HOMELAND SECURITY ACADEMIC PARTNERSHIP COUNCIL

Combatting Online Child Sexual Exploitation and Abuse Subcommittee

Office of Partnership and Engagement
June 3, 2024

Homeland
Security

This publication is presented on behalf of the Homeland Security Academic Partnership Council (HSAPC) Combatting Online Child Sexual Exploitation and Abuse (CSEA) Subcommittee, chaired by Suzanne Elise Walsh, for the Secretary of the Department of Homeland Security (DHS), Alejandro N. Mayorkas.

Suzanne Elise
Walsh

Digitally signed by Suzanne
Elise Walsh
Date: 2024.06.04 22:21:38
-04'00'

Suzanne Elise Walsh, Chair
President, Bennett College

This page is intentionally left blank.

TABLE OF CONTENTS

SUBCOMMITTEE MEMBERS

Suzanne Elise Walsh (Chair)	President, Bennett College
Elisa Villanueva Beard	Chief Executive Officer, Teach For America
Assistant Chief Rudy Perez	President, National Association of School Resource Officers
Randi Weingarten	President, American Federation of Teachers

HSAPC STAFF

Patrese Roberts	Acting Deputy Director, HSAPC, Office of Academic Engagement, Office of Partnership and Engagement
Alexander Jacobs	Senior Director, HSAPC Support
Hayley LeCourt Itri	HSAPC Contractor Support
Cori Dawson	HSAPC Contractor Support

EXECUTIVE SUMMARY

On November 14, 2023, Secretary Mayorkas tasked the Homeland Security Academic Partnership Council (HSAPC) with forming a subcommittee on Combatting Online Child Sexual Exploitation and Abuse (CSEA) to develop the Department of Homeland Security's (DHS) strategy to protect academic community stakeholders from incidents of CSEA, consistent with the Department's authorities.

The Secretary tasked this Subcommittee with reviewing the program and stakeholder feedback, and providing recommendations, with specific insights into:

- The development of guidelines and best practices for educators and academic institutions:
    - *Understand and reduce risks of CSEA:* Creating strategies to help educators comprehend and mitigate the dangers of online CSEA.
    - *Establish processes to detect and report online CSEA:* Setting up procedures and protocols for identifying and reporting incidents of online CSEA.
    - *Partner with law enforcement and support communities:* Collaborating with law enforcement and community organizations to assist in investigations and support victims.
- Assessment of DHS educational, awareness, and school safety resources:
    - *Prevent, detect, and report online CSEA:* Evaluating the effectiveness of DHS resources aimed at preventing, detecting, and reporting online CSEA.
    - *Best practices for content delivery:* Identifying the most effective methods for delivering educational content, determining appropriate deliverers, and prioritizing audiences.

The Subcommittee makes the following primary findings:

- There is a lack of understanding of online CSEA or an avoidance of the topic/crime due to the uncomfortable subject.
- CSEA is broader and more pervasive than the old terminology of "child pornography."
- CSEA stands as a heinous and abhorrent crime on the ascent, and presently, the Department is grappling to keep pace with its rapid growth.
- A significant disparity exists in both the volume and quality of reports submitted to the National Center for Missing and Exploited Children (NCMEC) CyberTipline.
- Financial sextortion of teenage boys aged 13 - 17 is a major growing concern.
- A plethora of excellent resources exist to address prevention and law enforcement approaches to online CSEA and are well coordinated across agencies; however, caring adults do not know that any of them exist and do not know how to access them.

- Law enforcement is not going to get us out of this growing challenge of exploitation of young people.

The key findings and recommendations published together provide guidance for helping educators and caring adults understand and reduce the risks of online CSEA.

The key findings highlight the alarming rise and pervasiveness of CSEA. There is a significant lack of understanding and avoidance of discussing online CSEA among trusted adults, which puts children at risk. CSEA is broader than traditional “child pornography,” encompassing various crimes like child sexual abuse material (CSAM), online enticement, financial sextortion, livestreaming (e.g., rape by proxy), emerging threat of generative artificial intelligence (AI), and revictimization (e.g., image takedown). The staggering volume of reports to the NCMEC has skyrocketed from one million in 2014 to an estimated 36 million in 2023, with most reports originating outside the U.S., and yet, there is a disparity in the quality and volume of reports, with many tips being non-actionable and often involving international perpetrators. Newer trends like financial sextortion targeting teenage boys are escalating rapidly. While excellent resources exist for prevention and law enforcement, they are not well known or accessible to caring adults. Addressing CSEA requires more than just law enforcement; it calls for comprehensive education and collaboration among students, families, and educators.

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

1. Take a human-centered, ecosystem approach to education, prevention, and intervention.
2. Increase funding for rapid and actionable research to improve the quality and determine the most effective reported tips, education and training materials, and programs to allow for rapid prototyping and adjustments, and increase funding for training for those involved in investigations to be brought up to speed on the rapidly emerging technologies. Today it is generative AI; soon, it will be extended reality.
3. Increase mental health support for those who work on the frontlines of online CSEA investigations.
4. Further enhance the Know2Protect (K2P) campaign to be a one-stop shop for caring adults to reach out to with questions or for help.
5. Design resources that are age appropriate and with victims in crisis in mind. Avoid text heavy resource pages.
6. Remove and reduce barriers to abuse identification and help-seeking, such as shame, victim-blaming, and misconceptions about abuse.
7. Build on the K2P, Together We Can Stop Online Child Exploitation™ campaign by offering a certificate that requires true partnership, not just sign on.
8. Portion information into manageable sizes.

9. Increase collaboration with Big Tech companies, including social media companies, search engines, gaming platforms, streaming platforms, AI companies and platforms, and instant messaging and voice over internet protocol (VoIP) social platforms.

The recommendations emphasize a holistic, human-centered approach to combatting online CSEA. They call for increased funding for research and training to stay ahead of evolving technologies, and for comprehensive education and prevention programs involving all stakeholders, including children, caregivers, and law enforcement. The report suggests enhancing mental health support for those investigating CSEA, creating accessible and age-appropriate resources, and improving collaboration and feedback mechanisms with international bodies.

Additionally, it recommends making reporting processes clearer and more actionable, reducing barriers like shame and victim-blaming, and implementing targeted micro-campaigns to educate and empower caring adults. Lastly, it proposes initiatives like certification programs for teachers and community members to signal their readiness to support and protect young people from CSEA.

METHODOLOGY

In preparation for this report, the Subcommittee was briefed by the following stakeholders, subject matter experts, and leaders from DHS:

- Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Cyber Crime Center (C3),
- ICE HSI K2P
- United States Secret Service (USSS) Office of Intergovernmental and Legislative Affairs, Homeland Security Program/Forensic Services Division (FSD)/Criminal Investigation Division (CID)
- Science and Technology Directorate (S&T) Technology Centers Division (TCD),
- S&T Forensic & Criminal Investigations, S&T Forensic and Criminal Investigations Program, and
- Office of Strategy, Policy, & Plans (PLCY) Countering Transnational Organized Crime (CTOC).

Additionally, the Subcommittee received briefings from subject matter experts at external organizations including:

- U.S. Department of Justice (DOJ) Federal Bureau of Investigation (FBI) Science Technology Branch (STB),
- NCMEC, and
- WeProtect Global Alliance (GA).

KEY FINDINGS

There is a lack of understanding of online CSEA or an avoidance of the topic/crime due to the uncomfortable subject.

Well-intended, trusted adults (e.g., parents, families, teachers, and school administrators) avoid discussions of anything related to sex, and it is putting young people in harm's way. These are uncomfortable but necessary conversations that must take place from early ages through to late-teens, and caring adults must be prepared to help educate, prevent, and intervene.

- There are several excellent programs and resources available to help prevent, educate, and support children with regard to online CSEA. Several briefers indicated that schools do not like to invite them in to speak proactively and preventatively about online CSEA because of the "s" (sex) in CSEA. They are invited in after there is a tragedy.
- NCMEC "recently conducted a Harris poll to test what parents are most concerned about when it comes to protecting their children. Of the 5,000 people surveyed, 88% stated child abductions as their biggest concern. Online safety barely registered, shining a light on how most of the public is unaware of how frequent and close to home cases of child exploitation can be."[1]

CSEA is broader and more pervasive than the old terminology of "child pornography."

Online CSEA encompasses multiple yet distinctive crimes, each requiring education, prevention, and intervention relevant to the crime. Online CSEA can take many forms, including:

- Child sexual abuse material (CSAM),
- Online enticement and coercion (e.g., grooming),
- Financial sextortion,
- Livestreaming (e.g., rape by proxy),
- Emerging threat of generative AI, and
- Revictimization (e.g., image takedown).

CSEA stands as a heinous and abhorrent crime on the ascent, and presently, the Department is grappling to keep pace with its rapid growth.

- Fiscal year 2014 (FY14) was the first year that the NCMEC surpassed one million tips for children exploited.[2]

[1] Emma Henderson Vaughan, "'No Escape Room' Launches with New Data: Interactive Experience Exposes Dangers of Financial Sextortion," April 16, 2024. Last accessed May 29, 2024, https://www.missingkids.org/blog/2024/no-escape-room-launches-with-interactive-experience.

[2] Closed briefing on Friday, March 1, 2024.

- Eight years later, in Fiscal Year 2022 (FY22), that number was 32 million, with an estimated 36 million for Fiscal Year 2023 (FY23).[3]
- In 2023, monthly incoming volume of tips ranged from 1.5 to 7.7 million reports.[4]
- The volume of reports is astronomical and translates to nearly 99,000 reports per day.[5]
- The average time it takes to lock a child into a grooming conversation is 45 minutes, and it can take as little as 19 seconds.[6]
- There is a need to develop a DHS-wide resilience program to give the workforce and all employees working in this space the help they need.

A significant disparity exists in both the volume and quality of reports submitted to the NCMEC CyberTipline.

- There is not an established feedback loop of what "useful tips" are for NCMEC to make the reported tips actionable.
- There is a gap within processes, protocols, and the reporting.
- 90% of the reports received by the NCMEC CyberTipline originate outside of the United States, indicating that the individuals reported are not located within the U.S.[7] Being aware of non-English terminology, having consistent terms, and close international collaboration is essential to intervene.
- To address the reporting gaps, there needs to be enhanced collaboration with the International Crimes Against Children (ICAC) Task Force Program and NCMEC to ensure that efforts are not only actionable but also valuable, providing fulfillment for both parties involved.

Financial sextortion of teenage boys aged 13 - 17 is a major growing concern.

- Financial sextortion is a newer trend NCMEC has been seeing over the last three years.
    - Financial sextortion cases have accelerated over the past few years, with blackmail occurring rapidly after initial contact.
    - Rapid escalation of blackmail, exacerbated by generative AI, increases distress for victims and can lead to tragic outcomes, including death by suicide.
    - Between 2021 and 2023, the number of online enticement reports increased by 323%.[8]

[3] National Center for Missing and Exploited Children, "2023 Cyber Tipline Report." Last accessed May 29, 2024, https://www.missingkids.org/content/dam/missingkids/pdfs/2023-CyberTipline-Report.pdf.

[4] Closed briefing on Wednesday, March 6, 2024.

[5] National Center for Missing and Exploited Children, "2023 Cyber Tipline Report." Last accessed May 29, 2024, https://www.missingkids.org/content/dam/missingkids/pdfs/2023-CyberTipline-Report.pdf. Thirty-six million reports divided by 365 days averages to approximately 98,630 reports per day.

[6] Shailey Hingorani, Maddi Gore, and Natalia Greene, *Global Threat Assessment 2023* (WeProtect Global Alliance, October 17, 2023). Last accessed May 29, 2024, https://www.weprotect.org/global-threat-assessment-23/.

[7] National Center for Missing and Exploited Children, "2023 Cyber Tipline Report." Last accessed May 29, 2024, https://www.missingkids.org/content/dam/missingkids/pdfs/2023-CyberTipline-Report.pdf.

[8] National Center for Missing and Exploited Children, "Sextortion by the Numbers." Last accessed May 29, 2024, https://www.missingkids.org/theissues/sextortion.

- Financial schemes originating mostly from West Africa are targeting young boys, pressuring them to engage in explicit conduct to extort them for anything with monetary value.
- The burden of solving and reporting this exploitation today lies on the victim/child, which is unrealistic because children are not always aware this is what is happening to them, and they should not have to carry this responsibility.

A plethora of excellent resources exist to educate the public, provide resources to prevent children from becoming victims, and demonstrate how to intervene when online CSEA occurs in a community. However, caring adults do not know that these DHS resources exist and do not know how to access them.

- The resources tend to be most sophisticated in the areas of education and prevention but are not as strong with helping *detect* CSEA.
- Examples of excellent resources include:
  - DHS's K2P campaign, including revamped Project iGuardians™,
  - Childhood Smart Program (CSP) via USSS, and
  - TakeItDown via NCMEC.

Law enforcement is not going to get us out of this growing challenge of exploitation of young people.

- Law enforcement is typically good at responding to crimes after they occur. CSEA however, requires a proactive, preventative approach, like identifying and intervening before harm happens. This requires collaboration with Big Tech, educators, and other caring adults.
- A whole of society approach is necessary. We need to educate students, families, and educators alike. The Know2Protect campaign is a good first step as it collaborates with multiple public and private sector partners to educate the public, especially parents and teens, about the risks and preventive measures related to online exploitation.
- "Public-private partnerships and targeted trainings are essential to raising awareness and educating the public; identifying, protecting, and supporting victims; and bringing perpetrators to justice. By partnering with national sports leagues, youth-serving organizations, and gaming, technology, and other private sector organizations, Know2Protect will help educate the public, save lives, and prevent tragedies." – Secretary Mayorkas. Moreover, "the best way to keep kids safe online is to provide helpful information where they are: on social media and online gaming platforms, and through clubs, sporting events, and organizations. By partnering with a range of companies to raise awareness and disseminate educational messaging, we are keeping kids safe from online predators," -- Know2Protect Campaign Director Kate Kennedy. [9]

[9] Department of Homeland Security, "DHS Launches Know2Protect™ Public Awareness Campaign to Combat Online Child Exploitation and Abuse with Many Public and Private Sector Partners," April 17, 2024. Last accessed May 30, 2024, https://www.dhs.gov/news/2024/04/17/dhs-launches-know2protecttm-public-awareness-campaign-combat-online-child.

RECOMMENDATIONS

Recommendation #1: Take a human-centered, ecosystem approach to education, prevention, and intervention.

"Everyone has a part to play. Young people need to know how to avoid dangerous situations. Caregivers need to know the signs of exploitation and abuse and how to intervene." – Secretary Mayorkas

- Include all stakeholders in designing informational materials (children, caring adults, victims/survivors, law enforcement). Hold focus groups to help improve materials.
- Hold cross-stakeholder trainings in local communities and online so that everyone knows the part they can play.
    - Create easy-to-find and easy-to-use guides for caregivers to easily recognize the signs of exploitation and abuse. The guides should provide clear signs that consider any differences based on age, gender/gender identity, or race.
    - Update the DHS K2P How2Report information page with a clear header for caring adults that directs them on how to intervene.
- Change how we talk about CSEA[10] in three critical ways:
    - Move from talking about CSEA as inevitable/out of control to talking about hope and solutions. If the language is only about how CSEA is inevitable or out of control, it stops people from engaging in education or prevention because they do not see either as helpful. They simply do not engage. "Hope and solutions" gives caring adults a sense that there is something they can do to educate, prevent, and intervene.
    - Move away from framing CSEA as solely a criminal or parental issue to one where the education, prevention, and intervention strategies are about shared values of all stakeholders and therefore collective responsibility to protect young people.
    - Move from a focus that is primarily on addressing criminality via the technology and move to a focus on a collectivized engagement of all stakeholders to focus on prevention.

Recommendation #2: Increase funding in two critical areas: a) rapid and actionable research to improve the quality and determine the most effective reported tips, education and training materials, and programs to allow for rapid prototyping and adjustments; and b) training for those involved in investigations to be brought up to speed on the rapidly emerging technologies.

The crimes are quickly evolving and so must the research and responses. It is critical to know what works.

[10] Closed briefing on April 5, 2024.

- Today it is generative AI; soon, it will be eXtended reality. Investigative agents need to be on the cutting edge of understanding the evolving technology and how it is being used for online CSEA.
- Additional research questions should explore intersectionality in online CSEA (age, race/ethnicity, gender, disabilities, sexual orientation).
- Develop a dashboard to help make sense of all the data that is being collected.

Recommendation #3: Increase mental health support for and research about those who work on the frontlines of online CSEA investigations.

- DHS S&T posed a profound and underdiscussed question: How does the secondary and vicarious trauma, and constantly seeing more moral injury impact our ability to employ a victim-centered approach to not re-traumatize victims and to meet victims where they are?
- To take a victim-centered approach, investigative agents/case officers must take care of their own mental and emotional wellbeing. This includes access to mental health support such as practices used by the military in their work with those who have returned from or otherwise experienced combat zones.
- Vicarious and secondary trauma of frontline investigators are emerging areas in mental health. More rapid and actionable research is needed to identify what works and then access must be given quickly to investigators.

Recommendation #4: Further enhance the K2P campaign to be a one-stop shop for caring adults to reach out to with questions or for help.

- Elevate the K2P tip line (*833-591-KNOW* (*5669*)) as the top recommended phone number for victims or their caregivers to reach help immediately rather than listing contact local law enforcement as the first solution on the campaign's "How2Protect" webpage. Directing people in crisis to a vague statement of "reach out to local law enforcement" stifles the ability of caring adults to help intervene.
- Create and implement a three-digit hotline that can be leveraged by victims and parents.
- What is the one location where teachers can go to pull curriculum?
  - Educators need a clear place to go for resources that can be used in different classes. The phrase "Campaign Resources" on the K2P site could be renamed to indicate that this is more than a campaign — it is a set of resources to reinforce key messages.
  - Hashtag materials with ideas for where they can be added to a lesson plan (e.g., #healthclass, #healthyrelationships, #digitalcitizenship).

Recommendation #5: Design resources that are age appropriate and with victims in crisis in mind. Avoid text heavy resource pages.

- Create videos and/or visuals to access resources more easily.

- NCMEC's microsite "Is Your Explicit Content Out There?"[11] has outstanding content and detail which includes step-by-step instructions for different platforms[12] (Google, Discord, Facebook, Instagram, Imgur, Kik, Microsoft Products, Reddit, Snapchat, TikTok, Tumblr, X (formerly Twitter), YouTube, etc.) outlining the processes to have content removed and/or make a report to the NCMEC CyberTipline. DHS should provide feedback to NCMEC to improve the site to include screenshots of the steps, not just the words for how to take content down.
- When someone is in crisis or helping someone in crisis, their brain will process visuals faster than words. The words should accompany it, but the visuals would be helpful.
- To better help caring adults and law enforcement partner in reporting and investigations, the DHS "How2Report" information page[13] is great; however, it is too word heavy.
    - The reporting tips should go right after the "to submit a report" box. Telling people where to report without the information about what to report nearby makes it a challenge.

Recommendation #6: Remove and reduce barriers to abuse identification and help-seeking, such as shame, victim-blaming, and misconceptions about abuse.

- Empower children with age-appropriate knowledge and tools to help them navigate online spaces safely.
- Make reporting information more prevalent, similar to human trafficking campaign posters throughout airports and in restrooms.
- More interactive, age-appropriate content such as NCMEC's "No Escape Room"[14] can be powerful tools for young people and caring adults alike.
    - Consider creating versions of No Escape Room from different stakeholder perspectives. Use the same storyline but show it from the parent, teacher, and law enforcement lenses, and ask participants interactive questions.

Recommendation #7: Build on the K2P campaign by offering a certificate that requires true partnership, not just sign on.

- Develop a "Here We Know2Protect Our Youth from Exploitation and Abuse" program, including stickers and posters that can hang on doors, be placed in windows, or otherwise be displayed by educators, parents, and churches, etc. The people in the office or community would need to go through training using the materials already created by Project iGuardians™ and take a final quiz that "certifies" them as a "K2P

[11] National Center for Missing and Exploited Children, "Is Your Explicit Content Out There?" Last accessed May 29, 2024, https://www.missingkids.org/gethelpnow/isyourexplicitcontentoutthere.
[12] National Center for Missing and Exploited Children, "Reporting to Companies." Last accessed May 29, 2024, https://www.missingkids.org/gethelpnow/isyourexplicitcontentoutthere#reporting.
[13] Department of Homeland Security (DHS) Know2Protect (K2P), "How2Report." April 17, 2024. Last accessed May 29, 2024, https://www.dhs.gov/know2protect/how-to-report.
[14] National Center for Missing and Exploited Children, "No Escape Room." Last accessed May 29, 2024, https://noescaperoom.org/.

Resource" or an "iGuardian." To be a "safe space" for CSEA youth, the caring adult will need to demonstrate that they:
  - Know the issues, recognize the signs of exploitation and abuse and where to find resources such as the K2P site, USSS CSP and NCMEC resources,
  - Are ready to support a young person by providing a non-judgmental environment to educate the young person and/or help to intervene, and
  - Can provide workshops on prevention to young people, families, or educators.
- The certification sticker, sign, or badge signals to a young person that there is a trusted adult who will not judge them and who is there to help. That person knows how to access all the resources to help a young person with their CSEA issue or question.
- Create a corps of college students who are "certified" to be near-peer mentors and presenters with high schoolers and younger children. Consider using education, psychology, social work, and criminal justice students, especially so that they enter the profession already aware of online CSEA and are not afraid of it.
- Certify health educators. Online CSEA should be part of health instruction in schools and offered at every level of education with age-appropriate information using Project iGuardians™ as an example.

Recommendation #8: Portion information into manageable sizes.

Rather than focus campaigns and social media on all aspects of CSEA, create micro-campaigns for adults working with children in key sectors such as education, mental health, and pediatrics.

- Just like companies do with phishing training, have a CSEA reporting training/ simulation.
- Create a micro-campaign on detecting CSEA for caring adults.
- Create a micro campaign on partnering with law enforcement on investigations for teachers and other caring adults.
- Create a micro-campaign on how to be a supportive adult.
- Create a micro-campaign on mobile phone safety.

Recommendation #9: Increase collaboration with Big Tech companies, including social media companies, search engines, gaming platforms, streaming platforms, AI companies and platforms, and instant messaging and voice over internet protocol (VoIP) social platforms.

- Share NCMEC or other CSEA-related data on a regular basis with Big Tech to demonstrate the exponential growth and harm.
- Beyond signing up to be a "partner," Big Tech needs to create easy-to-find (and easy-to-use) reporting buttons for children, in addition to easy ways to preserve CSEA for investigators.

- Partnerships between tech firms and law enforcement agencies can enhance safety and security by facilitating quicker response times, improved information sharing, and more efficient crime prevention tactics.
- Require tech companies to report regularly on their efforts to detect and remove CSEA content. This includes transparency reports detailing the number of incidents detected, actions taken, and improvements made to their systems. Any detected content must be swiftly reported to authorities like DHS and NCMEC.
- Require regular, independent audits of tech companies' content moderation practices and tools to ensure they are effective and up to date. Audits should be submitted to DHS for review and sanctions if necessary.

CONCLUSION

This report directly responds to the need for developing guidelines and best practices to equip educators and academic institutions in the fight against online CSEA. The key findings underscore the urgency of understanding the risks and scope of CSEA, while the recommendations provide a comprehensive roadmap for reducing those risks. Establishing clear processes and protocols for detecting and reporting suspected CSEA is addressed through recommendations like increasing research funding, creating a one-stop reporting hub, and reformatting guidance to be more visual and actionable.

Enhancing partnerships between schools and law enforcement to support investigations and victims is tackled through recommendations such as certification programs, training educators as trusted resources, promoting help-seeking behaviors, and utilizing interactive tools from multiple perspectives. Moreover, the report assesses existing DHS resources, highlighting the need for simplified, age-appropriate materials delivered via targeted micro-campaigns. Prioritizing audiences like students, parents, educators and identifying trusted messengers like near-peer mentors is also emphasized.

Only through cohesive, actionable training and open dialogues can the education sector break the silence and play its vital role in preventing and combatting online CSEA. By shining a bright light on this crime through cohesive partnerships, we can disrupt the rapid escalation of online CSEA and create a safer digital world for all children and families.

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 Com batting 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 ICE HSI C3
Kristen Best	Principal Director	DHS PLCY CTOC
Iain Drennan	Executive Director	WeProtect GA
Ashley H. Freiberger	Director of Legislative Affairs	NCMEC CyberTipline
Shailey Hignorani	Head of Policy, Advocacy, and Research	WeProtect GA
Joan Hoback	Deputy Special Agent in Charge (DSAC)	DHS USSS FSD
Tanner Hubbard	Special Agent (SA)	DHS USSS CID
Kathryn Kennedy	Campaign Director	DHS ICE HSI K2P
Amy Leffler	Social Scientist	DHS S&T TCD
Fallon McNulty	Director	NCMEC CyberTipline
William Mancino	Special Agent in Charge (SAC)	DHS USSS CID
Katie Noyes	Section Chief	DOJ FBI STB
Kevin Plourde	Assistant Special Agent in Charge (ASAC)	DHS USSS CID
Michael G. Prado	Deputy Assistant Director	DHS ICE HSI C3
Jason Rees	Special Agent in Charge (SAC) (Acting)	DHS USSS OLA Homeland Security Program
Patricia Wolfhope	Subject Matter Expert (SME)	DHS S&T Forensic and Criminal Investigations Program, Digital Forensics