National Forum on the Prevention of Cyber Sexual Abuse

Boston College Libraries seeks $148,545.00 in funding from the Institute of Museum and Library Services (IMLS) through the National Leadership Grant for Libraries under the National Forum Grant program and Community Catalyst categories. Over a two year timeline, we will use this funding to convene a series of virtual and in-person meetings that unite library workers from around the United States with experts in cyber-related sexual abuse prevention. This Forum is to be attended by primarily academic library workers and select public, school, and tribal library workers in addition to a diverse range of academics, attorneys, social workers, and law enforcement officials, and will provide practical resources to develop a roadmap for outreach and instruction. With this curricular roadmap, library workers will be better equipped not only to help patrons who have been or are at risk of being targeted for crimes such as nonconsensual pornography, cyberstalking, deepfakes, and sexual extortion, but also to strategize and advocate for systemic change. We see this area of outreach and instruction in digital privacy as a critical but neglected form of digital literacy that library workers are uniquely poised to direct.

1. Statement of National Need

1.1 Summary

Crimes relating to technology-facilitated sexual violence are growing in the United States at a rate that has surpassed our government's ability to pass laws that allow for recourse.[1] This environment is exacerbated by a culture of shaming that pressures victims to remain silent lest they face public disgrace. The majority of victims of cyber sexual abuse are those whose sexual agency is most threatened in the physical world, including women; Black, Indigenous, and other People of Color (BIPOC); and LGBTQIA+-identifying persons (Citron 2014; Ruvalcaba and Eaton 2020). Extant library-based digital privacy education focuses more on technical know-how and less on the nuanced emotional and legal terrain associated with digital abuses. This Forum, if funded, would: 1) build and foster a community of experts to address this dire gap in education, 2) define a curriculum that is sensitive to victims' trauma, and 3) create a roadmap for the sustainable incorporation of this curriculum into library outreach, instruction, advocacy, and service.

Although the primary audience of this Forum is academic library workers, we recognize that cyber sexual abuse affects all types of library communities. As such, we will also invite participants from public, school, and tribal libraries to the Forum. It is our hope that the smaller scope of this initial project will inspire collaboration across different types of libraries and launch future outreach initiatives throughout the broader library community.

1.2 Brief Introduction to Cyber Sexual Abuse

Throughout this proposal, we use the term "cyber sexual abuse" synonymously with "technology-facilitated sexual violence" to refer to the "diverse ways in which criminal, civil, or otherwise harmful sexually aggressive and harrassing [behaviors] are being perpetrated with the aid or use of digital communication technologies" (Powell and Henry 2018, 5). These terms encompass crimes such as nonconsensual pornography, known more commonly as "revenge porn," although it is not always revenge-motivated (Citron and Franks 2019); sexual extortion; cyberstalking; deepfakes (Chesney and Citron 2018); intimate partner violence; sexual harassment; and other related abuses (Henry and Powell 2016).

1.3 Current Legal State of Cyber Sexual Abuse

[1] This is perhaps most evident in the United States with the Intimate Privacy Protection Act (2016), the Ending Nonconsensual Online User Graphic Harassment Act (2017), and the Stopping Harmful Image Exploitation and Limiting Distribution Act (2019), all of which have been introduced to Congress without resolution, although there has been bipartisan support in each case. For an international analysis, see Henry and Powell 2016.

To counter the culture of victim shaming and foster more self-reporting, some law enforcement agencies such as the Federal Bureau of Investigation (FBI) are actively pursuing cases related to technology-facilitated sexual abuse and publicizing their drive to bring justice to these types of criminals. Increasing outreach about the gravity of cyber sexual assault will demonstrate to society (including victims) that attackers will be held responsible for this category of crime. Doing so will engender trust, raise awareness for similar crimes, and may eventually lead to more comprehensive legislation. Although the FBI can pursue cases that violate federal laws (e.g., cyberstalking and distribution of child sexual abuse material), some forms of cyber sexual violence have not yet been criminalized under federal law (e.g., nonconsensual pornography and sexual extortion).

The resulting patchwork of applicable state laws has left state and local law enforcement without uniform direction or initiative to combat these crimes. This confusion, augmented by a lack of education and context, has led to many well-documented incidents of law enforcement officials trivializing reported cyber sexual abuses. Victims have reported hearing everything from "there's nothing we can do" to "if you didn't want those photos on the Internet, you shouldn't have taken them" (Goldberg 2019; Citron 2014). In some cases, an underage victim can themselves be charged with manufacturing child pornography if they shared photos of their own body with a confidant, even if this confidant then distributes the images without their consent (Stern 2019). Furthermore, the marginalized groups that are disproportionately targets of these crimes may initially be hesitant to reach out directly to law enforcement for other cultural reasons.

Victims of sexual aggression often do not report their assault to law enforcement due to a variety of institutionalized obstacles (Dewan 2108). As in the physical world, the vast majority of victims of cyber sexual abuse are women (Citron 2014, 13; Pew Research Center 2017). Furthermore, exploratory research on nonconsensual pornography suggests that bisexual women, bisexual men, and gay men have the highest rate of victimization (Ruvalcaba and Eaton 2020; Waldman 2019). Victims may be underage or undocumented as well.

Cyber sexual abuse also overlaps with intimate partner violence (Freed et al. 2017), which disproportionately affects people of color in the United States–especially multiracial populations and American Indian/Alaska Natives (Smith et al. 2017). Because people of color face complex dilemmas when considering reporting a crime to law enforcement, the Forum intends to explore the variety of options available to the victim in order to develop a victim-centered approach to this form of digital privacy training. By identifying resources that library staff can recommend to patrons, the Forum's newly trained attendees will build a coordinated community response that is centered around the importance of the victim's unique lived experience.

1.4 Cyber Sexual Abuse and Libraries

Nonprofits such as the Cyber Civil Rights Initiative (CCRI), the Electronic Frontier Foundation (EFF), FemTechNet, HACK*BLOSSOM, and the National Network to End Domestic Violence (NNEDV) have developed helpful online resources for victims. What these platforms lack, however, is a trusted and wide-reaching mechanism for coordinated and sustainable instruction and outreach.

By leveraging our training, ethics, and position of trust in campuses and local communities, library workers can contribute to and amplify the critical work that these nonprofits have started. Academic libraries are well-situated to bridge the gap between nonprofits and communities, given their broad experience with outreach and instruction related to information literacy, as well as direct access to the age group most frequently targeted for cyber sexual abuse (Ruvalcaba and Eaton 2020). A bumper crop of recent IMLS-funded efforts to raise privacy awareness have demonstrated how libraries can successfully increase privacy literacy in our communities. A 2015 grant established the Data Privacy Project, which trains New York City-based library staff in the fundamentals of digital privacy (IMLS 2015; Data Privacy Project, n.d.). In 2018, the University of Wisconsin, Milwaukee hosted a national forum in New York City to discuss library values and privacy in

national digital strategies (IMLS 2017a). The findings from their output inspired the 2019-2021 creation of Privacy Advocacy Guides for libraries, which focus on digital security basics, privacy audits, and data lifecycle management (IMLS 2019). Montana State University hosted a separate national forum in 2018 to address library-wide understanding of web privacy and web analytics (IMLS 2018). In 2018-2019, the Library Freedom Institute infused the library community with energy for privacy and digital security basics through its pilot and first full train-the-trainer instruction programs (IMLS 2017b).

The increased visibility of privacy advocacy from these forums and projects has had a ripple effect throughout the library community, as shown most clearly through the recent work of professional associations. In 2017, the Digital Library Federation (DLF) formed the new Technologies of Surveillance Working Group (renamed the Privacy and Ethics in Technology Working Group in March 2020) to address privacy and anti-surveillance via instruction, advocacy, and technology audits (Kim 2017). The following year, the American Library Association's (ALA) Library and Information Technology Association (LITA) led a webinar series on privacy in libraries (LITA 2018). In 2019, the Privacy Subcommittee of the ALA's Intellectual Freedom Committee updated Article VII of the Library Bill of Rights to underscore library patrons' rights to privacy and confidentiality (Caldwell-Stone 2019). In 2020, the New England chapter of the Association for Information Science and Information Technology (NEASIST) selected "The Privacy Puzzle" as their annual conference theme (ASIS&T 2019). All of this points to both a growing concern in the library community to understand the privacy needs of our workers, patrons, and communities as well as a hunger to take action to protect it.

These initiatives recognize that surveillance disproportionately harms marginalized groups and propose greater education as a solution to reduce this harm. Until 2019, the majority of this library instruction provided an overview of digital security and recommended tools and strategies that attendees could employ, for instance, to reduce their data flow and better safeguard their logins. These lessons were geared toward people who had a general interest in better protecting their privacy and security. In 2019, the DLF Technologies of Surveillance Instruction and Outreach subgroup (co-led by Paige Walker, the Project Director of this grant) recognized that these workshops often do not attract the people who have the most critical need to protect their privacy. For instance, some workshops attracted technologists who already had a skillful grasp of privacy practices. In other words, curriculum based around digital security tended to attract those with a pre-existing interest in digital security.

To offset this trend, the Instruction and Outreach subgroup disassembled the standard digital security overview curriculum and broke it into a series of tools (Walker et al. 2019). They drafted a series of scenarios to contextualize these tools for external audiences. The online dating scenario, for example, begins with a premise: "You are a user of Tinder, Grindr, OkCupid, or another online dating platform and are interested in meeting a partner while maintaining your personal privacy and safety." It then proceeds to show readers how to identify their risks, how to reduce their risks, and where to learn more. By prioritizing the relatable context in which privacy is threatened rather than the technical mechanisms of available tools, these guides can be more effective with audiences who do not have a prior interest in privacy tools.

1.5 National Forum on the Prevention of Cyber Sexual Abuse

By using the DLF working group's framework to recontextualize digital privacy literacy through the lens of an at-risk persona, we can specifically address cyber-enabled sexual violence. This recontextualization is a critical step in reaching desired audiences and creating a lasting impact. A National Forum on the Prevention of Cyber Sexual Abuse, if funded, would build upon prior grant projects and professional output by filling this gap in our community's current dialogue. It would provide the time and space to: 1) gather experts in the disparate fields of libraries, academia, law enforcement, and social work; 2) nurture this cross-pollinating community; and 3) develop a path forward for informed, sensitive, and sustainable instruction. Through this Forum, library workers

can amplify the digital literacy work begun by libraries and nonprofits by collaborating on an instructional roadmap that is specialized for cyber sexual abuse.

This Forum is exploratory because the production of a successful and impactful roadmap is dependent upon building a shared community of engaged participants. Because this nascent community will be interdisciplinary, it will be essential to first explore the values of libraries as they relate to academia, social work, and law enforcement. Through this exploration, the Forum community will build a common understanding, establish trust, apply library values to the context of cyber sexual abuse, and unite to protect our home communities from these crimes. In particular, we strive to build the bridge between law enforcement and library workers carefully and deliberately in order to retain the central importance of library patrons in our efforts to create this roadmap.

This strong Forum community will then act as a catalyst, galvanizing the academic library world at large to increase outreach and instruction about technology-facilitated sexual abuse. Through the Forum, we hope to build meaningful partnerships with academic library associations such as DLF, the HBCU Library Alliance, ACRL, and ALA. These associations may then sustain the momentum catalyzed by the Forum and use their widespread reach to educate library communities, empower victims and at-risk populations, and advocate for impactful systemic change.

2. Project Design

2.1 Project Goals and Risks

The goals of the Forum are fivefold:

1. Foster a diverse, trusted community that is capable of assessing the nuanced sociocultural, legal, and technical pressures that comprise technology-facilitated sexual violence;
2. Listen to and share expertise at the Forum event itself;
3. Produce a fully-formed first draft of a curricular roadmap for academic libraries;
4. Disseminate the curricular roadmap and solicit community feedback via a webinar, social media, email discussion lists, conference presentations, and other developing virtual spaces; and
5. Expand and sustain the community through integration with DLF and related organizations.

We have identified four main risks to the efficacy of the Forum. Primarily, the presence of law enforcement at the Forum may make attendees—particularly people of color—feel unwelcome. The project team cares deeply about the safety of all attendees, and will prioritize their comfort throughout the Forum process. We will limit law enforcement participation to those who have demonstrated expertise protecting victims of related crimes (e.g., victim specialists, prosecutors, and investigators). Furthermore, we will inform all invited guests that law enforcement will attend the Forum, which will allow all invitees to make an independent and informed decision as to whether they will participate. We will ensure that legal advocates such as immigration attorneys are present at the Forum, and we will circulate a Know Your Rights document with attendees in advance of the meeting. The Forum itself will be held in Boston, a sanctuary city, and law enforcement attendance to the Forum will be limited to one day. We will also hold a pre-Forum meeting that will enable us to listen to the concerns of library worker attendees and incorporate their input into our planning of the Forum event. Through taking these precautions, we hope to create a safe environment for all attendees.

A second risk addresses the confidentiality and safety of the victims whose assaults may be discussed during the Forum. To reduce this risk, victims' names will never be identified at any of the related Forum events. If this is done by accident, names will not be recorded in the community notes or on social media. Furthermore, community notes will be vetted for sensitive information before they are made available on the Forum website. We will also consider other risk-reducing strategies, including a "leave your device at the door" policy during sessions in which the most sensitive topics will be discussed.

A third risk involves the scope of the Forum itself. Past interdisciplinary events have shown that discussions of technology-facilitated sexual abuse can evolve into legal debates about the Communications Decency Act and/or government access to encryption backdoors. These topics are complex and polarizing; to focus on them risks dividing the Forum attendees. The goal of this event is to build and foster a community that will create victim-centered instruction, rather than debate complex legal topics. To mitigate this potential, the project team will make clear that the scope of the Forum and related events is limited to discussing these crimes as the laws stand now, rather than how they might be affected by future legal or policy changes.

A fourth risk is the limited diversity of the project team. While we aim to recruit members of marginalized groups disproportionately impacted by cyber sexual abuse to attend this Forum, they are not represented on our current project team. The exploratory nature of this leadership grant will establish and deepen our relationships with these essential stakeholders. We anticipate that this Forum grant would lay the groundwork for a subsequent project grant, whose future team would include these stakeholders among its members.

2.2 Personnel

Paige Walker (Project Director) is the Digital Collections and Preservation Librarian at Boston College, where she supervises the privacy and security of digital content and chairs the Privacy Working Group. Paige co-led the DLF Technologies of Surveillance Instruction and Outreach subgroup, which focused on developing digital privacy resources. In addition to her MSLIS, she received an MS in Cybersecurity Policy and Governance, during which she researched the technological mechanisms of cyberstalking. Paige is an ALA Emerging Leader and an elected member of the National Digital Stewardship Alliance's Leadership Group. She spends her free time leading cryptoparties (Kalish 2017) and volunteering with the Cyber Civil Rights Initiative.

Chelcie Juliet Rowell (Co-Investigator) is the Head of Digital Scholarship at Tufts University. She is currently secretary of the ACRL Digital Scholarship Section and served as co-chair of the DLF Digital Library Pedagogy Working Group from January 2018 through December 2019. In these roles, she has developed expertise in inclusive meeting facilitation, project management, instructional design, and digital pedagogy. She continually strives to enact values of social justice and intersectional feminism in her professional practice.

Emily Singley (Co-Investigator) is the Head of Systems and Applications at Boston College Libraries, where she also serves as the Libraries' Data Security Officer. She co-chairs two library technology committees for the Boston Library Consortium and advocates for library patron privacy as a member of the NISO-led SeamlessAccess.org project.

Adam Jazairi (Co-Investigator) is a software engineer at the Massachusetts Institute of Technology Libraries. He previously worked at Boston College Libraries, where he co-chaired the Privacy Working Group.

The Cyber Civil Rights Initiative (Consultant) is one of the nation's preeminent nonprofit organizations working to combat online abuses that threaten civil rights and civil liberties. Their work protects vulnerable groups from the devastating harms caused by nonconsensual pornography, deepfakes, cyberstalking, doxing, and other forms of online abuse. Their efforts are focused on four main areas, including legal reform, tech policy innovation, victim support, and research.

2.3 Structure

This planning, execution, and conclusion of the Forum will take place over a two-year period from August 2020 through July 2022. In the first phase, the project team will plan the Forum event, recruit diverse Forum participants, and facilitate a shared understanding through readings and virtual discussions. In the second phase, the Forum event will gather participants to listen and share expertise, explore how academic libraries may frame

this digital literacy, and outline a curricular roadmap. In the third phase, the project team will formalize this roadmap, share their findings via publicly available platforms and conference presentations, and strategize with DLF leaders to incorporate Forum findings into ongoing efforts of the Privacy and Ethics in Technology Working Group. This will ensure the sustainability of Forum output and allow for future revisions and iterations. These phases are outlined in further detail below. In order to foster cross-disciplinary communication, attendees will be selected from the following categories:

I. Library Workers

Academic library workers will be the key beneficiaries of this event and will form the bulk of the attendees. A call for participation shared throughout the broad landscape of library networks will encourage diverse and inclusive representation among academic libraries, which will in turn make the deliverable more effective in the library community writ large. We will also include workers from public, school, and tribal libraries in order to encourage cross-community dialogue. Library workers who have confirmed interest include: **Eliza Bettinger** (Lead Librarian for Digital Scholarship at Cornell University), **Andy Boyles Petersen** (Digital Scholarship Librarian at Michigan State University), **Michelle Gibeault** (Scholarly Engagement Librarian for the Humanities at Tulane University and co-chair of DLF Privacy and Ethics in Technology Working Group), **Samantha Lee** (Head of Reference Services at Enfield Public Library), **Tonya Ryals** (Assistant Director for the Craighead County Jonesboro Public Library), **Dorothea Salo** (Faculty Associate at University of Wisconsin at Madison), **Yasmeen Shorish** (Data Services Coordinator and Associate Professor at James Madison University), and **Scott W. H. Young** (UX & Assessment Librarian at Montana State University and co-chair of DLF Privacy and Ethics in Technology Working Group).

II. Activists, Nonprofit Workers, and Social Workers

Activists, nonprofit workers, and social workers will provide firsthand expertise of victims' struggles and advise on how library workers can design curriculum sensitive to related trauma. Professionals who have expressed interest include: **Asia Eaton** (Associate Professor in Psychology at Florida International University), **Katelyn Bowden** (Founder and Director of Battling Against Demeaning and Abusive Selfie Sharing "BADASS" Army), **Eva Galperin** (Director of Cybersecurity at EFF), **Michelle Gonzalez** (Executive Director at CCRI), **Liam Lowney** (Executive Director at Massachusetts Office for Victim Assistance), **Erica Olsen** (Director of NNDEV's Safety Net), **Francesca Rossi** (Licensed Clinical Social Worker at Thriving Through), and **Andrew Sta.Ana** (Director of Law and Policy at Day One).

III. Academics

Scholars who have contributed to the growing body of expert research on technology-facilitated sexual violence will add further grounding and perspective to our discussions. Academics who have expressed interest include: **Danielle Citron** (Professor of Law at Boston University, 2019 MacArthur Genius Fellow, and Vice President of CCRI), **Mary Anne Franks** (Professor of Law at University of Miami and President of CCRI), **Deborah Hurley** (Adjunct Professor of the Practice of Cybersecurity and Associate Faculty Director, Data Privacy, Brown University), **Tom Ristenpart** (Associate Professor at Cornell Tech and the Department of Computer Science, Cornell University), and **Ari Ezra Waldman** (Professor of Law and Director of the Innovation Center for Law and Technology at New York Law School, Founder and Director of the Institute for CyberSafety).

IV. Legal Professionals

Investigators and prosecutors with experience related to cyber sexual abuse cases will provide expert perspective, which will enable library workers to construct a curricular roadmap that responds to real-world threats. Legal professionals who have confirmed interest include: **Elisa D'Amico** (Partner at

K&L Gates LLP), **Julie A. Dahlstrom** (Director & Clinical Associate Professor, Immigrants' Rights and Human Trafficking Program, Boston University School of Law), **FBI Boston**, and **Carrie Goldberg** (Owner, C.A. Goldberg, PLLC).

2.3.1 Phase 1: Pre-Forum Planning and Community Building

The impact of this grant depends largely upon the successful recruitment of a diverse and engaged body of participants. As such, the majority of the project team's pre-Forum planning will be dedicated to selecting and cultivating this body of thirty to forty experts.

In order to identify and encourage diverse library workers, including underrepresented populations, to attend, the project team will send a call for participation across email discussion lists, newsletters, social media, and library professional networks. This call for participation will be distributed across many academic library communities, including Historically Black Colleges and Universities (HBCUs), Tribal Colleges and Universities (TCUs), community colleges, and small liberal arts colleges. The survey will ask interested individuals to explain their interest in the project and ask them to elaborate on the unique perspective they would bring to the Forum. Attendance will be limited, and the team will prioritize the intentional recruitment of members of marginalized communities from different geographic regions in the United States. Doing so will create not only a more well-balanced Forum event, but also a more effective output.

We will also reach out to those involved with previous privacy-related IMLS-funded projects, especially those who worked on the *Collections As Data* project, the National Forum on *Library Values and Privacy in our National Digital Strategies*, the *National Forum on Web Privacy and Web Analytics*, the *Privacy Advocacy Guides for Libraries* project, and the *Privacy in Libraries* project. This collaboration will allow us to sustainably build upon the groundbreaking work that these projects have begun in recent years.

Once participants have been identified and have confirmed availability, the project team will share DLF's Code of Conduct (DLF, n.d.) and our enforcement policy with them, and include a click-through agreement that all interested attendees must complete in order to qualify for participation and reimbursement. We will also share introductory resources such as scholarly articles, publicly available documentation of cases, and examples of extant curricula with all confirmed participants via email. Attendees will be encouraged to read the included literature prior to the Forum event itself in order to establish a shared depth of knowledge in the subject of cyber sexual abuse. The project team will also create a Forum website to facilitate organization and communication.

The project team will also give library worker participants the opportunity to attend a virtual meeting in which the participants can meet each other and ask questions in a space that is free from law enforcement participants. This separate space will facilitate community building between library workers, providing them with a means to ask introductory or sensitive questions that they may feel intimidated to ask at the actual Forum. It will also give the project team the ability to listen to participants' concerns about law enforcement attendance and incorporate them into Forum planning. In this phase, the project team will also consult with institutional ombuds offices for input on group facilitation and communication strategies, and will voluntarily seek to appoint an ombudsperson trained in conference moderation.

2.3.2 Phase 2: National Forum

The physical Forum event will take place over the span of three days in May 2021 at Boston College. Each day will be centered around a different theme. Proceedings will be documented via shared notes with rotating assigned notetakers, as well as with a Forum hashtag and subsequent archival capture of this hashtag activity.

Day One: Introduction

The Forum will begin with a welcome, a land acknowledgement, an overview of the Code of Conduct, and a content warning that invites attendees to step out of the room if they feel they need to do so for any reason. A keynote speaker will open the Forum with a statement that emphasizes the importance of outreach and education in communities that are more vulnerable to these crimes. Attendees will then break into mixed groups and complete activities that define vocabulary, establish a shared understanding of key terminology, and clarify the objectives of the Forum. After a break, a panel of victim specialists, social workers, attorneys, and investigators will review a composite of cyber sexual abuse cases. This moderated panel will culminate with questions regarding the role libraries may have in instruction of and outreach for technology-facilitated sexual violence.

Day Two: Application

The second day will begin with a brief welcome and a review of the Code of Conduct. After this, scenarios based on real-world cases will be presented to the attendees. These scenarios will be carefully selected to demonstrate both a range in categories of victims as well as a range in technologies used to perpetuate sexual violence. For instance, we might examine:

- How an LGBTQ-identifying man is relentlessly doxxed by an ex-boyfriend who sets up hundreds of impersonating accounts on online dating platforms (C.A.Goldberg 2018).
- How a twenty-something woman is harassed, stalked, and 'swatted' by a former Craigslist roommate using anonymizing services (Department of Justice 2018).
- How an undocumented woman is tracked and harassed by her partner using default programs such as Find My Phone (Freed et al. 2017).

For each scenario, group members will identify: 1) which technologies were used in the crime, 2) the sociocultural context in which the attacker was capable of perpetrating the crime, 3) the steps the victim may have taken against the attacker, 4) how the victim might have been able to reduce the risk of this abuse before it began, 5) which resources the victim may need before, during, and after the perpetration of cyber sexual abuse, and 6) opportunities for trusted community service providers like library workers to provide support.

Day Three: Action and Roadmap

The third and final day of the Forum will focus on how library workers can take action against these crimes. Participants will outline a curriculum roadmap that identifies how academic libraries may increase outreach and instruction about technology-facilitated sexual abuse. The first few days of the Forum will shape the contents of this roadmap, but possible topics may include:

- Statement of need and role for library workers in the prevention of cyber sexual abuse
- Recommendations for future development of specific instructional materials (e.g., lesson plans for outreach events, pamphlets, and/or website)
- Key relationships and resources for library workers (e.g., campus counseling services)
- Detailing different implementation strategies for institutions

Social worker attendees will provide vital input on how and when library staff may interact with victims, as well as when and how they may have to respond to a mandatory duty to report. Furthermore, participants will identify key relationships (e.g., local networks of social workers, state-run victim services programs, or campus/local/state/federal law enforcement) and establish how and when it is appropriate for library workers or victims to contact these stakeholders. The development of these workflows will be centered around the safety and security of diverse library patrons, and will address the complexities of groups that may be resistant to contacting law enforcement about their victimhood.

2.3.3 Phase 3: Post-Forum Events and Sustainability

The third phase of the project will focus on the formalization and dissemination of Forum output. Particular attention will be paid to the confidentiality risks associated with these discussions. Notes and social media posts will be vetted for sensitive content prior to being archived and/or made available publicly on the Forum website and subsequently in the DLF repository.

The project team will review, distill, and refine the recommendations produced at the Forum event to produce a curricular roadmap. This roadmap will provide an overview for cyber sexual abuse instruction at academic libraries, focusing on techniques both to reduce the risk of victimization as well as to respond to victimization.

After the project team has finalized this first curricular draft, they will share it with the Forum participants for further comment and review. Following this review, they will disseminate their output and solicit feedback from the academic library community. This will be accomplished through: 1) a free, open webinar that reviews the Forum itself, provides an overview of the draft curricular roadmap, and invites community feedback for the output; 2) advertisements through social media and various library communications venues that encourage feedback; 3) appearances on related podcasts; and 4) select conference presentations by various members of the project team that review the Forum, publicize the draft output, and welcome responses.

The intent of this Forum is to catalyze library-wide conversation around our field's role in the instruction of and advocacy for the prevention of cyber sexual abuse. As such, our draft curricular roadmap will be a living document rather than a canonical version of instructional curriculum. In order to accomplish this, the project team has reached out to the coordinators of DLF's Privacy and Ethics in Technology Working Group, who have confirmed interest in sustaining the project through their community. Hosting Forum output on the working group's Open Science Framework (OSF) repository under a CC BY 4.0 license will allow the library community to revise and expand the draft curriculum as they see fit. We hope that this work would continue to incorporate the expertise of cross-disciplinary Forum attendees, since a major goal of the Forum is to develop this community and deepen relationships across fields.

By broadcasting and disseminating our output in such a way, we hope to encourage the library community to build upon our resources and incorporate them into future work such as regional workshops or webinars that reach high-risk library patrons. This could include pursuing future funding that expands this digital privacy literacy initiative to serve public, school, and tribal libraries, as well as translating the roadmap and resources into Spanish, Haitian, Portuguese, and Mandarin, among other languages. Furthermore, we hope to pursue future funding for a subsequent project that would include more diverse stakeholders on the project team and address a different phase of project maturity. Therefore, the exploratory National Forum on the Prevention of Cyber Sexual Abuse will itself be a roadmap for future projects that are scaled to include more public, school, and tribal library workers.

2.4 Project Timeline

Phase	**Duration**	**Activities**
1. Pre-Forum Planning and Community Building	August 2020 – May 2021	● Circulate call for participation, notify those selected ● Share DLF Code of Conduct and Forum-specific enforcement policy; secure confirmation from participants ● Circulate pre-Forum reading material ● Host pre-Forum virtual meeting for library workers ● Incorporate feedback from virtual meeting into planning

2. National Forum Event	May 2021	● Three-day Forum event at Boston College
3. Post-Forum Events and Sustainability	May 2021 – July 2022	● Review Forum output ● Draft curricular roadmap ● Disseminate draft via virtual webinar, invite feedback ● Solicit feedback via email discussion lists and social media ● Present at relevant conferences, invite further feedback ● Incorporate feedback into draft roadmap, host on DLF OSF repository ● Identify future funding opportunities to expand program

3. Diversity Plan

The success of this Forum is dependent upon the participation of library workers with diverse lived experiences. In the call for participation, we will privilege funding the attendance of members of the underrepresented and marginalized communities that are disproportionately victimized by technology-facilitated sexual violence. We will recruit from many types of academic library communities, including HBCUs, TCUs, community colleges, and small liberal arts colleges. To foster an environment of inclusion, we will require that all attendees read and agree to abide by the Code of Conduct. We will draw upon DLF's years of experience to co-develop a policy that enforces DLF's Code of Conduct at the Forum itself and at all related Forum events.

The project team is aware of tensions that may arise from the inclusion of law enforcement officials at this event. To address this, the project team will consult with attendees during the planning stage of the Forum, and will incorporate these concerns into the Forum itself. The project team prioritizes the safety and security of library workers and privileges the inclusion of their voices in this Forum project.

4. Statement of National Impact

This national Forum, centered on the prevention of cyber sexual abuse, would give library workers a dedicated space to address our previously inchoate role in this environment of abuse that targets our most vulnerable communities. Funding such an event would 1) break down silos, 2) foster communities of library and cross-disciplinary experts, and 3) expand our digital privacy instruction to address this critical dearth of outreach.

This exploratory project will lay the foundation for this broader community. It will construct a team of diverse experts that clarifies the role of academic library workers in the fight against technology-facilitated sexual violence. The resulting curricular roadmap will, through its dissemination via social media, webinars, conference presentations, and podcasts, open a much-needed library-wide conversation on cyber sexual abuse. After incorporating profession-wide suggestions into the roadmap, an adaptable version will be made available on an open-source repository for reuse throughout the community. With future funding, this output could then be translated into non-English languages or otherwise transformed to address needs specific to public, school, and tribal libraries.

A National Forum on the Prevention of Cyber Sexual Abuse would have a major impact on the library community as well as the well-being of library patrons. By linking extant communities dedicated to abuse prevention, we will take a victim-centered approach to development of cyber sexual abuse instruction and begin to create a coordinated community response that can be adopted and sustained throughout academic libraries in the United States.

Activities		2020					2021				
		August	September	October	November	December	January	February	March	April	May
Phase 1: Pre-Forum Planning and Community Building	Create website, recruit participants										
	Select participants, confirm commitment										
	Circulate introductory material										
	Host Pre-Forum virtual meeting										
	Incorporate meeting feedback into Forum planning										
Phase 2: The National Forum											

Activities		2021							2022						
		June	July	August	September	October	November	December	January	February	March	April	May	June	July
Phase 3a: Dissemination	Draft curricular roadmap														
	Virtual webinar, solicit feedback														
	DLF 2021, solicit feedback														
	Library Collective 2022, solicit feedback														
	LOEX 2022, solicit feedback														
Phase 3b: Revision	Incorporate feedback														
	Present at ALA Annual 2022														
Phase 3c: Sustainability	Host content on DLF repository														
	Identify future funding opportunities														

DIGITAL PRODUCT FORM

INTRODUCTION

The Institute of Museum and Library Services (IMLS) is committed to expanding public access to digital products that are created using federal funds. This includes (1) digitized and born-digital content, resources, or assets; (2) software; and (3) research data (see below for more specific examples). Excluded are preliminary analyses, drafts of papers, plans for future research, peer-review assessments, and communications with colleagues.

The digital products you create with IMLS funding require effective stewardship to protect and enhance their value, and they should be freely and readily available for use and reuse by libraries, archives, museums, and the public. Because technology is dynamic and because we do not want to inhibit innovation, we do not want to prescribe set standards and practices that could become quickly outdated. Instead, we ask that you answer questions that address specific aspects of creating and managing digital products. Like all components of your IMLS application, your answers will be used by IMLS staff and by expert peer reviewers to evaluate your application, and they will be important in determining whether your project will be funded.

INSTRUCTIONS

If you propose to create digital products in the course of your IMLS-funded project, you must first provide answers to the questions in **SECTION I: INTELLECTUAL PROPERTY RIGHTS AND PERMISSIONS.** Then consider which of the following types of digital products you will create in your project, and complete each section of the form that is applicable.

SECTION II: DIGITAL CONTENT, RESOURCES, OR ASSETS

Complete this section if your project will create digital content, resources, or assets. These include both digitized and born-digital products created by individuals, project teams, or through community gatherings during your project. Examples include, but are not limited to, still images, audio files, moving images, microfilm, object inventories, object catalogs, artworks, books, posters, curricula, field books, maps, notebooks, scientific labels, metadata schema, charts, tables, drawings, workflows, and teacher toolkits. Your project may involve making these materials available through public or access-controlled websites, kiosks, or live or recorded programs.

SECTION III: SOFTWARE

Complete this section if your project will create software, including any source code, algorithms, applications, and digital tools plus the accompanying documentation created by you during your project.

SECTION IV: RESEARCH DATA

Complete this section if your project will create research data, including recorded factual information and supporting documentation, commonly accepted as relevant to validating research findings and to supporting scholarly publications.

SECTION I: INTELLECTUAL PROPERTY RIGHTS AND PERMISSIONS

A.1 We expect applicants seeking federal funds for developing or creating digital products to release these files under open-source licenses to maximize access and promote reuse. What will be the intellectual property status of the digital products (i.e., digital content, resources, or assets; software; research data) you intend to create? What ownership rights will your organization assert over the files you intend to create, and what conditions will you impose on their access and use? Who will hold the copyright(s)? Explain and justify your licensing selections. Identify and explain the license under which you will release the files (e.g., a non-restrictive license such as BSD, GNU, MIT, Creative Commons licenses; RightsStatements.org statements). Explain and justify any prohibitive terms or conditions of use or access, and detail how you will notify potential users about relevant terms and conditions.

We intend to produce a curricular roadmap for reuse across the national library community. As such, this output will be licensed with Creative Commons Attribution 4.0 International (CC BY 4.0), which allows for copying, redistributing, and adapting the content with attribution.

A.2 What ownership rights will your organization assert over the new digital products and what conditions will you impose on access and use? Explain and justify any terms of access and conditions of use and detail how you will notify potential users about relevant terms or conditions.

This material will be made publicly and freely available via the Digital Library Federation's Open Science Framework repository. Users will be notified of the CC BY 4.0 license through the OSF's user interface, which displays the license at the top of each web page.

A.3 If you will create any products that may involve privacy concerns, require obtaining permissions or rights, or raise any cultural sensitivities, describe the issues and how you plan to address them.

We will vet all content for privacy concerns, permissions, and sensitivities. Areas with privacy concerns and permissions/rights issues will be removed from any content. If cultural sensitivities (e.g., descriptions of violence that may be triggering to some readers) are identified as a necessary part of this output, we will include content warnings on the hosting website and in the output document itself.

We will collect personal information of interested attendees in our call for participation (CFP), likely via a Google Form, but it will not be retained after the CFP has concluded and participants have confirmed their attendance at the Forum. We will also collect possibly personal information when asking library worker attendees for input on planning the Forum itself. This feedback will be incorporated into planning, but the data itself will not be retained for privacy purposes.

SECTION II: DIGITAL CONTENT, RESOURCES, OR ASSETS

A.1 Describe the digital content, resources, or assets you will create or collect, the quantities of each type, and the format(s) you will use.

The Forum website will be hosted on bc.edu, and will list the project description, team, and resources. Ultimately, the roadmap we produce will be distributed and archived as an openly available document in a freely available preservation format, likely a PDF. We will also produce a Twitter archive of Forum hashtag activity, exported as a CSV spreadsheet and Wakelet story. The roadmap and Twitter archive will be archived in DLF's OSF repository, and the Forum website will also be maintained after the project concludes.

A.2 List the equipment, software, and supplies that you will use to create the digital content, resources, or assets, or the name of the service provider that will perform the work.

We will use widely available services and software such as Google Forms, Google Docs, Microsoft Word, and Adobe Acrobat to produce our digital content. We will archive Twitter hashtags with Wakelet. Web content will be created with WordPress or Hugo templates using the Libraries' existing web infrastructure.

A.3 List all the digital file formats (e.g., XML, TIFF, MPEG, OBJ, DOC, PDF) you plan to use. If digitizing content, describe the quality standards (e.g., resolution, sampling rate, pixel dimensions) you will use for the files you will create.

PDF, HTML, CSV

Workflow and Asset Maintenance/Preservation

B.1 Describe your quality control plan. How will you monitor and evaluate your workflow and products?

Our Project Director will lead the development of content, including monitoring and evaluating our workflow and products. Furthermore, key personnel will provide support and feedback on this evaluation. By opening our product up to the library community before its publication on OSF, we will also give nationwide library workers the ability to evaluate and inform our products, regardless of their attendance at the Forum.

The Boston College Libraries accessibility experts will review content and ensure that it meets accessibility standards. The digital preservation team will quality check format outputs for preservation quality.

B.2 Describe your plan for preserving and maintaining digital assets during and after the award period. Your plan should address storage systems, shared repositories, technical documentation, migration planning, and commitment of organizational funding for these purposes. Please note: You may charge the federal award before closeout for the costs of publication or sharing of research results if the costs are not incurred during the period of performance of the federal award (see 2 C.F.R. § 200.461).

We will host a Forum website through Boston College for the duration of the project (August 2020-July 2022). This resource will serve to publicize our project before, during, and after the in-person Forum event. Following the conclusion of the project, the website and our output will be hosted in DLF's publicly available OSF repository, which allows for open-source storage and version control.

Metadata

C.1 Describe how you will produce any and all technical, descriptive, administrative, or preservation metadata or linked data. Specify which standards or data models you will use for the metadata structure (e.g., RDF, BIBFRAME, Dublin Core, Encoded Archival Description, PBCore, PREMIS) and metadata content (e.g., thesauri).

Our files will not be connected to extensive metadata, but will be archived in DLF's OSF repository in compliance with OSF's metadata standards.

C.2 Explain your strategy for preserving and maintaining metadata created or collected during and after the award period of performance.

DLF's OSF repository allows for versioning, which preserves both content and metadata through Google Cloud. Files are checked for integrity using cyclic redundancy checks, which minimizes the risk of bit rot and/or data corruption. Google Cloud also stores logs indefinitely in cold storage.

C.3 Explain what metadata sharing and/or other strategies you will use to facilitate widespread discovery and use of the digital content, resources, or assets created during your project (e.g., an API [Application Programming Interface], contributions to a digital platform, or other ways you might enable batch queries and retrieval of metadata).

Beyond dissemination through webinars, conferences, and email discussion forums, Boston College Libraries' Forum website will follow search optimization best practices. It will be discoverable via web crawlers. We will publicize both the Forum website and the archived content on the OSF repository using social media.

Access and Use

D.1 Describe how you will make the digital content, resources, or assets available to the public. Include details such as the delivery strategy (e.g., openly available online, available to specified audiences) and underlying hardware/software platforms and infrastructure (e.g., specific digital repository software or leased services, accessibility via standard web browsers, requirements for special software tools in order to use the content, delivery enabled by IIIF specifications).

For the duration of the Forum, project resources and content will be available on the Forum project website run on BC's library platform and/or WordPress. In the last month of the project grant, finalized output will be hosted on DLF's OSF repository and made openly available online. No special tools will be needed to use the content. All content will undergo an accessibility review by the Boston College accessibility team.

D.2. Provide the name(s) and URL(s) (Universal Resource Locator), DOI (Digital Object Identifier), or other persistent identifier for any examples of previous digital content, resources, or assets your organization has created.

N/A

SECTION III: SOFTWARE

General Information

A.1 Describe the software you intend to create, including a summary of the major functions it will perform and the intended primary audience(s) it will serve.

N/A

A.2 List other existing software that wholly or partially performs the same or similar functions, and explain how the software you intend to create is different, and justify why those differences are significant and necessary.

N/A

Technical Information

B.1 List the programming languages, platforms, frameworks, software, or other applications you will use to create your software and explain why you chose them.

N/A

B.2 Describe how the software you intend to create will extend or interoperate with relevant existing software.

N/A

B.3 Describe any underlying additional software or system dependencies necessary to run the software you intend to create.

N/A

B.4 Describe the processes you will use for development, documentation, and for maintaining and updating documentation for users of the software.

N/A

B.5 Provide the name(s), URL(s), and/or code repository locations for examples of any previous software your organization has created.

N/A

Access and Use

C.1 Describe how you will make the software and source code available to the public and/or its intended users.

N/A

C.2 Identify where you will deposit the source code for the software you intend to develop:

Name of publicly accessible source code repository:

N/A

URL:

N/A

SECTION IV: RESEARCH DATA

As part of the federal government's commitment to increase access to federally funded research data, Section IV represents the Data Management Plan (DMP) for research proposals and should reflect data management, dissemination, and preservation best practices in the applicant's area of research appropriate to the data that the project will generate.

A.1 Identify the type(s) of data you plan to collect or generate, and the purpose or intended use(s) to which you expect them to be put. Describe the method(s) you will use, the proposed scope and scale, and the approximate dates or intervals at which you will collect or generate data.

N/A

A.2 Does the proposed data collection or research activity require approval by any internal review panel or institutional review board (IRB)? If so, has the proposed research activity been approved? If not, what is your plan for securing approval?

N/A

A.3 Will you collect any sensitive information? This may include personally identifiable information (PII), confidential information (e.g., trade secrets), or proprietary information. If so, detail the specific steps you will take to protect the information while you prepare it for public release (e.g., anonymizing individual identifiers, data aggregation). If the data will not be released publicly, explain why the data cannot be shared due to the protection of privacy, confidentiality, security, intellectual property, and other rights or requirements.

N/A

A.4 What technical (hardware and/or software) requirements or dependencies would be necessary for understanding retrieving, displaying, processing, or otherwise reusing the data?

N/A

A.5 What documentation (e.g., consent agreements, data documentation, codebooks, metadata, and analytical and procedural information) will you capture or create along with the data? Where will the documentation be stored and in what format(s)? How will you permanently associate and manage the documentation with the data it describes to enable future reuse?

N/A

A.6 What is your plan for managing, disseminating, and preserving data after the completion of the award-funded project?

N/A

A.7 Identify where you will deposit the data:

Name of repository:

N/A

URL:

N/A

A.8 When and how frequently will you review this data management plan? How will the implementation be monitored?

N/A