more effective. In other words, there is no need to tell the whole story in order to get the message out; the message can leave the audience to make certain assumptions and interpretations on the missing details. However, it was also noted that the Al-Qaeda narrative is thought-provoking and generates debate, and counter-narratives should therefore not be overly-simplistic.

Some of these lessons in terms of the Al-Qaeda narrative are also applicable to countering the ISIS narrative, particularly online. For example, the ISIS narrative uses strong emotional messages, carried out through posting photos on Twitter and in Dabiq of their perceived successes and the atrocities of its enemies. ISIS has also developed a strategy for responding quickly to current events and using social media to recruit and radicalize. ISIS uses the Twitter app called the "Dawn of Glad Tidings" to inform its followers on the latest news of the group, and more importantly, create a synchronized Twitter

campaign through user accounts that is capable of sending thousands of tweets controlled by one or two media managers into cyberspace in an instant.⁴ This means that ISIS has mastered the ability to get the message out quickly, and with very little effort. Recent statistical analysis of #AllEyesOnISIS corroborates this suggestion—that a low number of tweeters using this hashtag accounted for a large amount of the hashtag’s activity.⁵ Finally, the ISIS narrative utilizes a clear, and perhaps more tangible call to action than even Al-Qaeda can claim; joining the organizations means traveling to Iraq or Syria to fight in an ongoing physical battle.

Flexibility and Creativity in Counter-Narrative Design

In designing counter- and positive narratives, participants noted that there needs to be more of an emphasis on flexibility; narratives will not be perfect the first time, and more should be done in terms of allowing the narratives to be shaped and changed in an organic process. However, it was mentioned that creative and flexible narratives are often challenging to produce, particularly if the narratives are being funded by bureaucratic government agencies. In order to adhere to standards of measurement and evaluation for this type of funding, counter-narrative designers often do not have enough flexibility to respond creatively.

In the current context of ISIS and the speed of social media interactions, flexibility seems to be especially applicable. Grassroots counter-narratives movements against ISIS have seemingly capitalized on this strategy; responding to ISIS trapping the Yezidi community in the mountains and advances on Erbil in early August 2014 with #Yezidis/#Yazidis and #TwitterKurds respectively. Moreover, as a response to the beheading of American journalist James Foley by ISIS members, the hashtag #ISISMediaBlackout began trending

on Twitter.⁶ The hashtag has maintained some popularity after the subsequent beheadings of American journalist Steven Sotloff and David Haines, a British citizen and aid worker.

At the expert meeting, there was also a discussion regarding using counter-narratives as a starting point for interactive debate. However, it was also pointed out that this interactive debate requires listening, and a real response to the narrative that considers the points being made (rather than complete rejection). This sort of two-way discussion is only possible, however, if there is secure space to do so in terms of accessibility to the violent extremist narrative, and legal ability for messengers to interact.

With regards to creativity, the participants also noted that expertise on messaging, particularly internet messaging, already exists in the private sector, for example, through marketing firms, technology companies and public relations strategists. Participants recommended that the private sector be included with policymakers, practitioners and the community in the discussion of creating specific counter-narratives against Al-Qaeda. It was recommended that all of these actors be convened to work together to create a better and more effective counter-narrative.

MESSENGER

Local messengers

Participants generally agreed that credible voices at the grassroots level are needed to counter the everyday messaging of violent extremist organizations. Participants also emphasized that face-to-face interactions are still very important, even in a society where Internet access is high. One participant recommended that social network analysis may be useful in determining how ideas spread within a

4 Berger, J.M.. “How ISIS Games Twitter.” The Atlantic. <http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/> (accessed September 16, 2014).

5 “Analyzing the ISIS.” War on the Rocks. <http://warontherocks.com/2014/06/analyzing-the-isis-twitter-storm/> (accessed September 16, 2014).

6 The Washington Post. “#ISISMediaBlackout goes viral following purported execution of James Foley.” Washington Post. <http://www.washingtonpost.com/news/checkpoint/wp/2014/08/19/isismediablackout-goes-viral-following-purported-execution-of-james-foley/> (accessed September 16, 2014).

community, and that this analysis would be a good baseline for identifying the appropriate messengers.

Victims of Terrorism

There was general agreement that the stories of victims of terrorism can be powerful voices against the violent extremist narrative. However, it was also noted that the effectiveness of these narratives have not decisively been shown, and – given the sensitive nature and potential detrimental effect of such initiatives on victims’ physical and emotional well-being – more research was needed to determine if victims’ narratives prevented individuals from joining violent extremist organizations or encouraged them to move away from political violence.

Former Violent Extremists

Participants also discussed whether or not former members of violent extremist organizations were effective messengers for counter-narratives. Whilst there have been past attempts at incorporating formers’ narratives into counter-narratives (for example, the Against Violent Extremism (AVE) Network), there are also many obstacles in engaging in discourse with former Al-Qaeda operatives, both practical and legal ones. Participants suggested that it was difficult to find former Al-Qaeda members who are willing to speak out against the organization. It was also noted that there are many legal obstacles to engaging with former violent extremists who are incarcerated, which means that willing former members are not always reachable. It was also discussed that in some cases formers do not want to participate in counter-narratives because they want to put that part of their life behind them, and do not want to remind others of their previous activities.

Youth

Participants agreed that youth in most contexts are not just recipients of counter-narratives, but can be powerful generators of counter-narratives. One participant mentioned that crowd-sourcing on social media or other online platforms could be one way of generating and delivering youth-based content for counter-narratives.

Governments

There was also a discussion regarding the idea that governments are not always the most credible voice. On the other hand, participants remarked that governments generally have a large degree of authority over the general population, and their narratives may be effective at reaching a larger audience. Finally, it was also noted that government action may be more powerful than words, and governments should consider the performative effect of their actions and the (counter-) narrative these feed into. In other words, counter-terrorism measures and responses to a situation are alternative or counter-narratives by themselves.

Protecting the Messengers

There was also a discussion of protecting the safety and security of those who present the counter-narratives and alternative narratives as being a high priority for those working on the topic. Direct engagement in a battle of ideas against Al-Qaeda and its affiliates can put individuals and groups in danger of being targeted, both physically and emotionally. For example, outspoken civil society or religious leaders may become targets of future attacks. Former violent extremists may be seen by Al-Qaeda as traitors, and could quickly become a target if their personal security is not guaranteed. Moreover, when working with victims of terrorism who speak out against violent

extremism, it is important to keep in mind that they might be subject to harassment in online forums or social media. Similarly, the stories and narratives of victims and survivors of terrorism can be emotionally draining, and facilitators should be careful that they are not re-traumatized by telling their story too many times.

It was strongly agreed that there should be special care to ensure humane and sensitive treatment towards those volunteering to be messengers for counter-narratives to Al-Qaeda, including those involved in videos and messages online. This includes involving the messenger in pre-production strategy and design; ensuring the products offer a rounded and honest reflection of them rather than being an exaggerated view for the purpose of achieving CVE aims; allowing messengers to maintain editorial control of products they feature in; ensuring the messengers are part of the production process rather than a commodity; ensuring their physical safety; providing support and shielding against inevitable trolling and online attacks that will emerge; and giving them the opportunity to be part of the roll out and delivery process.

TARGET AUDIENCE

Participants agreed that in terms of the target audience, there should be a focus on the communities that relevant actors identify as vulnerable to violent extremism. These communities could be geographically based (i.e. local), or globally based (i.e. online, social media etc.). Communities might also include those who feel connected to a war or conflict in a foreign country, regardless of the individuals' country of origin or nationality.

The main recommendation that came out of the discussions with regards to the target audience was that more research is needed to understand how a specific target audience responds to certain ideas. This research can help tailor the arguments and narratives to the audience.

Questionnaires about the target audience may be one tool that could accomplish this. It was also suggested that the target audience should be involved at all stages of developing the counter-narrative to enhance the effectiveness of that counter-narrative's reception.

Finally, it was noted that in terms of Al-Qaeda's strategy for their own target audience, Al-Qaeda and similar organizations have goals on three levels. First, they aim to gain passive support from the general public, at very least that the general public does not actively aid their enemy. Second, they aim to recruit sympathizers to their cause. Finally, they seek to turn sympathizers into active supporters. With these three goals in mind, participants recommended that counter-narratives should address these different target audiences, and approaches should be adapted accordingly.

Medium

Discussions on effective mediums for counter-narratives resulted in a general agreement that there is too much focus on the Internet as the medium for counter-narratives. While participants agreed that the Internet alone, including social media, is an effective tool, they also noted that radio, SMS, newspapers and print media are still major and sometimes the main forms of communication in many countries. Therefore, the medium itself should, as with other components of the counter-narrative, be adapted to fit the local context. There was also a discussion of finding the right entry points into the community for counter-narratives. The message has to be available in the spaces (physical and virtual) that are frequented by the target audience in order for it to have any effect.

Participants also noted that the medium of the narrative is not limited to forms of media; that some violent extremists also use cultural elements and symbols, including public rallies, popular

bands and concerts, t-shirts, figurines, flags and symbols. In other words, participants recommended that countering the narrative of Al-Qaeda and similar organizations also means creating alternative symbols, images and cultures. The use of creating a culture has been especially prevalent in ISIS' media campaign as of late—ISIS banners have been seen in numerous countries around the world, including in Europe and the United States, and there have been reports of ISIS t-shirts, figurines and flags available for purchase online.⁷

Along these same lines, participants noted that celebrities and sports stars may be effective in producing counter-narratives from a cultural aspect. Participants discussed how music could be an effective tool for counter-narratives. However, at the same time some participants noted that in some cases, some types of musical expression are forbidden by Al-Qaeda leaders, and may not be as effective at reaching the target audiences.

Participants suggested that in terms of the Internet, counter-narratives should also include counter-imaging and counter-videos. The Al-Qaeda narrative utilizes images with strong emotional appeal, including graphic violence used against those they deem as innocent; counter-narratives may be effective if they exploit the injustices that Al-Qaeda uses to achieve their aims. With regards to YouTube videos, it was recommended that the videos remained short and to the point; unnecessary information risks losing the attention of the viewer. Participants recommended that thumbnails and ads could be utilized to help connect viewers to material that provides more information, and that the comments section of YouTube videos is often just as important as the video itself.

⁷ "The Perfect Gift for the Jihadi on Your Shopping List." Vocativ. <http://www.vocativ.com/world/Iraq-world/can-now-buy-isis-hoodie-online/> (accessed September 16, 2014).

Programs and Projects on Counter-Narratives

Participants agreed that there have been many meetings on communications and counter-narratives, but there is very little to show in terms of tangible outcomes and concrete follow-up. Moreover, there is currently no sustainable or long-lasting effort to create and coordinate counter-narratives.

Participants generally expressed their concern over the lack of real programs working on counter-narratives to violent extremism (including Al-Qaeda), and funding associated with these programs. In order to address this concern, the participants' brainstorming produced more than a dozen different project ideas. Some of the project and program outlined are more concrete (planned), while others are in initial stages. The main highlights are listed below:

1. Communication Exposition for CVE

Hedayah and the Global Counter-Terrorism Forum (GCTF) plan to host a Communications Exposition to bring together approximately 200 technical experts, government officials, civil society and community leaders, and communications experts too share tools, strategies and products for countering the narrative of violent extremists, including Al-Qaeda.

2. Testing the effectiveness of the Test EMI-20 instrument on Al-Qaeda narratives and counter-narratives.

This tool is designed to assess the presence of extremism, but needs rigorous testing before it can be distributed. The tool can be found here: <http://www.icct.nl/download/file/ICCT-Schmid-Violent-Non-Violent-Extremism-May-2014.pdf>.

3. Providing social media training against hate speech and hate crimes and other manifestations of extremism.

One existing program aims to teach youth skills to build their own counter-messages that are aimed at their peers in their own communities. The project now is aimed at preventing travel to Somalia and Syria in the US context, but could be expanded to other localities, where relevant.

4. Expanding on grassroots counter-narratives online to include animated videos for distribution on social media.

This program is in a pilot stage, and is currently being tested. Utilizing some of the existing online animation tools, these videos focus on refuting Al-Qaeda narratives by challenging their facts and raising questions about their interpretations of current affairs. They also focus on raising doubts of violent extremist actions. Because they are produced using existing online animation tools, they can be generated quickly in response to current events (See: www.abdullahx.com).

5. Training local actors on technical capabilities of counter-narratives.

This sort of training could include capabilities on smart phones (such as video recording), social media tools, or online animation and translation tools. Participants also emphasized that once a training program is established, training should focus on training trainers as force multipliers. Governments and the private sector can work together to design the training program in a way that is tailored to local audiences, while using the latest technical capabilities.

6. Creating dialogue within the communities on violent extremism to generate counter-narrative content.

This could be done in a number of ways. For example, one participant suggested presenting a case study on how an individual is radicalized (based on a real-life case) and discussing with the community how they could/would/should intervene to prevent violent extremism, as well as the tools they would need to intervene. Another suggestion would be to present an actual narrative (such as a video, magazine or speech) of Al-Qaeda to a group of youth or students, and asking the audience to identify the main differences between the Al-Qaeda narrative and their own religious understanding. This could be followed by a discussion focused on creating counter-narratives. A third suggestion, which is based on an existing program, brings groups together from opposing communities in a conflict whereby both sides have a vested interest in peace. Together, they can produce those counter-narratives that would be most effective at overcoming further polarization and conflict between the two groups.

7. Engaging journalists and civil society to work together on how stories are presented in the media.

One participant suggested a roundtable of media representatives with civil society representatives to discuss the ways in which media conveys ideas in their community that is in support of, rather than working against, efforts to counter violent extremism. Another participant suggested to provide training on conflict-sensitive journalism to journalists reporting in areas of violent extremism.

8. Creating a central hub for information on counter-narratives.

This would include tracking existing narratives and creating a platform for community dialogue on counter-narratives. This could also potentially include a data hub of information on the target audiences that would be selected for receiving the

counter-narratives. The hub could also include a training component for communities (especially youth) for tracking target audiences online.

9. Developing legal tools for allowing communities to work on counter-narratives

This includes promoting a legal space for individuals and groups interested in countering the Al-Qaeda narrative to do so in a way that does not make those working on the counter-narratives in terms of interacting with hard Al-Qaeda messengers seem like a security threat.

10. Lecture series on violent extremism and related topics with university students.

In areas where recruitment into Al-Qaeda occurs in universities, a lecture series that debates and debunks myths of Al-Qaeda may be useful. This lecture series would allow students to engage in critical debates of the morality, legality and effectiveness of the actions of Al-Qaeda and affiliated groups, including the atrocities of the violence that Al-Qaeda uses against other Muslims.

11. Systematic unmasking of Al-Qaeda's claims and half-truths.

This counter-narrative campaign would delegitimize Al-Qaeda by fact-checking the claims and premises of Al-Qaeda on an on-going basis and debunking claims by Al-Qaeda based on theological, historical, humanitarian argumentation.

12. CVE messaging through sports league.

Utilizing sports leagues as a way to reach the community, the messaging campaign of the current program has three main components. First, the messaging campaign directly involves local sports leagues (existing) and trains coaches

on CVE messaging. Second, the messaging campaign takes advantage of the live matches, where players themselves are also trained on CVE messages in pre- and post-match presentations. Third, the live broadcast of the matches on TV and radio provides an additional opportunity for the CVE messages to be reinforced and projected.

13. Mobile theatre troops in madrasas and orphanages.

This helps to address youth recruitment into Al-Qaeda by developing live theatre performances to address push and pull factors in rural areas where the Internet, social media, radio and TV are less effective. The theatre focuses on face-to-face engagement with youth, and engages the youth in discussions of violent extremism (particularly suicide bombing) based on the local context.

CONCLUSION

The meeting clarified that countering the narrative of Al-Qaeda is at least as important as controlling and diminishing its violence, since Al-Qaeda's narrative brings new recruits into its ranks. The meeting also elucidated some important recommendations and tools for setting up and improving counter-narrative frameworks, as well as tangible programs that could be carried out in the counter-narrative field. Moreover, as shown with examples from ISIS and their media campaign, these suggestions and tools may also be applicable beyond the main Al-Qaeda group, and also apply in other manifestations of violent extremism.

Attractive alternative narratives can contribute to the prevention of radicalization and recruitment if they are delivered to the target audience by trusted sources. It is vital that such narratives are based on parallel actions that alone can bestow credibility to a narrative. It was agreed that working on the community level was key; community leaders that are informed of potential radicalization and recruitment to violent extremism in their own communities are better partners in efforts to counter violent extremism in those communities. Current thinking and action on counter-narratives and alternative narratives is still fragmented and program development and implementation under-resourced. Governments can provide the tools and resources for monitoring and countering extremism, assist communities in creating a space for counter-narratives, be open and transparent in their efforts to stand up to Al-Qaeda and related organizations, and address genuine and realistic grievances that may contribute to radicalization and recruitment.

Factsheet:
A Comprehensive U.S. Government Approach to Countering Violent Extremism

The nature and range of terrorist and violent extremist threats has evolved quickly, in a media environment that often seizes on the sensational. As a society it is vital for all of us to come together to channel the positive energy of communities, and the private sector toward building a greater sense of awareness, engagement, and resilience.

Policy Context

In August 2011, the White House released *Empowering Local Partners to Prevent Violent Extremism in the United States*, the first national strategy to prevent violent extremism domestically. In December 2011, a corresponding Strategic Implementation Plan outlined the specific steps departments and agencies will take to achieve the strategy's central goal of preventing violent extremists and their supporters from radicalizing, recruiting, or inspiring individuals or groups in the United States to commit acts of violence.

Successfully preventing violent extremism requires a range of tools beyond traditional law enforcement activities. CVE often involves undercutting terrorist ideologies and local drivers of radicalization, and it is therefore equally if not more important that civil society and non-governmental actors participate, particularly given government's legal and credibility limitations in this space. As such, the underlying premise of a comprehensive approach to countering violent extremism in the United States includes two key provisions: (1) local communities are the solution to violent extremism; and (2) consideration must be provided for each community's local dynamics.

At the federal level, the Department of Homeland Security (DHS), the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and the National Counterterrorism Center (NCTC) are implementing the strategy by working together with other agencies to ensure a coordinated, whole-of-government approach. In the field, local governments and law enforcement agencies continue to build relationships within their communities through established community policing and community outreach mechanisms. In this respect, decades of community-based problem solving, local partnerships, and community-oriented policing provides a basis for addressing violent extremism as part of a broader mandate of community safety, with an emphasis on crime prevention.

What is CVE?

The term "Countering Violent Extremism" refers to efforts focused on preventing all forms of ideologically based extremist violence, to include prevention of successful recruitment into terrorist groups. It is distinct from disruptive actions which focus on stopping acts of terrorism by those who have already subscribed to violence.

CVE efforts include awareness building, counternarrative measures, and intervention programs:

- **Violent extremism awareness:** programs that build awareness of the violent extremism (such as briefings on radicalization, recruitment, and indicators).
- **Counternarrative measures:** programs or messages that directly address and counter the violent extremist recruitment narrative (such as encouraging community-led counternarratives online).
- **Intervention measures:** programs that facilitate intervention in a person’s pathway to radicalization before the line of criminal activity is crossed (such as community-led intervention models).

Broad community outreach and engagement efforts, made in the effort to address civil rights protections, or advance common community goals (such as bullying prevention or anti-gang efforts) that are conducted for the purpose of building stronger communities, and not explicitly CVE, can nonetheless have important CVE benefits by reducing alienation of vulnerable minority populations and assisting in developing integrated and resilient communities.

Role of Local Partners

CVE efforts rely heavily on well-informed and equipped families, local communities, and local institutions. Communities play a strong role in CVE efforts—they are the first line of defense against violent extremists, and are best suited to lead in both counternarrative and intervention measures. Communities have more credibility than government to challenge the ideological underpinnings of violent extremist groups, and they are more suited to know when and how to engage with a vulnerable individual. .

Community Engagement on CVE

The U.S. Government has conducted outreach in various cities across the country with law enforcement, public safety officials, and directly to communities around the threat of violent extremism and terrorist recruitment. They have used certain “CVE Tools” that include the Community Awareness Briefing (CAB), as well as the Community Resilience Exercise (CREX).

- The Community Resilience Exercise (CREX) is a half-day table-top exercise designed to improve communication between law enforcement and communities and to share ideas on how best to build community resilience. DHS’s Office for Civil Rights and Civil Liberties (CRCL) and NCTC have worked with U.S. Attorneys and other local partners to implement this exercise—which involves an unfolding scenario of possible violent extremist activity—in cities across the United States.
- The Community Awareness Briefing (CAB) is a presentation designed to help communities and law enforcement develop understanding of violent extremist recruitment tactics and explore ways to collectively prevent and address such public safety threats at the local level. It is updated continually with new information or from feedback. Due to the growing number of individuals traveling to foreign conflicts, such

as Syria and Iraq, the Community Awareness Briefing now includes information relating to the foreign fighter recruitment. The Community Awareness Briefing has been conducted by multiple U.S. cities over the past few years.

“Three Region” Pilot Program

Over the past several months, non-governmental and governmental stakeholders in the Greater Boston region, Los Angeles, and Minneapolis-St. Paul have been collaborating to develop locally-driven prevention frameworks that best address the unique issues facing their communities. In the same way local partners have developed frameworks to address drug and gang prevention, they are developing frameworks to address violent extremism prevention. This pilot encourages stakeholders to collectively evaluate solutions and determine resources and expertise available or needed to implement those solutions.

Local stakeholders— which include public health professionals, mental health experts, educators, faith-based leaders, non-governmental organizations and local, state and federal government - are in the best position to identify needs and gaps in services, assess existing local programs, leverage existing networks, define and develop measurable goals and implement solutions.

The Federal Government’s role is to marshal efforts and, as appropriate, provide support to communities so they may enhance their ability to respond to the needs of individuals and families.

Importance of Intervention Options

There are important non-law enforcement efforts that communities can take to engage with vulnerable individuals before they turn to extremist violence. We can learn from intervention approaches in other situations, such as gang prevention. CVE intervention aims to use the same principles and we can make real progress by adapting the kinds of programs we are using in non-counterterrorism areas for our needs. Some examples of successful programs include:

- Montgomery County, MD, where communities and law enforcement are collaborating to bring together faith-based leaders, as well as education and mental health officials to help at-risk youth.
- The World Organization for Resource Development and Education (WORDE), partnered with the Montgomery County Chief of Police to set up an intervention board. This program has successfully convened local government resources, such as mental health professionals and school officials, as well as interfaith leaders who help with religious counseling. The intervention board receives referrals from the community, and the board identifies accessible government and community resources.
- Also, the Muslim Public Affairs Council released their Safe Spaces Initiative, which is essentially a guide for community centers on how to deal with violent extremism in their communities using a phased approach of prevention, intervention, and ejection.

Counternarratives

- Communities have also taken a lead in creating counternarratives to violent extremists. For instance, Somali communities in Minneapolis have created The Truth About Al Shabaab and Broken Dreams to highlight the bankrupt ideology of this terrorist group. And communities are utilizing social media to challenge ISIL online.

Portions of this document are unreadable, a readable copy is attached.

ISIS IN AMERICA



FROM RETWEETS TO RAQQA

Lorenzo Vidino and Seamus Hughes
December 2015

Program on Extremism
THE GEORGE WASHINGTON UNIVERSITY

ISIS IN AMERICA: FROM RETWEETS TO RAQQA

Lorenzo Vidino and Seamus Hughes
December 2015

Program on Extremism

THE GEORGE WASHINGTON UNIVERSITY

CONTENTS

| | | |
|--|---|---------------------|
| Acknowledgments | ▪ | v |
| Foreword | ▪ | vii |
| Executive Summary | ▪ | ix |
| Introduction | ▪ | 1 |
| A Snapshot of ISIS in America | ▪ | 5 |
| From Keyboard Warriors to Battlefield Commanders: Understanding the Spectrum of ISIS in America | ▪ | 15 |
| Conclusion | ▪ | 33 |
| Appendix | ▪ | 35 |

Illustrations

| | | |
|--|---|--------------------|
| 1. Young (left) and Dakhllalla | ▪ | 1 |
| 2. Young's Twitter account | ▪ | 1 |
| 3. ISIS Recruits in the U.S. Legal System | ▪ | 6 |
| 4. Excerpt from missing persons report filed by family of the Somali-American teens | ▪ | 8 |
| 5. Tweet posted by the 16-year-old Denver girl | ▪ | 8 |
| 6. Reposted by one of the Denver girls on Tumblr on the anniversary of their failed trip | ▪ | 8 |
| 7. Hoda Muthana's high school yearbook portrait | ▪ | 9 |
| 8. Muthana on life in the caliphate, January 2015 | ▪ | 9 |
| 9. El Gammal, December 2013 | ▪ | 10 |
| 10. Samy identifies himself: excerpt from El Gammal's criminal complaint | ▪ | 10 |

(continued on next page)

Illustrations, continued

11. Soofi (left) and Simpson ■ [10](#)
12. Usaamah Abdullah Rahim ■ [11](#)
13. Amiir Farouk Ibrahim’s American passport ■ [11](#)
14. Douglas McCain, aspiring rapper turned jihadist ■ [12](#)
15. Hanad Abdullahi Mohallim’s Twitter profile ■ [12](#)
16. Abdullah Ramo Pazara (right) in Syria ■ [12](#)
17. Abu Muhammad al Amriki explains his defection to ISIS ■ [13](#)
18. One of Abu Khalid al Amriki’s final tweets ■ [13](#)
19. News of Abu Khalid al Amriki’s death circulates on Twitter ■ [13](#)
20. Abu Abdullah al Amriki ■ [14](#)
21. ISIS announces Abu Abdullah al Amriki’s death ■ [14](#)
22. Moner Abu Salha, a.k.a. Abu Hurayra al Ameriki ■ [16](#)
23. Ariel Bradley celebrates the Chattanooga shootings ■ [16](#)
24. Snapshot of life in the caliphate: image from Ariel Bradley’s Instagram account ■ [17](#)
25. Mohammed Hamzah Khan on Twitter ■ [20](#)
26. Elton Simpson pledges allegiance to ISIS before his attack ■ [21](#)
27. The Radicalization Echo Chamber ■ [22](#)
28. Examples of ISIS supporters’ imagery on social media ■ [23](#)
29. Clockwise: A user announces a new account; examples of node, shout-out, and amplifier accounts ■ [24](#)
30. Clockwise: Interjecting in the #BlackLivesMatter conversation; sharing a quote from Anwar al Awlaki; dismissing ISIS critics as “coconuts” ■ [25](#)
31. From the U.S. to Syria: Abdullah Ramo Pazara ■ [27](#)
32. Nader Saadeh ■ [28](#)
33. Alaa Saadeh ■ [28](#)
34. Samuel Topaz on Facebook ■ [28](#)
35. Facebook post by Mohamed Saeed Kodaimati ■ [29](#)
36. Mohamed Saeed Kodaimati ■ [29](#)
37. Shannon Maureen Conley ■ [30](#)
38. Christopher Lee Cornell ■ [31](#)

ACKNOWLEDGMENTS



About the Program on Extremism

ens extremism research as a distinct field of study. The Program aims to develop pragmatic policy solutions

FOREWORD

by Jane Harman

Foreign Affairs

have to leave their basements to find extremist messages.

ISIS in America

ISIS in America

clear, one size doesn't fit all. Homegrown terrorists don't fit a single profile. Using social media, our enemies can



in America: From Retweets to Raqqa

ISIS Jane Harman is president and chief executive of the Woodrow Wilson Center in Washington. She represented California's 36th Congressional District for nine terms.

EXECUTIVE SUMMARY

-

-

thizers. The Program on Extremism has identified some

-

-

of primary content, some (the “amplifiers”) just retweet

-
-
-
-
-
-

-

offline dynamics complement one another.

-

-

- The profiles of individuals involved in ISIS-related ac

involvement with ISIS varies significantly, ranging from

INTRODUCTION

officer, was a sophomore chemistry major at MSU.



FIG. 1 Young (left) and Dakhllalla



FIG. 2 Young's Twitter account.

Subbanabu Wa Ta'ala, Arabic for "The most glorified, the highest"]."

1. WAPT News, "2 Mississippi Residents Charged with Trying to Join ISIS: Jaelyn Delshaun Young, Muhammad Oda Dakhllalla Arrested," August 12, 2015.
2. *United States of America v. Jaelyn Delshaun Young and Muhammad Oda Dakhllalla*, Criminal Complaint (August 8, 2015).
3. Ibid.
4. Ibid.
5. Ibid.

mujabideen

conflicts (e.g. Bosnia and Chechnya) or provided material

out the 2000s and early 2010s varied significantly in terms of their profiles, organizational affiliations, and operational

its affiliates, others were nothing more than sympathizers

From Hijackings to Hashtags: The Evolution of Jihadism in America

and its affiliates have been thwarted over the last decade),

-
6. WAPT News, "2 Mississippi Residents Charged with Trying to Join ISIS: Jaelyn Delshaun Young, Muhammad Oda Dakhllalla Arrested," August 12, 2015.
 7. An inherently controversial and arguably improper term, "jihadism" refers to the ideology adopted by groups such as al Qaeda and ISIS. The authors are aware that the term "jihad" has a number of meanings and that most Muslims use the term in ways different than these groups.
 8. J.M. Berger, *Jihad Joe: Americans Who Go to War in the Name of Islam* (Washington DC: Potomac Books, 2011).
 9. See Lorenzo Vidino, "Homegrown Jihadist Terrorism in the United States: A New and Occasional Phenomenon?," *Studies in Conflict & Terrorism* 32, no. 1 (January 2009): 1-17.
 10. For more on jihadist networks in the U.S., see Brian Michael Jenkins, "Stray Dogs and Virtual Armies Radicalization and Recruitment to Jihadist Terrorism in the United States Since 9/11," RAND Corporation, Occasional Paper, 2011.; Risa A. Brooks, "Muslim 'Homegrown' Terrorism in the United States: How Serious Is the Threat?" *International Security* 36, no. 2 (Fall 2011): 7-47.; Charles Kurzman, "Muslim-American Terrorism in the Decade Since 9/11," Triangle Center on Terrorism and Homeland Security, February 2012.; Scott Matthew Kleinmann, "Radicalization of Homegrown Sunni Militants in the United States: Comparing Converts and Non-Converts," *Studies in Conflict and Terrorism* 35, no. 4 (2012): 278-297.; Jerome P. Bjelopera, "American Jihadist Terrorism: Combating a Complex Threat," Congressional Research Service, January 23, 2013.; Charles Kurzman, "Muslim-American Terrorism: Declining Further," Triangle Center on Terrorism and Homeland Security, February 1, 2013.; Jessica Zuckerman, Steven P. Bucci, and James Jay Carafano, "60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism," The Heritage Foundation, July 2013.; and Lorenzo Vidino, "From KSM's Genius to Sheer Amateurism: The Post-9/11 Evolution of the Terrorist Threat in the United States," in Bruce Hoffman and Fernando Reinares, eds., *The Evolution of the Global Terrorist Threat: From 9/11 to Osama bin Laden's Death* (Columbia University Press, 2014), 3-28.
 11. Testimony of Robert S. Mueller, III, Director of the Federal Bureau of Investigation, United States Senate, *Annual Worldwide Threat Assessment*, Select Committee on Intelligence, February 5, 2008.

are significantly smaller than in most European countries.

and its various affiliates but also the Taliban, Pakistan's
fighting in foreign conflicts, particularly in Afghanistan,

hadist scene," assuming a coherent one exists, is signifi

This figure clearly indicates that a small but
significant number of American citizens and residents

flict in Syria, the successes achieved on the ground by

ed more than 25,000 foreign fighters from more than 100

residents have become foreign fighters in Syria and Iraq, a

-
12. Jack Cloherty and Pierre Thomas, "Attorney General's Blunt Warning on Terror Attacks," *ABC News*, December 21, 2010.
 13. Charles Kurzman, "Muslim-American Terrorism in 2013," Triangle Center on Terrorism and Homeland Security, February 5, 2014, p. 2.
 14. Scott Shane, "Homegrown Extremists Tied to Deadlier Toll than Jihadists in U.S. Since 9/11," *The New York Times (NYT)*, June 24, 2015.
 15. United Nations' Security Council, "Action Against Threat of Foreign Terrorist Fighters Must be Ramped Up, Security Council Urges in High-Level Meeting," 7453rd Meeting (AM), May 29, 2015.
 16. Peter R. Neumann, "Foreign Fighter Total in Syria/Iraq Now Exceeds 20,000; Surpasses Afghanistan Conflict in the 1980s," The International Centre for the Study of Radicalisation and Political Violence (ICSR), January 26, 2015.

Searching for Answers

The numbers in the U.S., while similarly difficult to measure precisely, are significantly lower than those in

travel to Syria to participate in the conflict.”

later, the Office of the Director of National Intelligence es

traveled or attempted to travel to the conflict area, a few

fighters is small compared to those who sympathize with

ine every aspect of such a complex and fluid phenomenon,

The report consists of two parts. The first examines all the United States for ISIS-related activities since the first

Publicly available information confirms a sharp surge

-
17. Testimony of Michael B. Steinbach, Assistant Director of the FBI, *Terrorism Gone Viral: The Attack in Garland, Texas and Beyond*, House Homeland Security Committee, June 3, 2015.
 18. Barbara Starr, “A Few Dozen Americans’ in ISIS Ranks,” *CNN*, July 15, 2015.
 19. Tom Vanden Brook, “ISIL Activity Drives up Pentagon Threat Level,” *USA Today*, May 8, 2015.
 20. Kevin Johnson, “Comey: Feds have Roughly 900 Domestic Probes about Islamic State Operatives,” *USA Today*, October 23, 2015.

CHAPTER 1

A Snapshot of ISIS in America

Statistics on ISIS Recruits in the U.S. Legal System

plaints, indictments, affidavits, and courtroom transcripts.

Individuals our researchers identified were classified into three categories: Legal Cases, "At-Large," and

Defying any cookie-cutter profile of the American ISIS

a plethora of verifiable information on these individuals.

Individuals' affiliations to ISIS were relatively clear, allowing re

Age

identified by the Program on Extremism as having connections

rested. Some of these individuals are identified by name,

was Tairod Pugh, a former Air Force officer who was 47 at

The final (also non-comprehensive) category con

well-identified individuals who have died under various

identified persons who are allegedly American who have died fighting in Syria and/or Iraq.

Legal Status

Gender

Converts

Use of Informants/Stings

desire to build a strict Islamic society), others are specific

enforcement officer. Since 9/11, the FBI has regularly

Time Frame

Travel Abroad

Location

Domestic Terror Plot

-
21. Department of Justice, "Transcript of Assistant Attorney General John P. Carlin's Briefing at the Foreign Press Center on the Foreign Terrorist Threat and Other National Security Issues," September 28, 2015.
 22. See, for example, Saltman and Smith, "'Till Martyrdom Do Us Part,'" ISD and ICSR, May 2015. See also Edwin Bakker and Seran de Leede, "European Female Jihadists in Syria: Exploring an Under-Researched Topic," International Centre for Counter-Terrorism—The Hague (ICCT), April 2015.
 23. Erin Marie Saltman and Melanie Smith, "'Till Martyrdom Do Us Part': Gender and the ISIS Phenomenon," Institute for Strategic Dialogue (ISD) and ICSR, May 2015, p. 70.
 24. Pew Research Center, "Converts to Islam," July 21, 2007.
 25. Johnson, "Comey: Feds have Roughly 900 Domestic Probes about Islamic State Operatives," *USA Today*, October 23, 2015.

personnel and funds—to fighters in Syria and Iraq.

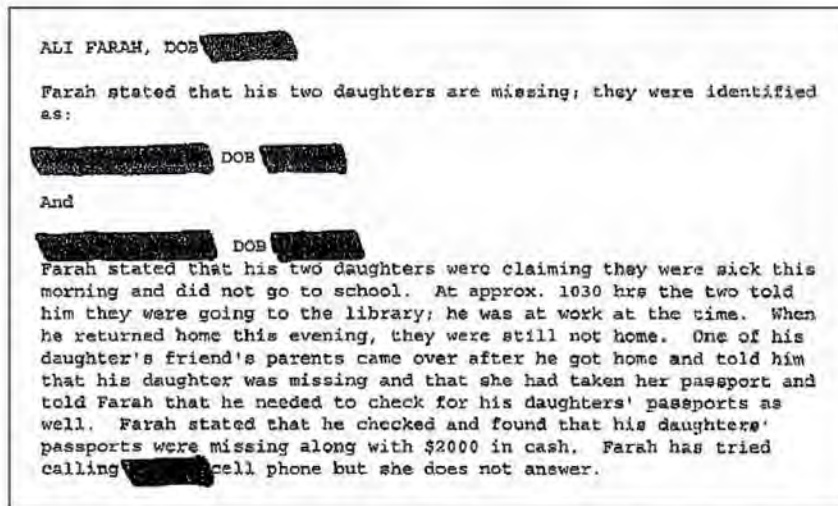
Recruits Who Remain “At-Large”

linked to ISIS is much larger. Our researchers identified a

Waqqas, an influential recruiter within ISIS’s online net
nom de guerre

“At-Large” cohort have no common profile.

Hijrah to the Islamic State



ALI FARAH, DOB [REDACTED]

Farah stated that his two daughters are missing; they were identified as:

[REDACTED] DOB [REDACTED]

And

[REDACTED] DOB [REDACTED]

Farah stated that his two daughters were claiming they were sick this morning and did not go to school. At approx. 1030 hrs the two told him they were going to the library; he was at work at the time. When he returned home this evening, they were still not home. One of his daughter's friend's parents came over after he got home and told him that his daughter was missing and that she had taken her passport and told Farah that he needed to check for his daughters' passports as well. Farah stated that he checked and found that his daughters' passports were missing along with \$2000 in cash. Farah has tried calling [REDACTED] cell phone but she does not answer.

FIG. 4 Excerpt from missing persons report filed by family of the Somali-American teens.



FIG. 5 Tweet posted by the 16-year-old Denver girl.

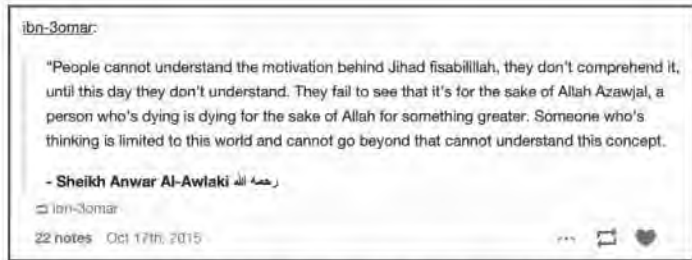


FIG. 6 Reposted by one of the Denver girls on Tumblr on the anniversary of their failed trip.

26. Islamic State of Iraq and Syria (ISIS), “Hijrah to the Islamic State: What to Packup, Who to Contact, Where to Go, Stories & More,” 2015.

of four Western passports with the caption, “Bonfire soon,

bijrab

As profiled in a *BuzzFeed*

Scotland who made headlines as one of the first Western

Under the pretense of going to Atlanta for a college field trip, Muthana boarded a flight to Turkey.

Australian foreign fighter named Suhan al Rahman (a.k.a.



FIG. 7 Hoda Muthana's high school yearbook portrait.



FIG. 8 Muthana on life in the caliphate, January 2015.

27. Ellie Hall, “Inside The Online World Of Three American Teens Who Allegedly Wanted To Join ISIS,” *BuzzFeed News*, October 27, 2014.
28. Jesse Paul and Bruce Finley, “Parents Reported \$2,000 Missing as Teens Headed to Join Islamic State,” *The Denver Post*, October 21, 2014.
29. Ellie Hall, “Gone Girl: An Interview With An American In ISIS,” *BuzzFeed News*, April 17, 2015. Information in the proceeding article was integrated with interviews conducted by the Program on Extremism’s staff.
30. Jon Anderson, “Hoover Woman Joins ISIS: Meet Hoda Muthana who Fled U.S. to Syria,” *AL.com*, April 20, 2015.
31. Ashley Fantz and Atika Shubert, “From Scottish Teen to ISIS Bride and Recruiter: The Aqsa Mahmood Story,” *CNN*, February 24, 2015.
32. Hall, “Gone Girl,” *BuzzFeed News*, April 17, 2015.
33. *Ibid.*
34. *Ibid.*
35. *Ibid.*

Once he joined ISIS in Syria, Samy's phone and computer were temporarily confis



FIG. 9 El Gammal, December 2013.

The Deceased: Uncle Sam's Shaheed

profile. For clarity purposes, this cohort was or

26. On or about January 16, 2015, approximately eleven days before his scheduled departure from the United States, CC-1, via social media, contacted CC-2.⁴ The following exchange occurred, in substance and relevant part:

| | | |
|-------------|------|--|
| 1/16, 17:05 | CC-1 | As-Salamu Alaikum Ateyya my name is Samy, I'm Gammal's friend. He told me you could help me with a career opportunity in Istanbul. I'll be visiting soon to look for an internship for the summer inshaAllah. I'd really appreciate your help. Please reply whenever you get the chance. BarakAllahu feek [may Allah bless you] [emphasis added] |
|-------------|------|--|

FIG. 10 Samy identifies himself: excerpt from El Gammal's criminal complaint.

Killed in America

Elton Simpson Nadir Hamid Soofi

to travel to Somalia to fight for al Shabaab.

Usaamah Abdullah Rahim

was shot and killed by local police officers in his hometown after charging



FIG. 11 Soofi (left) and Simpson

36. *United States of America v. Ahmed Mohammed El Gammal*, Criminal Complaint, (August 20, 2015).

37. *Ibid.*

38. *Ibid.*

39. *Ibid.*

40. Matt Pearce and Nigel Duara, "Texas Gunman's Mother: 'He Just had a Normal American Upbringing,'" *Los Angeles Times*, May 5, 2015.

41. Eugene Volokh, "Why Elton Simpson, One of the Texas Shooters, had Been Acquitted of an Earlier Terrorism-Related Offense," *The Washington Post*, May 4, 2015.

42. Elliott C. McLaughlin, "ISIS Jihadi Linked to Garland Attack has Long History as Hacker," *CNN*, May 7, 2015.

notified of his death in December 2014.

Killed in Syria/Iraq and Clearly Identified
Sixto Ramiro Garcia

His family was notified of his



FIG. 12 Usaamah
Abdullah Rahim

Amiir Farouk Ibrahim

Yusuf Jama



FIG. 13 Amiir Farouk Ibrahim's American
passport.

43. *United States of America v. David Wright and Nicholas Rovinski*, Criminal Complaint, (June 12, 2015). See also Susan Zalkind and Katie Zavadski, "Boston's Wannabe Beheader 'Liked' ISIS Enough to Kill," *The Daily Beast*, June 3, 2015.

44. *Ibid.*

45. *United States of America v. Asher Abid Khan*, *Arraignment/Detention Hearing*, (June 1, 2015).

46. *Ibid.*

47. *Ibid.*

48. Betsy Hiel and Carl Prine, "Pittsburgh Man Reportedly Dead in Syria," *WPXI.com*, July 26, 2013.

49. Bill Roggio, "American Passport Found at al Qaeda Base in Northern Syria," *The Long War Journal*, July 23, 2013.

50. Laura Yuen, Mukhtar Ibrahim and Sasha Aslanian, "Called to Fight: Minnesota's ISIS Recruits," *Minnesota Public Radio (MPR) News*, March 25, 2015.

51. *Ibid.*

52. Yuen, Ibrahim and Aslanian, "Called to Fight," *MPR News*, March 25, 2015.

53. *Ibid.*

Douglas McCain

was identified by the passport in his pocket, was report

Abdirahmaan Muhumed

a Quran and a rifle captioned “Sham.”

Hanad Abdullahi Mohallim

Abdullah Ramo Pazara

Omar al Shishani and led a brigade of fighters of Balkan



FIG. 14 Douglas McCain, aspiring rapper turned jihadist.



FIG. 15 Hanad Abdullahi Mohallim's Twitter profile.



FIG. 16 Abdullah Ramo Pazara (right) in Syria.

-
54. Cassandra Vinograd and Ammar Cheikh Omar, “American Douglas McArthur McCain Dies Fighting for ISIS in Syria,” *NBC News*, August 26, 2014.
 55. Ibid.
 56. Mukhtar Ibrahim, “Jihad in Syria Lures Somalis from Minnesota,” *MPR News*, June 12, 2014.
 57. Ibid.
 58. Michael Walsh, “ISIS Terrorist from Minnesota Worked at Major American Airport: Report,” *New York Daily News*, September 3, 2014. See also Mukhtar Ibrahim and Peter Cox, “Douglas McArthur McCain, A Man with Minnesota Ties, Killed in Syria,” *MPR News*, August 7, 2014.
 59. Laura Yuen, Mukhtar Ibrahim and Sasha Aslanian, “From MN Suburbs, They Set out to Join ISIS,” *MPR News*, March 25, 2015.
 60. Andrea Huncar, “3 ISIS Recruits from Edmonton Believed Killed,” *Canadian Broadcasting Corporation (CBC) News*, January 16, 2015.
 61. *United States of America v. Hodzic, et al.*, Indictment, (February 5, 2015).
 62. Robert Patrick, “Allegations of St. Louis Terrorism Support Rooted Back in Bosnian War,” *St.LouisToday.com*, April 11, 2015. See also Radio Sarajevo, “U Siriji Poginuo Ramo Pazara, Komandant Džihadista iz BiH,” September 25, 2014.
 63. SAFF, “U Siriji Poginuo I Ramo Pazara iz Teslića,” September 24, 2014.; Radio Sarajevo, “U Siriji Poginuo Ramo Pazara, Komandant Džihadista iz BiH,” September 25, 2014.; *Slobodna Bosna*, “Ramo Abdullah Pazara: Sprski Ratnik i Islamski Fanatik,” February 19, 2015.

Killed in Syria/Iraq and Not Clearly Identified

mation on individuals identified as Americans in ISIS pro
paganda who reportedly died either fighting or as suicide

One of these individuals is a man who identified
kunya **Abu Muhammad al Amriki**



FIG. 17 Abu Muhammad al Amriki explains his defection to ISIS.

*Revealing the Treachery of
Jabhat al Nusra*



FIG. 18 One of Abu Khalid al Amriki's final tweets.

Speaking in English in front of the black ISIS flag,

Abu Khalid al Amriki

used at least five distinct Twitter accounts to spread his
views. The little that is known about his offline persona



FIG. 19 News of Abu Khalid al Amriki's death circulates on Twitter.

64. YouTube, "Revealing the Treachery of Jabhat al Nusra," February 10, 2014.

65. Alastair Jamieson, "Alleged American ISIS Commander Abu Muhammad Al-Amriki Killed: Reports," *NBC News*, January 28, 2015.

in a video produced by one of ISIS's official media outlets (camouflage and a bandana and holding an AK-47 rifle al Cambodi), a prominent Australian foreign fighter and

stated, "You fly a remote control plane halfway across the

Two unidentified individuals who used *kunyas*

Abu Dawoud al Amriki

of one of its official media outlets, Al Bayan Radio, in **Abu Abdullah al Amriki**



FIG. 20 Abu Abdullah al Amriki



FIG. 21 ISIS announces Abu Abdullah al Amriki's death.

66. Lauren Williams, "Meeting a Daesh jihadist in Syria," *The Saturday Paper*, July 18, 2015. Our research team attempted to identify Abu Khalid's alleged American wife but was unsuccessful. According to court records, he did at some point communicate with Keonna Thomas, an American arrested in the U.S., but there is no indication that their relationship was anything more than an online friendship.
67. Aaron Y. Zelin, "al-Hayāta Media Center Presents a New Video Message from The Islamic State: 'Stories From the Land of the Living: Abū Khālid al-Kambūdi,'" *Jihadology.net*, April 21 2015.
68. Assabah.com, "American Suicide Bomber Abu Dawoud in the Ranks of 'Daesh: The Iraqi Army Takes on the Battle to Retake Tikrit," March 4, 2015.
69. Ibid.
70. "ISIS says American suicide bomber carried out Iraq attack," *Al Arabiya*, August 19, 2015.

CHAPTER 2

From Keyboard Warriors to Battlefield Commanders: Understanding the Spectrum of ISIS in America

vious section show, the profiles of American ISIS sympa

financing, or fighting—are extremely diverse. Ranging from grown men who had flirted with jihadist militancy

officer to a single mother of two young children, these in

Syrian conflict. Many were outraged by the appalling

who were not Muslim—and led some to take the first

around fulfilling perceived religious obligations, such as *hijrah*

71. Colonel John M. “Matt” Venhaus, U.S. Army, “Why Youth Join al-Qaeda,” *United States Institute of Peace*, May 2010.



FIG. 22 Moner Abu Salha, a.k.a. Abu Hurayra al Ameriki

sive profile in *BuzzFeed News*

“She was definitely always looking for love,” said a for

“When I first met her she was a Christian, and then she was

and personal fulfillment.”

who is the first American known to have died in a suicide

married and had a child. Likely under the influence of her

In contrast, he described life fighting in Syria as

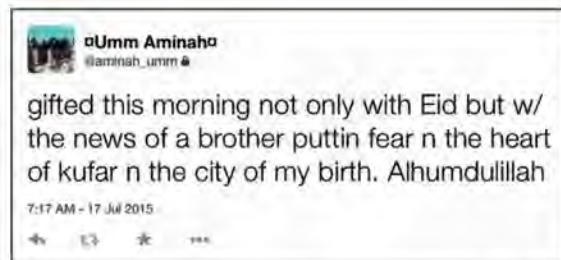


FIG. 23 Ariel Bradley celebrates the Chattanooga shootings.

-
72. Testimony of Nicholas J. Rasmussen, Director, National Counterterrorism Center, *Countering Violent Extremism: The Urgent Threat of Foreign Fighters and Homegrown Terror*, House Homeland Security Committee, February 11, 2015.
 73. Mona El-Naggar and Quynhanh Do, “Video Released of U.S. Bomber in Syria,” *New York Times*, July 31, 2014.
 74. Ibid.
 75. Ellie Hall, “How One Young Woman Went From Fundamentalist Christian to ISIS Bride,” *BuzzFeed News*, July 20, 2015.
 76. Ibid.

Still, it is difficult to fully comprehend the complex

which killed five military personnel in her hometown,

in sha Allah
Emaan *Kuffr*

dynamics that influence U.S.-based ISIS sympathizers.

The Role of Social Media

for something to define herself, an identity to cling to.”



FIG. 24 Snapshot of life in the caliphate: image from Ariel Bradley’s Instagram account.

77. Hall, “How One Young Woman Went From Fundamentalist Christian to ISIS Bride,” *BuzzFeed News*, July 20, 2015.

78. *Ibid.*

way for potential recruits to find like-minded indi

Officials in the U.S. have expressed similar concerns.
The Terrorist Threat to the US Homeland,

The spread of radical—especially Salafi—Internet

to the possibility that others may become sufficient

Violent Islamist Extremism, the Internet, and the Homegrown Terrorist Threat

can they find a great deal of information there, but

-
79. Tim Stevens and Peter R. Neumann, “Countering Online Radicalisation: A Strategy for Action,” ICSR, March 16, 2009, p. 12.
 80. Netherlands’ Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Ministry of International Affairs and Kingdom Relations), “Jihadis and the Internet,” Netherlands’ National Coordinator for Counterterrorism, February 2007, p. 91.
 81. United States Office of the Director of National Intelligence, National Intelligence Council, “The Terrorist Threat to the US Homeland,” *National Intelligence Estimate*, July 2007.
 82. U.S. Senate Committee on Homeland Security and Governmental Affairs (HSGAC), “Violent Islamist Extremism, the Internet, and the Homegrown Terrorist Threat,” May 8, 2008.

tremist figures or significant events.”

U.S. officials have repeatedly highlighted how ISIS uses social media to reach a significantly wider audience

Grooming from Afar

New York Times

propaganda, you had to go find it. Find where
Inspire

Inspire

to Islam, Alex was motivated by a “horrified curiosity” to

-
83. Similar findings were reached in this report. See also National Counterterrorism Center, “Radicalization Dynamics: A Primer,” September 2010, p. 18; HSGAC, “Zachary Chesser: A Case Study in Online Islamist Radicalization and Its Meaning for the Threat of Homegrown Terrorism,” February 16, 2012.
 84. Testimony of James B. Comey, Director, Federal Bureau of Investigation (FBI), Senate Select Committee on Intelligence, *Counterterrorism, Counterintelligence, and the Challenges of “Going Dark,”* July 8, 2015.
 85. Ibid.
 86. Ryan J. Reilly, “If You’re Trying To Join ISIS Through Twitter, The FBI Probably Knows About It,” *Huffington Post*, July 9, 2015.
 87. Rukmini Callimachi, “ISIS and the Lonely Young American,” *NYT*, July 27, 2015.
 88. Ibid.
 89. Ibid.



FIG. 25 Mohammed Hamzah Khan on Twitter.

Times

Travel Agents

Times

church. But, behind closed doors, she was a full-fledged

old sister had also been active online, trying to find ways she communicated with an English-speaking ISIS fighter

time on her computer, her grandmother confiscated her elec

90. Rukmini Callimachi, "ISIS and the Lonely Young American," *NYT*, July 27, 2015.

91. *Ibid.*

92. Janet Reitman, "The Children of ISIS," *The Rolling Stone*, March 25, 2015.

93. *Ibid.*

94. *United States of America v. Mohammed Hamzah Khan*, Criminal Complaint (October 6, 2014).

bafiz bafiza

The Echo Chamber

Devil on the Shoulder

Americans Elton Simpson and Nadir Soofi to attack the

tact with a well-known British foreign fighter, Abu Hussain

fied as American supporters of ISIS.

Individuals were coded as Americans if they self-identified

kunya

Simpson and Soofi then drove from Arizona to Garland in a vehicle loaded with assault rifles, body armor, and other weapons. Before the attack, Simpson tweeted a final time, using a hashtag

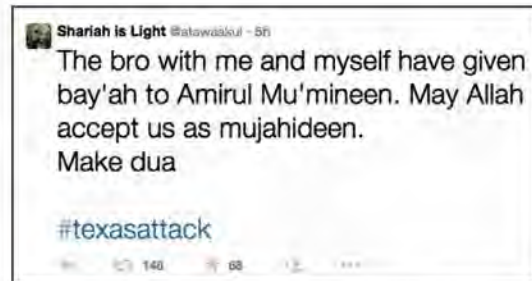


FIG. 26 Elton Simpson pledges allegiance to ISIS before his attack.

95. Kevin Sullivan, "Three American Teens, Recruited Online, Are Caught Trying to Join the Islamic State," *The Washington Post*, December 8, 2014.
96. Jethro Mullens and Ted Rowland, "Who is Mohammed Hamzah Khan?," *CNN*, October 7, 2014.
97. Scott Shane, "Texas Attacker Left Trail of Extremist Ideas on Twitter," *NYT*, May 5, 2015.
98. Jim Sciutto, Pamela Brown, Paul Cruickshank and Paul Murphy, Texas attacker tweeted with overseas terrorists, *CNN*, May 5, 2015.
99. Rita Katz, "The Power of a Tweet: Elton Simpson and the #TexasAttack," *SITE Intelligence Group (SITE)*, May 5, 2015.
100. Katz, "The Power of a Tweet" *SITE*, May 5, 2015.
101. Pierre Thomas, Mike Levine, Jack Date and Jack Cloherty, "ISIS: Potentially 'Thousands' of Online Followers Inside US Homeland, FBI Chief Warns," *ABC News*, May 7, 2015. The term has also been used by Assistant Attorney General John Carlin: United States Department of Justice, "Assistant Attorney General John P. Carlin Delivers Remarks on Domestic Terrorism at an Event Co-Sponsored by the Southern Poverty Law Center and the George Washington University Center for Cyber and Homeland Security's Program on Extremism," October 14, 2015.

FIG. 27
THE RADICALIZATION ECHO CHAMBER

The figure is a collage of various social media posts and images. At the top left, there is a photo of a person holding a flag with Arabic text. Next to it is a photo of a lion with the caption 'Dabiq witness'. To the right is a tweet from 'Aashir al amriki' dated July 3, with the text 'Contact me on telegram : brothers only, Inshallah.' Below this is a tweet from 'Abu Sa'ad Al-Amriki' dated July 29, mentioning '4th Account, Suspend, I will just return!' and '#DieInYourRageKuffar'. In the middle left, there is a tweet titled 'BAQIYA SHOUTOUT #6' with a colorful graphic. To its right is a photo of a hand holding a grenade with 'HAVE A NICE DAY' written on it. Below that is a tweet from 'Abu Cowboy' dated June 12, stating 'Hijrah does not stop as long as there is still jihad'. In the bottom left, there is a tweet from 'at Amriki' with the text 'Guilty of what? When will we begin to stand up and let the entire world hear "Yes, I am honored to have been chosen?"'. To its right is a tweet from 'abdullah al-american' dated June 12, asking for prayers for migration. Below that is a tweet from 'Umm Nazaral' dated June 14, mentioning a deleted account. To the right of that is a photo of a man with a beard and a 'PERF' sticker. In the bottom right, there is a tweet from 'Abu Sa'ad Al-Amriki' dated June 8, warning about FBI informants. Other elements include a photo of a woman in a headscarf, a photo of a person in a dark setting, and a photo of a fire.

belonging to an American was reaffirmed on a few occa



A significant number of American ISIS supporters use avatars of black flags, lions, and green birds.



FIG. 28 Examples of ISIS supporters' imagery on social media.

jihad

102. McNeil tweeted a screenshot of his Twitter suspension (at the time, his 14th suspension). He neglected to remove a small part of his Google ID, which led to a number of Google+ pages. After reviewing the videos on each page, a link was found to a video posted on YouTube, which was subsequently linked to a Facebook profile with his real name and location. One of his Facebook status updates from last year matched with materials from his 10th Twitter account prior to suspension.
103. The term "green bird" indicates a status one reaches when he or she dies (becomes a *shabeed*, or martyr) and reaches *jannah*, or heaven. It is a scriptural reference from a *hadith*, or reported saying from the prophet Mohammad, that celebrates the virtues of martyrdom. Jihadists term fallen comrades "green birds" to eulogize them as pious, faithful Muslims.

fluctuate over time. Reflecting these dynamics, their ac

fiers, and shout-outs.

nodes

news articles, and official ISIS tweets, allowing them to

Amplifiers

ating a new account becomes increasingly difficult, leading some to turn to others for assistance. The user's first tweet is often an image of the Twitter notification of suspension,

shout-out



FIG. 29 Clockwise: A user announces a new account; examples of node, shout-out, and amplifier accounts.

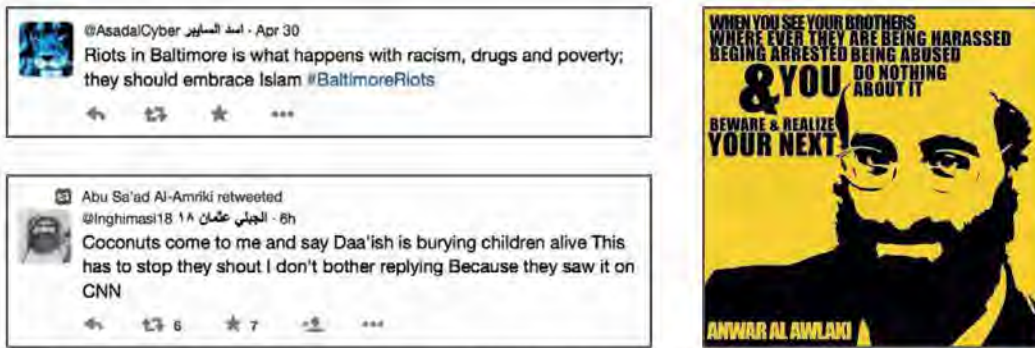


FIG. 30 Clockwise: Interjecting in the #BlackLivesMatter conversation; sharing a quote from Anwar al Awlaki; dismissing ISIS critics as “coconuts.”

104. Our researchers include a number of Arabic speakers who reviewed Arabic-language accounts for individual who self-identified as American and found a small contingent of Americans using Arabic as their primary language.

105. Justine Drennan, “Islamic State Supporters Urge Baltimore Rioters to Join Extremist Cause,” *Foreign Policy*, April 28, 2015.

these scenarios, online and offline dynamics complement

Real-World Clusters: ISIS's Den in America

form at the margins of radical mosques, Salafist orga

a significantly more nuanced reality in which the impor

typical of the European reality, occurs on a significantly

analysis revealed that while some individuals fit the pro
file of the "lone actor," others were part of a cluster of

als whose radicalization was confined to the virtual space,

Americans traveling to fight in conflict zones is not a new

small groups, the first wave providing moral and logistical

an attempt to stem travel to conflict areas.

Minneapolis was unique to the Somali conflict. This con

106. B. Todd Jones, "Operation Rhino," *Office of the United States Attorneys*, July 8, 2015.

one of the first to leave Minneapolis to join al Shabaab, becoming a

who later departed for Somalia to join the fight.

While the Minneapolis cohort has received significant media



emir

FIG. 31 From the U.S. to Syria: Abdullah Ramo Pazara

lars, which they sent to Pazara and families of ISIS fighters in the

107. Paul McEnroe, Abby Simons and Libor Jany, "From the Heartland to Jihad: How a Group of Young Men from Minnesota Were Drawn Into ISIL's Campaign of Terror," *Minnesota StarTribune*, September 20, 2015.
108. McEnroe, Simons and Jany, "From the Heartland to Jihad," *Minnesota StarTribune*, September 20, 2015.
109. Yuen, Ibrahim and Aslanian, "Called to Fight," *MPR*, March 25, 2015.
110. Robert Patrick, "Allegations of St. Louis Terrorism Support Rooted Back in Bosnian War," *St. Louis Post-Dispatch*, April 11, 2015.
111. Patrick, "Allegations of St. Louis Terrorism Support Rooted Back in Bosnian War," *St. Louis Post-Dispatch*, April 11, 2015. See also Radio Sarajevo, "U Siriji Poginuo Ramo Pazara, Komandant Džihadista iz BiH," September 25, 2014.
112. Robert Patrick, "Woman Pleads Guilty in Terror Funding Case with St. Louis Ties," *St. Louis Post-Dispatch*, September 28, 2015.

goods, tactical gear and clothing, firearms accessories, optical equipment and range finders, rifle scopes, equip

while fighting against Kurdish forces in Kobane in the fall

group. The five spent their days absorbing, discussing, and



FIG. 32 Nader Saadeh



FIG. 33 Alaa Saadeh



FIG. 34 Samuel Topaz on Facebook.

113. *United States of America v. Ramiz Zijad Hodzic, et. al.*, Indictment (February 5, 2015).

114. Associated Press (AP), "Bosnian Immigrants Plead Not Guilty in Terror Financing Case," *Yahoo! News*, February 11, 2015; Radio Sarajevo, "U Siriji Poginuo Ramo Pazara, Komandant Džihadista iz BiH," September 25, 2014.; SAFE, "U Siriji Poginuo i Ramo Pazara iz Teslića," September 24, 2015.; Slobodna Bosna, "Ramo Abdullah Pazara: Srpski Ratnik i Islamski Fanatik," February 18, 2015.

115. *United States of America v. Alaa Saadeh*, Criminal Complaint (June 26, 2015).

116. *Ibid.*

117. The Program on Extremism has decided not to disclose details about these cases so as not to compromise any potential investigation.

Wide Spectrum of Support Roles

of Abdullah Ramo Pazara, researchers identified a number



FIG. 35 Facebook post by Mohamed Saeed Kodaimati.



FIG. 36 Mohamed Saeed Kodaimati

118. *United States of America v. Mohamad Saeed Kodaimati*, Criminal Complaint (April 23, 2015).
119. Kristina Davis, "San Diegan Accused of Hiding ISIS Links," *The San Diego Union-Tribune*, April 23, 2015.
120. *United States of America v. Mohamad Saeed Kodaimati*, Criminal Complaint (April 23, 2015).
121. Ibid.
122. Ibid.
123. Ibid.
124. Ibid.

to the U.S. but was prevented from boarding his flight in



FIG. 37 Shannon Maureen Conley

out of the church's campus, causing church officials to

Conley stated she wanted to wage jihad against "kafir" in
A certified nurse, she

crut is Shannon Conley, a Colorado native who first
appeared on the radar of the FBI Denver Field Office fol

fighters and admitted to owning *Al Qaida's Doctrine for
Insurgency: Abd Al-Aziz Al-Muqrin's A Practical Course for
Guerilla War*
ISIS fighter on Skype, who pushed her to join him in Syria

125. *United States of America v. Mohamad Saeed Kodaimati*, Criminal Complaint (April 23, 2015).

126. *Ibid.*

127. *Ibid.*

128. *Ibid.*

129. *Ibid.*

130. *United States of America v. Shannon Maureen Conley*, Criminal Complaint (April 9, 2014).

131. *Ibid.*

132. *Ibid.*

133. *Ibid.*

134. *Ibid.*

135. *Ibid.*

136. *Ibid.*



FIG. 38 Christopher Lee Cornell

semi-automatic rifles and approximately 600 rounds of

installations in Chattanooga in July 2015 left five dead.

arrested while attempting to board a flight to Germany at

137. Michael Martinez, Ana Cabrera and Sara Weisfeldt, "Colorado Woman Gets 4 Years for Wanting to Join ISIS," *CNN*, January 24, 2015.
138. AP, "Teachers: Ohio Man Accused in Terror Plot a Typical Student," *WHSV.com*, January 15, 2015.
139. Ben Brumfield, Pamela Brown and Dana Ford, "FBI Says Plot to Attack U.S. Capitol was Ready to Go," *CNN*, January 15, 2015.
140. Brumfield, Brown and Ford, "FBI Says Plot to Attack U.S. Capitol was Ready to Go," *CNN*, January 15, 2015.
141. Kimball Perry and Patrick Brennan, "Father: Terror Plot Suspect was a 'Momma's Boy,'" *Cincinnati.com*, January 23, 2015.
142. *United States of America v. Christopher Lee Cornell*, Criminal Complaint (January 14, 2015).
143. *Ibid.*
144. *Ibid.*
145. Jonathan Dienst and Miguel Almaguer, "Mohammad Youssef Abdulazeez Downloaded Recordings from Radical Cleric, Officials Say," *NCB News*, July 21, 2015.
146. Greg Jaffe, Cari Wade Gervin and Thomas Gibbons-Neff, "Tenn. Gunman Used Drugs, Struggled with Clash of Faith," *The Washington Post*, July 18, 2015.
147. Abby Ohlheiser, "What we Know about Alton Nolen, Who as been Charged with Murder in the Oklahoma Beheading Case," *The Washington Post*, September 30, 2014.

attacked four New York Police Department officers with

an ISIS-affiliated Australian jihadist, a white supremacist,

pressure cooker filled with nails.

-
148. Michael Pearson, "Who is Oklahoma Beheading Suspect Alton Nolen?," *CNN*, September 30, 2014.
 149. Agence France-Presse, "New York Police Brand Hatchet Attack 'Terrorist' Act," *Yahoo News!*, October 24, 2015.
 150. Caitlin Nolan, Kerry Burke, Rocco Parascandola, Joseph Stepansky and Thomas Tracy, "Hatchet-wielding Man Shot Dead by NYPD Cops in Queens; Police Eye Possible Terrorism Motive," *New York Daily News*, October 24, 2014.
 151. Garrett Pelican, "Orange Park Man, 20, Indicted in 9/11 Memorial Bomb Plot," *First Coast News*, September 15, 2015.
 152. Katie Zavadski, "'Terrorist' Troll Pretended to be ISIS, White Supremacist, and Jewish Lawyer," *The Daily Beast*, September 11, 2015.
 153. *United States of America v. Joshua Ryne Goldberg*, Criminal Complaint (September 10, 2015).

CONCLUSION

Countering ISIS's American Recruits

tal but insufficient on its own. Moreover, many early-stage

ISIS territory. On a more mundane level, others find them

Our research identified 71 ISIS recruits in the U.S. legal system—a figure far short of the 250-plus Americans who, according to government officials, have attempted to or ac

ter to action. For some that will mean boarding a flight

targeting the “infidels” inside America.

sponse. Because there is no standard recruit profile,

makers, law enforcement officials, civic leaders, teachers,

graphic data and personality profiles surveyed in this report,

154.

immunity for some returning foreign fighters, as their mes

tality of life under ISIS firsthand or finding a more positive outlet for the quest that led them to ISIS in the first place. U.S. officials would do well to provide avenues for their stories to be amplified to help dissuade would-be recruits.

APPENDIX

The 71 individuals charged for ISIS-related activities (as of November 12, 2015)

Mufid Elfgeeh

What explains the recent surge in American jihadi recruits? Who are the Americans lured by the siren songs of ISIS's propaganda? How do they embrace such radical ideology? What do they seek?

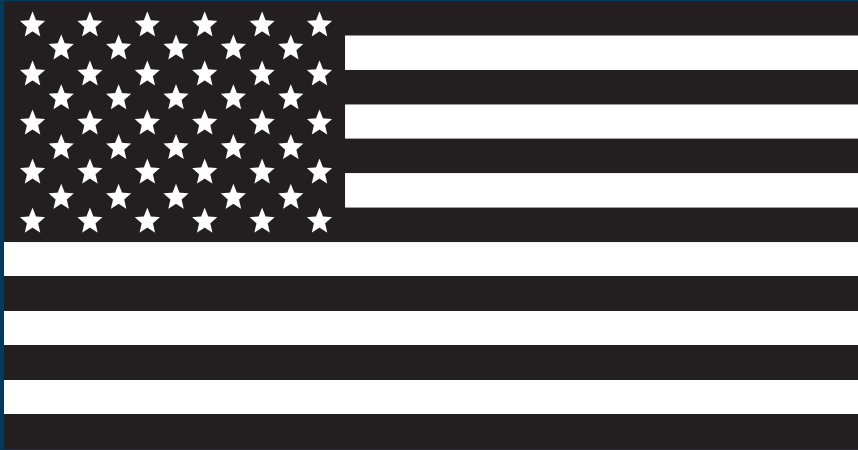
This report provides a comprehensive overview of ISIS-related radicalization and mobilization in the United States.

Program on Extremism

THE GEORGE WASHINGTON UNIVERSITY

www.cchs.gwu.edu/program-extremism ■ @gwupoe

ISIS IN AMERICA



FROM RETWEETS TO RAQQA

Lorenzo Vidino and Seamus Hughes
December 2015

Program on Extremism

THE GEORGE WASHINGTON UNIVERSITY

ISIS IN AMERICA: FROM RETWEETS TO RAQQA

Lorenzo Vidino and Seamus Hughes
December 2015

Program on Extremism

THE GEORGE WASHINGTON UNIVERSITY

All rights reserved. Printed in the United States of America. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from the publisher.

© 2015 by Program on Extremism

Program on Extremism
2000 Pennsylvania Avenue NW, Suite 2210
Washington, DC 20052
www.cchs.gwu.edu/program-extremism

CONTENTS

| | | |
|--|---|---------------------|
| Acknowledgments | ▪ | v |
| Foreword | ▪ | vii |
| Executive Summary | ▪ | ix |
| Introduction | ▪ | 1 |
| A Snapshot of ISIS in America | ▪ | 5 |
| From Keyboard Warriors to Battlefield Commanders: Understanding the Spectrum of ISIS in America | ▪ | 15 |
| Conclusion | ▪ | 33 |
| Appendix | ▪ | 35 |

Illustrations

| | | |
|--|---|--------------------|
| 1. Young (left) and Daxhlalla | ▪ | 1 |
| 2. Young's Twitter account | ▪ | 1 |
| 3. ISIS Recruits in the U.S. Legal System | ▪ | 6 |
| 4. Excerpt from missing persons report filed by family of the Somali-American teens | ▪ | 8 |
| 5. Tweet posted by the 16-year-old Denver girl | ▪ | 8 |
| 6. Reposted by one of the Denver girls on Tumblr on the anniversary of their failed trip | ▪ | 8 |
| 7. Hoda Muthana's high school yearbook portrait | ▪ | 9 |
| 8. Muthana on life in the caliphate, January 2015 | ▪ | 9 |
| 9. El Gammal, December 2013 | ▪ | 10 |
| 10. Samy identifies himself: excerpt from El Gammal's criminal complaint | ▪ | 10 |

(continued on next page)

Illustrations, continued

11. Soofi (left) and Simpson ■ [10](#)
12. Usaamah Abdullah Rahim ■ [11](#)
13. Amiir Farouk Ibrahim’s American passport ■ [11](#)
14. Douglas McCain, aspiring rapper turned jihadist ■ [12](#)
15. Hanad Abdullahi Mohallim’s Twitter profile ■ [12](#)
16. Abdullah Ramo Pazara (right) in Syria ■ [12](#)
17. Abu Muhammad al Amriki explains his defection to ISIS ■ [13](#)
18. One of Abu Khalid al Amriki’s final tweets ■ [13](#)
19. News of Abu Khalid al Amriki’s death circulates on Twitter ■ [13](#)
20. Abu Abdullah al Amriki ■ [14](#)
21. ISIS announces Abu Abdullah al Amriki’s death ■ [14](#)
22. Moner Abu Salha, a.k.a. Abu Hurayra al Ameriki ■ [16](#)
23. Ariel Bradley celebrates the Chattanooga shootings ■ [16](#)
24. Snapshot of life in the caliphate: image from Ariel Bradley’s Instagram account ■ [17](#)
25. Mohammed Hamzah Khan on Twitter ■ [20](#)
26. Elton Simpson pledges allegiance to ISIS before his attack ■ [21](#)
27. The Radicalization Echo Chamber ■ [22](#)
28. Examples of ISIS supporters’ imagery on social media ■ [23](#)
29. Clockwise: A user announces a new account; examples of node, shout-out, and amplifier accounts ■ [24](#)
30. Clockwise: Interjecting in the #BlackLivesMatter conversation; sharing a quote from Anwar al Awlaki; dismissing ISIS critics as “coconuts” ■ [25](#)
31. From the U.S. to Syria: Abdullah Ramo Pazara ■ [27](#)
32. Nader Saadeh ■ [28](#)
33. Alaa Saadeh ■ [28](#)
34. Samuel Topaz on Facebook ■ [28](#)
35. Facebook post by Mohamed Saeed Kodaimati ■ [29](#)
36. Mohamed Saeed Kodaimati ■ [29](#)
37. Shannon Maureen Conley ■ [30](#)
38. Christopher Lee Cornell ■ [31](#)

ACKNOWLEDGMENTS

THIS REPORT was made possible by the dedicated work of the Program on Extremism's staff, including its Research Associates, Sarah Gilkes and Patrick Hoover, who played an integral role in developing the research methodology, collecting the data, and contributing to written analysis; and the Program's team of Research Assistants: Audrey Alexander, Brooklyn Granowicz, Seth Harrison, Netanel Levitt, Raed Mourad, and Nicole Rickard. Thank you to Larisa Baste for her assistance in formatting the report.



The views expressed in this publication are solely those of the authors, and not necessarily those of the George Washington University.

About the Program on Extremism

The Program on Extremism provides analysis on issues related to violent and non-violent extremism. The Program spearheads innovative and thoughtful academic inquiry, producing empirical work that strengthens extremism research as a distinct field of study. The Program aims to develop pragmatic policy solutions that resonate with policymakers, civic leaders, and the general public. The Program is part of the Center for Cyber and Homeland Security (CCHS) at the George Washington University.

FOREWORD

by Jane Harman

IN 2007, as a Member of Congress, I introduced the Violent Radicalization and Homegrown Terrorism Prevention Act. We were just starting to understand how terrorists could manipulate the Internet—Twitter was one year old—and my bill would have established a national commission to study the issue and advise Congress. After passing the House by an overwhelming bipartisan vote, the proposal was blocked in the Senate over claims it would reestablish J. Edgar Hoover’s COINTELPRO—a huge distortion.

Eight years later, the issue couldn’t be more urgent. The new radicalization crosses borders. Loners don’t have to leave their basements to find extremist messages. Some radical Islamists coordinate complex attacks using PlayStations, while some hatch plots without ever contacting a known terrorist. Paris, Beirut, a Russian jet downed over Sinai: these are just the most recent outbreaks of a terrorist pandemic.

In a democracy like ours, the expression of radical views is protected by the Constitution. Violent action—inspired by those beliefs—is not. Our challenge is to identify the triggers for violence and intervene at just the right moment to prevent it. But as *ISIS in America* makes clear, one size doesn’t fit all. Homegrown terrorists don’t fit a single profile. Using social media, our enemies can micro-target their audiences, selling a narrative we need to learn to counter.

Efforts like George Washington University’s Program on Extremism have a critical role to play. Based on extensive interviews, court records, and media reports, *ISIS in America: From Retweets to Raqqa* is a comprehensive study of known ISIS recruits in the United States. More

than 50 have been arrested this year alone, a new record, and hundreds are the targets of ongoing investigations. What drew them to ISIS’s twisted fantasy? How do we pull them away? How can we identify the next lone wolf before he—or she—sets off the next pressure cooker bomb?

This report is a deep, responsible start. It takes a 21st century approach: the Internet overhauled radicalization, and it should also upgrade the way we study it. As I argued this year in *Foreign Affairs*, some of the most important intelligence is no longer secret. Some of the best information is open-source, plastered on message boards or a 19-year-old’s Twitter feed. Policymakers have been slow to adapt; spies would still rather squint at satellite photos than scrape Facebook feeds.

As the head of the Wilson Center, chartered by Congress to bridge the worlds of scholarship and policy, I welcome this contribution to our national conversation. It is consistent with our values and our First Amendment principles to ask tough questions. We can’t win if we fear the answers. Going forward, *ISIS in America* will be a critical resource for scholars, citizens, and policymakers. It will form common ground for dialogue as we confront a shared challenge: maximizing liberty and security. I look forward to more work from the Program on Extremism, thank them for this effort, and applaud their commitment to knowledge in the public service.



Jane Harman is president and chief executive of the Woodrow Wilson Center in Washington. She represented California’s 36th Congressional District for nine terms.

EXECUTIVE SUMMARY

- WHILE NOT AS LARGE as in many other Western countries, ISIS-related mobilization in the United States has been unprecedented. As of the fall of 2015, U.S. authorities speak of some 250 Americans who have traveled or attempted to travel to Syria/Iraq to join the Islamic State in Iraq and Syria (ISIS) and 900 active investigations against ISIS sympathizers in all 50 states.
- Seventy-one individuals have been charged with ISIS-related activities since March 2014. Fifty-six have been arrested in 2015 alone, a record number of terrorism-related arrests for any year since 9/11. Of those charged:
 - The average age is 26.
 - 86% are male.
 - Their activities were located in 21 states.
 - 51% traveled or attempted to travel abroad.
 - 27% were involved in plots to carry out attacks on U.S. soil.
 - 55% were arrested in an operation involving an informant and/or an undercover agent.
- A small number of Americans have been killed in ISIS-related activities: three inside the U.S., at least a dozen abroad.
- The profiles of individuals involved in ISIS-related activities in the U.S. differ widely in race, age, social class, education, and family background. Their motivations are equally diverse and defy easy analysis.
- Social media plays a crucial role in the radicalization and, at times, mobilization of U.S.-based ISIS sympathizers. The Program on Extremism has identified some 300 American and/or U.S.-based ISIS sympathizers active on social media, spreading propaganda, and interacting with like-minded individuals. Some members of this online echo chamber eventually make the leap from keyboard warriors to actual militancy.
- American ISIS sympathizers are particularly active on Twitter, where they spasmodically create accounts that often get suspended in a never-ending cat-and-mouse game. Some accounts (the “nodes”) are the generators of primary content, some (the “amplifiers”) just retweet material, others (the “shout-outs”) promote newly created accounts of suspended users.
- ISIS-related radicalization is by no means limited to social media. While instances of purely web-driven, individual radicalization are numerous, in several cases U.S.-based individuals initially cultivated and later strengthened their interest in ISIS’s narrative through face-to-face relationships. In most cases online and offline dynamics complement one another.
- The spectrum of U.S.-based sympathizers’ actual involvement with ISIS varies significantly, ranging from those who are merely inspired by its message to those few who reached mid-level leadership positions within the group.

INTRODUCTION

LIKE MOST NEWLYWED COUPLES, 22-year-old Mohammad Oda Dakhllalla and his 19-year-old wife Jaelyn Delshaun Young were planning for their future. Dakhllalla, the son of a local imam, was about to start graduate school at Mississippi State University (MSU). Young, a one-time high school cheerleader and the daughter of a Vicksburg, Mississippi, police officer, was a sophomore chemistry major at MSU.¹ Yet, unbeknownst to nearly all their relatives and acquaintances, the couple had developed a parallel life and conceived a secret honeymoon: traveling to Syria to join the Islamic State in Iraq and Syria (ISIS).

In the early months of 2015 the couple's radical musings on Twitter attracted the attention of the Federal Bureau of Investigation (FBI). During a four-month investigation, Dakhllalla and Young repeatedly expressed their wish to contribute to the growth of ISIS's self-proclaimed caliphate to undercover FBI agents online. Young—who went by “Aaminah al-Amriki” on Twitter—asserted that she was “skilled in math and chemistry and worked at an analytical lab here at my college campus,” and that she wished to “raise little Dawlah [ISIS] cubs.” She claimed Dakhllalla wanted to do propaganda work to “assure [Muslims] the US media is all lies when regarding Dawlah” and later, “join the Mujahideen.”²

In another conversation, Young informed an agent that after their Islamic wedding, the couple intended to make the journey to Syria.³ She explained, “Our story will be that we are newlyweds on our honeymoon,” adding, “In sha Allah the planning will land us in Dawlah with the grace of Allah swt [Subbanabu Wa Ta'ala, Arabic for ‘The most glorified, the highest’].”⁴ As their anticipated departure date inched closer, the couple penned farewell letters to their families explaining their actions were both deliberate and voluntary.⁵

The couple's plans never materialized. Just as the pair set out on their journey to Syria, the FBI arrested them at a small regional airport in Mississippi on August 8, 2015. Young and Dakhllalla were charged with



FIG. 1 Young (left) and Dakhllalla



FIG. 2 Young's Twitter account.

1. WAPT News, “2 Mississippi Residents Charged with Trying to Join ISIS: Jaelyn Delshaun Young, Muhammad Oda Dakhllalla Arrested,” August 12, 2015.
2. *United States of America v. Jaelyn Delshaun Young and Muhammad Oda Dakhllalla*, Criminal Complaint (August 8, 2015).
3. Ibid.
4. Ibid.
5. Ibid.

attempting and conspiring to provide material support and resources to a designated foreign terrorist organization.⁶

The couple's arrest made national news, arriving at the tail end of a summer that saw an unprecedented number of ISIS-related arrests across the country. While the U.S.-based ISIS supporters who have been charged come from a wide range of ethnic and socio-economic backgrounds, many share core characteristics: they were American-born, under age 30, and had no previous history of radical views or activities. How could these seemingly ordinary young American men and, in growing numbers, women, be attracted to the world's most infamous terrorist organization? There is no simple answer to this question, as each individual's radicalization has its own unique dynamics. Still, cases like that of Dakhllalla and Young are increasingly emblematic of the dynamics of radicalization seen throughout America over the last few years.

From Hijackings to Hashtags: The Evolution of Jihadism in America

Violent extremism of the jihadist inspiration is not a new phenomenon in America.⁷ Already in the 1980s, a small number of American citizens and residents traveled to

Afghanistan to join the *mujahideen* seeking to repel the Soviet invasion.⁸ Throughout the 1990s, scattered clusters of American-based militants were involved in other foreign conflicts (e.g. Bosnia and Chechnya) or provided material support to al Qaeda and other Sunni extremist groups. One such cluster based out of New York and New Jersey carried out one of the earliest attacks on U.S. soil, the 1993 World Trade Center bombing.⁹

After the September 11, 2001, attacks, the U.S. counterterrorism community adopted a more aggressive posture, resulting in the discovery of dozens of individuals and cells across the country. American jihadists operating throughout the 2000s and early 2010s varied significantly in terms of their profiles, organizational affiliations, and operational capabilities.¹⁰ While some had deep links to al Qaeda and its affiliates, others were nothing more than sympathizers of jihadist ideology lacking operational connections.

Over time, the greatest threat to the U.S. homeland came to be posed not so much by groups operating overseas (although a number of plots conceived by al Qaeda and its affiliates have been thwarted over the last decade), but from "self-radicalized, homegrown extremists in the United States."¹¹ In fact, in 2010 then-Attorney General Eric Holder indicated that the terrorist threat had "changed

6. WAPT News, "2 Mississippi Residents Charged with Trying to Join ISIS: Jaelyn Delshaun Young, Muhammad Oda Dakhllalla Arrested," August 12, 2015.

7. An inherently controversial and arguably improper term, "jihadism" refers to the ideology adopted by groups such as al Qaeda and ISIS. The authors are aware that the term "jihad" has a number of meanings and that most Muslims use the term in ways different than these groups.

8. J.M. Berger, *Jihad Joe: Americans Who Go to War in the Name of Islam* (Washington DC: Potomac Books, 2011).

9. See Lorenzo Vidino, "Homegrown Jihadist Terrorism in the United States: A New and Occasional Phenomenon?," *Studies in Conflict & Terrorism* 32, no. 1 (January 2009): 1-17.

10. For more on jihadist networks in the U.S., see Brian Michael Jenkins, "Stray Dogs and Virtual Armies Radicalization and Recruitment to Jihadist Terrorism in the United States Since 9/11," RAND Corporation, Occasional Paper, 2011.; Risa A. Brooks, "Muslim 'Homegrown' Terrorism in the United States: How Serious Is the Threat?" *International Security* 36, no. 2 (Fall 2011): 7-47.; Charles Kurzman, "Muslim-American Terrorism in the Decade Since 9/11," Triangle Center on Terrorism and Homeland Security, February 2012.; Scott Matthew Kleinmann, "Radicalization of Homegrown Sunni Militants in the United States: Comparing Converts and Non-Converts," *Studies in Conflict and Terrorism* 35, no. 4 (2012): 278-297.; Jerome P. Bjelopera, "American Jihadist Terrorism: Combating a Complex Threat," Congressional Research Service, January 23, 2013.; Charles Kurzman, "Muslim-American Terrorism: Declining Further," Triangle Center on Terrorism and Homeland Security, February 1, 2013.; Jessica Zuckerman, Steven P. Bucci, and James Jay Carafano, "60 Terrorist Plots Since 9/11: Continued Lessons in Domestic Counterterrorism," The Heritage Foundation, July 2013.; and Lorenzo Vidino, "From KSM's Genius to Sheer Amateurism: The Post-9/11 Evolution of the Terrorist Threat in the United States," in Bruce Hoffman and Fernando Reinares, eds., *The Evolution of the Global Terrorist Threat: From 9/11 to Osama bin Laden's Death* (Columbia University Press, 2014), 3-28.

11. Testimony of Robert S. Mueller, III, Director of the Federal Bureau of Investigation, United States Senate, *Annual Worldwide Threat Assessment*, Select Committee on Intelligence, February 5, 2008.

from simply worrying about foreigners coming here, to worrying about people in the United States, American citizens—raised here, born here, and who for whatever reason, have decided that they are going to become radicalized and take up arms against the nation in which they were born.”¹²

American jihadists have engaged in a broad spectrum of activities, ranging from providing logistical support to several foreign terrorist organizations (mainly al Qaeda and its various affiliates but also the Taliban, Pakistan’s Lashkar-e-Taiba, Indonesia’s Jemaah Islamiyah, etc.) to fighting in foreign conflicts, particularly in Afghanistan, Iraq, and Somalia. In several cases these individuals planned attacks on U.S. soil. Authorities have thwarted most of these plots. In fact, many were conceived partially after prodding from the FBI, which since 9/11 has made abundant use of “sting operations” to prevent aspiring jihadists from committing acts of violence. On other occasions, American militants succeeded, as in the cases of Little Rock (2009), Fort Hood (2009), and Boston (2013).

Between 2001 and 2013, more than 200 U.S. citizens and permanent residents were convicted of terrorism-related activities.¹³ This figure clearly indicates that a small but significant number of American citizens and residents embrace jihadist ideology and are committed to using violence, at times against fellow Americans, to this end.

Of course, when analyzed in comparative terms, these numbers and dynamics can be seen in a different light. Some argue that other forms of extremism constitute an equal, if not larger, threat to American domestic security. A study by the New America Foundation, for example, has calculated that since 9/11 almost twice as many Americans have been killed by white supremacists and other anti-government domestic radicals than by Islamist extremists.¹⁴

Moreover, while the challenge of jihadist radicalization certainly exists in the United States, its intensity and size

are significantly smaller than in most European countries. Due to multiple concurring factors—such as a comparatively more integrated American Muslim community and the sporadic and geographically-limited presence of radicalizing agents (radical mosques, extremist preachers, and recruiting networks)—America has witnessed little of the radicalization dynamics seen in countries such as France, Great Britain, Belgium, and Denmark. The American “jihadist scene,” assuming a coherent one exists, is significantly smaller, more decentralized, and less professional than that of most European countries.

By 2011 the jihadist threat on both sides of the Atlantic appeared to have somewhat plateaued. To be sure, the problem of homegrown radicalization clearly still existed. But the somewhat stagnant level of the threat, better law enforcement and intelligence practices, and the enthusiasm generated in the West by the promise of the Arab Spring suggested that jihadism was a manageable and potentially even subsiding problem.

In the last four years, though, jihadism in the West has received a boost triggered by staggering events on the ground in the Middle East. In particular, the conflict in Syria, the successes achieved on the ground by ISIS and other jihadist groups, and ISIS’s formation of a self-proclaimed caliphate have had a magnetic draw for many young Western Muslims.

The scale of this recent mobilization is unprecedented. In May 2015, the United Nations Security Council estimated more than 25,000 foreign fighters from more than 100 countries have joined ISIS and other jihadist groups in Syria.¹⁵ Even though precise data is virtually impossible to obtain, it is believed that some 5,000 European citizens or residents have become foreign fighters in Syria and Iraq, a number that dwarfs all previous mobilizations (Afghanistan, Bosnia, Chechnya, Iraq, Somalia, and Mali) combined.¹⁶

12. Jack Cloherty and Pierre Thomas, “Attorney General’s Blunt Warning on Terror Attacks,” *ABC News*, December 21, 2010.

13. Charles Kurzman, “Muslim-American Terrorism in 2013,” Triangle Center on Terrorism and Homeland Security, February 5, 2014, p. 2.

14. Scott Shane, “Homegrown Extremists Tied to Deadlier Toll than Jihadists in U.S. Since 9/11,” *The New York Times (NYT)*, June 24, 2015.

15. United Nations’ Security Council, “Action Against Threat of Foreign Terrorist Fighters Must be Ramped Up, Security Council Urges in High-Level Meeting,” 7453rd Meeting (AM), May 29, 2015.

16. Peter R. Neumann, “Foreign Fighter Total in Syria/Iraq Now Exceeds 20,000; Surpasses Afghanistan Conflict in the 1980s,” The International Centre for the Study of Radicalisation and Political Violence (ICSR), January 26, 2015.

Particularly alarming are numbers from certain countries, such as the 1,200 estimated to have left France, and the 400 who left Belgium, a country of only 11 million.

The numbers in the U.S., while similarly difficult to measure precisely, are significantly lower than those in most European countries. In June 2015 the FBI stated that “upwards of 200 Americans have traveled or attempted to travel to Syria to participate in the conflict.”¹⁷ A few weeks later, the Office of the Director of National Intelligence estimated that more than 250 individuals from the U.S. had traveled or attempted to travel to the conflict area, a few dozen had joined the ranks of ISIS, and some 20 had died.¹⁸

Moreover, the surge in the number of American foreign fighters is small compared to those who sympathize with and embrace ISIS’s ideology. American authorities have consistently said that the popularity of ISIS’s propaganda, driven largely by its savvy social media tactics, wholly overshadows that of al Qaeda. Tellingly, in May 2015 FBI Director James Comey spoke of “hundreds, maybe thousands” of ISIS sympathizers and potential recruits across the country, disclosing that the Bureau had related investigations running in all 50 states.¹⁹ A few months later, in October 2015, Comey revealed that the FBI had a staggering 900 active investigations against homegrown violent extremists.²⁰

Publicly available information confirms a sharp surge of jihadist activities in the U.S., especially when compared to dynamics seen in the years since the wave of arrests following 9/11. Since March 2014, 71 individuals in one way or another linked to ISIS have been charged in the U.S. for terrorism-related activities. The number of arrests has spiked in recent months, with 56 arrested since January 2015. In the same period, a handful of attacks have occurred across the country.

Searching for Answers

What explains the recent surge in American jihadi recruits? Who are the Americans lured by the siren songs of ISIS’s propaganda? How do they embrace such radical ideology, turning their backs on their country and, in most cases, their families? Do they do so by themselves or in clusters of like-minded individuals? Once radicalized, what do they seek: to join the ISIS caliphate between Syria and Iraq or to carry out attacks in the U.S.?

Answers to these and related questions concerning ISIS mobilization in the U.S. have puzzled authorities and the public alike. To shine new light on them, the staff at the George Washington University’s Program on Extremism engaged in a six-month study of the recent surge in domestic radicalization. The result is this report, which, while unable to examine every aspect of such a complex and fluid phenomenon, provides a comprehensive overview of ISIS-related radicalization and mobilization in the United States.

The report consists of two parts. The first examines all cases of U.S. persons arrested, indicted, or convicted in the United States for ISIS-related activities since the first case in March 2014. A wide array of legal documents related to these cases provides empirical evidence for identifying several demographic factors related to the arrested individuals. This section also looks at the cases of other Americans who, while not in the legal system, are known to have engaged in ISIS-inspired behavior.

The second part of the report examines various aspects of the ISIS-related mobilization in America. Here the report analyzes the individual motivations of ISIS supporters; the role of the Internet and, in particular, social media, in their radicalization and recruitment processes; whether their radicalization took place in isolation or with other, like-minded individuals; and the degree of their tangible links to ISIS.

17. Testimony of Michael B. Steinbach, Assistant Director of the FBI, *Terrorism Gone Viral: The Attack in Garland, Texas and Beyond*, House Homeland Security Committee, June 3, 2015.

18. Barbara Starr, “A Few Dozen Americans’ in ISIS Ranks,” *CNN*, July 15, 2015.

19. Tom Vanden Brook, “ISIL Activity Drives up Pentagon Threat Level,” *USA Today*, May 8, 2015.

20. Kevin Johnson, “Comey: Feds have Roughly 900 Domestic Probes about Islamic State Operatives,” *USA Today*, October 23, 2015.

CHAPTER 1

A Snapshot of ISIS in America

IT IS APPARENT that the U.S. is home to a small but active cadre of individuals infatuated with ISIS's ideology, some of whom have decided to mobilize in its furtherance. This section attempts to provide an overview of this demographic by drawing on research that attempted to reconstruct the lives—both real and virtual—of U.S.-based ISIS supporters. The research effort was based on legal documents, media reports, social media monitoring, and interviews with a variety of individuals, though there were at times limitations to both the amount and reliability of publicly available information.

Individuals our researchers identified were classified into three categories: Legal Cases, “At-Large,” and Deceased. The Legal Cases include instances where people have entered the U.S. legal system for ISIS-related activities. As of November 12, 2015, 71 individuals have been charged on ISIS-related charges. Legal documents provide a plethora of verifiable information on these individuals. As such, both the degree and the nature of these individuals' affiliations to ISIS were relatively clear, allowing researchers to draw meaningful statistical conclusions. (All those included in this category are presumed innocent until proven guilty.)

The second (in this case, non-comprehensive) category, “At Large” cases, is composed of all Americans identified by the Program on Extremism as having connections to ISIS but who, for various reasons, have not been arrested. Some of these individuals are identified by name, others only by a pseudonym.

The final (also non-comprehensive) category consists of ISIS-linked individuals who have died. This group encompasses the three people killed in the U.S.; well-identified individuals who have died under various circumstances in Syria and/or Iraq; and less clearly identified persons who are allegedly American who have died fighting in Syria and/or Iraq.

Statistics on ISIS Recruits in the U.S. Legal System

Over the course of six months, our researchers reviewed more than 7,000 pages of legal documents detailing ISIS-related legal proceedings, including criminal complaints, indictments, affidavits, and courtroom transcripts. Supplemented by original research and interviews with prosecutors, reporters, and, in some select cases, families of the charged individuals, the Program developed a snapshot of the 71 individuals who have been charged for various ISIS-related activities.

Defying any cookie-cutter profile of the American ISIS supporter, these 71 individuals constitute an incredibly heterogeneous group. In fact, they come from an array of ethnic groups and a range of socio-economic and educational statuses. A deeper analysis of some of these individuals and their radicalization and/or mobilization trajectories is provided below.

To better understand this group, researchers developed nine data points, each corresponding to a distinct demographic factor or arrest characteristic.

Age

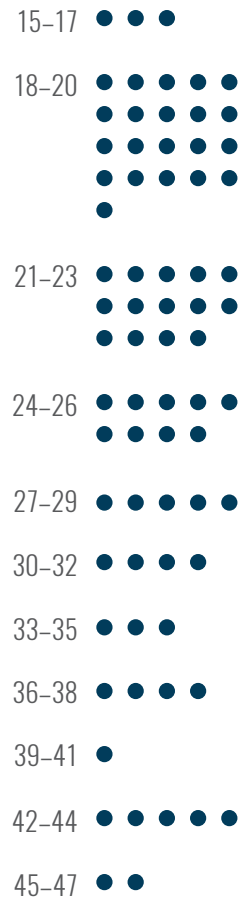
The youngest U.S. person arrested for ISIS-related activities was an unnamed 15-year-old boy. Two others were minors, ages 16 and 17 at the time of their arrests. The oldest was Tairod Pugh, a former Air Force officer who was 47 at the time of his arrest. The average age of the American ISIS supporter at the time of charges is 26.

Mirroring a pattern witnessed in most Western countries, the age of those arrested in connection with ISIS is on average lower than that of individuals arrested on terrorism-related charges in the past. As U.S. Assistant Attorney General John Carlin has noted, “In over 50 percent of the cases the defendants are 25 years or younger,

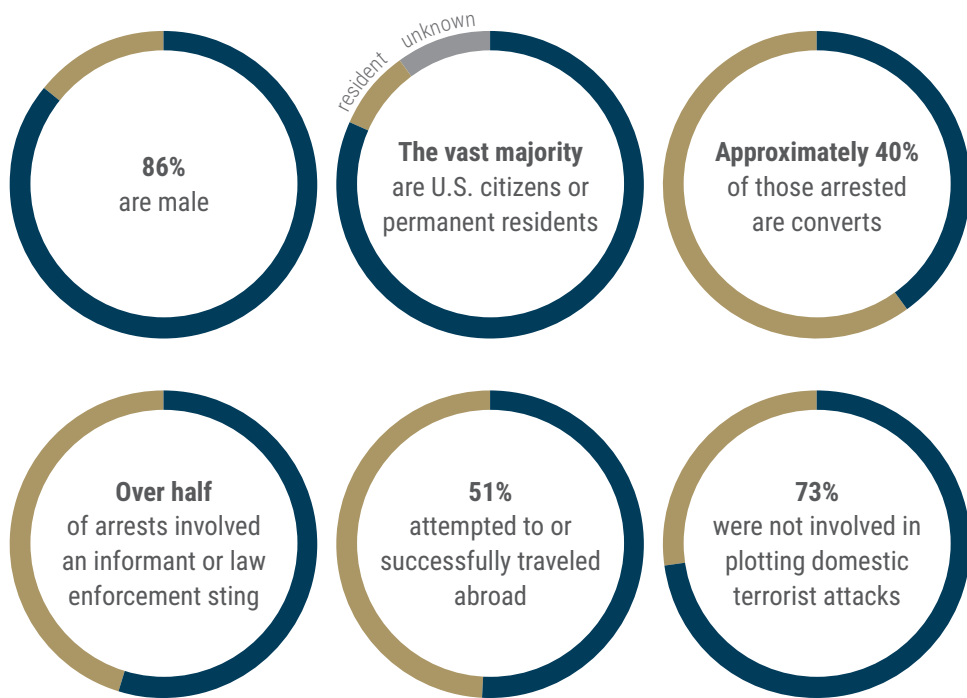
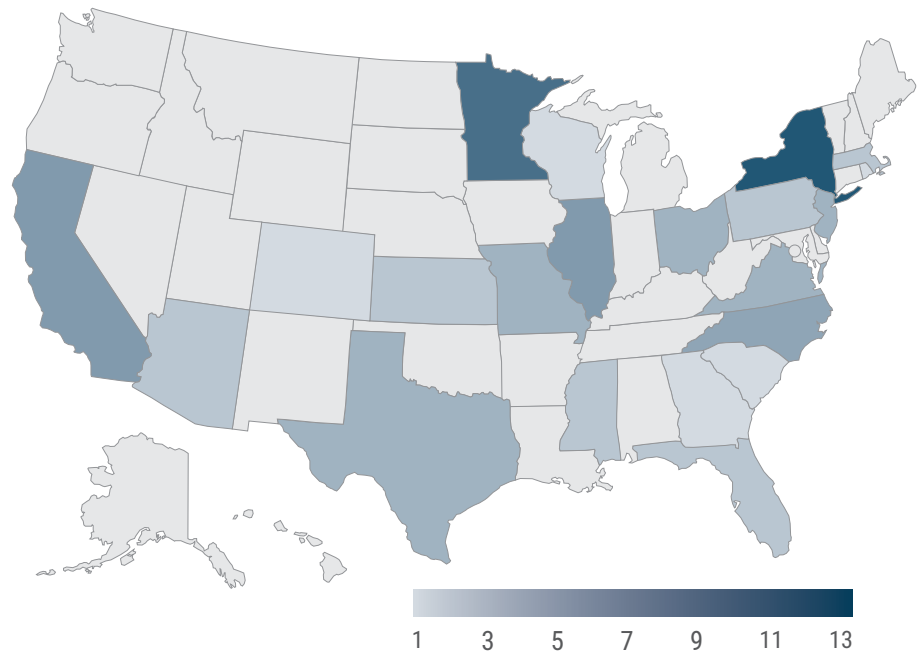
FIG. 3
ISIS RECRUITS IN THE U.S. LEGAL SYSTEM

Age

● = 1 person



Numbers by State



56 individuals
were arrested in 2015, the largest number of terrorism arrests in a single year since September 2001.

and in over a third of the cases they are 21 years or younger. . . . That is different than the demographic we saw who went to support core al Qaida in the Afghanistan FATA (Federally Administrated Tribal Areas) region.”²¹

Gender

Sixty-one of the seventy-one individuals (86%) are male. Nonetheless, women are taking an increasingly prominent role in the jihadist world. A handful of studies have attempted to identify the reasons why ISIS’s ideology attracts a growing number of Western women.²² While some of these motivations are identical to that of their male counterparts (i.e. the search for a personal identity and the desire to build a strict Islamic society), others are specific to women. The role of women in ISIS varies from propaganda disseminators and recruiters to those as the “wife of jihadist husband” and “mother to the next generation.”²³

Time Frame

The tempo of ISIS-related arrests has increased markedly in 2015. An overwhelming majority (56 individuals) were arrested for ISIS-related activities this year. This represents the largest number of terrorism arrests in a single year since September 2001.

Location

While the FBI has stated that there are active ISIS-related investigations in all 50 states, to date only 21 states have had at least one arrest within their borders. New York saw the highest number of cases (13), followed closely by Minnesota (11).

Legal Status

The vast majority of individuals charged are U.S. citizens (58) or permanent residents (6), underscoring the home-grown nature of the threat. Researchers were unable to determine the legal status of seven individuals.

Converts

Approximately 40% of those arrested are converts to Islam. Given that an estimated 23% of the American Muslim population are converts, it is evident that converts are overrepresented among American ISIS supporters.²⁴

Use of Informants/Stings

Over half (39) of the individuals were arrested after an investigation involving an informant or undercover law enforcement officer. Since 9/11, the FBI has regularly employed this tactic in terrorism investigations, with a remarkable conviction success rate. At the same time, the use of this tool has caused friction with segments of the American Muslim community.

Travel Abroad

Fifty-one percent of those charged with ISIS-related activities attempted to travel abroad or successfully departed from the U.S. In October 2015, FBI Director Comey revealed that the Bureau had noted a decline in the number of Americans seeking to travel overseas, although he did not elaborate on what elements triggered this shift.²⁵

Domestic Terror Plot

An overwhelming majority of those charged (73%) were not involved in plotting terrorist attacks in the U.S. Most U.S.-based ISIS supporters were arrested for intent to do

21. Department of Justice, “Transcript of Assistant Attorney General John P. Carlin’s Briefing at the Foreign Press Center on the Foreign Terrorist Threat and Other National Security Issues,” September 28, 2015.

22. See, for example, Saltman and Smith, “‘Till Martyrdom Do Us Part,’” ISD and ICSR, May 2015. See also Edwin Bakker and Seran de Leede, “European Female Jihadists in Syria: Exploring an Under-Researched Topic,” International Centre for Counter-Terrorism—The Hague (ICCT), April 2015.

23. Erin Marie Saltman and Melanie Smith, “‘Till Martyrdom Do Us Part’: Gender and the ISIS Phenomenon,” Institute for Strategic Dialogue (ISD) and ICSR, May 2015, p. 70.

24. Pew Research Center, “Converts to Islam,” July 21, 2007.

25. Johnson, “Comey: Feds have Roughly 900 Domestic Probes about Islamic State Operatives,” *USA Today*, October 23, 2015.

harm overseas or for providing material support—namely personnel and funds—to fighters in Syria and Iraq.

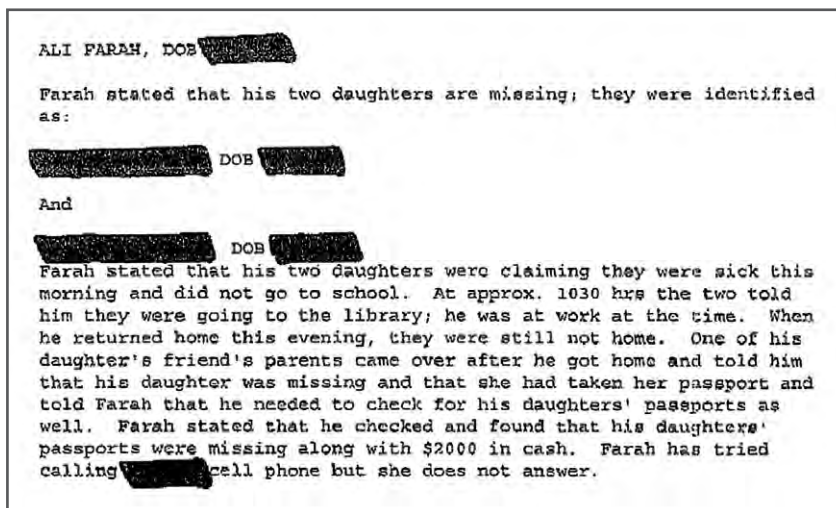
Recruits Who Remain “At-Large”

The 71 indictments are merely the tip of the iceberg, as U.S. authorities estimate that the number of individuals linked to ISIS is much larger. Our researchers identified a few dozen individuals with reported ISIS links who have not been charged. Similar to those in the legal system, the “At-Large” cohort have no common profile.

Among them, for example, are three teenage girls from the suburbs of Denver, two Somali-American sisters aged

15 and 17, and their 16-year-old friend of Sudanese descent. The trio lived a normal and comfortable life among their unsuspecting families and peers. Over a number of months, the girls engaged with ISIS supporters online, posting ISIS propaganda and expressing their desire to travel to Syria. One of their online contacts was Umm Waqqas, an influential recruiter within ISIS’s online network. The *nom de guerre* Umm Waqqas, which allegedly belongs to a woman, is one of only three accounts listed as a contact from those seeking to travel to Syria in ISIS’s 2015 guidebook *Hijrah to the Islamic State*.²⁶

One morning in October 2014 the sisters left home under the guise of going to the library while their Sudanese



ALI FARAH, DOB [REDACTED]

Farah stated that his two daughters are missing; they were identified as:

[REDACTED] DOB [REDACTED]

And

[REDACTED] DOB [REDACTED]

Farah stated that his two daughters were claiming they were sick this morning and did not go to school. At approx. 1030 hrs the two told him they were going to the library; he was at work at the time. When he returned home this evening, they were still not home. One of his daughter's friend's parents came over after he got home and told him that his daughter was missing and that she had taken her passport and told Farah that he needed to check for his daughters' passports as well. Farah stated that he checked and found that his daughters' passports were missing along with \$2000 in cash. Farah has tried calling [REDACTED] cell phone but she does not answer.

FIG. 4 Excerpt from missing persons report filed by family of the Somali-American teens.



FIG. 5 Tweet posted by the 16-year-old Denver girl.

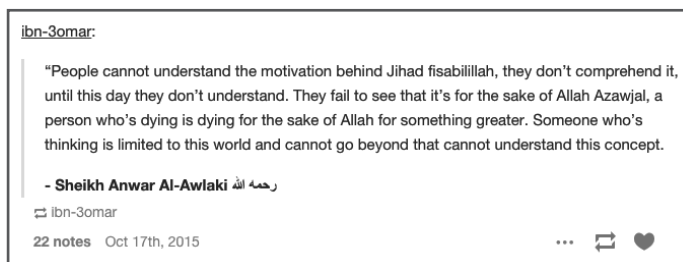


FIG. 6 Reposted by one of the Denver girls on Tumblr on the anniversary of their failed trip.

26. Islamic State of Iraq and Syria (ISIS), “Hijrah to the Islamic State: What to Packup, Who to Contact, Where to Go, Stories & More,” 2015.

friend boarded the bus to school. But instead of studying, the minors went to Denver International Airport, where their Syria-bound journey began. “Please make dua for us three,” the 15-year-old tweeted the morning of her departure, “It’s extremely urgent!”²⁷ Their hopes were dissipated by German authorities who—acting on a tip from the FBI that had been passed on by the sisters’ father—detained them at Frankfurt International Airport and placed them on a plane back to Denver. Upon their return, U.S. authorities released the trio to their families without charges.²⁸

The story of the Denver girls resembles that of Hoda Muthana, a young Yemeni-American woman from Hoover, Alabama.²⁹ As profiled in a *BuzzFeed* feature piece, Muthana grew up a modest, quiet girl from a conservative household.³⁰ However, at the age of 17 she began to distance herself from the local Muslim community and immersed herself in Islamic fundamentalist literature accessible online. She created an alter-ego on Twitter, gaining thousands of followers and interacting with like-minded Muslims across the world. One of them was Aqsa Mahmood, a 19-year-old from Scotland who made headlines as one of the first Western females to travel to Syria.³¹ Muthana allegedly communicated extensively with Mahmood, ultimately modeling her own departure on the example of her Scottish friend’s.³² Under the pretense of going to Atlanta for a college field trip, Muthana boarded a flight to Turkey.

Within a month of her arrival in Syria she married an Australian foreign fighter named Suhan al Rahman (a.k.a. Abu Jihad al Australi), who was later killed in an airstrike.³³ From her home in Raqqa, Muthana continues to propagate ISIS’s message online. For example, she uploaded a picture

of four Western passports with the caption, “Bonfire soon, no need for these anymore.”³⁴ On March 19, 2015—months before the Garland shooting—Muthana incited violence, tweeting: “Veterans, Patriot, Memorial etc Day parades . . . go on drive by’s + spill all of their blood or rent a big truck n drive all over them. Kill them.”³⁵

While he also planned his *bijrab* to Syria with the help of ISIS sympathizers online, 24-year-old New Yorker “Samy” (as he is referred to in legal proceedings) traveled a different path. According to his family, Samy started expressing increasingly radical religious views and became a more vocal opponent of American foreign policy in the



FIG. 7 Hoda Muthana’s high school yearbook portrait.



FIG. 8 Muthana on life in the caliphate, January 2015.

27. Ellie Hall, “Inside The Online World Of Three American Teens Who Allegedly Wanted To Join ISIS,” *BuzzFeed News*, October 27, 2014.

28. Jesse Paul and Bruce Finley, “Parents Reported \$2,000 Missing as Teens Headed to Join Islamic State,” *The Denver Post*, October 21, 2014.

29. Ellie Hall, “Gone Girl: An Interview With An American In ISIS,” *BuzzFeed News*, April 17, 2015. Information in the proceeding article was integrated with interviews conducted by the Program on Extremism’s staff.

30. Jon Anderson, “Hoover Woman Joins ISIS: Meet Hoda Muthana who Fled U.S. to Syria,” *AL.com*, April 20, 2015.

31. Ashley Fantz and Atika Shubert, “From Scottish Teen to ISIS Bride and Recruiter: The Aqsa Mahmood Story,” CNN, February 24, 2015.

32. Hall, “Gone Girl,” *BuzzFeed News*, April 17, 2015.

33. *Ibid.*

34. *Ibid.*

35. *Ibid.*

Middle East in 2014.³⁶ He began discussing his views online, where he engaged a fervent Muslim Brotherhood supporter from Arizona, 42-year-old Ahmed Mohammed El Gammal. Within a matter of months, El Gammal visited Samy in New York. Three months later, El Gammal allegedly facilitated the young man's journey to Syria.

Once he joined ISIS in Syria, Samy's phone and computer were temporarily confiscated to prevent contact with the outside world. During a break from his training, he reached out to his brother to apologize for his "sudden disappearance" and to reassure him that "everything is normal and safe."³⁷ After completing three weeks of intense religious training with ISIS, Samy told his brother excitedly that he would begin a month of military training, after which he would become a "regular employee [of ISIS]."³⁸ A Facebook message posted in the spring of 2015 suggests that Samy's experience with ISIS was everything he thought it would be: "I live in bilad al Islam now, the real bilad al Islam, and its [sic] beautiful."³⁹

The Deceased: Uncle Sam's Shaheed

As with the cohorts of legal cases and at-large recruits, American ISIS supporters who have been killed similarly defy a homogenous demographic profile. For clarity purposes, this cohort was organized by where the individual died.

Killed in America

Elton Simpson and **Nadir Hamid Soofi**, both residents of Phoenix, Arizona, were killed on May 4, 2015, in an attempted attack on the American Freedom Defense Initiative's Muhammad Art Exhibit and Cartoon Contest in Garland, Texas.⁴⁰ Simpson, a convert to Islam, previously served three years of probation for lying to the FBI about attempting to travel to Somalia to fight for al Shabaab.⁴¹ Before the attack, Simpson communicated online with various British and American ISIS members, who encouraged him to carry out the operation.⁴²

Usamah Abdullah Rahim, a resident of Roslindale, Massachusetts, was shot and killed by local police officers in his hometown after charging



FIG. 9 El Gammal, December 2013.

26. On or about January 16, 2015, approximately eleven days before his scheduled departure from the United States, CC-1, via social media, contacted CC-2.¹ The following exchange occurred, in substance and relevant part:

| | | |
|-------------|------|--|
| 1/16, 17:05 | CC-1 | As-Salamu Alaikum Ateyya my name is Samy, I'm Gammal's friend. He told me you could help me with a career opportunity in Istanbul. I'll be visiting soon to look for an internship for the summer inshaAllah. I'd really appreciate your help. Please reply whenever you get the chance. BarakAllahu feek [may Allah bless you] [emphasis added] |
|-------------|------|--|

FIG. 10 Samy identifies himself: excerpt from El Gammal's criminal complaint.



FIG. 11 Soofi (left) and Simpson

36. *United States of America v. Ahmed Mohammed El Gammal*, Criminal Complaint, (August 20, 2015).

37. *Ibid.*

38. *Ibid.*

39. *Ibid.*

40. Matt Pearce and Nigel Duara, "Texas Gunman's Mother: 'He Just had a Normal American Upbringing,'" *Los Angeles Times*, May 5, 2015.

41. Eugene Volokh, "Why Elton Simpson, One of the Texas Shooters, had Been Acquitted of an Earlier Terrorism-Related Offense," *The Washington Post*, May 4, 2015.

42. Elliott C. McLaughlin, "ISIS Jihadi Linked to Garland Attack has Long History as Hacker," *CNN*, May 7, 2015.

them with a knife.⁴³ Authorities allege that prior to the incident Rahim conspired with his nephew, David Wright, and Rhode Island resident Nicholas Rovinski, as well as additional unnamed conspirators, to assassinate individuals within the U.S. on behalf of ISIS. On the morning of June 2, 2015, Rahim changed his plans and called Wright to explain that he wanted to act imminently and target the police. Once law enforcement approached him in the parking lot of the CVS drugstore where he worked, he lunged at them with a knife and was shot and killed.⁴⁴

Killed in Syria/Iraq and Clearly Identified

Sixto Ramiro Garcia, a Houston resident, traveled to Syria in March 2014.⁴⁵ Garcia, a convert to Islam, conspired to join ISIS with fellow Houston resident Asher Abid Khan, but was left to cross the Turkey-Syria border alone after Khan returned to Texas.⁴⁶ His family was notified of his death on December 25, 2014, via a Facebook message from Garcia's account.⁴⁷ The circumstances surrounding Garcia's death remain a mystery.

Amiir Farouk Ibrahim, a dual U.S.-Egyptian citizen and Pittsburgh resident, traveled to Syria in early 2013.⁴⁸ Ibrahim was reportedly killed in July 2014 in a clash with Kurdish forces. Representatives from the Syrian Observatory for Human Rights found both of his passports among the ruins of a town that had been held by ISIS.⁴⁹

Yusuf Jama, a native of Minneapolis, traveled to Syria in June 2014.⁵⁰ Prior to leaving the U.S., Jama attempted to travel to Syria in May 2014 with fellow Minneapolis

resident Guled Omar—who was later arrested and indicted on material support charges—and another individual. But the trio delayed their plans in light of pushback from Omar's family.⁵¹ Additionally, Jama lived with Mohamed Osman, whom authorities believe traveled to Somalia in July 2012 to join al Shabaab.⁵² Although the circumstances surrounding Jama's death are unknown, his family was notified of his death in December 2014.⁵³



FIG. 12 Usaamah Abdullah Rahim



FIG. 13 Amiir Farouk Ibrahim's American passport.

43. *United States of America v. David Wright and Nicholas Rovinski*, Criminal Complaint, (June 12, 2015). See also Susan Zalkind and Katie Zavadski, "Boston's Wannabe Beheader 'Liked' ISIS Enough to Kill," *The Daily Beast*, June 3, 2015.

44. *Ibid.*

45. *United States of America v. Asher Abid Khan*, *Arraignment/Detention Hearing*, (June 1, 2015).

46. *Ibid.*

47. *Ibid.*

48. Betsy Hiel and Carl Prine, "Pittsburgh Man Reportedly Dead in Syria," *WPXI.com*, July 26, 2013.

49. Bill Roggio, "American Passport Found at al Qaeda Base in Northern Syria," *The Long War Journal*, July 23, 2013.

50. Laura Yuen, Mukhtar Ibrahim and Sasha Aslanian, "Called to Fight: Minnesota's ISIS Recruits," *Minnesota Public Radio (MPR) News*, March 25, 2015.

51. *Ibid.*

52. Yuen, Ibrahim and Aslanian, "Called to Fight," *MPR News*, March 25, 2015.

53. *Ibid.*

Douglas McCain, a convert to Islam raised between Chicago and Minneapolis, left the U.S. for Syria, via Turkey, in or around April 2014.⁵⁴ McCain, whose body was identified by the passport in his pocket, was reportedly killed in August 2014 during a clash between ISIS and the Free Syrian Army in the Aleppo countryside.⁵⁵

Abdirahmaan Muhumed, a dual U.S.-Somali citizen from Minneapolis, traveled to Syria in or around January 2014.⁵⁶ Muhumed's friends and family learned of his presence in Syria when he uploaded a photo of himself with a Quran and a rifle captioned "Sham."⁵⁷ Muhumed was allegedly killed in August 2014 in the same Aleppo-area

clash as McCain, whom he knew from the U.S.⁵⁸

Hanad Abdullahi Mohallim, a native of Apple Valley, Minnesota, was 18 years old when he left the U.S. for Syria on March 9, 2014.⁵⁹ Reports suggest that Mohallim was killed in action in January 2015.⁶⁰

Abdullah Ramo Pazara, a St. Louis resident of Bosnian origin, left the U.S. for Syria in May 2013, shortly after becoming a naturalized U.S. citizen.⁶¹ While in Syria, he allegedly rose to the rank of deputy to top ISIS commander Omar al Shishani and led a brigade of fighters of Balkan origin.⁶² Pazara was reportedly killed in action in the fall of 2014 near Kobane.⁶³



FIG. 14 Douglas McCain, aspiring rapper turned jihadist.



FIG. 15 Hanad Abdullahi Mohallim's Twitter profile.



FIG. 16 Abdullah Ramo Pazara (right) in Syria.

54. Cassandra Vinograd and Ammar Cheikh Omar, "American Douglas McArthur McCain Dies Fighting for ISIS in Syria," *NBC News*, August 26, 2014.

55. Ibid.

56. Mukhtar Ibrahim, "Jihad in Syria Lures Somalis from Minnesota," *MPR News*, June 12, 2014.

57. Ibid.

58. Michael Walsh, "ISIS Terrorist from Minnesota Worked at Major American Airport: Report," *New York Daily News*, September 3, 2014. See also Mukhtar Ibrahim and Peter Cox, "Douglas McArthur McCain, A Man with Minnesota Ties, Killed in Syria," *MPR News*, August 7, 2014.

59. Laura Yuen, Mukhtar Ibrahim and Sasha Aslanian, "From MN Suburbs, They Set out to Join ISIS," *MPR News*, March 25, 2015.

60. Andrea Huncar, "3 ISIS Recruits from Edmonton Believed Killed," *Canadian Broadcasting Corporation (CBC) News*, January 16, 2015.

61. *United States of America v. Hodzic, et al.*, Indictment, (February 5, 2015).

62. Robert Patrick, "Allegations of St. Louis Terrorism Support Rooted Back in Bosnian War," *St.LouisToday.com*, April 11, 2015. See also Radio Sarajevo, "U Siriji Poginuo Ramo Pazara, Komandant Džihadista iz BiH," September 25, 2014.

63. SAFF, "U Siriji Poginuo I Ramo Pazara iz Teslića," September 24, 2014.; Radio Sarajevo, "U Siriji Poginuo Ramo Pazara, Komandant Džihadista iz BiH," September 25, 2014.; *Slobodna Bosna*, "Ramo Abdullah Pazara: Sprski Ratnik i Islamski Fanatik," February 19, 2015.

Killed in Syria/Iraq and Not Clearly Identified

The Program on Extremism uncovered videos and information on individuals identified as Americans in ISIS propaganda who reportedly died either fighting or as suicide bombers. It was not possible to ascertain the real identity of these individuals, nor were researchers able to verify the authenticity of the information provided by ISIS. Yet some appear to have intriguing stories, having allegedly occupied important positions within ISIS or having carried out suicide attacks.

One of these individuals is a man who identified himself with the *kunya* **Abu Muhammad al Amriki** (Abu Muhammad the American) and claimed to have lived in the U.S. for “ten or eleven years” prior to leaving with his family to join Jabhat al Nusra (JN) in Syria (before changing his allegiance to ISIS). Featured in a nine minute video titled *Revealing the Treachery of Jabhat al Nusra* posted on numerous video sharing sites, Abu Muhammad al Amriki recounted how he left the al Qaeda–linked group because he believed it was working with the Free Syrian Army, as it allowed a convoy of arms bound for the outwardly secular and tacitly Western-supported rebel group to enter Syria.⁶⁴ Speaking in English in front of the black ISIS flag, the man recalled how the incident led him to switch his allegiance to ISIS, with which he became a local emir in an area near the border with Turkey. Though details are sparse, in early 2015 news of his death began circulating on ISIS-linked websites.⁶⁵

Another American to have reportedly died in Syria is **Abu Khalid al Amriki**. A known personality in the ISIS English-language social media scene, Abu Khalid al Amriki used at least five distinct Twitter accounts to spread his views. The little that is known about his offline persona comes from an interview he gave to an Australian paper, in which he revealed that his wife, whom he left behind in the U.S., was arrested on terrorism charges shortly after



FIG. 17 Abu Muhammad al Amriki explains his defection to ISIS.



FIG. 18 One of Abu Khalid al Amriki’s final tweets.



FIG. 19 News of Abu Khalid al Amriki’s death circulates on Twitter.

64. YouTube, “Revealing the Treachery of Jabhat al Nusra,” February 10, 2014.

65. Alastair Jamieson, “Alleged American ISIS Commander Abu Muhammad Al-Amriki Killed: Reports,” *NBC News*, January 28, 2015.

his departure.⁶⁶ In late April 2015, Abu Khalid appeared in a video produced by one of ISIS's official media outlets, Al Hayat Media Center. Abu Khalid is dressed in camouflage and a bandana and holding an AK-47 rifle while standing next to Neil Prakash (a.k.a. Abu Khalid al Cambodi), a prominent Australian foreign fighter and ISIS propagandist.⁶⁷ Reports of Abu Khalid's death at the hands of a coalition airstrike surfaced on social media in late September 2015. In an ironic twist of fate, one of his last tweets using the Twitter handle @AK47_Backup stated, "You fly a remote control plane halfway across the world to kill an enemy that you are to [sic] coward to meet face to face."

Two unidentified individuals who used *kunyas* ending in "al Amriki" were heralded as ISIS suicide attackers by the group in 2015. One, **Abu Dawoud al Amriki**, reportedly rammed a truck packed with explosives into a gathering of soldiers in Iraq's Salahuddin province.⁶⁸ ISIS posted an image of Abu Dawoud on the Twitter page of one of its official media outlets, Al Bayan Radio, in March.⁶⁹ The other, **Abu Abdullah al Amriki**, allegedly drove an SUV laden with explosives into Iraqi army barracks near Beiji in August 2015.⁷⁰



FIG. 20 Abu Abdullah al Amriki



FIG. 21 ISIS announces Abu Abdullah al Amriki's death.

66. Lauren Williams, "Meeting a Daesh jihadist in Syria," *The Saturday Paper*, July 18, 2015. Our research team attempted to identify Abu Khalid's alleged American wife but was unsuccessful. According to court records, he did at some point communicate with Keonna Thomas, an American arrested in the U.S., but there is no indication that their relationship was anything more than an online friendship.

67. Aaron Y. Zelin, "al-Hayāta Media Center Presents a New Video Message from The Islamic State: 'Stories From the Land of the Living: Abū Khālid al-Kambūdi,'" *Jihadology.net*, April 21 2015.

68. Assabah.com, "American Suicide Bomber Abu Dawoud in the Ranks of 'Daesh: The Iraqi Army Takes on the Battle to Retake Tikrit," March 4, 2015.

69. Ibid.

70. "ISIS says American suicide bomber carried out Iraq attack," *Al Arabiya*, August 19, 2015.

CHAPTER 2

From Keyboard Warriors to Battlefield Commanders: Understanding the Spectrum of ISIS in America

AS THE DATA AND ANALYSIS provided in the previous section show, the profiles of American ISIS sympathizers—from those who merely tout the group’s ideology online to those intimately involved in ISIS recruitment, financing, or fighting—are extremely diverse. Ranging from grown men who had flirted with jihadist militancy for over a decade to teenagers who have only recently converted to Islam, from the son of a Boston area police officer to a single mother of two young children, these individuals differ widely in race, age, social class, education, and family background.

Individuals with such diverse backgrounds are unlikely to be motivated by the same factors. Policymakers and academics around the world have formulated a number of explanatory theories about the underlying factors driving people to radicalize. Some focus on structural factors such as political tensions and cultural cleavages, the so-called “root causes” of radicalization. Others stress personal factors such as the shock of a life-changing event. Matt Venhaus captures the diversity of the individuals attracted to jihadist ideology, categorizing them as revenge seekers, status seekers, identity seekers, and thrill seekers.⁷¹ But it is clear that these categories are not exhaustive and that, in many cases, an individual exhibits the characteristics of more than one category. In substance, most experts agree that radicalization is a highly complex and individualized process, often shaped by a poorly understood interaction of structural and personal factors.

In many cases examined by our research team, an underlying sense of sympathy and compassion appeared to play an important role in initially motivating young Americans to become interested and invested in the Syrian conflict. Many were outraged by the appalling violence Bashar al Assad’s regime used to suppress the Syrian rebellion and the subsequent inaction on the part of the international community. Pictures and videos capturing the aftermath of civilian massacres perpetrated by the regime, displayed widely in both social and mainstream media, rocked the consciences of many—from those with an existing strong Sunni identity to those who were not Muslim—and led some to take the first steps to militancy.

A major shift began as the anti-regime rebellion in Syria came to be increasingly dominated by militant groups. By the time ISIS formally declared its caliphate in June 2014, the motivations of recruits appeared to revolve more around fulfilling perceived religious obligations, such as performing *hijrah* (migration from a non-Muslim society to a Muslim one, as per the prophet Mohammad’s migration from Mecca to Medina) and the opportunity to participate in the creation of a utopian Islamic society.

But ideological motivations are deeply intertwined with, and impossible to separate from, personal motives. The National Counterterrorism Center (NCTC) observes that those who embrace ISIS’s ideology tend to be “disenfranchised individuals seeking ideological, religious

71. Colonel John M. “Matt” Venhaus, U.S. Army, “Why Youth Join al-Qaeda,” *United States Institute of Peace*, May 2010.



FIG. 22 Moner Abu Salha, a.k.a. Abu Hurayra al Ameriki

and personal fulfillment.”⁷² A search for belonging, meaning, and/or identity appears to be a crucial motivator for many Americans (and other Westerners) who embrace ISIS’s ideology.

This search for meaning was perfectly encapsulated in the words of Moner Abu Salha, the 22-year-old Floridian who is the first American known to have died in a suicide mission in Syria on behalf of Jabhat al Nusra. “I lived in America,” stated Abu Salha in a 2014 video. “I know how it is. You have all the fancy amusement parks and the restaurants and the food and all this crap and the cars. You think you’re happy. You’re not happy. You’re never happy. I was never happy. I was always sad and depressed. Life sucked.”⁷³ In contrast, he described life fighting in Syria as “the best I’ve ever lived.”⁷⁴

Despite coming from a quite different background, a fellow American who made the journey to Syria has reportedly displayed a similar malaise. Ariel Bradley was born in an underprivileged family in the Chattanooga suburb of Hixson (the same suburb where the perpetrator of the July 2015 Chattanooga shooting Mohammad Abdulazez lived). Bradley was homeschooled by her evangelical

Christian mother until she rebelled and left home as a teenager. According to friends interviewed for her extensive profile in *BuzzFeed News*, Bradley spent the following years wandering in search of something.⁷⁵

“She was definitely always looking for love,” said a former roommate “always looking for that sense of belonging.” Another friend recalled Bradley’s “clearly segmented life”: “When I first met her she was a Christian, and then she was a socialist, and then she was an atheist, and then a Muslim. As far as I could tell it was always in relation to whatever guy she was interested in, so if she meets a guy that’s an atheist then she’s an atheist, falls into that for a year. Then the guy leaves and she meets somebody new, and it starts all over again. . . . It seemed like whatever guy she was with, she would just crawl into his skin and kind of become him.”⁷⁶

At one point Bradley fell in love with a Muslim patron of the pizza parlor where she used to work. To get close to him, she converted to Islam. While things never worked out with the original love interest, Bradley began frequenting Muslim marriage websites where, in August 2011, she met an Iraqi man living in Sweden. Shortly thereafter the two married and had a child. Likely under the influence of her husband, Bradley’s faith became increasingly conservative and militant. In early 2014 the couple left for Syria, where they have reportedly been living in ISIS-controlled territory. Bradley is active online, particularly on Twitter and

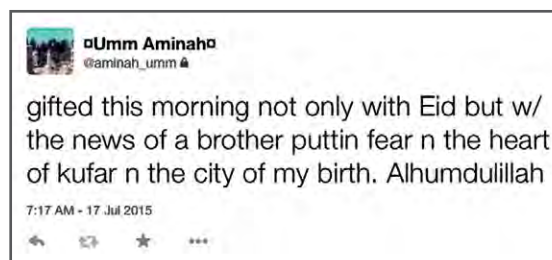


FIG. 23 Ariel Bradley celebrates the Chattanooga shootings.

72. Testimony of Nicholas J. Rasmussen, Director, National Counterterrorism Center, *Countering Violent Extremism: The Urgent Threat of Foreign Fighters and Homegrown Terror*, House Homeland Security Committee, February 11, 2015.

73. Mona El-Naggar and Quynhanh Do, “Video Released of U.S. Bomber in Syria,” *New York Times*, July 31, 2014.

74. Ibid.

75. Ellie Hall, “How One Young Woman Went From Fundamentalist Christian to ISIS Bride,” *BuzzFeed News*, July 20, 2015.

76. Ibid.

Instagram, where she discusses her life and praises ISIS. In the immediate aftermath of the Chattanooga attacks, which killed five military personnel in her hometown, she tweeted: “*in sha Allab* [God willing] this will make the camps of *Emaan* [believers] and *Kuffr* [non-believers] known within Chattanooga.”⁷⁷

It is tempting to caricature Bradley as a naïve girl with personal problems whose jihadist trajectory is the outcome of an unfortunate childhood. It is also easy to assume that her actions were driven by a quest for a romantic partner. But, even in the most extreme cases, multiple factors contribute to an individual’s decision. Her friend’s analysis highlights this dynamic: “Be it religion, be it a man, be it a marriage, be it a child, be it ISIS, Ariel was always looking for something to define herself, an identity to cling to.”⁷⁸ Given her particular pattern of behavior, it is likely that Bradley might have accepted other extremist ideologies, if circumstances allowed, so long as they satiated her hunger for community, love, and identity.

Still, it is difficult to fully comprehend the complex mental processes that led Bradley, like other young Americans, to embark on such an extreme journey to the ISIS caliphate. What is apparent is that ISIS and its propaganda machine have been particularly adept at exploiting the emotions, needs, and weaknesses of young Americans, irrespective of their demographic backgrounds. What follows is an examination of the online and physical world dynamics that influence U.S.-based ISIS sympathizers.

The Role of Social Media

Extremist groups inspired by a range of ideologies have embraced the Internet for a variety of purposes. As a 2009 report by the International Centre for the Study of Radicalisation at King’s College London observes:

The Internet can be used by extremists to illustrate and reinforce ideological messages and/or narratives. Through the Internet, potential recruits can



FIG. 24 Snapshot of life in the caliphate: image from Ariel Bradley’s Instagram account.

77. Hall, “How One Young Woman Went From Fundamentalist Christian to ISIS Bride,” *BuzzFeed News*, July 20, 2015.

78. *Ibid.*

gain near-instantaneous access to visually powerful video and imagery which appear to substantiate the extremists' political claims. . . . The Internet makes it easier to join and integrate into more formal organizations. It provides a comparatively risk-free way for potential recruits to find like-minded individuals and network amongst them, enabling them to reach beyond an isolated core group of conspirators. . . . It creates a new social environment in which otherwise unacceptable views and behaviour are normalised. Surrounded by other radicals, the Internet becomes a virtual 'echo chamber' in which the most extreme ideas and suggestions receive the most encouragement and support.⁷⁹

Western governments tend to agree on the importance of the Internet in radicalization processes. The dynamic has been described with clarity by the Netherlands' domestic intelligence agency (AIVD) in an extensive report that calls the Internet "the turbocharger of the jihadi movement." The report argues:

There is a large group of Muslims, mostly young people, in non-Muslim Western countries, who feel isolated within the societies in which they live. Because these youngsters see their future in the West, unlike their parents, while at the same time experiencing a strong element of distrust for Western society, they are looking for their own identity and for a position to adopt in Western society. . . . When hunting for answers to these questions, they may end up in an environment with which they are familiar and which is easily accessible, namely the Internet. Not only can they find a great deal of information there, but

they can also become part of a virtual (Muslim) community, exchanging ideas and blowing off steam by expressing their frustration with other like-minded individuals who share their fate.⁸⁰

Officials in the U.S. have expressed similar concerns. The 2007 National Intelligence Estimate, titled *The Terrorist Threat to the US Homeland*, observes:

The spread of radical—especially Salafi—Internet sites, increasingly aggressive anti-U.S. rhetoric and actions, and the growing number of radical, self-generating cells in Western countries indicate that the radical and violent segment of the West's Muslim population is expanding, including in the United States. The arrest and prosecution by law enforcement of a small number of violent Islamic extremists inside the U.S.—who are becoming more connected ideologically, virtually, and/or in a physical sense to the global extremist movement—points to the possibility that others may become sufficiently radicalized that they will view the use of violence here as legitimate.⁸¹

In May 2008, the U.S. Senate Committee on Homeland Security and Governmental Affairs published a report titled *Violent Islamist Extremism, the Internet, and the Homegrown Terrorist Threat* in which the committee warns about the increased frequency with which U.S.-based militants are active online.⁸² A 2010 report by NCTC contends that "the Internet and related information technologies—such as Web forums, blogs, social networking sites, and e-mail—that serve as platforms for extremist propaganda and discourse can enable and advance the radicalization process and help mobilize

79. Tim Stevens and Peter R. Neumann, "Countering Online Radicalisation: A Strategy for Action," ICSR, March 16, 2009, p. 12.

80. Netherlands' Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (Ministry of International Affairs and Kingdom Relations), "Jihadis and the Internet," Netherlands' National Coordinator for Counterterrorism, February 2007, p. 91.

81. United States Office of the Director of National Intelligence, National Intelligence Council, "The Terrorist Threat to the US Homeland," *National Intelligence Estimate*, July 2007.

82. U.S. Senate Committee on Homeland Security and Governmental Affairs (HSGAC), "Violent Islamist Extremism, the Internet, and the Homegrown Terrorist Threat," May 8, 2008.

individuals who may not be geographically near key extremist figures or significant events.”⁸³

U.S. officials have repeatedly highlighted how ISIS uses social media to reach a significantly wider audience much faster than any group in the past. “ISIL blends traditional media platforms, glossy photos, in-depth articles, and social media campaigns that can go viral in a matter of seconds,” argued FBI Director Comey in a July 2015 testimony before the U.S. Senate. “No matter the format, the message of radicalization spreads faster than we imagined just a few years ago.”⁸⁴ He continued, “Social media has allowed groups, such as ISIL, to use the Internet to spot and assess potential recruits. With the widespread horizontal distribution of social media, terrorists can identify vulnerable individuals of all ages in the United States—spot, assess, recruit, and radicalize—either to travel or to conduct a homeland attack. The foreign terrorist now has direct access into the United States like never before.”⁸⁵ Comey further elaborated on the novelty of ISIS social media use:

Your grandfather’s al Qaeda, if you wanted to get propaganda, you had to go find it. Find where *Inspire* magazine was and read it. If you want to talk to a terrorist, you had to send an email into *Inspire* magazine and hope that Anwar al Awlaki would email you back. Now all that’s in your pocket. All that propaganda is in your pocket, and the terrorist is in your pocket. You can have direct communication with a terrorist in Syria all day and night, and so the effect of that—especially on troubled minds and kids—it works! It’s buzz,

buzz, buzz, buzz, buzz. It’s the constant feed, the constant touching, so it’s very, very different and much more effective at radicalizing than your grandfather’s al Qaeda model.⁸⁶

Indeed, ISIS’s ability to directly and constantly reach Americans through social media has manifested itself in a number of ways: 1) triggering or advancing their radicalization process; 2) helping them mobilize to leave for Syria to join the group; and 3) inciting them to carry out attacks in America. The following examples illustrate this three-fold manifestation.

Grooming from Afar

An archetypal case of ISIS’s online radicalization and recruitment campaign was chronicled in an illuminating *New York Times* story on “Alex,” a 23-year-old girl from rural Washington state.⁸⁷ Alex lived with her grandparents from an early age, after her mother lost custody due to drug addiction. A college dropout who, in her own words, lived “in the middle of nowhere” and had no connection to Islam, Alex was motivated by a “horrified curiosity” to seek out ISIS supporters after reading news of the execution of American journalist James Foley.⁸⁸

Within several months, she was exchanging messages and conversing over Skype with various ISIS-linked recruiters.⁸⁹ Over time, Alex, who had previously expressed a desire to “live a faith more fully,” was meticulously groomed online, her new friends showering her with money, books, gift cards, and chocolate. She soon converted to Islam and slowly embraced ISIS’s ideology. Her new friends offered Alex a previously lacking sense of

83. Similar findings were reached in this report. See also National Counterterrorism Center, “Radicalization Dynamics: A Primer,” September 2010, p. 18; HSGAC, “Zachary Chesser: A Case Study in Online Islamist Radicalization and Its Meaning for the Threat of Homegrown Terrorism,” February 16, 2012.

84. Testimony of James B. Comey, Director, Federal Bureau of Investigation (FBI), Senate Select Committee on Intelligence, *Counterterrorism, Counterintelligence, and the Challenges of “Going Dark,”* July 8, 2015.

85. *Ibid.*

86. Ryan J. Reilly, “If You’re Trying To Join ISIS Through Twitter, The FBI Probably Knows About It,” *Huffington Post*, July 9, 2015.

87. Rukmini Callimachi, “ISIS and the Lonely Young American,” *NYT*, July 27, 2015.

88. *Ibid.*

89. *Ibid.*

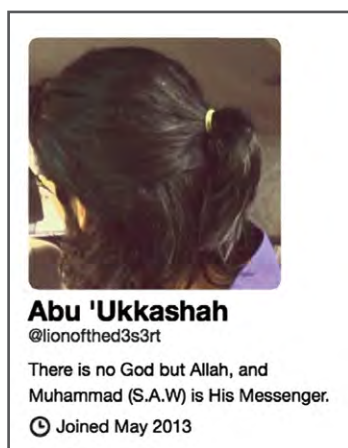


FIG. 25 Mohammed Hamzah Khan on Twitter.

belonging: hours after declaring her conversion online, the number of individuals following her on Twitter doubled, prompting her to tweet, “I actually have brothers and sisters. I am crying.”⁹⁰ Alex began to live what the *Times* categorizes as a double life. In public, she continued teaching Sunday school classes at her grandparents’ church. But, behind closed doors, she was a full-fledged believer in ISIS’s ideology.

An ISIS supporter from the U.K.—who turned out to be a married middle-aged father with a criminal record of multiple arrests—spent hours each day grooming Alex. He eventually told her that it is a sin for Muslims to live among non-believers, and extended an invitation for her to travel to Austria, marry a 45-year-old ISIS supporter, and then move to Syria.

Realizing that Alex was spending an inordinate amount of time on her computer, her grandmother confiscated her electronics and confronted her online contacts via Skype. With her double life exposed, Alex promised to stop communications with ISIS sympathizers and allowed her grandmother

to change her Twitter and email passwords. But the companionship her like-minded friends provided was apparently too good to give up. The *Times* claims that, despite her promise, Alex has continued to be active in the online ISIS scene.⁹¹

Travel Agents

In addition to helping radicalize individuals, online ISIS supporters have been instrumental in providing both advice and logistical support to Americans attempting to travel to Syria. This dynamic played out in October 2014 when three siblings from Chicago were stopped at O’Hare International Airport on their way to Syria.

The journey had been meticulously planned by the eldest sibling, 19-year-old engineering student Mohammed Hamzah Khan. Khan, a graduate of an Islamic school in the Chicago suburbs, had been active online and met a man known as Abu Qaqa on Twitter, whom he soon communicated with using personal messaging platforms such as Kik and WhatsApp.⁹² According to authorities, it was Abu Qaqa who provided Khan with the phone number of an individual to call upon landing in Turkey. Khan’s 17-year-old sister had also been active online, trying to find ways to travel to Syria. Using the Twitter name “Umm Bara,” she communicated with an English-speaking ISIS fighter who went by the name Abu Hud—known on Twitter as the “Paladin of Jihad”—and popular as result of his Tumblr series #DustyFeet, a de facto travel guide for would-be recruits.⁹³ A search of the siblings’ home found a step-by-step guide to crossing the Turkish border, contact information for four individuals involved in smuggling ISIS volunteers, including Abu Qaqa, and handwritten farewell letters addressed to their parents.⁹⁴

Another aspect of the Khans’ story is noteworthy. While “Alex” and many other ISIS sympathizers are individuals with limited or no knowledge of Islam, the Khan siblings grew up steeped in religious studies. All three attended

90. Rukmini Callimachi, “ISIS and the Lonely Young American,” *NYT*, July 27, 2015.

91. *Ibid.*

92. Janet Reitman, “The Children of ISIS,” *The Rolling Stone*, March 25, 2015.

93. *Ibid.*

94. *United States of America v. Mohammed Hamzah Khan*, Criminal Complaint (October 6, 2014).

Islamic schools and had become *hafiz* or *hafiza*, a term given to those who have memorized the entire Quran.⁹⁵ The eldest even taught youth at a local mosque.⁹⁶

Devil on the Shoulder

While the case dynamics remain somewhat murky, ISIS social media appears to have played a role in pushing Americans Elton Simpson and Nadir Soofi to attack the Muhammad Art Exhibit and Cartoon Contest in Garland, Texas. A few months before the attack Simpson, who had been involved in jihadist activities for over a decade, became an active participant in the community of U.S.-based ISIS sympathizers on social media. Simpson also made contact with a well-known British foreign fighter, Abu Hussain al Britani, and Mohamed Abdullahi Hassan (a.k.a. Mujahid Miski), a prominent Somali-American English-speaking propagandist.⁹⁷ Ten days before the attack, Miski posted about the Garland event with a clear exhortation: “The brothers from the Charlie Hebdo attack did their part. It’s time for the brothers in the #US to do their part.”⁹⁸

Simpson, via a Twitter account with the username “Shariah is Light” and an avatar of the late al Qaeda propagandist Anwar al Awlaki, responded to Miski’s call to arms, publicly asking his friend in Somalia to “dm” (Direct Message, a private message on Twitter) him.⁹⁹ Simpson and Soofi then drove from Arizona to Garland in a vehicle loaded with assault rifles, body armor, and hundreds of rounds of ammunition. Prior to the attack, Simpson tweeted a final time, using a hashtag #texasattack. The hashtag was quickly picked up by Abu Hussain al Britani and circulated throughout the

pro-ISIS community on Twitter in an effort to encourage others to commit similar acts.¹⁰⁰

The Echo Chamber

U.S. authorities estimate that several thousand Americans consume ISIS propaganda online creating what has been described as a “radicalization echo chamber.”¹⁰¹ American ISIS activists and sympathizers are active on a variety of platforms, from open forums like Facebook, Google+, and Tumblr to more discrete messaging applications such as Kik, Telegram, surespot, and the dark web. But Twitter is by far the platform of choice of this informal echo chamber. For this reason, our researchers focused on the Twitter activities of approximately 300 individuals identified as American supporters of ISIS.

Identifying the 300 individuals was challenging because most online ISIS sympathizers seek anonymity. Individuals were coded as Americans if they self-identified as such; if Twitter’s geo-location software placed them within the U.S.; or if they used a variation of the *kunya* “al



FIG. 26 Elton Simpson pledges allegiance to ISIS before his attack.

95. Kevin Sullivan, “Three American Teens, Recruited Online, Are Caught Trying to Join the Islamic State,” *The Washington Post*, December 8, 2014.

96. Jethro Mullens and Ted Rowland, “Who is Mohammed Hamzah Khan?,” *CNN*, October 7, 2014.

97. Scott Shane, “Texas Attacker Left Trail of Extremist Ideas on Twitter,” *NYT*, May 5, 2015.

98. Jim Sciutto, Pamela Brown, Paul Cruickshank and Paul Murphy, Texas attacker tweeted with overseas terrorists, *CNN*, May 5, 2015.

99. Rita Katz, “The Power of a Tweet: Elton Simpson and the #TexasAttack,” *SITE Intelligence Group (SITE)*, May 5, 2015.

100. Katz, “The Power of a Tweet” *SITE*, May 5, 2015.

101. Pierre Thomas, Mike Levine, Jack Date and Jack Cloherty, “ISIS: Potentially ‘Thousands’ of Online Followers Inside US Homeland, FBI Chief Warns,” *ABC News*, May 7, 2015. The term has also been used by Assistant Attorney General John Carlin: United States Department of Justice, “Assistant Attorney General John P. Carlin Delivers Remarks on Domestic Terrorism at an Event Co-Sponsored by the Southern Poverty Law Center and the George Washington University Center for Cyber and Homeland Security’s Program on Extremism,” October 14, 2015.

FIG. 27
THE RADICALIZATION ECHO CHAMBER

The figure is a collage of various social media posts and images. It includes:

- A tweet from **Aashir al amriki** (@aashiralamriki) dated Jul 3, with the text "Contact me on telegram · brothers only. Inshallah." and 1 retweet.
- A tweet from **Abu Sa'ad Al-Amriki** (@AbuSaadAlamriki) dated Jun 28, with the text "4th Account, Suspend, I will just return! #DiInYourRageKuffar #SHOUTOUT please Jazakum Allahu khayran" and 14 retweets.
- A tweet from **Abu Cowboy** (@abumuwahidXXXX) with the text "Hijrah does not stop as long as there is still jihad (Sh Anwar Al-Awlaki)" and 1 retweet.
- A tweet from **Aashir al Amriki** (@AashirAmriki) dated Jun 12, with the text "Make dua for me for my migration soon! Make Bayah To Sheikh Almunineen every day. Inshallah and salaam" and 12 retweets.
- A tweet from **al Amriki** with the text "Guilty of what? When will we begin to stand up and let the entire world hear "Yes, I am honored to have been chosen?" **Bolingbrook man charged with trying to join ISIL pleads guilty**".
- A tweet from **Umm Nazarat** (@ummspectacles) with the text "@ummrada3 @RareNiqab_14 the same thing happened to me, I had to get someone to make this account 4 me, I couldn't make anymore :(".
- A tweet from **Jannah Bride** (@JannahBride) dated Mar 4, with the text "Mujahideen are true real men fighting for Allah (swt). Not like wimps in Detroit good for nothing thugs. #detroitmuslims #JihadiJohn".
- A tweet from **Abu Sa'ad Al-Amriki** (@AbuSaadAlamriki) dated Jun 8, with the text "Ya ikhwan, be aware of FBI informants etc here amongst us, careful who you be following and who follows you, Allah ma3kum".
- A tweet from **BAQIYA SHOUTOUT 66** (@baqya66R) with the text "SHOUTOUT PLEASE SUPPORT Umm MaryamProtected Tweets @JustUkhtMaryam2 Umm MaryamProtected Tweets @JustUkhtMaryam2".
- A tweet from **abdullah al-american** (@abualyousef) with the text "Wants to live under the shade of the caliphate. Islamic state in America".
- A tweet from **Generation Awlaki** (@ShAnwarAwlaki5) with the text "A page dedicated to the sayings of our beloved Shaykh Anwar Al Awlaki, may Allaah accept him amongst the shuhada. Wife of Shahid".
- A tweet from **Abu Harb Al Amriki** (@sham_reason) with the text "Happily married. Ask for surespot id. living in Dar ul Kufr".
- A tweet from **New Era Jihadi 13** (@NewEraJihadi13) dated Jun 17, with the text "Bismillah. Kuffar spending millions while I spend less then 2 minutes to make another account".
- Images: A hand holding a flag with Arabic text, a lion, a hand holding a lit flare, a hand holding a grenade with "HAVE A NICE DAY" written on it, a person in a headscarf, a person with a beard and a "PERF" sticker, a person with a "I SHIP US" sticker, a person with a "KUFFAR!" sticker, a person with a "SHOOTING" sticker, and a person with a "SHOOTING" sticker.

Amriki” in their Twitter username or handle. Additionally, researchers analyzed the content of English-speaking ISIS sympathizers for syntax, spelling, word selection, and cultural context and cross-referenced lists of followers to isolate Americans from the much larger English-speaking ISIS community on Twitter. The categorization of an account as belonging to an American was reaffirmed on a few occasions, most frequently when an individual’s criminal complaint and/or indictment made reference to social media accounts. In at least one case—that of Terrence McNeil—a technical mistake by an ISIS supporter on social media revealed their identity as an American.¹⁰²

While American ISIS supporters tend to be male, nearly one third of the accounts examined are purportedly operated by women. Additionally, supporters broadly divided into two sets: those who locate themselves in Syria and Iraq and those still in America but aspiring to assist ISIS in a number of ways. Those in the former group often maintain their network of friends in the U.S. after arriving in ISIS territory. They post near real-time updates of ISIS-led attacks and life in the caliphate, encouraging their fellow Americans to make the trek and, at times, scolding their real-world and online friends for their lack of commitment to the cause.

A significant number of American ISIS supporters use avatars of black flags, lions, and green birds.¹⁰³ A particularly clever account uses a picture of the Detroit Lions, combining a distinctly American pride in an NFL team and the popular Islamic symbol of bravery very frequently used by ISIS supporters. Images, quotes, and links to lectures of the deceased radical cleric Anwar al Awlaki are favorites of the American ISIS scene. Increasingly photos of other Americans who have been arrested on terrorism charges, killed waging *jihad* abroad, or were responsible for homegrown terrorist attacks are used as avatars.

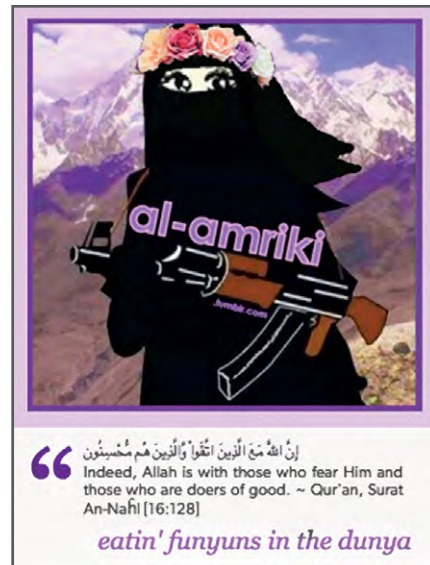


FIG. 28 Examples of ISIS supporters’ imagery on social media.

102. McNeil tweeted a screenshot of his Twitter suspension (at the time, his 14th suspension). He neglected to remove a small part of his Google ID, which led to a number of Google+ pages. After reviewing the videos on each page, a link was found to a video posted on YouTube, which was subsequently linked to a Facebook profile with his real name and location. One of his Facebook status updates from last year matched with materials from his 10th Twitter account prior to suspension.

103. The term “green bird” indicates a status one reaches when he or she dies (becomes a *shahed*, or martyr) and reaches *jannah*, or heaven. It is a scriptural reference from a *hadith*, or reported saying from the prophet Mohammad, that celebrates the virtues of martyrdom. Jihadists term fallen comrades “green birds” to eulogize them as pious, faithful Muslims.

As with many online communities, participants in the American ISIS Twitter scene exhibit distinct styles, roles, personalities, and degrees of commitment, which often fluctuate over time. Reflecting these dynamics, their accounts can be divided into three categories: nodes, amplifiers, and shout-outs.

The **nodes** are the leading voices that enjoy a prominent status within the larger community and are the primary content creators for the network. A group of two or three clustered users will often swap comedic memes, news articles, and official ISIS tweets, allowing them to pool followers and more easily spread content both to new audiences and throughout their network.

Amplifiers largely do not generate new content but rather retweet and “favorite” material from popular users. Ultimately, because they post little, if any, original content, it is often unclear whether these accounts correspond to real-life ISIS sympathizers or are programmed to post automatically.

Finally, **shout-out** accounts are a unique innovation and vital to the survival of the ISIS online scene. They

primarily introduce new, pro-ISIS accounts to the community and promote newly created accounts of previously suspended users, allowing them to quickly regain their pre-suspension status. Although they tweet little substantive content, shout-out accounts tend to have the largest followings in the Twitter landscape and therefore play a pivotal role in the resilience of ISIS’s Twitter community.

While American ISIS accounts are suspended with some frequency, these suspensions have become a badge of honor and a means by which an aspirant can bolster his or her legitimacy. In most suspension cases, a new (and often more than one) account with a variation of the previous username is created within hours. As American ISIS supporters are continuously suspended from Twitter, creating a new account becomes increasingly difficult, leading some to turn to others for assistance. The user’s first tweet is often an image of the Twitter notification of suspension, proving that they are the owner of the previous account, along with a request for shout-outs. The new accounts are then retweeted by others, allowing the user to regain his or her previous online following.

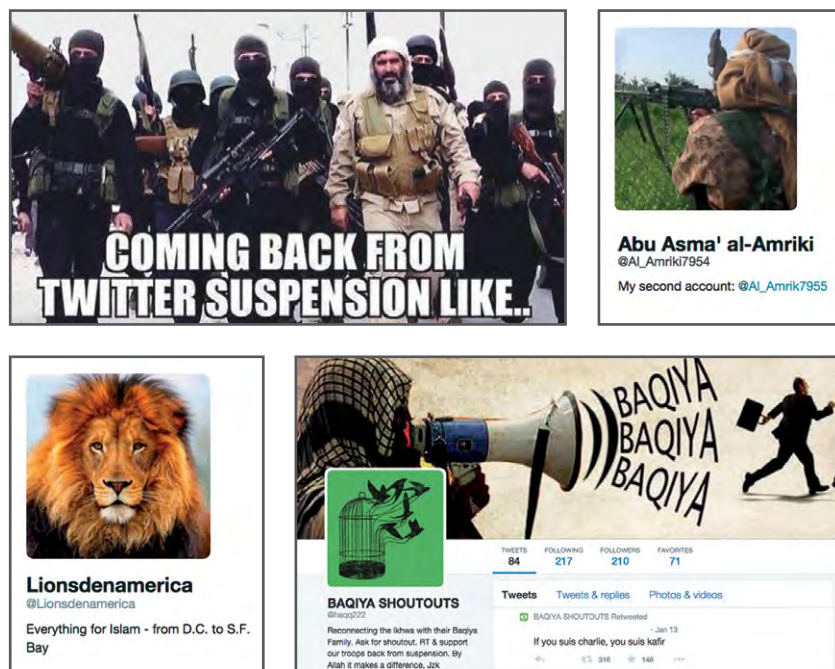


FIG. 29 Clockwise: A user announces a new account; examples of node, shout-out, and amplifier accounts.

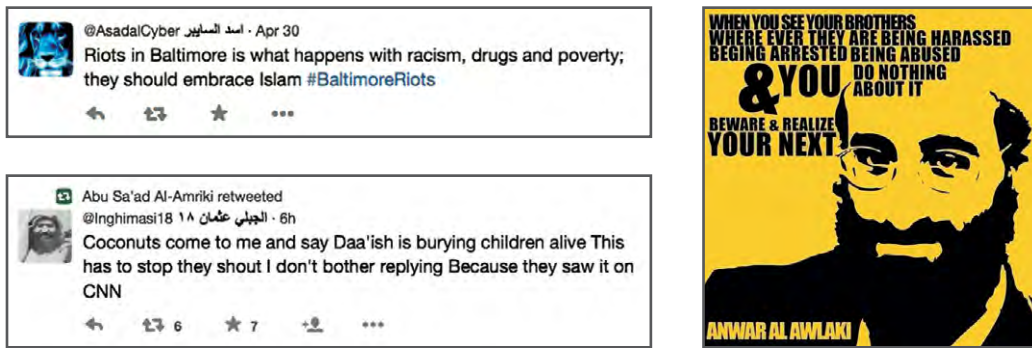


FIG. 30 Clockwise: Interjecting in the #BlackLivesMatter conversation; sharing a quote from Anwar al Awlaki; dismissing ISIS critics as “coconuts.”

Shout-out accounts have further bolstered connectivity by employing Twitter’s List function, which allows users to view all tweets by list members on a single page, gain access to full member lists, and weed out suspicious or contrarian accounts. American ISIS supporters have begun sharing ever-expansive lists of individuals to block through the website Block Together, a task that was previously un-delegated and decentralized. In the past individual accounts would collect a handful of accounts to block and share the list with peers via a series of tweets of posts from the website JustPaste.it. While it is unclear who is curating these lists, American ISIS supporters constantly capitalize on new tools to extend the tenure of their accounts.

Communicating primarily in English, American ISIS supporters discuss a wide range of topics, from open support for gruesome acts of terror to boringly benign banter.¹⁰⁴ When ISIS releases propaganda materials in foreign languages (namely Arabic), members of the American community often ask the larger online ISIS echo chamber for translation assistance. Popular content for American ISIS supporters’ posts include photos, videos, and discussion of human rights abuses committed by the Syrian, American, Israeli, and various Arab governments; news of ISIS’s military victories and provision of social services; photos of deceased ISIS militants

commemorating their status as martyrs; and mocking of Western (and now also Russian) leaders’ perceived weakness and ignorance.

On occasion, American ISIS supporters exploit hashtags related to U.S. policies and political movements. For example, some tried interjecting in the #BlackLivesMatter conversation in an attempt to bolster their support among African American Muslims and spread their propaganda to unsuspecting Americans of all backgrounds. Using Black Lives Matter–related hashtags, American ISIS supporters and globally based ISIS recruiters alike have sought to capitalize on unrest in Ferguson, Missouri, and Baltimore, trying to tailor their U.S.-targeted propaganda to resonate with segments of the African American community.¹⁰⁵

American accounts, like the larger ISIS echo chamber, tend not to tolerate dissent and silence attempts at nuance. Muslim religious leaders, particularly those living in the West, who condemn ISIS are routinely dismissed as “coconuts,” a derogatory term used to insult those accused of denying their Muslim identity. Many U.S.-based Muslim scholars and activists, even those from conservative backgrounds, are subject to routine death threats.

American ISIS supporters also act as “spotters” for future recruits. Our researchers observed real-time cases of

104. Our researchers include a number of Arabic speakers who reviewed Arabic-language accounts for individual who self-identified as American and found a small contingent of Americans using Arabic as their primary language.

105. Justine Drennan, “Islamic State Supporters Urge Baltimore Rioters to Join Extremist Cause,” *Foreign Policy*, April 28, 2015.

recently converted Americans pulled into the ISIS echo chamber. In one case the seemingly naïve individual posted general questions about religion, to which ISIS supporters quickly responded in a calm and authoritative manner. After a few weeks, the accounts of hardened ISIS supporters slowly introduced increasingly ardent views into the conversation. The new recruit was then invited to continue the conversion privately, often via Twitter's Direct Message feature or on other private messaging platforms such as surespot.

Real-World Clusters: ISIS's Den in America

The role of social media in recent developments in the jihadist scene in America, as elsewhere, is central. Yet, it would be incorrect to overemphasize the impact of social media by considering it the sole medium of radicalization and mobilization for American ISIS supporters. A close examination of the individuals analyzed for this study reveals a significantly more nuanced reality in which the importance of social media, while present in virtually all cases, differs substantially from case to case.

To be sure, cases of web-driven, individual radicalization have increased in frequency with the rise of ISIS. Individuals like Shannon Conley and Christopher Cornell (discussed below) are quintessential examples of individuals whose radicalization was confined to the virtual space, completely devoid of contact with like-minded individuals in the physical world.

Yet, in other cases the role of the Internet is not as all-encompassing, but rather complementary to equally, if not more, important dynamics in the physical world. In these cases, individual ISIS sympathizers did not begin their radicalization trajectories alone in front of a computer screen, but rather via face-to-face interactions through preexisting social contacts who already embraced jihadist ideology. Over time, these individuals tend to form a cluster: a small informal group of like-minded individuals whose internal dynamics reinforce the beliefs of its members. Just as the virtual community of ISIS supporters acts

as an echo chamber, these real-life connections reinforce and strengthen individual commitment to ISIS.

Individuals who belong to these informal clusters typically become consumers of jihadist propaganda on the Internet. While the online echo chamber undoubtedly contributes to the individual's and thus the cluster's radicalization, the one-on-one and group dynamics cultivated in the physical world sometimes play a greater role. In these scenarios, online and offline dynamics complement one another, both contributing to and accelerating the cluster's members' radicalization.

These group dynamics are also common in several European countries, where informal clusters often form at the margins of radical mosques, Salafist organizations, or student groups, or simply through the interaction of like-minded acquaintances in the neighborhoods of many European cities and towns. As with other radicalization-related dynamics, this phenomenon, typical of the European reality, occurs on a significantly smaller scale and less frequently than in the U.S. Yet, our analysis revealed that while some individuals fit the profile of the "lone actor," others were part of a cluster of individuals of varying sophistication who radicalized and mobilized together.

The U.S. case that most closely resembles these European dynamics is that of the Minneapolis cluster. Americans traveling to fight in conflict zones is not a new phenomenon for the Minneapolis–St. Paul area. From 2007 to approximately 2009, nearly two dozen individuals, mostly ethnic Somalis, absconded from the U.S. to join the terrorist group al Shabaab.¹⁰⁶ The departing left in small groups, the first wave providing moral and logistical support to those who followed. In response, the FBI began a massive investigation, dubbed Operation Rhino, in an attempt to stem travel to conflict areas.

At the time, some analysts argued that the wave from Minneapolis was unique to the Somali conflict. This contention was challenged in 2014, when a number of Somali Americans shifted their focus from Somalia to Syria. Since

106. B. Todd Jones, "Operation Rhino," *Office of the United States Attorneys*, July 8, 2015.

then, at least 15 individuals have traveled or attempted to travel to join ISIS.¹⁰⁷ They relied on a well-worn recruiting apparatus that leveraged deep personal, familial, and community relations. Chief among that recruiting network was Mohamed Abdullahi Hassan, one of the first to leave Minneapolis to join al Shabaab, becoming a linchpin who recruited others to follow his example. A similar dynamic occurred with Abdi Nur who, after joining ISIS in 2014, sent messages back to his friends in Minneapolis offering contact information and fake passports.¹⁰⁸ Many of the Somali-American ISIS recruits grew up in the same community, attended the same schools, and worshiped at the same mosque. Several of these individuals inherited connections to al Shabaab, including one individual whose older brother joined the group and another who lived with a friend who later departed for Somalia to join the fight.¹⁰⁹

While the Minneapolis cohort has received significant media attention, a less known but equally revealing case unfolded in St. Louis, Missouri. At the center of the cluster is a charismatic Bosnian immigrant, Abdullah Ramo Pazara. A veteran of the Bosnian civil war, Pazara came to America in the second half of the 1990s and lived a seemingly unremarkable life. He married, worked as a truck driver and developed a passion for motorcycles. But in 2011, after both his marriage and trucking business unraveled, he developed an interest in a literalist interpretation of Islam.¹¹⁰ In 2013, just days after obtaining U.S. citizenship, Pazara left for Syria, where he quickly rose to the rank of *emir* (commander) of a Balkan-dominated battalion working under well-known top ISIS commander Omar al Shishani.¹¹¹

Pazara's actions were supported by the efforts of a small group of Bosnian Americans. The men and women lived in St. Louis (home to America's largest Bosnian population) and suburban Illinois towns, but a handful originally hailed from the Bosnian town of Teslic. The group collected almost eight thousand dollars, which they sent to Pazara and families of ISIS fighters in the Balkans.¹¹² Coordinating their activities through Facebook and



FIG. 31 From the U.S. to Syria: Abdullah Ramo Pazara

107. Paul McEnroe, Abby Simons and Libor Jany, "From the Heartland to Jihad: How a Group of Young Men from Minnesota Were Drawn Into ISIL's Campaign of Terror," *Minnesota StarTribune*, September 20, 2015.

108. McEnroe, Simons and Jany, "From the Heartland to Jihad," *Minnesota StarTribune*, September 20, 2015.

109. Yuen, Ibrahim and Aslanian, "Called to Fight," *MPR*, March 25, 2015.

110. Robert Patrick, "Allegations of St. Louis Terrorism Support Rooted Back in Bosnian War," *St. Louis Post-Dispatch*, April 11, 2015.

111. Patrick, "Allegations of St. Louis Terrorism Support Rooted Back in Bosnian War," *St. Louis Post-Dispatch*, April 11, 2015. See also Radio Sarajevo, "U Siriji Poginuo Ramo Pazara, Komandant Džihadista iz BiH," September 25, 2014.

112. Robert Patrick, "Woman Pleads Guilty in Terror Funding Case with St. Louis Ties," *St. Louis Post-Dispatch*, September 28, 2015.

email, the group also purchased “United States military uniforms, tactical combat boots, surplus military goods, tactical gear and clothing, firearms accessories, optical equipment and range finders, rifle scopes, equipment, and supplies” for Pazara’s battalion in Syria.¹¹³ Authorities dismantled the ring in February 2015, arresting six individuals (three men and three women) on terrorism-related charges. Pazara was reported killed while fighting against Kurdish forces in Kobane in the fall of 2014.¹¹⁴

While the Minneapolis and St. Louis clusters each revolved around an ethnic bond, a separate cluster in the greater New York City area came together in a different



FIG. 32 Nader Saadeh



FIG. 33 Alaa Saadeh

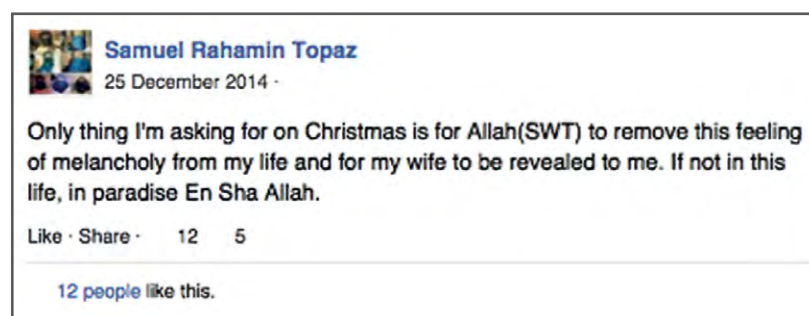


FIG. 34 Samuel Topaz on Facebook.

way and had a more heterogeneous makeup. The group initially connected as early as November 2012, when the then-teenage Nader Saadeh, a New Jersey resident of Jordanian/Palestinian descent, shared his jihadist sympathies with the like-minded Munther Omar Saleh, a teenager from Queens.¹¹⁵ In late 2014, Nader involved his older brother Alaa Saadeh and Samuel Topaz, a high school friend of mixed Jewish/Dominican descent from Fort Lee who had converted to Islam. In addition, Saleh soon incorporated Staten Island’s Fareed Mumuni into the group. The five spent their days absorbing, discussing, and sharing ISIS propaganda—both online and in the physical world. The FBI, which had the group under surveillance for months, listened in as the young men discussed building a “small army” and traveling to the Middle East.¹¹⁶

By the spring of 2015 the group had cemented their plans to join ISIS. Despite Nader’s initially successful travel to Amman, he was arrested by Jordanian authorities in the days following his arrival. In the wake of Nader’s arrest, the FBI swooped in, arresting the four remaining members of the cluster in the New York area. The arrest of Mumuni escalated, as the native of Ghana used a kitchen knife to attack FBI agents attempting to execute a search warrant of his home.

The Program on Extremism’s research has uncovered the presence of other small groups of apparent ISIS sympathizers in various American cities.¹¹⁷ One of them, located in Texas, revolves around a few charismatic individuals and an Islamic studies group. Another, based in the suburbs of a large Midwestern city, appears to be composed of former high school friends and a handful of their

113. *United States of America v. Ramiz Zijad Hodzic, et. al.*, Indictment (February 5, 2015).

114. Associated Press (AP), “Bosnian Immigrants Plead Not Guilty in Terror Financing Case,” *Yahoo! News*, February 11, 2015; Radio Sarajevo, “U Siriji Poginuo Ramo Pazara, Komandant Džihadista iz BiH,” September 25, 2014.; SAFE, “U Siriji Poginuo i Ramo Pazara iz Teslića,” September 24, 2015.; Slobodna Bosna, “Ramo Abdullah Pazara: Srpski Ratnik i Islamski Fanatik,” February 18, 2015.

115. *United States of America v. Alaa Saadeh*, Criminal Complaint (June 26, 2015).

116. *Ibid.*

117. The Program on Extremism has decided not to disclose details about these cases so as not to compromise any potential investigation.

acquaintances. As in most small clusters throughout the U.S., members of both come from diverse ethnic backgrounds and reinforce an active online life with regular interactions in the physical space.

Wide Spectrum of Support Roles

The diversity of American ISIS recruits also extends to the roles they take on in support of the cause. At one end of the spectrum is a small yet alarming number of Americans who have managed to establish deep, real world connections to ISIS. In addition to the aforementioned example of Abdullah Ramo Pazara, researchers identified a number of cases in which Americans traveled to Syria and Iraq and developed important connections to the organization.

One such case that received relatively little media attention is that of the Kodaimati clan, a Syrian-American father and his two sons who became enmeshed in shifting dynamics of two terrorist organizations. One of the sons, Mohamed Saeed Kodaimati, moved to the U.S. in 2001 where he lived for years and became an American citizen.¹¹⁸ In December 2012, Saeed (as he is referred to in the criminal complaint) traveled from San Diego to Istanbul.¹¹⁹ After three months in Turkey, Saeed was arrested by authorities and spent 35 days in prison, where he

met and interacted with a bevy of Syrian rebels, criminals, and jihadists.¹²⁰

Following his release, he travelled to Syria and began working in the JN-run Sharia Authority of Hanano district in the Aleppo governorate. In his own words, Saeed became their “media person,” posting updates on the Authority’s work on various Facebook pages.¹²¹ Sometime later, his association with JN took a much more operational role. Saeed, his father, and his younger brother—whom he refers to as “Rahmo”—began participating in combat operations with JN against the Syrian army.¹²² Saeed’s father was injured on a return trip from the frontlines, apparently by a rocket attack resulting in “shrapnel that went through his side and out through his back.”¹²³ After ISIS seized control of parts of his neighborhood from JN, Saeed became an interlocutor between the two terrorist organizations. He told a friend via Facebook that his “role is more of reconciliatory one . . . I am a mediator for those who have a problem with Da’ish [ISIL].”¹²⁴ He was allowed

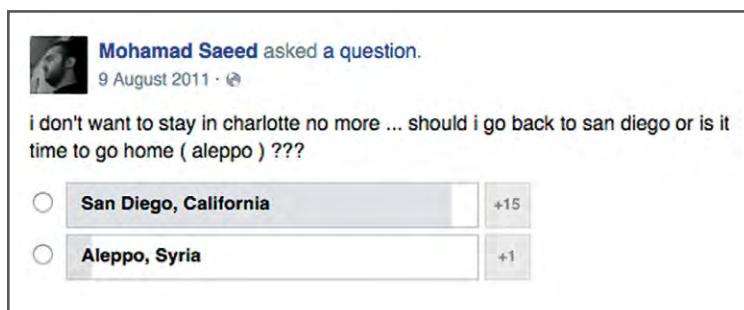


FIG. 35 Facebook post by Mohamed Saeed Kodaimati.

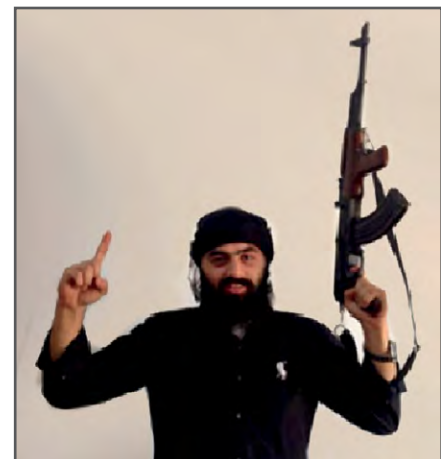


FIG. 36 Mohamed Saeed Kodaimati

118. *United States of America v. Mohamad Saeed Kodaimati*, Criminal Complaint (April 23, 2015).

119. Kristina Davis, “San Diegan Accused of Hiding ISIS Links,” *The San Diego Union-Tribune*, April 23, 2015.

120. *United States of America v. Mohamad Saeed Kodaimati*, Criminal Complaint (April 23, 2015).

121. *Ibid.*

122. *Ibid.*

123. *Ibid.*

124. *Ibid.*

to keep his weapons and, while stating to the FBI he never swore allegiance to ISIS, he claimed that “they know me, who I am, and I don’t have any problems with them.”¹²⁵

After three years in Syria, Saeed attempted to return to the U.S. but was prevented from boarding his flight in Turkey.¹²⁶ Local authorities sent him to the U.S. embassy, where law enforcement and diplomatic security questioned him regarding his activities in Syria.¹²⁷ Over the course of several discussions, he grossly mischaracterized his time in Syria, contending that he did not participate in any violent activity.¹²⁸ Confronted with his Facebook messages and photos corroborating authorities’ belief that he served in the ranks of terrorist groups, Saeed returned to the U.S. and pled guilty to providing false statements to the FBI.¹²⁹

On the opposite end of the mobilization spectrum, a more common typology is those whose contributions to ISIS fail to exceed online declarations of support and personal fantasies of joining the group. These are the cases of people, most often indicted for attempting to provide material support to ISIS, whose links to ISIS are largely limited to the virtual realm.

A prime example of the disturbed wannabe ISIS recruit is Shannon Conley, a Colorado native who first appeared on the radar of the FBI Denver Field Office following a confrontation with a local church.¹³⁰ During the several months she attended the church, Conley complained she was being treated unfairly due to her Muslim views and dress, making her feel like a “terrorist.”¹³¹



FIG. 37 Shannon Maureen Conley

Conley showed up one day and began sketching the layout of the church’s campus, causing church officials to ban her from the premises.¹³²

In one of her many interviews with law enforcement, Conley stated she wanted to wage jihad against “kafir” in order to protect Muslim lands.¹³³ A certified nurse, she expressed the desire to become a “housewife and camp nurse” for ISIS militants in Syria.¹³⁴ Obsessed with guerrilla warfare, she became a U.S. Army Explorer to learn American combat tactics that she could then teach to ISIS fighters and admitted to owning *Al Qaida’s Doctrine for Insurgency: Abd Al-Aziz Al-Muqrin’s A Practical Course for Guerilla War*.¹³⁵ She began communicating with a Tunisian ISIS fighter on Skype, who pushed her to join him in Syria as his wife.¹³⁶ The invitation prompted the FBI to contact

125. *United States of America v. Mohamad Saeed Kodaimati*, Criminal Complaint (April 23, 2015).

126. *Ibid.*

127. *Ibid.*

128. *Ibid.*

129. *Ibid.*

130. *United States of America v. Shannon Maureen Conley*, Criminal Complaint (April 9, 2014).

131. *Ibid.*

132. *Ibid.*

133. *Ibid.*

134. *Ibid.*

135. *Ibid.*

136. *Ibid.*



FIG. 38 Christopher Lee Cornell

Conley's parents, who joined authorities in an effort to keep Conley in the U.S. Despite their efforts, Conley's father discovered a one-way plane ticket to Turkey and contacted the FBI. The following day, his daughter was arrested while attempting to board a flight to Germany at Denver International Airport.¹³⁷

A similar case is that of Christopher Lee Cornell. Born in a Cincinnati suburb, Cornell wrestled in high school and is remembered by teachers as a "typical student."¹³⁸ After graduating in 2012, Cornell, described by his father as a "big mama's boy" whose best friend was a cat, lived with his parents and was unemployed.¹³⁹ In the summer of 2014 Cornell converted to Islam, growing his beard

and donning traditional Muslim clothing.¹⁴⁰ He became increasingly angry, isolated, and withdrawn, often attracting harassment from neighbors.¹⁴¹ Cornell developed an online persona as Raheel Mahrus Ubaydah and a network of contacts—among them an FBI undercover operative.¹⁴² Cornell informed the operative of his plans to attack the U.S. Capitol and set off a series of pipe bombs.¹⁴³ He was arrested in January 2015 after purchasing several semi-automatic rifles and approximately 600 rounds of ammunition as part of an FBI sting.¹⁴⁴

Determining a link to ISIS has proven challenging in a few recent cases. The most prominent is that of Mohammad Abdulazeez, the shooter whose attacks on two military installations in Chattanooga in July 2015 left five dead. Following the incident, investigators discovered Abdulazeez operated a blog focusing on Islamist themes, and downloaded copies of Anwar al Awlaki's sermons. Yet authorities were unable to determine a link to or a demonstrated interest in ISIS.¹⁴⁵ Suggesting additional or concurrent potential explanations for his actions, before the attack Abdulazeez allegedly stopped taking his anti-depression medication and regularly consumed illegal narcotics.¹⁴⁶

A second incident that escapes easy categorizations took place in Oklahoma in September 2014, when 31-year-old convert Alton Nolen beheaded a former coworker. Nolen carried out the gruesome act shortly after having been suspended from his job, potentially indicating that he was motivated by personal reasons.¹⁴⁷ On the other hand,

137. Michael Martinez, Ana Cabrera and Sara Weisfeldt, "Colorado Woman Gets 4 Years for Wanting to Join ISIS," *CNN*, January 24, 2015.

138. AP, "Teachers: Ohio Man Accused in Terror Plot a Typical Student," *WHSV.com*, January 15, 2015.

139. Ben Brumfield, Pamela Brown and Dana Ford, "FBI Says Plot to Attack U.S. Capitol was Ready to Go," *CNN*, January 15, 2015.

140. Brumfield, Brown and Ford, "FBI Says Plot to Attack U.S. Capitol was Ready to Go," *CNN*, January 15, 2015.

141. Kimball Perry and Patrick Brennan, "Father: Terror Plot Suspect was a 'Momma's Boy,'" *Cincinnati.com*, January 23, 2015.

142. *United States of America v. Christopher Lee Cornell*, Criminal Complaint (January 14, 2015).

143. *Ibid.*

144. *Ibid.*

145. Jonathan Dienst and Miguel Almaguer, "Mohammad Youssef Abdulazeez Downloaded Recordings from Radical Cleric, Officials Say," *NCB News*, July 21, 2015.

146. Greg Jaffe, Cari Wade Gervin and Thomas Gibbons-Neff, "Tenn. Gunman Used Drugs, Struggled with Clash of Faith," *The Washington Post*, July 18, 2015.

147. Abby Ohlheiser, "What we Know about Alton Nolen, Who as been Charged with Murder in the Oklahoma Beheading Case," *The Washington Post*, September 30, 2014.

the act's modalities and the fact that Nolen, while having no known contact with ISIS, was an avid consumer of jihadist propaganda online, suggest that the case could be more than an ordinary incident of workplace violence.¹⁴⁸

Similarly unclear is the case of Zale Thompson, who attacked four New York Police Department officers with a hatchet in October 2014.¹⁴⁹ His online search history shows an interest in jihadist videos, some of which included ISIS material.¹⁵⁰ However, Thompson, who was described by law enforcement as a loner with possible mental problems, also consumed black nationalist and other anti-government propaganda online, making an

even inspirational link to ISIS uncertain at best.

Perhaps the most puzzling is the case of Joshua Ryne Goldberg, a 20-year-old Jewish Floridian who was arrested in September 2015 for distributing information relating to a bomb plot targeting a 9/11 memorial ceremony in Kansas City.¹⁵¹ Goldberg had multiple online personas: an ISIS-affiliated Australian jihadist, a white supremacist, a feminist, and a free-speech radical.¹⁵² Regardless of his life as a virtual troll, Goldberg did nonetheless provide an individual, who unbeknownst to Goldberg was an FBI informant, with instructions for constructing a bomb from a pressure cooker filled with nails.¹⁵³

148. Michael Pearson, "Who is Oklahoma Beheading Suspect Alton Nolen?," *CNN*, September 30, 2014.

149. Agence France-Presse, "New York Police Brand Hatchet Attack 'Terrorist' Act," *Yahoo News!*, October 24, 2015.

150. Caitlin Nolan, Kerry Burke, Rocco Parascandola, Joseph Stepansky and Thomas Tracy, "Hatchet-wielding Man Shot Dead by NYPD Cops in Queens; Police Eye Possible Terrorism Motive," *New York Daily News*, October 24, 2014.

151. Garrett Pelican, "Orange Park Man, 20, Indicted in 9/11 Memorial Bomb Plot," *First Coast News*, September 15, 2015.

152. Katie Zavadski, "'Terrorist' Troll Pretended to be ISIS, White Supremacist, and Jewish Lawyer," *The Daily Beast*, September 11, 2015.

153. *United States of America v. Joshua Ryne Goldberg*, Criminal Complaint (September 10, 2015).

CONCLUSION

Countering ISIS's American Recruits

THIS REPORT has provided a look inside the bubble of American ISIS sympathizers, a diverse and diffuse scene that the FBI estimates include hundreds, if not thousands, of individuals. To be sure, most of the participants in this counter-culture will never make the leap from talk to action, from being keyboard warriors to actual militancy. Some will mature out of what is just an awkward adolescent phase. Others simply lack the personality traits necessary for committing terror attacks or setting out for ISIS territory. On a more mundane level, others find themselves restrained by the practical commitments of their daily lives.

Nonetheless, a subset of the Americans inside the domestic ISIS bubble, whether they operate individually or in small clusters, will at some point move from chatter to action. For some that will mean boarding a flight to the Middle East. For others, it will entail gathering the equipment needed to carry out an attack inside the United States. The decision to attack the home front may follow unsuccessful attempts to link up with recruiters overseas. In other cases, the attacker's horizon remains focused on targeting the "infidels" inside America.

The diversity of ISIS's American recruits and the wide range of ways they demonstrate their support requires careful consideration prior to any potential policy response. Because there is no standard recruit profile, there is also no silver bullet that will blunt ISIS's allure. Recognizing this complexity is a vital initial step for policymakers, law enforcement officials, civic leaders, teachers, and parents when crafting effective solutions.

Stepping back to consider the implications of the demographic data and personality profiles surveyed in this report, several essential policy recommendations emerge:

First, the number of ISIS recruits in America and the

complex scene they comprise poses a challenge that cannot be solved solely by arrests. Law enforcement vigilance is vital but insufficient on its own. Moreover, many early-stage ISIS sympathizers have not necessarily broken any laws. A comprehensive preventive approach to radicalization is necessary. Unfortunately, the resources devoted to countering violent extremism (CVE) by the U.S. government remain woefully inadequate for the task at hand.¹⁵⁴ Robust funding and dynamic programs are needed immediately.

Second, an effective alternative to arrest is intervention to help sway individuals from the path of radicalization. Our research identified 71 ISIS recruits in the U.S. legal system—a figure far short of the 250-plus Americans who, according to government officials, have attempted to or actually traveled to Syria and Iraq. Why those 180 individuals are not in the legal system has several explanations, including the fact that many cases fail to meet the legal threshold for arrest. This factor reinforces the need for the government to create a framework for targeted interventions with radicalized individuals by non-law enforcement groups, as well as legal parameters so that interveners are not at risk of civil and criminal liability if their efforts fail.

Third, while interventions are a potential solution for Americans already on the path to radicalization, it would be even more effective to prevent citizens from even starting that perilous journey. Researchers and civic leaders should empirically analyze which messaging resonates best with audiences commonly targeted by ISIS, recognizing that a range of narratives deployed for unique audiences will likely be necessary.

Fourth, there are individuals and organizations that would like to implement counter-ISIS messaging online, yet worry that their activities might inadvertently attract the attention of law enforcement. For instance, several

154. Lorenzo Vidino and Seamus Hughes, "Countering Violent Extremism in America," Program on Extremism, June 2015.

American Muslims consulted for this report expressed willingness to engage ISIS supporters online yet hesitated to do so for fear of falling onto the FBI's radar by engaging in dialogue with radicals. The government should provide legal guidance and recommend best practices so that potential counter-messengers can make informed decisions on whether and how to engage.

Finally, there is a largely untapped opportunity to leverage American ISIS recruits who have become disillusioned with the cause. These individuals have dropped out for a variety of reasons, whether experiencing the brutality of life under ISIS firsthand or finding a more positive outlet for the quest that led them to ISIS in the first place. U.S. officials would do well to provide avenues for their stories to be amplified to help dissuade would-be recruits.

The government should consider, within reason, limited immunity for some returning foreign fighters, as their messages are more likely to resonate than those delivered by most other counter-messaging programs.

While jihadist causes have lured American recruits for several decades, the surge spurred by the rise of ISIS and its sophisticated marketing of its counter-culture to impressionable Americans is unprecedented. The data and vignettes provided in this report illuminate the complexity of the threat and caution against simple solutions. In their response to this challenge, American political and civic leaders will need to be bold, experimental, and receptive to novel policies and initiatives in order to defeat ISIS and protect some of our fellow citizens from falling into its clutches.

APPENDIX

The 71 individuals charged for ISIS-related activities (as of November 12, 2015)

| | |
|-------------------------------|----------------------------|
| Abdi Nur | John T Booker |
| Abdirahman Yasin Daud | Jonas 'Yunus' Edmonds |
| Abdul Malik Abdul Kareem | Joshua Ray Van Haften |
| Abdullahi Mohamud Yusuf | Justin Nojan Sullivan |
| Abdurasul Hasanovich Juraboev | Keonna Thomas |
| Abror Habibov | Leon Nathan Davis III |
| Adam Dandach | Mediha Medy Salkicevic |
| Adnan Abdihamad Farah | Michael Todd Wolfe |
| Ahmed Mohammed El Gammal | Miguel Moran Diaz |
| Akba Jihad Jordan | Mohamad Saeed Kodaimati |
| Akhror Saidakhmetov | Mohamed Abdihamid Farah |
| Akmal Zakirov | Mohamed Abdullahi Hassan |
| Alaa Saadeh | Mohammad Hamza Khan |
| Alexander Ciccolo | Mufid Elfgeeh |
| Alexander E Blair | Muhammad Oda Dakhlalla |
| Ali Saleh | Muhanad Badawi |
| Ali Shukri Amin | Munther Omar Saleh |
| Arafat Nagi | Nader Elhuzayel |
| Armin Harcevic | Nader Saadeh |
| Asher Abid Khan | Nicholas Rovinski |
| Asia Siddiqui | Nicholas Teausant |
| Avin Marsalis Brown | Nihad Rosic |
| Bilal Abood | Noelle Velentzas |
| Christopher Lee Cornell | Ramiz Zijad Hodzic |
| David Wright | Reza Niknejad |
| Dilkhayot Kasmiov | Robert C. McCollum |
| Donald Ray Morgan | Samuel Rahamin Topaz |
| Fareed Mumini | Sedina Unkić Hodzic |
| Guled Ali Omar | Shannon Maureen Conley |
| Hamza Naj Ahmed | Tairod Nathan Webster Pugh |
| Hanad Mustafe Musse | Terrence McNeil |
| Harlem Suarez | Unnamed minor (PA) |
| Hasan Edmonds | Unnamed minor (SC) |
| Heather Elizabeth Coffman | Yusra Ismail |
| Jaelyn Delshaun | Zacharia Yusuf Abdurahman |
| Jasminka Ramic | |

What explains the recent surge in American jihadi recruits? Who are the Americans lured by the siren songs of ISIS's propaganda? How do they embrace such radical ideology? What do they seek?

This report provides a comprehensive overview of ISIS-related radicalization and mobilization in the United States.

Program on Extremism

THE GEORGE WASHINGTON UNIVERSITY

www.cchs.gwu.edu/program-extremism ■ @gwupoe