NATIONAL LEADERSHIP GRANTS FOR LIBRARIES

Sample Application LG-260197-OLS-26
Project Category: National Implementation

Chief Officers of State Library Agencies

Amount awarded by IMLS:	$266,710
Amount of cost share:	$0

The Chief Officers of State Library Agencies will enhance public libraries' resilience against cybersecurity threats, especially ransomware attacks. The results of this project will improve the capacity of library staff, library Board members and other interested stakeholders to assess the risk of a cybersecurity attack. The project will result in A Guide to Cybersecurity for Library Stakeholders; A Cybersecurity Checklist for Library Stakeholders; A Guide to Recovering from a Ransomware Incident: A Library Perspective; and A Cybersecurity Scorecard to be filled out privately by libraries. This project will draw upon and collaborate with an Advisory Team that includes key stakeholders: state librarians, public library directors of various sizes (to ensure representation of both small rural libraries, large urban libraries, and tribal libraries), public library information technology managers, cybersecurity specialists and representatives of vendors serving the library technology market.

Attached are the following components excerpted from the original application.

- Narrative
- Schedule of completion

When preparing an application for the next deadline, be sure to follow the instructions in the most recent Notice of Funding Opportunity for the grant program to which you are applying.

Introduction

The Chief Officers of State Library Agencies (COSLA) is seeking a National Implementation Grant in the amount of $266,720 from the Institute of Museum and Library Services National Leadership Grants for Libraries (NLG-L) program for a two-year project aimed at enhancing public libraries' resilience against cybersecurity threats, especially ransomware attacks. This proposal responds to **IMLS's Objective 1.3 of the NLG-L Program Goal to "provide broad access to and preservation of information and collections through libraries and archives."** The results of this project will enhance the capacity of library staff, library Board members and other interested stakeholders to assess the risk of a cybersecurity attack. This project will specifically focus on identifying the existence or absence of cybersecurity protections (including software, hardware, policies and procedures) in public library systems of various sizes. It will consider the unique challenges faced by smaller rural libraries, larger urban public library systems, and tribal libraries. Partnering with COSLA in this proposal are library technology consultants Joe Matthews (JRM Consulting) and Carson Block (Carson Block Consulting Inc.).

Project Justification

Broadly, this proposal to IMLS's NLG-L responds to Goal 1 and Objectives 1.1 and 1.2 in IMLS's 2022-2026 strategic plan:

- **Goal 1: Champion Lifelong Learning**
  - **Objective 1.1** Advance shared knowledge and learning opportunities for all
  - **Objective 1.2** Support the training and professional development of the museum and library workforce

The project will support these goals and objectives by developing a set of best practices to counter cybersecurity threats and communicating these best practices to key stakeholders. These best practices will help ensure the security of public infrastructure by protecting systems from cybersecurity attacks, ensuring that the nation's public libraries remain a viable source of information. The results of this project will enhance the capacity of library staff, library Board members and other interested stakeholders to assess the risk of a cybersecurity attack.

More specifically, this proposal responds to **NLG-L Program Goal, Objective 1.3:** Provide broad access to and preservation of information and collections through libraries and archives by enhancing information infrastructures through greater security.

While cybersecurity threats are an ever-increasing challenge in our connected world, the threat of ransomware (where a bad actor encrypts computer files until a fee is paid to unlock them) has become a menace for all types of organizations, including public libraries. Public libraries in Boston, Contra Costa County (CA), Dallas (TX), St. Louis (MO), Seattle (WA), Spartanburg County (SC), and Westchester County (NY) have all experienced ransomware attacks. Even larger libraries such as the British Library and the Toronto Public Library have suffered digital extortion events that have led to being unable to use their

automated systems for several months as they attempt to restore service. According to a report by IBM, the cost of a data breach averaged $4.35 million, 83% of organizations have experienced more than one data breach, 59% of organizations do not employ zero trust security architecture, and 45% of the breaches occurred in the cloud.[1] Given the complexity of information technology hardware, software and the relationships between all technology components, public library stakeholders often do not even know what questions to ask, how to assess risk, or what measures can help prevent and respond to cybersecurity threats.

The primary target audience for this proposal are public libraries in rural, urban and tribal communities, but the ultimate beneficiaries are the people served in libraries across the United States who count on libraries for access to essential services on the Internet. Some functions, such as finding a job, seeking medical care, conducting business, participating in government, and more are increasingly a digital-only experience. The endless possibilities of digital networks have given us an unprecedented sense of connectedness and opportunity for convenience, improving the way we communicate and interact and giving us access to seemingly limitless information and resources. We are now able to communicate with each other instantaneously, download apps that connect to our cars and homes, and live a significant portion of our life through our phones and computers.

Public libraries now play a critical role in offering free public internet access. They are a key source of news, social capital, and access to electronic government services and information for a significant proportion of the U.S. population. Directly informing objective 1.2, many people use libraries for finding work and launching small businesses. Downtime due to successful cyberattacks puts these services at direct risk. Additionally, there has been a lack of focus on the technological measures that are needed in public libraries to protect the integrity of the library systems themselves from cyber attacks.

This project builds upon and compliments national efforts aimed at improving the security of public institutions. Acknowledging the increasing importance of effective cybersecurity and advanced firewall services, the Federal Communications Commission announced in November 2023 the creation of a Schools and Libraries Cybersecurity Pilot Program that will spend $200 million over three years for the purchase of equipment and services.[2] While the program covers the costs of security devices and services, it may not address the specific knowledge that technical people and decision makers need to select security measures that are best suited for their libraries, or take into account the vast differences in the condition and configuration of technology equipment and in libraries across the US. One of the biggest challenges is that cyber security is a moving target as new threats are discovered almost daily in the network of hardware and software that hackers are constantly trying to exploit.

Public Libraries in rural, urban and tribal communities are the target audience for this proposal. Libraries in rural and tribal areas that lack technical skills to continually improve and manage cybersecurity risk leaving behind community members who rely on public access technologies and connectivity. Many libraries without access to skilled technical staff are

[1] IBM (2023). *Cost of a Data Breach Report 2022*.
[2] FCC News (2023). FCC Proposes Creation of Schools and Libraries Cybersecurity Pilot Program.

unaware of cybersecurity best practices that would minimize the risks associated with maintaining connectivity in their communities. Addressing these needs through this project will support NLG-L Objectives 1.1 and 1.2.

Of the over 9,000 public library administrative entities in the United States, 44.4% of the total are located in geographic areas classified as rural.[3] In addition, there are 574 Native American/Native Hawaiian and Alaska Native entities recognized by the US Government, many of which have libraries serving communities, schools and higher education institutions.[4] Common problems faced by public, school and academic libraries large and small include old and/or obsolete equipment; software that is not up to date; insufficient bandwidth; firewalls, switches and routers that are not configured using best practices; and infrequent system backups.

Many public libraries are dependent on a city or county IT department for cybersecurity support, and yet these IT departments may assign a low priority to library challenges or are under-resourced. By collaborating directly with public libraries and those that may provide information technology services to libraries, this project will gather more information about what technological measures are in place to protect information technology from cybersecurity attacks.

The work done by this project will result in materials both physical and digital, audio and visual, that will be purpose-built to sustain the work of libraries around the country to protect their systems from cyber threats. We believe that this work is critical to the well-being of our nation's libraries and, consequently, the ability of communities to rely on and trust their libraries to keep their infrastructure safe from harm.

Project Work Plan

This project will draw upon and collaborate with an Advisory Team that includes key stakeholders: state librarians, public library directors of various sizes (to ensure representation of both small rural libraries, large urban libraries, and tribal libraries), public library information technology managers, cybersecurity specialists and representatives of vendors serving the library technology market. The Advisory Committee will also include at least one pilot participant in the FCC Cybersecurity Program (the Miami-Dade Public Library) to assist with coordination of the programs and identifications of this grant can strengthen library security even further. Garfield Swaby (Senior Director, IT) and Jay Haque of the New York Public Library, Curtis Wiliams (IT Program Manager, San Diego Public Library) and others have expressed interest in being members of the Advisory Team. Advisory Team members will provide project guidance, review drafts of a library security checklist, reports, project deliverables, provide feedback on the quality and effectiveness of the work performed by the project team, and participate in the planned in-person and remote Library Cybersecurity presentations.

---

[3] The Institute of Museum and Library Services. (2020). Public Libraries in the United States: Fiscal year 2017, Volume I. Washington, DC: The Institute.

[4] https://www.usa.gov/indian-tribes-alaska-native

The goal of this project is to assess the current state of cybersecurity preparedness of public libraries and to develop and share best practices for library directors and board members. Additionally, the project aims to create a practical checklist to help libraries understand the risks that they face, and to prepare and share a guide to responding to a cybersecurity incident in a library.

Year One:

- Create a project Advisory Team
- Conduct interviews with library directors and board members to learn of their cybersecurity concerns and fears.
- Develop and implement project communications strategies to solicit contribution and collaboration, to engage the library and IT communities, and to share project outputs.
- Identify cybersecurity best practices through a literature review.
- Preparing three project report deliverables:
    - **A Guide to Cybersecurity for Library Stakeholders**. This Guide will identify key questions to ask and provide a process to assess the risk of a cybersecurity incident.
    - **A Cybersecurity Checklist for Library Stakeholders**. The checklist will identify potential threats to IT hardware, software and organizational policies to help libraries determine their level of risk.
    - **A Guide to Recovering from a Ransomware Incident: A Library Perspective**. This guide will outline recommended steps to take in the event of a ransomware incident in a library setting.

Year Two:

- Create and distribute a **Library Security Scorecard** (covering cybersecurity measures) to allow libraries to rate their own security readiness and take actions to improve.
- Conduct in-person outreach (in the format of a “Library Cybersecurity Conference”) through multiple events adjacent to or part of existing events including the American Library Association (ALA) conference, the Public Library Association (PLA) conference, Library Technology Conferences, the Association of Tribal Libraries, Archives and Museum (ATALM) conference and other opportunities.The Project Team would invite information technology professionals from libraries that have experienced a cybersecurity incident to share what they have learned from the experience and what steps they have taken to enhance cybersecurity measures in their library. The perspectives of these library professionals would be complimented by inviting cybersecurity experts to talk about the current state-of-the-art concerning the tools and techniques that can and should be used to counter cybersecurity threats. Library directors who have experienced a ransomware incident would be invited to share what measures were taken to recover from the ransomware incident that their library experienced.
- Conduct in-person outreach activities for State Librarians in partnership with COSLA.
- Prepare a project report that would include an evaluation.

Tasks Detail

Literature Review. The two project co-principal investigators will prepare a literature review that identifies cybersecurity best practices from a management perspective. The resources available from the Center for Internet Security (CIS) and the Cybersecurity & Infrastructure Security Agency (CISA) will be included in this literature review.

Conducting Interviews. The two project co-principal investigators will interview twenty-five public library directors and IT managers about the broad policy issues of cybersecurity. These interviews aim to learn about the concerns of library directors, library Board members and the library management team concerning the risks of a cybersecurity attack on their library. Some of the libraries that received FCC grants will be included in those who are interviewed.

Prepare the First Project Publication. The combination of the interviews and the literature review will form the foundation for the creation of the first project deliverable: A Guide to Cybersecurity for Library Stakeholders. The Guide would identify the key questions to ask and provide a process to assess the risk that a library would experience a cybersecurity incident. Possible questions might include:

- Is cybersecurity a topic that is on the Library Board's meeting agenda?
- Does the library have an up-to-date inventory of IT assets? Network switches, hubs, repeaters, routers, firewalls, servers, desktop computers, software licenses, …. ?
- Are any of these devices or software nearing their end-of-life when support ends?
- How frequently are backups made of our various systems? Where is the backup data stored?
- When was the last time the backup data was used to restore a system?
- Does the library store personal identifying information of its customers, e.g., credit card numbers, social security numbers, etc.? Does the library need to store this information?
- Does the library have an Incident Response Plan? A Disaster Recovery Plan? A Business Continuity Plan?
- What percent of the IT budget is devoted to cybersecurity?

A draft of the Guide will be sent to the Advisory Team for their review and comments. Additional reviews will be provided by interested COSLA members. The comments will be incorporated into the document and a final version of the Guide will be prepared. The goal is to develop a guide that builds upon the success of the IMLS-funded "Toward Gigabit Libraries" toolkit. The toolkit, which received three Laura Bush 21st Century Librarian grants developed a format for technical information that is accessible and useful for all levels of technical expertise, from laypeople to information technology professionals, translating highly technical and accurate information into knowledge, concepts and actions accessible to all, regardless of technology knowledge, background or skills.[5]

[5] The three IMLS-funded grants for the Toward Gigabit Libraries toolkit are RE-00-15-0110-15 https://www.imls.gov/grants/awarded/re-00-15-0110-15; RE-246219-OLS-20 https://www.imls.gov/grants/awarded/re-246219-ols-20 Full proposal: https://www.imls.gov/sites/default/files/project-proposals/re-246219-ols-20-full-proposal.pdf; and RE-256732-OLS-24 https://imls.gov/grants/awarded/re-256732-ols-24; Full proposal: https://www.imls.gov/sites/default/files/project-proposals/re-256732-ols-24-full-proposal.pdf

Prepare the Second Project Publication. The Co-Principal Investigators will prepare a draft of A Cybersecurity Checklist for Library Stakeholders. The checklist would identify possible threats to information technology hardware and software as well as organizational policies as a way for a library to determine their level of risk. The checklist will identify a broad range of issues that should be considered and identify a range of risk depending on the current situation.

A range of IT and information system control areas form the technical line of defense against cyberattacks. These include:

- **Network and perimeter security.** A network perimeter demarcates the boundary between an organization's intranet and the external or public-facing internet. Vulnerabilities here create the risk that attackers can use the internet to attack resources connected to it.
- **Endpoint security.** Endpoints are network-connected devices, such as laptops, mobile phones and servers. Endpoint security protects these assets and, by extension, data, information or assets connected to these assets from malicious actors or campaigns.
- **Application security.** This protects data or code within applications, both cloud-based and traditional, before and after applications are deployed.
- **Data security.** This comprises the processes and associated tools that protect sensitive information assets, either in transit or at rest. Data security methods include encryption, which ensures sensitive data is protected, and creating data backups.
- **Identity and access management (IAM).** IAM enables the right individuals to access the right resources at the right times for the right reasons.
- **Distributed Resources Security.** Modern networks consist of "on premise" and "cloud" computing resources; while the library may be responsible for Network and perimeter security, vendors may be responsible (in some but not all cases) for the security of cloud resources.
- **Zero trust architecture.** This removes implicit trust ("This user is inside my security perimeter") and replaces it with adaptive, explicit trust ("This user is authenticated with multifactor authentication from an organization's laptop with a functioning security suite").

A draft of the Guide will be sent to the Advisory Team and interested COSLA members for their review and comments. The comments will be incorporated into the document and a final version of the Checklist will be prepared.

Prepare the Third Project Publication. The project will prepare a draft of A Guide to Recovering from a Ransomware Incident: A Library Perspective. This guide would identify the recommended steps that should be taken should a ransomware incident occur in a library setting.

Carson Block, Co-Principal Investigator for this proposal, was a Subject Matter Expert for the first grant, and Co-Project Manager for the second and third grants.

A draft of the Guide will be sent to the Advisory Team and interested COSLA members for their review and comments. The comments will be incorporated into the document and a final version of the Checklist will be prepared.

Create and Distribute a Cybersecurity Scorecard. The co-principal investigators originally contemplated surveying public library directors to gather their perceptions about the challenges associated with cybersecurity, and conducting a more technical survey for library information technology managers asking about their current cybersecurity measures. However, upon further thought, it was determined that survey data about the conditions of library security (even anonymised) could be used by threat actors in attacks. Instead, the project will create and distribute a similar instrument in the form of a "Cybersecurity Scorecard" to be used by libraries privately to assess their risks and provide a path for improvements. To evaluate the distribution and effectiveness of this tool, the project team will report the number of distributed Cybersecurity Scorecards, and conduct a simple anonymised survey asking two questions: 1) Did your library complete the Scorecard? And 2) Have you made or are you making improvements based on what you learned?

Cybersecurity Webinars. The Co-Principal Investigators will conduct five bi-monthly webinars in the second year that will discuss important cybersecurity issues and interview individuals associated with a library that has experienced a cybersecurity incident.

Conduct in-person outreach (in the format of a "Library Cybersecurity Conference") through multiple events tied to existing opportunities including ALA, PLA, COSLA, Library Technology Conferences, selected state library conferences, and other opportunities.The Project Team would invite information technology professionals from libraries that have experienced a cybersecurity incident to share what they have learned from the experience and what steps they have taken to enhance cybersecurity measures in their library. These library professionals would be complimented by inviting cybersecurity experts to talk about the current state-of-the-art concerning the tools and techniques that can and should be used to counter cybersecurity threats. Library directors who have experienced a ransomware incident would be invited to share what measures were taken to recover from the ransomware incident that their library experienced.

Evaluation

The project team has developed a draft Performance Measurement Plan for this application that will be enhanced by advice from the advisory board. Metrics will include both quantitative and qualitative evaluation of activities. Please see the attached *Perfmeasurement.pdf*

Project Results

The project will result in five primary deliverables:

- *A Guide to Cybersecurity for Library Stakeholders*. The Guide would identify the key questions to ask and provide a process to assess the risk that a library would experience a cybersecurity incident.

- *A Cybersecurity Checklist for Library Stakeholders*. The checklist would identify possible threats to information technology hardware and software as well as organizational policies as a way for a library to determine their level of risk.
- *A Guide to Recovering from a Ransomware Incident: A Library Perspective*. This guide would identify the recommended steps that should be taken should a ransomware incident occur in a library setting.
- *A Cybersecurity Scorecard* to be filled out privately by the library.
- *A Webinar Series on Cybersecurity Topics.* Five bi-monthly webinars in the second program year that will discuss important cybersecurity issues and interview individuals associated with a library that has experienced a cybersecurity incident.

A final report that includes program evaluation will also be published at the conclusion of the project.

All materials will be published under a Creative Commons Non-Commercial-Share-Alike 4.0 (or higher) license to allow for free, non-profit use of the deliverables to allow for the greatest distribution and adaptability. In addition, ALA Publishing has expressed interest in publishing the three publications, which would further extend the dissemination of project results to the ALA community. The project findings will be shared through publications, presentations (in-person and virtual), the project website (hosted by COSLA), and social media. We anticipate that the three publications will be accessible on most state library websites. The project team will make project related presentations at the annual American Library Association Conference, the annual COSLA Conference and selected state library conferences. The Cybersecurity Webinars would be accessible via YouTube after the webinars have been broadcast. Finally, COSLA will maintain the project website for the deliverables for a period of five years after the project is complete.

In order to create sustainable deliverables, the project co-investigators will focus on enduring concepts, principles and strategies while demonstrating how to incorporate emerging trends, techniques and technologies. In addition, two years after the completion of this project, the two project co-principal investigators will review the three publications to ensure that the information contained within them is still relevant and timely.

Schedule of Completion

The project will be planned, implemented, and managed by Joe Matthews and Carson Block, two experienced library consultants, who will be the primary project personnel. Carson Block's office includes administrative and publishing support which will be included in the project work. The project will be supported by State Library Staff (through in-kind donations of time to perform research, create awareness, facilitate communications with all libraries in their respective states, and assist with in-person events), and a volunteer Advisory Board of experienced technology experts. Progress will be tracked via a project management platform (such as Monday.com) where tasks, deliverables, and deadlines will be listed and reported.

It is anticipated that this project will take two years to complete as detailed in the exhibits below:

Year 1: September 2026 - August 2027

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	**IMLS Cybersecurity Project Work Plan**												
2	**Year 1**	***Month***	***Month***	***Month***	***Month***	***Month***	***Month***	***Month***	***Month***	***Month***	***Month***	***Month***	***Month***
3	**Activity**	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***
4													
5	Recruit and interact with Advisory Team members	X ----------	----------										
6													
7	**Prepare a draft of A Guide to Cybersecurity for Library Stakeholders**			X---------									
8	Advisory Team reacts to the draft of A Guide to Cybersecurity for Library Stakeholders				X-----								
9	Prepare the final version of A Guide to Cybersecurity for Library Stakeholders						X------						
10													
11	**Prepare a draft of A Cybersecurity Checklist for Library Stakeholders**						X----------						
12	Share draft with the Advisory Team							X------					
13	Prepare the final version of A Cybersecurity Checklist for Library Stakeholders								X-------				
14													
15	**Prepare a draft of A Guide to Recovering from a Ransomware Incident: A Library Perspective**									X----------			
16	Share draft with the Advisory Team										X-------		
17	Prepare a final version of A Guide to Recovering from a Ransomware Incident: A Library Perspective											X---------	

Year 2: September 2027 - August 2028

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	**IMLS Cybersecurity Project Work Plan**												
2	**Year 2**	***Month***	***Month***	***Month***	***Month***	***Month***	***Month***	***Month***	***Month***	***Month***	***Month***	***Month***	***Month***
3	**Activity**	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***
4													
5	Cybersecurity Webinars		X		X		X		X		X		
6													
7	Distribute a library security scorecard to public libraries												
8	Draft the scorecard	X---											
9	Share draft with Advisory Team		X--------										
10	Incorporate comments in the scorecard		X----										
11	Invite survey participants			X----------									
12	Prepare a report summarizing the reults of the scorecard					X----------							
13	Share the draft report with the Advisory Team						X-----						
14	Incorporate comments in the Final Report								X--------				
15									X----				
16	Presentation to COSLA of the scorecard results									X			
17													
18	**Conduct one-day and a half-day Library Cybersecurity Conference presentations**												
19	Prepare for the presentation	X----------											
20	Present conference presentations at state and national conferences		X---		X---		X---		X---		X---		
21													
22	Project evaluation										X ----------		
23													
24	Prepare and submit final project report												X