



FAITH-BASED SECURITY ADVISORY COUNCIL

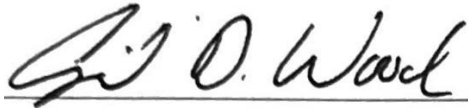
Combatting Online Child Sexual Exploitation
and Abuse Subcommittee

Faith-Based Security Advisory Council
June 24th, 2024



Homeland
Security

This publication is presented on behalf of the Faith-Based Security Advisory Council (FBSAC) Combatting Online Child Sexual Exploitation and Abuse (CSEA) Subcommittee Co-Chaired by April Wood and Chandru Acharya, for the Secretary of the Department of Homeland Security (DHS), Alejandro N. Mayorkas.

A handwritten signature in black ink that reads "April D. Wood". The signature is written in a cursive style and is positioned above a thin horizontal line.

April D. Wood, Co-Chair
President and CEO, National Voluntary
Organizations Active in Disasters

A handwritten signature in black ink that reads "Chandru Acharya". The signature is written in a cursive style and is positioned above a thin horizontal line.

Chandru Acharya, Co-Chair
President, South Asian American
Voices for Impact

This page is intentionally left blank.



TABLE OF CONTENTS

SUBCOMMITTEE MEMBERS.....	5
FBSAC STAFF.....	5
EXECUTIVE SUMMARY.....	6
KEY FINDINGS.....	7
RECOMMENDATIONS.....	9
CONCLUSION.....	10
APPENDIX 1: TASKING LETTER.....	11
APPENDIX 2: SUBJECT MATTER EXPERTS AND OTHER WITNESSES.....	15

SUBCOMMITTEE MEMBERS

April D. Wood

President and CEO, National Voluntary
Organizations Active in Disasters

Chandru Acharya

President, South Asian American Voices for
Impact

Mohamed Magid

Executive Imam, All-Dulles Area Muslim
Society (ADAMS) Center

Tracie Baker

Deputy Chief, Arlington, Texas Police
Department

Kimberly J. Burgo

Vice President of Disaster Operations,
Catholic Charities USA

Leslie Copeland-Tune

Senior Associate General Secretary &
Advocacy Direct, National Council of the
Churches of Christ in the USA (NCC)

FBSAC STAFF

Nicole Rosich

Alternate Designated Federal Officer (ADFO)

Erika Amaya

ADFO

Susan Schneider

ADFO

Pamela Dampeer

Senior Advisor, FBSAC Support

Sofi Forwood

FBSAC Support

EXECUTIVE SUMMARY

On November 14, 2023, Secretary Mayorkas tasked the FBSAC with forming a subcommittee on Combatting Online Child Sexual Exploitation and Abuse (CSEA) to develop DHS strategies that can be used to protect faith-based community stakeholders and the public from incidents of CSEA, consistent with the Department's authorities. In response to the taskings, the Subcommittee focused its recommendations on addressing the following:

1. How DHS can partner with faith-based organizations to inform faith-based leaders and communities about recognizing and responding appropriately to incidents of online CSEA; and
2. How DHS can help bring awareness to faith-based communities and help empower, engage, and foster community involvement with faith-based leaders to mobilize resources to mitigate and respond to CSEA.

The Subcommittee recognizes the many efforts being made by DHS and the Federal Bureau of Investigation (FBI) to address CSEA. We applaud these efforts and strongly encourage these efforts to continue. The Secretary of Homeland Security recognizes the importance of combatting online CSEA, an often-underreported crime that has been increasing at alarming rates, and views it a priority to protect victims and impacted communities by expanding and further investing in public education, community and law enforcement resources, and digital forensic resources to combat the rise in online CSEA.

The following consistent themes and key findings emerged from the numerous briefings delivered to the Subcommittee:

- A lack of awareness regarding CSEA, and the challenges often encountered in framing conversations around the nature of CSEA are a barrier to faith-based communities' ability to combat online CSEA effectively.
- The role of technology companies and social media platforms is critical to curbing and combatting online CSEA and providing a safe place for children.
- Children may experience a lack of a safe space within their households, schools, faith groups, and other communities to bring up CSEA crime-related issues or threats with their parents or with religious/community leaders.
- Partnerships and multi-agency collaboration play a critical role in maximizing limited resources, sharing information, and augmenting efforts to combat online CSEA.
- Advocacy is needed for additional legislation to protect children from online CSEA.

To address these findings, the Subcommittee makes the following recommendations to DHS:

- Support and strengthen public awareness programs such as Know2Protect (K2P) and Project iGuardian by expanding funding and designing a strategy to engage faith-based communities.

- Integrate DHS resources into learning management platforms with culturally sensitive and multi-lingual assets used by faith-based organizations to ensure access.
- Create a liaison position within DHS to support agencies within each of DHS's 10 regions across the country that can help support DHS CSEA initiatives locally and implement these initiatives within faith-based and educational institutions, which are where large target audiences frequent.
- Encourage and incentivize technology companies to prioritize child safety through proactive engagement, collaboration, and regular outreach.
- Advocate for stronger legislation from Congress to protect children and youth from online CSEA and aid investigations.

KEY FINDINGS

There has been a significant increase in online CSEA reporting and occurrences over the last few years and there are currently not enough resources to adequately protect children from bad actors aimed at perpetrating online CSEA and financial sexual extortion (sextortion). According to the National Center for Missing and Exploited Children (NCMEC), there has been a 323% increase in the amount of online enticement reports from 2021 to 2023¹. In 2023, there was an exponential increase in volume of up to 36.2 million reports coming into the tip line which translates to about 99,000 reports on average each day. Prevention and protection are critical to reducing the incidents of online CSEA and faith-based organizations play a key role in community engagement and outreach.

There are a number of efforts working well that could be expanded upon, to include bolstering the resources of existing programs, outreach, and structures. The DHS Center for Faith Based and Neighborhood Partnerships plays a vital role in engaging and sharing information with the faith-based community at a national level. In addition, other structures such as Internet Crimes Against Children (ICAC) Task Forces and dedicated Community Relations Officers (CRO)'s are an important part of multi-agency cross collaboration but remain under resourced and may not be connected to the broader faith community. Key partnerships with NCMEC, WeProtect Global Alliance, and the technology sector are in place and working well but other opportunities to expand engagement are needed.

The lack of awareness about CSEA and the challenges encountered in framing conversations around the nature of CSEA act as a barrier to combat online CSEA effectively.

There is a systemic lack of understanding of the nature and extent of the challenge posed by online CSEA. There is a significant increase in child sexual abuse material (CSAM), sextortion, and grooming. The deployment of artificial intelligence-based tools by perpetrators for committing these crimes has made both prevention and detection of CSEA-related crimes challenging. The absence and/or avoidance of conversations and discussions around CSEA may be attributed to the discomfort faced by various stakeholders

¹ National Center for Missing and Exploited Children, "2023 Cyber Tipline Report." Last accessed June 5, 2024, <https://www.missingkids.org/content/dam/missingkids/pdfs/2023-CyberTipline-Report.pdf>.

such as parents/guardians, lawmakers, teachers, faith leaders, and children due to the stigma around the topic of CSEA and lack of appropriate language to help engage various age groups and communities.

The role of technology companies and social media platforms is critical to curbing and combatting online CSEA and providing a safe space for children.

Currently, the role of technology and social media companies in preventing and reporting CSEA is voluntary and not based on legislative mandates. Technology companies have little or no civil liability with CSAM. Law enforcement agencies are unable to perform at optimum potential due to non-standard policies, practices, and processes adopted by the technology companies, resulting in delayed reporting, lack of meaningful information within the cyber tip line reports, and low data retention time frames of around thirty days. The adoption of end-to-end encryption by technology companies also poses a risk of reduction in reporting to the cyber tip lines.

Children may experience the lack of a conducive environment within households, schools, faith groups, and other communities to bring up CSEA crime related issues or threats with their parents, teachers, or with religious and community leaders.

Children may experience helplessness and shame due to the nature of CSEA crimes. Given their vulnerability, children may find it difficult to communicate their problems and seek support. Due to lack of education and information about CSEA crimes, parents are not able to provide adequate space for children to openly discuss the matter. Teachers, faith, and community leaders also face similar challenges in providing a conducive environment within schools and faith communities that is comforting and supportive to victims of CSEA.

Partnerships and multi-agency collaboration play a critical role in maximizing limited resources, sharing information, and augmenting efforts to combat online CSEA.

The utilization of strategic partnerships allows for resource sharing, cross sector communication, and varied expertise working together to combat online CSEA. Briefing agencies affirmed the value of critical partnerships and expressed concern about a lack of resources, both human and financial, to expand partner engagement beyond current levels. The lack of open dialogue between DHS and faith-based leaders at the national, state, and local levels has resulted in minimal actionable measures taking place.

Advocacy is needed for additional legislation to protect children from online CSEA.

In May of 2024, President Biden took an important step to protect children by signing into law the Revising Existing Procedures On Reporting via Technology (REPORT) Act, which changed the requirements for electronic communication service providers and remote computing service providers to submit reports to NCMEC when they become aware of violations involving the online sexual exploitation of children. While this was a significant step towards preventing online CSEA, more legislative protections are needed to ensure the safety and well-being of children and youth.

RECOMMENDATIONS

Recommendation #1: Support and strengthen public awareness programs such as K2P and Project iGuardian by expanding funding and designing a strategy to engage faith-based communities.

In order to achieve the K2P campaign's goals of education, prevention, and intervention, additional funding and staff is needed. Public awareness campaigns can create and elevate awareness on the rapidly escalating threat of online CSEA and educate audiences about those threats. The scope of these campaigns should be broad as well as focused - targeting the specific communities of children, parents, policymakers, faith and community leaders, and the general public. Designing a strategic roadmap to engage faith-based communities, and vulnerable and underserved populations will ensure that K2P reaches larger audiences and has a greater impact on preventing CSEA.

Recommendation #2: Integrate DHS resources into learning management platforms with culturally sensitive and multi-lingual assets used by faith-based organizations to ensure access.

Identify vendors and content providers used by faith-based organizations and work with them to incorporate curriculum material such as K2P and iGuardian. Providing already developed content and training enables faith-based organizations to quickly and cost effectively incorporate this material into existing training programs. This will provide all stakeholders with the necessary tools and opportunities to provide assistance, reassurance, comfort, and support to CSEA victims. Multi-lingual programming and cultural sensitivities are a key component of access. Access to resources, findings, and information related to CSEA crime can empower parents, teachers, and community leaders, such as clergy and faith leaders, to educate children about best preventative practices and also provide them adequate space to communicate with trusted adults.

Recommendation #3: Create a liaison position within DHS to support agencies within each of DHS's 10 regions across the country which can help support DHS CSEA initiatives locally and implement these initiatives within faith-based and educational institutions that serve large target audiences.

Creating the liaison position will allow for uniform and consistent messaging to be distributed on a national level and allow opportunities for DHS to create a multidisciplinary collaboration through which DHS, technology companies, social media platforms, local law enforcement, social services, mental health advocates, faith-based communities, and educational institutions all work together to help combat online CSEA. The liaison would work within the region to support educational initiatives, increase available resources, and highlight performance outcomes, giving legitimacy to DHS's sincerity in addressing CSEA in the faith-based community and the public.

Recommendation #4: Encourage and incentivize technology companies to prioritize child safety through proactive engagement, collaboration, and regular outreach.

We recommend that DHS take the lead in convening a Child Safety Forum or Council that pursues zero tolerance of CSEA and focuses on child online safety. Stakeholders in the Forum should include a DHS Liaison, faith leaders, school administrators, CSEA prevention experts, and technology company representatives. The Forum would facilitate dialogue between all the stakeholders and help build an eco-system that prioritizes child safety online.

In support of the above recommendation, we wish to highlight the success of cross-platform signal-sharing programs for companies to strengthen how they enforce their child safety policies. These programs enable increased prevention and detection capabilities, speed up identification of threats, build situational awareness of new predatory tactics, and strengthen reporting of criminal offenses. Coalitions and collaborative efforts could help the standardization of processes and encourage the adoption of best practices in prevention and reporting. An online child safety rating system could be a possible outcome of such collaborative efforts.

Recommendation #5: Advocate for stronger legislation from Congress to protect children and youth from online CSEA and aid investigations.

Support legislation that would provide powerful new tools to combat online child sexual abuse exploitation, which are urgently needed. Such legislation should: require online platforms to report child sex trafficking and online enticement; replace “child pornography” with “child sexual abuse material” in U.S. federal statutes and require extension of technology platforms’ data retention from 30 days to 365 days to enable investigators’ ability to thoroughly investigate these crimes. Legislation should also require platforms to participate in information sharing to remove defined CSAM imagery and use hash values to detect these images or videos on their services and remove this content.

CONCLUSION

In summary, online CSEA continues to escalate and pose a serious threat to our communities with emerging technologies, limited accountability, and not enough resources to combat the skyrocketing numbers over the last few years. A multidisciplinary approach spearheaded by DHS alongside the active participation and collaboration of all stakeholders including children, parents, technology companies, social media platforms, local law enforcement, social services, mental health advocates, faith-based communities and educational institutions will help to combat the menace of online CSEA.

There is need to center children’s rights and perspectives in designing interventions by creating mechanisms for young people to hold service providers accountable. From a community outreach perspective, there is a need for more formalized partnerships with faith-based organizations. From a preventative standpoint, industry-driven coalitions are found to be effective to improve both reporting and overall response to online CSEA. Finally, there is also need for legislation that criminalizes all forms of online CSEA and helps law enforcement agencies produce better results preventing crime and helping victims.

APPENDIX 1: TASKING LETTER

Secretary

U.S. Department of Homeland Security
Washington, DC 20528



November 14, 2023

MEMORANDUM FOR:

Bill Bratton
Co-Chair, Homeland Security Advisory Council

Jamie Gorelick
Co-Chair, Homeland Security Advisory Council

Kiran Kaur Gill
Chair, Faith Based Security Advisory Council

Elisa Villanueva Beard
Chair, Homeland Security Academic Partnership Council

CC:

Karen Tandy
Vice Chair, Homeland Security Advisory Council

Rabbi Julie Schonfeld
Vice Chair, Faith Based Security Advisory Council

Dr. Walter Bumphus
Vice Chair, Homeland Security Academic Partnership
Council

FROM:

Alejandro N. Mayorkas
Secretary

SUBJECT:

**Multi-Council Tasking on Combatting Online Child
Sexual Exploitation and Abuse**

The Department of Homeland Security is fortunate to have diverse advisory bodies, including the Homeland Security Advisory Council (HSAC), the Homeland Security Academic Partnership Council (HSAPC), and the Faith Based Security Advisory Council (FBSAC), to help address some of the most difficult challenges the Department confronts. The Councils have provided valuable advice and recommendations for DHS missions. Their inputs have guided us in, among other critical lines of effort, defending against the adversarial use of artificial intelligence (AI),

improving practices in the sharing of intelligence and information, advancing technological innovation, and improving our customers' experiences.

In this year's Quadrennial Homeland Security Review, the Department reaffirmed its five enduring homeland security missions and added a new sixth mission: to combat crimes of exploitation and protect victims. Our identification of this new mission reflects the importance of supporting victims and holding perpetrators accountable. Given the advancement and dominance of digital technologies, the Department has seen a dramatic increase in the prevalence and severity of online Child Sexual Exploitation and Abuse (CSEA), one of the most pernicious problems facing our country.

Each of our advisory Councils brings valuable expertise and different vantage points from which to view and identify solutions to this problem. The ability to have these Councils tackle this challenge simultaneously and collaboratively has the potential for significant impact. I respectfully request that the HSAC, HSAPC, and FBSAC each form a subcommittee to review DHS efforts to combat online CSEA in accordance with the guidance below.

I request that all three Councils develop independent reports, submit their findings and key recommendations to me no later than 150 days from the date of this memorandum, consistent with applicable rules and regulations.

Child Sexual Exploitation and Abuse

New internet-connected digital tools grant offenders unprecedented access to children, allowing this borderless crime to proliferate. To offer just a few data points: the National Center for Missing and Exploited Children (NCMEC or the Center), which analyzes reports of child sexual abuse materials, received over 32 million cyber tips in 2022. This corresponds to more than 88 million images and videos of child sexual abuse—a roughly 75 percent increase in only five years. Similarly, between 2021 and 2022, the Center documented 80,524 reports of attempted online exploitation, an 82 percent increase over the previous year. The United States not only has an increasing number of U.S. child victims, but it also leads the world in hosting perpetrators of these crimes.

Our Department has led the law enforcement response to these abhorrent crimes. The Homeland Security Investigations (HSI) Cyber Crimes Center, home to the Child Exploitation Investigations Unit (CEIU), is a global leader in this space. In Fiscal Year 2022 alone, DHS identified or rescued 1,170 child victims and arrested 4,459 individuals for crimes involving the sexual exploitation of children.

We know we cannot investigate and arrest our way out of this epidemic. DHS is prioritizing the fight against these crimes by expanding and further investing in public education, law enforcement, and digital forensic resources to fight online CSEA. The Department's efforts will benefit from the deep expertise of the Council members. Your review will be particularly timely; the Department plans to launch a first-of-its kind, government-led public awareness campaign to counter online CSEA, "Know2Protect: Together We Can Stop Online Child Exploitation.

We urgently need to harness the advantages of AI in this work, while addressing the new vulnerabilities AI creates. The DHS AI Task Force is working on digital forensic tools to help identify, locate, and rescue real victims of online child sexual exploitation and abuse and to identify the perpetrators. At the same time, investigators around the world are beginning to see fabricated AI images of child sexual abuse material, which threatens to redirect law enforcement officials away from investigating images of real children.

Given the need to accelerate our progress in the face of this evolving threat, I ask that the HSAC, HSAPC, and FBSAC each form a subcommittee to review and provide recommendations to counter online child sexual exploitation and abuse. The subcommittees will enhance our efforts and complement our ongoing work and should consider existing prevention frameworks and models from the public and private sectors.

The HSAC review and recommendations should include but not be limited to:

1. An assessment of how DHS can streamline and strengthen internal operations across components to effectively coordinate and collectively address online child sexual exploitation and abuse alongside our international partners, the technology industry, and non-governmental organizations.
2. An assessment and development of recommended actions for the technology industry to proactively identify, report, and prevent future sexual exploitation and abuse of children online. The assessment should include:
 - a. a review of existing authorities and how DHS could utilize these authorities to move our interests forward; and
 - b. identification of the barriers impeding industry from providing actionable information to law enforcement to identify victims and perpetrators.
 - c. An assessment to gauge the strengths, gaps, and opportunities in public awareness, industry engagement, and whole-of-community involvement. This assessment should include recommendations for cross-industry collaboration to raise public awareness of online CSEA.

The FBSAC review and recommendations should include but not be limited to:

1. Recommendations on how DHS can partner with faith-based organizations to inform faith-based leaders and communities about how to recognize and respond appropriately to incidents of online CSEA.
2. An assessment to gauge the strengths, gaps, and opportunities in faith-based community awareness, engagement, and whole-of-community involvement. This assessment should include recommendations for faith-based organization collaboration to raise public awareness of online CSEA.

The HSAPC review and recommendations should include but not be limited to:

1. Development of guidelines and best practices for educators and academic institutions to:
 - a. understand and reduce the risks of online CSEA;

- b. establish processes and protocols to detect and report online CSEA; and
 - c. partner with law enforcement and support communities to aid investigations and victims.
- 2. An assessment of DHS educational, awareness, and school safety resources to prevent, detect, and report online CSEA. This should include best practices for content delivery, including how it is delivered, who is delivering it, and audience prioritization.

APPENDIX 2: SUBJECT MATTER EXPERTS AND OTHER WITNESSES

Name	Title	Organization
Ronald Appel	Division Chief	DHS Homeland Security Investigations (HSI) Cyber Crimes Center (C3)
Mauria Atzil	Director of Youth Protection	United Synagogue of Conservative Judaism
Josh Benton	Vice President of North American Ministry	Send Relief
Kristen Best	Principal Director	DHS Office of Strategy, Policy, and Plans (PLCY) Counter Transnational Organized Crime (CTOC)
Iain Drennan	Executive Director, Secretariat of Child, and Youth Protection	WeProtect Global Alliance
Jaanhavi Ganesh	Northeast Regional Coordinator	Hindu Youth for Unity, Virtues, and Action (YUVA)
Shailey Hignorani	Head of Policy, Advocacy, and Research	WeProtect Global Alliance
Joan Hoback	Deputy Special Agent in Charge (DSAC)	DHS United States Secret Service (USSS) Foreign Service Division (FSD)
Amruta HoudeJaym	Advisor	Hindu YUVA
Tanner Hubbard	Special Agent	DHS USSS Criminal Investigations Division (CID)
Jaymin Kathiriya	President	Hindu YUVA
Kathryn Kennedy	Campaign Director	DHS ICE HSI K2P
Amy Leffler	Social Scientist	DHS Science & Technology (S&T)
Sean Litton	Executive Director	Technology Coalition
Emily Lock	Communications Lead	Technology Coalition
Viswajith Mallampati	Vice President	Hindu YUVA
William Mancino	Special Agent in Charge (SAC)	DHS USSS CID
Fallon McNulty	Director	NCMEC CyberTipline
Deacon Bernard Nojadera	Executive Director	United States Conference of Catholic Bishops
Kevin Plourde	Assistant Special Agent in Charge (ASAC)	DHS USSS CID
Jason Rees	SAC (Acting)	DHS USSS Office of Legislative Affairs (OLA) Homeland Security Program

Patricia Wolfhope	Subject Matter Expert (SME)	DHS S&T Forensic and Criminal Investigations Program, Digital Forensics
-------------------	--------------------------------	--