HOMELAND SECURITY ADVISORY COUNCIL

Combatting Online Child Sexual Exploitation and Abuse Subcommittee

June 6, 2024

Homeland Security

This publication is presented on behalf of the Homeland Security Advisory Council (HSAC) Combatting Online Child Sexual Exploitation and Abuse (CSEA) Subcommittee for the Secretary of the Department of Homeland Security, Alejandro N. Mayorkas.

Catherine Chen, HSAC CSEA Subcommittee Chair
Chief Executive Officer, Polaris

This page is intentionally left blank.

TABLE OF CONTENTS

SUBCOMMITTEE MEMBERS

Catherine Chen	Chief Executive Officer, Polaris
A.B. Culvahouse	Chair Emeritus and of Counsel, O'Melveny and Myers LLP
Danielle Gray	Executive in Residence, UnitedHealth Group
Ted Schlein	General Partner, Kleiner Perkins and Executive Chairman, Ballistic Ventures
Ali Soufan	Chairman and CEO, The Soufan Group, LLC
Megan Cutter	Managing Director, Polaris
Jillian Keschner	Analyst, The Soufan Group LLC
Joseph Shelzi	Analyst, The Soufan Group LLC

HSAC STAFF

Rebecca Sternhell	Acting Executive Director
Alexander Jacobs	Deputy Director
Joseph Chilbert	Senior Director
Cori Dawson	HSAC Support
Rachel Kaufman	HSAC Support

EXECUTIVE SUMMARY

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

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

1. Establish, resource, and empower an office within DHS to lead Departmental efforts to counter online CSEA and form a center within DHS to organize a whole-of-government approach to addressing online abuse and exploitation.
2. Leverage existing tools; develop and advocate for policy solutions.
3. Increase participation in the combatting of CSEA by the major platform vendors.
    a. Build a uniform technology platform with a public private partnership for monitoring and reporting on all investigations, past and present, open and closed. This platform would be used as the system of record for all investing agencies.
    b. Reframe and realign incentives to partnership through legislative actions.
4. Prioritize vicarious trauma and workplace well-being support for law enforcement, civil society employees, and other frontline staff who encounter CSEA material in their work.
5. Bolster and sustain DHS external engagement for the Know2Protect Campaign by expanding resources and outreach with the Department of Education (ED).
6. Lead engagement with economic and regulatory federal partners to increase the inter-departmental approach to combatting CSEA.

KEY FINDINGS

There is overlapping federal jurisdiction on combatting CSEA which can create confusion and inefficiencies.

Given the horrific nature of CSEA and its impact on child victims and those that identify, investigate, protect, and care for them, it is fitting that there are multiple agencies with a commitment to prevention and response. However, there is not a designated agency that currently owns a cohesive, coordinated approach. Within DHS, Homeland Security Investigations (HSI) and Cybersecurity and Infrastructure Security (CISA) lead coordinated, but different, educational awareness campaigns and response efforts. Combatting CSEA has evolved as a priority for DHS, when previously the 2020-2024 DHS National Strategy had listed combatting child sexual exploitation as an objective in securing cyberspace and critical infrastructure. Since then, the objective has been elevated to a priority on its own. Despite the elevation to a priority, DHS may not be resourced sufficiently for them to play a lead role for all the Departments on this issue.

The White House convenes an interagency task force focused on protecting youth mental health, safety, and privacy online with leadership from the Department of Health and Human Services (HHS), Center for Disease Control and Prevention (CDC), Department of Justice (DOJ), and DHS among many other government agencies. Because the White House task force is addressing prevention, HHS and CDC officials are focused on the public health implications of this crime, not the criminal justice related aspects of the crime.

Cross agency collaboration on investigations related to CSEA can be challenging, as there are many unknowns in the space and a lack of clarity around investigative agency roles. In addition to DHS, the Child Exploitation and Obscenity Section of DOJ, the Federal Bureau of Investigation (FBI), and the U.S. Secret Service (USSS) also engage in the prevention and response along with leading non-government organizations (NGOs), such as the National Center for Missing and Exploited Children (NCMEC) and Thorn. Additionally, compared to other national priorities like counterterrorism and anti-drug trafficking, both funding and personnel capacity for responding to CSEA are limited.

Despite overlapping jurisdictions, silos persist, necessitating a more cohesive approach within the Department and across the federal government. DHS needs a strategic framework with clear leadership directives to unify efforts and define its role in combatting online CSEA. Currently, there is a lack of government-wide alignment on the issue. Increased interagency collaboration and stakeholder engagement in this area are essential. DHS is well-positioned to lead coordination, drawing on successful models established post-9/11, such as the National Counterterrorism Center (NCTC) and the Joint Terrorism Task Force (JTTF).

DHS's engagement with entities outside of the Department or DOJ remains challenging, due to competing priorities. For example, prevention efforts are critical but involve multiple departments, including ED and HHS, which often appear disconnected despite DHS's policy leadership in combatting online CSEA. In addition, engaging with the private sector contains its own set of unique challenges, of which is primarily identifying CSEA in encrypted spaces while maintaining the privacy of the customer from unwarranted government intrusion. The initiative to pull together the diverse stakeholders, from government to private sector, must originate from DHS headquarters and should be communicated effectively through bulletins or other methods to provide guidance and tools. Having leadership over policy development can also help eliminate gaps and harmonize Departmental and agency efforts across the federal landscape.

Furthermore, DHS and S&T must collaborate to translate policy into actionable steps and educate field personnel. It is critical that all staff possess a basic understanding of the issues, know where to seek information, and understand the appropriate questions to ask. A concerted effort to align these disparate entities under a unified strategy is imperative for success.

Having DHS in a coordinating role and collective voice of the U.S. response is helpful from an international perspective. International governments who partner with the U.S. to combat online CSEA expressed concerns that there is not one point of contact from the White House. Simply, there is a need for more formalized coordination. The U.S. is a key partner to foreign

governments in responding to the CSEA threat. CSEA becoming a Secretary-level priority for DHS has been a significant tool for the U.S. to leverage in discussions. This could spur further discussions with international partners and increase innovative ideas to combat online CSEA, by sharing best practices and case information. For example, the United Kingdom (UK) considers CSEA to be a national security threat which has enabled them to leverage resources and assets on par with countering terrorism. If there were a single-entry point with authority that can speak for the U.S., it would be beneficial for engagement and would streamline the process.

There is a severe strain on the frontline investigative workforce from repeated and sustained exposure to CSEA.

Employee expertise and commitment is paramount in the fight against CSEA. The traumatic content investigators must engage with takes a profound toll on wellbeing, capacity, and turnover of the DHS workforce. Primary investigatory agencies like HSI bear the brunt of high caseloads, sustained exposure to horrific imagery, and oftentimes the visual proof that abuse is happening without the immediate ability to respond. The Secretary has prioritized employee wellness and there are clearly efforts underway to help address the burnout and mental health toll of this work. Some of the initiatives include harmonizing the benefits for employees, to ensure all have the most robust support – be it mental health counselors or childcare for their own children.

Additionally, there is a strain on the workforce due to the overwhelming caseload. Robust technology tools are needed to support data analysis for current and cold cases; at present too much of the work is manual. Though there are artificial intelligence (AI) pilots underway at the Department, such tools are not yet in widespread use, given resource and capacity constraints. These challenges need to be tackled by innovators across public and private sectors. The FBI is taking some steps to this end, partnering with U.C. Berkeley to host a multiday event with tech innovators, investigators, funders, and others to identify and address gaps and challenges. This is an example of how the Department can leverage a wide variety of stakeholders in its efforts to reduce trauma exposure, improve staff wellbeing, and advance technology going forward.

The pace at which emerging technology is growing and changing is outpacing the government and investigations.

Technology is accelerating at such rapidity that it is challenging to keep pace with tools to combat online CSEA. There is tension between scale and the speed of innovation. Greater funding is needed for the development of tools to combat online CSEA. As noted above, pilots like the FBI-U.C. Berkeley one can be one means of addressing the rapid pace of technology development. Federal funding for internally developed tools like Streamview, the DHS S&T tool that HSI uses to process and analyze the chat and email records and Victim ID, are equally as important.

In the same vein, DHS and S&T must ensure that officers working on CSEA have access to the most advanced technology, including AI and facial recognition tools. There is a delay in law

enforcement getting access to critical tools since the process for new technological software requires approval which can deter timely investigations of CSEA. Generative AI space is further complicating the investigative landscape. It is imperative that DHS learn more about which tools are out there and test the current models against live data. Upcoming initiatives like the FBI and U.C. Berkeley pilot provide a template for further action by the Department.

Both in the U.S. and abroad, the biggest emerging technological capability, and ultimate threat, is technology platforms rolling out End-to-End Encryption (E2EE). CSEA experts have expressed concern over the potential for E2EE to dramatically reduce the number of cyber tips being sent to law enforcement. Some of the companies consulted noted they are not moving fully to E2EE so law enforcement can continue to have access, however this was not the universal response. With the help of HSI Cyber Crimes Center (C3)'s partners in the UK and Australia, there are workarounds of this technology in some cases, but with privacy laws, this is not always possible.

There are limited incentives to technology companies to continue keeping their platforms safe.

There must be a commercial advantage to keeping a platform safe and free from CSEA. The Department should leverage the financial motivations of technology and social media platforms to its advantage. The platforms vary in sending CSEA reports, ranging from so much data where it overwhelms law enforcement resources to such minimal data that investigation is not viable. In briefings, we learned that companies are afraid of missing something, so they overreport CSEA, often overwhelming investigators with information that may or may not be actionable. On the other extreme end, especially in the context of end-to-end encryption, there is so little data being reported that it is challenging for law enforcement to respond.

DHS needs to have the technology capabilities to ensure that the private sector is incentivized to keep their platforms safe and free, while meeting their obligations to their customers' privacy. The UK demonstrated the possibility of scanning for sexual abuse materials on end-to-end encrypted social and online messaging platforms with a funding pilot.[1]

According to the private sector, the development of E2EE was in response to customer demand to ensure privacy from government intrusion. In briefings with law enforcement entities, E2EE presented a dilemma where private sector prioritized E2EE over removal of CSEA and reduced the quality of reporting to those entities for action. The balance between maintaining privacy via encryption and reporting criminal acts remain an 'evergreen' challenge that requires continuous introspection by the private sector and DHS which consumes valuable time and resources in combatting online CSEA.

[1] Rt Honorable Chris Philip MP and Rt Honorable Priti Patel MP, "Government Funds New Tech in the fight against online child abuse." 17 November 2021. Last accessed on 28 May 2024 at https://www.gov.uk/government/news/government-funds-new-tech-in-the-fight-against-online-child-abuse

There is a need for additional allies in the fight against CSEA.

Partnerships are the driving force to combat online CSEA. While interagency coordination and properly resourcing government entities is essential, it is not enough to combat CSEA. The Know2Protect campaign, for example, highlights the pursuit of partnerships to supplement resources provided. Snap was the first private sector company to sign on the Know2Protect. The company conducted research, granted ad space, is creating a "lens" for the campaign, and will distribute further surveys about young people's exposure to and knowledge of sexual harms in October 2024 and April 2025. However, not every technology company has been cooperative or open to forming partnerships.

Beyond traditional federal partners like the FBI and DOJ, additional federal allies are needed. CSEA proliferates for a multitude of reasons, one of which is profit. Large profits are being made from illicit activities, in violation of laws, regulations, and even terms of service. Engaging federal entities that have the ability to track, target, and investigate the use of financial systems has the potential to be a game changer. To date, relying on companies to 'do the right thing' has not yielded the desired results. Financial disincentives and liabilities are powerful federal tools to correct illicit and derogatory behavior. Developing mechanisms to bring other federal partners with their authorities to the fight against CSEA has the potential to make a profound difference. Beyond financial institutions, there are other regulatory entities that can further aid victims and investigators.

RECOMMENDATIONS

Recommendation #1: Establish, resource, and empower an office within DHS to lead Departmental efforts to counter online CSEA and form a center within DHS to organize a whole-of-government approach to addressing online abuse and exploitation.

To prioritize and secure resources for combatting online CSEA the Department should establish a Center, akin to a Fusion Center. Empowering such a center to coordinate across the Department will streamline efforts and enable the Department to bring its full capabilities to bear as a key participant in the whole-of-government approach to addressing online exploitation and abuse. By leveraging pre-existing government organizational models, such as those used to establish the NCTC and JTTF, this infrastructure will serve as a formal deconfliction point within the government, reducing existing barriers to information sharing and facilitating synchronous resource sharing.

The Center will spearhead inter-Departmental and interagency coordination efforts to counter online CSEA. DHS components, relevant law enforcement federal agencies (FBI, DOJ, USSS), and state and local authorities will be able to use the Center as a formal coordinating and deconfliction point to streamline their activities and build a common operating picture. Establishing this Center will also create a known touchpoint for departments focused on prevention and support including HHS and Education, NGOs (NCMEC, Thorn) and technology companies to engage as appropriate with government authorities to maximize information

sharing and promote unity of effort to counter online CSEA. International cooperation is crucial to comprehensively addressing this issue. As such, the Center will serve as a focal point for not only interagency, but also international cooperation by including representatives from Five Eye (FVEY) partner countries.

This Center will be responsible for facilitating and deconflicting operations and investigative activities. Convening analysts, law enforcement agents, and technology subject matter experts from across the Department and liaisons from adjacent government agencies will foster collaboration and effective allocation of resources. FBI and HSI analysts should determine a permissible way to work in hand in hand with the platforms on investigations and leads. This should be deemed as doing their jobs and not as "agent of the state" behavior. This ongoing continuous interaction between US law enforcement analysts and the platform analysts is critical. The key is that information sharing does not have to rise to some certain level before it is investigated, it becomes cooperative and iterative. Representatives from the S&T Directorate must be present within the Center to assist with integration and training on government owned technical solutions, both within the Center and at outstations responsible for CSEA. Moreover, the Center will facilitate White House engagement by providing dedicated seats on the Domestic Policy Council, National Economic Council, or National Security Council for collaboration.

The Center roles, responsibilities, and coordinating authorities must be formalized in a charter document to ensure it is sufficiently empowered to accomplish its mission. Adherent to this charter document, the Center can codify its coordinating relationships with external government and non-government entities through memoranda of understanding where needed.

Recommendation #2: Leverage existing tools; develop and advocate for policy solutions.

The Subcommittee recognizes the Department's effort to develop and identify strategies in combatting online CSEA. To capitalize on existing policies, and to avoid duplication of efforts, the Subcommittee recommends that DHS deploys holistic and intersectional solutions that rely on more than just a law enforcement response, and embrace incorporating public and private entities as part of the operational strategy while demanding increased responsibility from technology companies. The Center recommended above can utilize these policies to engage with USG agencies, such as HHS, ED, DOJ, FBI, and state, local, tribal, and federal stakeholders to lead, coordinate, and enable a whole-of-government approach. The following areas have been identified as critical to the development and implementation of policies to address online CSEA:

- The Department should prioritize and coordinate efforts across all levels of government and state, local, tribal, and territorial partners in countering online CSEA. The Department can model its approach as part of the "DHS Strategic Framework for Countering Terrorism and Targeted Violence." The UK has gone so far as to identify CSEA as a national security threat. This has proven effective in allowing for allocation of national level intelligence capabilities (i.e., UK's Government Communication Headquarters) to counter CSEA. By creating policy that allows for the incorporation of language that addresses online CSEA in future annual Homeland Threat Assessments, the Department could bring additional national level resources.

- The Department should identify and address training gaps and develop a standardized and enhanced reporting format for suspected instances of online CSEA while sharing the information in a timely manner.

- The Subcommittee recommends DHS ensures all entities focused on combatting online CSEA are adequately staffed and resourced at the Department and task force levels.

- The Department should explore opportunities, including those contained within proposed Congressional legislation, to ensure social media companies conduct robust risk assessments before they roll out major new features and require companies to conduct proactive scanning for potential child sexual abuse material (CSAM) circulating on their platforms.

- The Subcommittee advises that CSEA combatting policies should be data driven. We recommend all relevant research findings are shared across the government enterprise, and with external entities, partners, and victim advocates.

Recommendation #3: Increase participation in the combatting of CSEA by the major platform vendors.

3a. Study the feasibility of building a uniform technology platform with a public private partnership for monitoring and reporting on all investigations, past and present, open and closed. This platform would be used as the system of record for all investigating agencies.

There is clearly a need to have a unified system that all investigating parties can both update with the latest information and review existing open investigations and supporting information. Each of the different investigatory groups in the US plus our international partners have their own data sets which can result in a lack of coordination, deconfliction issues and missed opportunities for collaboration. In investigations like these, hours matter, let alone days, weeks, or months due to inefficient information sharing. Information sharing challenges stretch beyond the federal, state, and local government: Private sector entities, often the inadvertent facilitators of CSEA and frontlines of detection of such material, are critical holders of information.

We recommend the Department lead the creation of a technology council, based within the Center proposed above, that selects an architecture and starting technology base for the ingestion, correlation, and reporting of all active CSEA cases. To be clear, this should not be a venture that requires perfection from initiation, rather it should lean on existing domestic models (e.g., NYPD Shield Program[2]), other fusion cells, and international models to quickly identify an architecture that satisfies federal privacy and intelligence guidelines.

- All existing public and private stakeholders should be invited to submit requirements and potentially technology for the system.
- Include third parties in the design of the unified system or potentially assign the task of its delivery to one of these third parties.

[2] NYPD Shield: Countering Terrorism through Information Sharing. Last Accessed May 27, 2024, at https://www.nypdshield.org/

- Ensure the U.S.' international partners are also included to bolster the sense of ownership of the system.
- Aggregate all the shared information into the unified system and assign analysts from invested stakeholders to investigate and collaborate potential investigations.
- Encourage and require adoption and use across federal partners and with external stakeholders as further articulated in this report.

The goal of a unified system would be to successfully share data to combat CSEA. Investigating parties should annually review the system alongside third parties, international partners, and private sector to identify necessary improvements to keep pace with emerging technology while maintaining the primary purpose of the unified system.

3b. Reframe and realign incentives to partnership through legislative actions.

As discussed above, various social networking platforms play an important role in the detection and removal of CSEA. Each vendor has teams that work on the problem within Trust and Safety teams or initiatives. However, these teams' capacity are focused on ensuring compliance by the platforms rather than securing them against perpetrators of CSEA and supporting justice for victims. Just like with cybersecurity, an enterprise can have great compliance but not be very secure. The same goes for CSEA detection and prevention on the technology platforms. If the U.S. does not make progress with how platforms identify, remove, report, and investigate this type of content and these types of actions, we will not improve our posture.

Given the role platforms play, their compliance with federal guidelines alone is not enough to keep children safe. The goal of our interactions together must be actionable intelligence rather than simply compliance. True partnership, in addition to federal legislative changes is essential to effectively and meaningfully combatting CSEA. This means the shedding of silos and analysts working (virtually) shoulder-to-shoulder and sharing information in real time.

Platforms are reticent to share information with government regulatory or investigative agencies because the line between compliance and proactive support of an investigation (aka being an "agent of the government") becomes unclear. Technology companies need to shift their mindsets and the Department has an important role to play in ensuring that it is as easy and streamlined as possible to share information about CSEA with law enforcement agencies.

To encourage this cooperation, the Department should support legislation that eliminates the Section 230[3] liability shield for CSEA material. Currently platforms enjoy immunity from liability, even if they have done nothing to protect victims on their platforms. For some companies, especially those publicly traded, reputational harm from not working to combat CSEA is sufficient to spur some action. Unfortunately, for many platforms hosting the more insidious material and dark web content, this "shaming" is not enough. We therefore believe it is essential to make this moderate change to the application of Section 230 to truly motivate platforms to take the issue seriously. We are not recommending the Department engage in the

[3] 47 U.S. Code § 230 - Protection for private blocking and screening of offensive material. Last accessed May 28, 2024, at https://www.law.cornell.edu/uscode/text/47/230

larger battles over Section 230, but instead focus on where this statute has allowed CSEA and platform complacency to flourish.

Further, the Department might consider supporting modifications that allow Section 230 protections *to apply to CSEA*, when meaningful reporting and participation by platforms occurs. Looking to the Bank Secrecy Act's safe harbor provisions as a model, similar liability shields can be applied and lifted based on the degree of compliance with investigators protecting children from exploitation.

Legislative modifications become all the more pressing when one considers the pace of technology and acceleration of technologies like end-to-end encryption. Increasing use of end-to end encryption enhances privacy on the platforms but makes the detection and disruption of CSEA very difficult. We recommend at a minimum, outside of legislative action, platforms develop a model to assess confidence level of a potential threat to use as a threshold for breaking encryption. As noted above, a *safe harbor* should be created to incentivize the platforms to actively identify and remove all suspected content and report accounts that enable CSEA and the creation and distribution of CSAM.

These proposed realignments of "carrots and sticks" can motivate platforms to become allies while not opining on other aspects of the Section 230 debate. In forming tighter partnerships, the reporting and information sharing can be qualitatively better, easing investigative burdens, and allowing agents to address more cases.

Recommendation #4: Prioritize vicarious trauma and workplace well-being support for law enforcement, civil society employees, and other frontline staff who encounter CSEA material in their work.

CSEA investigations require law enforcement agents, investigators, and analysts to repeatedly encounter traumatizing content in the course of their work. Repeated exposure to materials depicting child sexual exploitation, engagement with victims and their families, and the challenges of these cases can lead to vicarious trauma and the need for additional mental health support. The Department has the opportunity to serve as a leader in this area and support its frontline employees in doing this difficult but essential work.

4a. The Department should develop a comprehensive program of support for frontline staff who are exposed to CSEA material in the course of their work. The Department has existing programs in place to support agents and analysts who work Child Exploitation Investigations, such as the Awareness and Resilience Mentoring for Operational Readiness program and aspects of ICE Peer Support. The Subcommittee recommends that the Department prioritize these efforts and continue to enhance existing support programs for frontline staff. Given the unique traumatic elements of CSEA cases and investigations, law enforcement agents, investigators and analysts require specialized support. The Department should identify and utilize examples of existing models to normalize support for frontline

workers experiencing vicarious trauma, both within and outside of law enforcement, including in the international space.

4b. The Department should work closely with the Office of the Chief Human Capital Officer (OCHCO) to ensure resources are allocated to hire personnel dedicated to providing mental health support to frontline staff. In order to effectively deliver on the comprehensive program outlined above, the Subcommittee recommends that the Department ensure the program is appropriately staffed and resourced. Trained personnel could be housed within the newly created Center to work closely with all Center personnel and any DHS personnel who are supporting these efforts. OCHCO will be a key partner in these efforts.

Recommendation #5: Bolster and sustain DHS external engagement for the Know2Protect Campaign by expanding resources and outreach with the ED.

The launch of the DHS' Know2Protect[4] Campaign on April 17th, 2024, in New York City in conjunction with National Child Abuse Prevention month marks significant effort and commitment from the Department toward equipping communities to prevent, identify and respond to CSEA. The Know2Protect Campaign will raise awareness about the rapidly escalating threat of online CSEA, and seeks to educate kids, parents, trusted adults, policymakers, and the broader public about online threats and empower them to help keep children safe online. The campaign goals are three-fold: education, prevention, and intervention. Additionally, the official in-person component of Know2Protect, Project iGuardian, plays a crucial role in training on topics related to CSEA in school settings. Project iGuardian has developed characters to be more relatable and informative for children, teenagers, and adults. Project iGuardian includes topics such as use of generative AI, sextortion, and grooming tactics. The Know2Protect homepage will have dedicated sections on how to report, geared toward children and teenagers.

The Council is eager to follow the implementation of these recommendations and those of the Homeland Security Academic Partnership Council (HSAPC) and Faith Based Security Advisory Council (FBSAC) CSEA reports, as we expect they will have recommendations relevant to their specific sectors and communities.

- **The Department should continue to support and resource the Know2Protect Campaign and plan to expand outreach.** The Subcommittee recommends that the Department leverage the Campaign to identify resource, partnership, and staffing needs to ensure that Know2Protect's important work continues. The Subcommittee learned from subject matter experts that awareness from children, teens, parents, caregivers, educators, and other stakeholders is an essential component of combatting CSEA and thus recommends that the Department also expand the outreach plan for Know2Protect in order to connect with more communities.

[4] DHS' Know2Protect, accessible at https://www.dhs.gov/know2protect, as of May 23, 2024.

- **The Department should propose collaboration with the ED and other avenues for in-school programming.** The Subcommittee recommends that the Department identify other areas of government that could leverage their reach to continue to expand the audience for Know2Protect and iGuardian programming. The ED is a logical starting place for these efforts. The HSAPC's CSEA subcommittee's recommendations will be relevant here and should inform the Department's approach in collaboration with the ED.

Recommendation #6: Lead engagement with economic and regulatory federal partners to increase the inter-departmental approach to combatting CSEA.

As noted in the findings, our FVEY partners have elevated combatting CSEA to a whole of government priority, coordinating policy making, regulation, and enforcement in the face of exponential increases in the level and sophistication of foreign and domestic online CSEA perpetration. The UK, for example, officially deemed online child sexual abuse as a national security threat and passed safety legislation focused exclusively on child sexual abuse. The UK Government CSEA response is understood to be a Prime Minister priority. The Out of the Shadow Index[5] has identified the UK as number one in tackling CSA compared to the U.S. ranking 13 out of the 60 countries assessed. The methodology they use is to analyze 60 countries that have 85% of the global child population of children. This ranking with the UK reflects how much backing and resources the UK has had in tackling this issue. Similarly, Australia has created an independent eSafety Commission with enhanced and specific statutory and regulatory authority, including coordinating a national strategy "cross government." An intentional goal of both regimes is mandating technology companies to keep their platforms safe and to report incidents of abuse, with the focus on the prevention side.

Replicating such a formal whole of government structure and inter-departmental coordination in the United States Government would require Congressional legislation and White House engagement. Nonetheless, and in addition to the DHS Secretary and the frontline DHS and DOJ offices and personnel specifically charged with countering and investigating CSEA, it is critical that other USG departments and agencies with regulatory and/or enforcement jurisdiction over aspects of the technology industry platform operations and/over the financial proceeds emanating from illicit CSEA activities view countering CSEA as a national policy priority and are attuned to the threat CSEA poses to the citizens of the United States.

By virtue of his peer relationship with other department and agency heads, the Secretary of DHS should advocate and encourage departments and agencies with complementary regulatory oversight and enforcement jurisdiction over technology industry platforms, and related online banking transactions and revenue streams, to more closely coordinate with DOJ to prevent, identify and punish child sexual exploitation and abuse. A non-exhaustive list of such agencies includes the Department of the Treasury and its banking regulators, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, and the Consumer Financial Protection

[5] The report is accessible at https://outoftheshadows.global, as of May 25, 2024.

Bureau. Other regulatory entities like the Federal Trade Commission and Federal Communications Commission, should also be robust partners in this fight.

Comparable efforts could be undertaken with the State Department to educate US Ambassadors and senior diplomats posted in foreign countries that are producers and distributors of online CSEA such that bilateral prevention and enforcement engagements with the relevant senior foreign officials can be mounted and sustained on a priority basis. Such engagements not infrequently would be a natural follow-on to ongoing efforts to combat Transnational Criminal Organizations and international financial criminal activity.

The vast revenues produced by the technology platforms and the growth in user traffic on those platforms are viewed as disincentivizing scanning for and eliminating banned CSEA materials and reporting same by the platforms. Such willful blindness can be discouraged through non-DHS regulators, foreign and domestic, directly or indirectly mandating prevention and reporting of online CSEA in Treasury's partnership with DHS and DOJ.

CONCLUSION

In summary, a unified federal government approach to combatting CSEA is needed, and DHS is uniquely situated to take the lead in coordinating this response. Through its leadership role, it can facilitate the creation and sustainment of a center that enhances communication between domestic, international, and private sector partners. On the federal side, this can help agency partners reimagine the application of their tools and authorities to bolster the fight against CSEA, supporting victims, forcing responsible private sector conduct and dismantling illegal networks. On the private side, the coordinating entity, leaning on a shared information platform, can integrate partners more fully into the fight against CSEA. The Department can further its impact by supporting legislative changes that financially disincentivize inertia and complacency in allowing CSEA to proliferate on the internet.

APPENDIX 1: TASKING LETTER

Secretary

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

Homeland Security

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
Erika Amaya	Special Assistant	Office of Partnership and Engagement
Ronald J. Appel	Division Chief	Homeland Security Investigation (HSI) Cyber Crimes Center (C3)
Keerthana Arjuna	Assistant Director	Child Protection and International Partnerships, Australian Attorney-General's Department
Jason Barry	Trust and Safety Manager	Meta
Jacqueline Beauchere	Global Head of Platform Safety	Snap Inc
Kristen Best	Principal Director	Countering Transnational Organized Crime, Office of Strategy, Policy, Plans (PLCY)
Tim Blackmore	International Lead	New Zealand Department of Internal Affairs Digital Safety
Leah Buck	International Lead	Tackling Child Sexual Abuse Unit, UK Home Office
Julia Cordua	CEO	Thorn
Antigone Davis	Vice President and Global Head of Safety	Meta
Ashley Freiberger	Director of Legislative Affairs	National Center for Missing and Exploited Children
Annabel Graham	Justice and Home Affairs First Secretary	British Embassy Washington DC
Joan Hoback	Deputy Special Agent in Charge	Forensic Services Division, United States Secret Service
Tanner Hubbard	Special Agent	Criminal Investigative Division, United States Secret Service
Marina Hunt	Senior Policy Officer	Child Protection and International Partnerships, Australian Attorney-General's Department
Luke Jones	National Security Attorney Advisor	Office of Law and Policy, National Security Division, U.S. Department of Justice
Ashley Katz	Director	Child Protection and International Partnerships, Australian Attorney-General's Department

Kate Kennedy	Campaign Director	Know2Protect Campaign, HSI
Amy Leffler	Social Scientist	DHS Science and Technology Directorate (S&T)
William Mancino	Special Agent in Charge	Criminal Investigative Division, United States Secret Service
Fallon McNulty	Director	Cybertipline, National Center for Missing and Exploited Children
Katie Noyes	Section Chief	Science and Technology Branch, FBI
Kevin Plourde	Assistant Special Agent in Charge	Criminal Investigative Division, United States Secret Service
Mike Prado	Deputy Assistant Director	HSI C3
Cinthya Rebaza	Director	Serious and Organized Crime, Public Safety Canada
Ravi Sinha	Director and Head of Child Safety	Meta
Emily Slifer	Director of Policy	Thorn
Marc-Antoine Therrien	Manager	National Strategy for Protection of Children from Sexual Exploitation on the Internet, Canada Public Safety
Patricia Wolfhope	Subject Matter Expert	DHS S&T