



Homeland Security Information Network – Faith Based Organizations (HSIN-FBO)

Collaborating to Protect Our Nation's Faith Based Organizations (FBO)

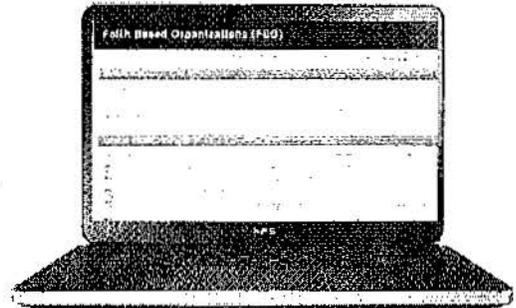
Successful protection of our nation's FBOs requires coordination and collaboration between FBOs, the Department of Homeland Security (DHS), other Federal agencies and State and Local government. The Homeland Security Information Network – Faith Based Organizations (HSIN-FBO), a community under HSIN-Critical Infrastructure (HSIN-CI), serves as a common platform to provide tactical and planning communication functionality among FBO security, safety, and disaster response partners. HSIN is a secure, unclassified, web-based communications system that serves as the primary, nationwide DHS collaboration system for sharing Sensitive But Unclassified Information.

Through HSIN-FBO Users:

- Gain access to HSIN-FBO and HSIN-CI, the nation's primary source for Sensitive But Unclassified critical infrastructure protection information
- Maintain a direct, trusted channel with DHS and other vetted security and safety partners
- Communicate information pertaining to threats, vulnerability, security, response and recovery activities affecting faith based and cross sector operations

HSIN Features:

- Enhanced Security and Identity Management through Two-Factor Authentication and Identity Proofing
- Relevant Content such as Infrastructure Protection Alerts, Information Bulletins, Announcements and Analysis
- Situational Updates and Incident Reports



Request Access to HSIN-FBO

To request access to HSIN-FBO, please email your name, employer, work email address and title/position description to hsinci@hq.dhs.gov

If you need more information regarding HSIN-FBO, please contact HSINCI@hq.dhs.gov.



Faith-based Security and Communications Advisory Committee

Homeland Security Advisory Council
May 2012



Secretary's Tasking of HSAC

The Department of Homeland Security (DHS) has a consistent history of reaching out to, and working with, faith-based organizations (FBOs) on a broad range of issues. Secretary Napolitano tasked the HSAC to “...explore current and potential security information sharing opportunities and methods between DHS and FBOs. The Committee will address how DHS can better support local security officers and organizations efforts to keep FBOs communities safe, secure, and resilient while providing recommendations to the HSAC for consideration.”



Secretary's Tasking (Cont.)

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

- **Structural Organization:** In times of crisis, FBO leaders often play a critical role in providing support and delivering accurate and trusted information to communities. How can DHS better support FBOs efforts to relay threat-based information to appropriate parties? How can information sharing be improved when DHS receives threat-specific information? How can DHS help FBOs more effectively receive and appropriately disseminate information?
- **Deepening the Partnership:** Two-way information sharing is a critical asset in preventing crime and terrorism in communities across the country. What immediate and long term steps can be taken to enhance this exchange? What roles can FBOs play in facilitating two-way information sharing? What mediums or mechanisms would best facilitate two-way information sharing? What roles can fusion centers play in ensuring that time-sensitive threats are relayed effectively to FBOs?



Development of Recommendations

- Recommendations were developed through a series of conference calls and two in-person meetings.
- From January 2012 to May 2012, the Faith-based Security and Communications Advisory Committee (FBAC) conducted a series of conference calls, meetings, and deliberations, engaging Subject Matter Experts from around the nation.
- Led by Co-Chairs Bonnie Michelman and Sheriff Leroy D. Baca, and Co-Vice Chairs John Hodson and Paul Goldenberg, the FBAC developed a series of principles, findings, and recommendations.



Faith-based Advisory Committee Value Statement

The members of the faith-based organizations that serve on the Department of Homeland Security Advisory Council's FBAC strongly, and uniformly denounce violence against any other faith-based organizations to include their houses of worship and those who worship. When any threats target one member of the faith-based community, they target all of us and will be met with stiff resistance in their attempt to divide us against hate.



Guiding Principles:

- We encourage further outreach and training in order to achieve social cohesion between FBOs.
- Ensure all outreach efforts are based on mutual respect, transparency and trust.
- The FBAC hopes that recommendations contained in this report benefit all FBOs.
- Provide safe places of worship for constituencies and protection of assets for all faiths.
- Protect our country and preserve our freedoms within our religious communities.
- Proactively diminish our risks.
- Build collaboration between state, local, tribal and FBOs.



General Findings

- **DHS recognizes the importance of sharing homeland security information with FBOs** – The Advisory Committee members felt strongly that the Secretary and the Department recognize the importance and value of a two-way security information process with FBOs to ensure their infrastructure is resilient and protected, by being a strategic and valuable partner in security awareness, prevention, planning, operations, and response.
- **A more formal relationship is wanted and required** - Both DHS and FBOs would benefit from stronger, more structured relationships that will strengthen the nation's security by the effective sharing of relevant, accurate, timely, and actionable homeland security information. Advisory Committee members felt that faith-based organizations would like to enhance the current partnership with DHS to a structured one that will establish better communications relationship regarding security between DHS and the faith-based organizations.



General Findings (Cont.)

- **Improved relationships** – FBOs recognize the importance of DHS in assisting them to ensure their infrastructure is resilient and protected. Faith-based institutions understand that they are located in communities and have a unique and critical role in the “home town” security strategy.¹
- **Faith-based organizational capacity** – FBOs currently have different capacities to implement a two-way security information sharing process. Many FBOs recognize and agree on the value of DHS and FBOs information sharing collaboration.



General Findings (Cont.)

- **Successful FBO information sharing models** – DHS has successful two-way homeland security information sharing models with various FBOs.
- **Resilience and protection** – FBOs are committed to the resilience and protection of their houses of worship and individuals who worship there.
- **Civil rights and civil liberties** – FBOs will work diligently to ensure civil liberties are preserved in their engagement with DHS or other Federal agencies.
- **Religious freedom** – FBOs will preserve principles of religious freedoms during any and all discussions with DHS or other Federal agencies.
- **Partners with law enforcement** – It is important that FBOs are not perceived as extensions of law enforcement but as partners with law enforcement entrusted by their own communities.



Recommendations to DHS on Sharing of Threat Information

1. **DHS should identify and work with FBOs to establish a formal two-way process for sharing homeland security information.**
2. **DHS should designate points of contact to interact with faith-based communities.**
 - DHS should designate a senior level full time position with access to senior DHS leadership within the DHS Headquarters whose primary responsibility is sharing homeland security and threat information issues with the faith-based community.
 - DHS should assign points of contact in each fusion center to work with their state and local faith communities.



Threat Information Recommendations (Cont.)

3. **DHS should support additional infrastructure to share security information with FBOs.**
 - Example:
 - DHS created a secure portal for DHS and FBOs to share information on the Homeland Security Information Network (HSIN).²
- 3(a). DHS should work with the FBOs on methodology and best practices for an effective information sharing network.



Threat Information Recommendations (Cont.)

4. **DHS should include FBOs in current and future planning documents.**
 - FBOs should be included in the communications and implementation plans of the National Terrorism Advisory System³ in order to ensure communities remain engaged and informed about potential terrorist threats and acts.
 - DHS should ensure that the FBOs information-sharing component is placed in the Presidential Policy Directive 8, specifically in the Resilience, Prevention and Protection sections under current revision status of the National Response Framework.⁴



Recommendations to DHS on Engagement and Outreach to FBOs

5. **DHS should increase its outreach to all FBOs at the local level to inform and educate individuals and communities about DHS, its mission, and to support security needs of the FBOs.**
 - DHS should leverage existing relationships between state and local law enforcement and local government officials as part of this outreach in order to streamline communication with local FBOs.
 - DHS should coordinate with fusion centers and Infrastructure Protection's⁵ Protective Security Advisors (PSA).
 - DHS should demonstrate that this initiative is a priority by allocating appropriate funds.



Recommendations to DHS on Engagement and Outreach to FBOs (Cont.)

6. **DHS should support collaborative forums to highlight the effectiveness of multilateral engagement and to build trust between FBOs and Public Safety officials.**
 - DHS should participate in community FBOs activities which build trust and highlight cooperation.
 - DHS should facilitate introduction to national and local incident emergency responders and local elected officials to advance FBOs own readiness and security infrastructure.



Recommendations to DHS on Engagement and Outreach to FBOs (Cont.)

7. **DHS should create messaging campaigns on FBO partnerships, which include public service announcements highlighting collaboration with state and local law enforcement.**
 - DHS should support FBOs in developing a comprehensive communication strategy (share best practices of timely actionable incident-specific collaboration among FBOs).
 - DHS should assist FBOs in assessing international threat information and its relevance to their domestic constituencies.

8. **DHS should continue the operations of the Homeland Security Advisory Council's FBAC and provide it with additional taskings focused on FBOs security.**



Recommendations to DHS on Engagement and Outreach to FBOs (Cont.)

9. **DHS should continue to develop and support DHS faith-based pilot projects (e.g., DHS pilot projects with the Office of Infrastructure Protection and with the Office of Intelligence and Analysis).**

10. **DHS through the FEMA grants process should continue to support and increase grant funding (e.g. federal, state, and local grants) to bolster FBOs homeland security information sharing, resilience efforts and infrastructure protection.**



Recommendations to DHS on Training and Best Practices

11. **DHS should train and monitor the Protective Security Advisors (PSA) to engage and work closely with faith-based communities on infrastructure protection, training, etc.**
 - DHS should create a PSA manual for collaborating with FBOs (e.g., train PSAs in cultural awareness, reporting procedures).
 - DHS should support and provide a “comprehensive” security response to FBOs such as: providing infrastructure resiliency assessments for houses of worship, information on significant events/meetings, cyber-security, etc.
 - DHS should work with its Federal partners to create a fusion center manual for collaborating with FBOs that further integrates federal, state and local law enforcement best practices.
 - DHS should provide additional funding for PSA support and training.



Recommendations to DHS on Training and Best Practices (Cont.)

- 12) **DHS should work with fusion centers and FBOs to educate each other on their respective roles and responsibilities.**
 - DHS should provide a “common-scenarios” quick reference guide for FBOs. For example it could include a matrix that highlights what to do if a certain scenario occurs.
 - DHS should develop FBO/fusion center joint training programs with strategic partners (e.g. an FBO fusion center liaison) on relationship-building and best practices. These programs should include local, state and federal law enforcement.
- 13) **DHS, in partnership with local law enforcement, should train interested FBOs on Suspicious Activity Reporting (SARs) and "If You See Something, Say Something™" to empower and encourage suspicious activity reporting.**



Recommendations to DHS on Training and Best Practices (Cont.)

- 14) **DHS should work with FBOs to share best practices and to assist them in developing a security manual for houses of worship, religious schools and faith-based activities.**
 - DHS should train and assist FBO representatives to assess information sharing capacity and security capabilities.
 - DHS should train FBOs to identify, communicate, and utilize their basic National Incident Management System⁷ roles for prevention and protection response.
- 15) **DHS provide an annual FBO award for security best practices.**
- 16) **DHS should include representatives of FBOs in the planning for the National Fusion Center Annual Training and other appropriate venues to initiate action around the mutual needs of FBOs and fusion centers.**



RECOMMENDATIONS FOR FAITH-BASED ORGANIZATIONS TO ENSURE EFFECTIVE 2-WAY INFORMATION SHARING

- 1. FBOs are encouraged to designate a security point of contact within their community and communicate who that person is with the designated DHS point of contact.**
- 2. FBOs should provide their information sharing security needs with the designated DHS point of contact.**
- 3. FBOs should provide DHS with qualitative and quantitative feedback to assure the security information product is disseminated, acted upon, and useful to the FBOs.**
- 4. FBOs should meet with their network to discuss information sharing, risk management, "If You See Something, Say SomethingTM" Campaign, etc.**



Members of the Faith-based Security and Communications Advisory Committee

Bonnie Michelman

Director of Police, Security and Outside Services at Massachusetts General Hospital/Partners Health Care (Co-Chair)

Leroy D. Baca

Sheriff, Los Angeles County (Co-Chair)

Paul Goldenberg

National Director, Secure Community Network (Co-Vice Chair)

John Hodson

Director, North America Division, Church Security Department, The Church of Jesus Christ of Latter-day Saints (Co-Vice Chair)

Salam Al-Marayati

President, Muslim Public Affairs Council

David Anba

Bishop, Coptic Orthodox Archdiocese of North America

Anju Bhargava

Founder, Hindu American Seva Charities

Kim Burgo

Vice President for Disaster Operations, Catholic Charities USA

Noel Castellanos

CEO, Christian Community Development Association

Mohamed Elibiary

Founder, Lone Star Intelligence, LLC

Eric Fusfield

Director of Legislative Affairs, B'nai B'rith International



Members of the Faith-based Security and Communications Advisory Committee (Cont.)

Terrance Mackey

Founder and Former President & Executive Director, National Coalition for Burned Churches and Community

Mohamed Magid

Executive Director, ADAMS Center

Mary Marr

Founder and President, Christian Emergency Network

Ingrid Mattson

Professor and Director, Duncan Black Macdonald Center for the Study of Islam and Christian-Muslim Relations

Lance McCune

Founder, Uniting Clergy and Police Training Program

Jack Munday

Director, Billy Graham Rapid Response Team

Eboo Patel

Founder and President, Interfaith Youth Core

Levi Shemtov

Executive Vice President, American Friends of Lubavitch

Suhag Shukla

Executive Director & Legal Counsel, Hindu American Foundation

Jasjit Singh

Associate Executive Director, Sikh American Legal Defense and Education Fund

Randy Vaughn

Director of Office of Disaster Management, National Baptist Convention



We'd like to thank the following for their contributions towards the Committee's efforts:

Dan Donaldson

Former Vice President, National Coalition for Burned Churches and Community

Michael Girguis

Father, St. Marks Coptic Orthodox Church

Kathleen Oldaker

Director, Disaster Response, Catholic Charities USA

Dickson Skipper

Director of Security, Billy Graham Rapid Response Team

Laurence Vaughn Sr.

Reverend, Mount Sinai Baptist Church



Subject Matter Experts

Haroon Azar

DHS Regional Director for Strategic Engagement-Los Angeles, DHS

Jeanine Brudenell

Officer, East African Community Liaison, Minneapolis Police Department

John Cohen

Principal Deputy Counter Terrorism Coordinator, Senior Advisor to the Secretary, DHS

Rabbi Abraham Cooper

Associate Dean of the Simon Wiesenthal Center

David Gersten

Director for Programs, The Office for Civil Rights and Civil Liberties, DHS

Ronald Haddad

Chief, Dearborn Police Department

Scott McAllister

Deputy Under Secretary, State & Local Program Office, Office of Intelligence and Analysis, DHS

Sherif Morsi

Deputy, Los Angeles County Sheriff's Department

Christy Riccardi

Special Advisor, Office of Infrastructure Protection, DHS

Dawn Scalici

Deputy Undersecretary for Analysis, Office of Intelligence and Analysis, DHS

Jannah Scott

Deputy Director, Office of Faith-based and Neighborhood Partnerships, FEMA, DHS

William Flynn

Principal Deputy Assistant Secretary, Infrastructure Protection, DHS

U.S. Department of Homeland Security



ENDNOTES

1. Home town security strategy - <http://www.dhs.gov/files/programs/hometown.shtm>
2. Homeland Security Information Network - http://www.dhs.gov/files/programs/gc_1156888108137.shtm
3. National Terrorism Advisory System - <http://www.dhs.gov/files/programs/ntas.shtm>
4. National Response Framework - <http://www.fema.gov/emergency/nrf/aboutNRF.htm>
5. Protective Security Advisors - http://www.dhs.gov/files/programs/gc_1265310793722.shtm
6. If You See Something, Say Something™ and Suspicious Activity Reporting - <http://www.dhs.gov/files/reportincidents/see-something-say-something.shtm>
7. National Incident Management System - <http://www.fema.gov/emergency/nims/>



Homeland Security

The Homeland Security Faith-based Information Sharing Pilot and HSIN-CS

The Department of Homeland Security partners with the Faith-Based Community on Critical Infrastructure Protection and Resilience

Pilot Overview

In order to advance the critical infrastructure protection and resilience strategy employed by the Department of Homeland Security (DHS), the DHS Office of Infrastructure Protection (IP) is working to implement the Secretary's DHS Faith-based initiative by expanding its partnership with Faith-Based communities through a Faith-Based Information Sharing Pilot program. This pilot has several goals:

- Identifying criteria for building information sharing partnerships with Faith-Based Organizations (FBOs) within the confines of Homeland Security.
- Gathering information-sharing requirements from actively-engaged FBOs.
- Establishing the fundamentals including governance, policy, processes, technology for building robust faith-based information sharing environments between DHS and FBO partners.

The DHS Faith-based Information Sharing Pilot seeks to enable recognized faith-based owners and operators of critical infrastructure to coordinate with each other and with the government more effectively so that they can better protect assets within their scope of responsibility.

Enabling Information Sharing on HSIN-CS

In support of the Faith-Based Information Sharing Pilot, IP collaborated with the DHS Faith-based community to gather requirements to build an information-sharing portal on the Homeland Security Information Network – Critical Sectors (HSIN-CS). Validated FBO users can coordinate on critical infrastructure protection and resilience issues and obtain approved DHS-sponsored products in a secure, virtual environment. Specifically, HSIN-CS allows users to:



Share sensitive information openly among trusted community members.



Access information from Members, DHS and other Federal, State and Local Government organizations using the Document Library.

- Engage in secure discussions and document sharing with a vetted sector peer group using the Discussion Board.



Host virtual presentations, live document review and editing, and live chat with other experts in your field using the Webinar Tool.



Stay up-to-date on emerging threats and incident information through Alerts and Notifications.

Office of
Infrastructure
Protection

Keeping America Safe,
Secure, and Resilient

www.dhs.gov/officeofinfrastructure

Making DHS Content Available to FBO Users

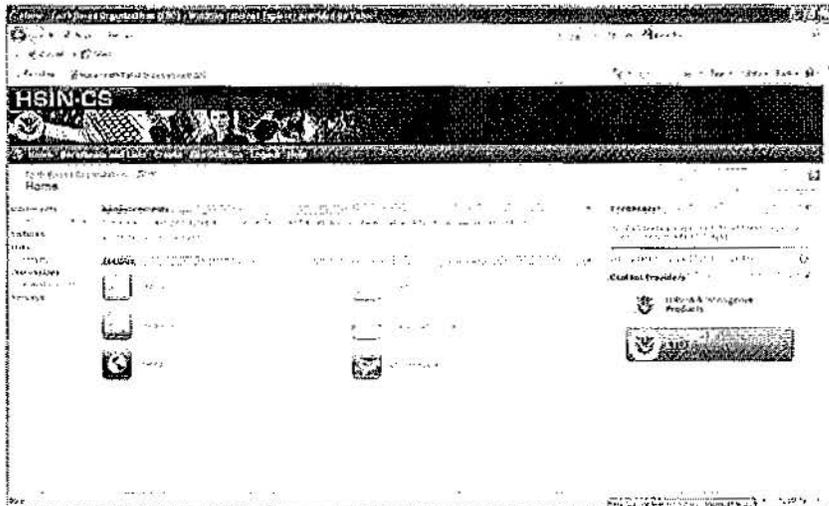
IP is currently in the process of determining the set of products that will be available to FBO users on HSIN-CS. Discussions are underway to ensure appropriate products are available to the Faith-Based community. Qualified information sharing partners will have access to a broad range of content up to SBU/FOUO, including:

- **Planning and Preparedness**
Risk Assessments, analysis products, guidance and security products, geospatial products and NISAC hurricane models, exercise and national event information.
- **Incident Reporting and Updates**
Real-time incident reports (SITREPS and SPOT Reports) and alerts.
- **Situational Awareness**
Daily and monthly open source reports on topics ranging from cyber security to emerging threats.
- **Education and Training**
IP training on topics ranging from critical infrastructure resilience to threat detection and reaction products.

FBO Criteria and Gaining Access to HSIN-CS

Qualification for participation in the DHS Faith-Based Information Sharing Pilot is determined on an organizational and an individual level. DHS is working to increase participation from the Faith-Based community. For a representative from the FBO to be considered for membership on the FBO portal within HSIN-CS, he/she must meet several criteria established by DHS and will be subject to validation procedures, including contact with his/her supervisor. The criteria are:

- Nominee is a United States citizen.
- Nominee works for or is a member of an actively engaged DHS-recognized FBO in a critical infrastructure protection and Resilience capacity.
- Nominee has a need-to-know for HSIN-CS FBO information.
- Nominee has a facility security role.



To request access to the FBO portal on HSIN-CS, please submit your name, organization, title/position, and work email to CIKRISAccess@dhs.gov.

The Office of Infrastructure Protection (IP) leads the national effort to mitigate risk to America's critical infrastructure from the full spectrum of 21st Century threats and hazards. IP coordinates with government and critical infrastructure owners and operators across 18 diverse sectors to enhance critical infrastructure resilience, strengthen protective programs, and share vital information.



**Homeland
Security**