Common Good Cyber Fund Logic Model:

Internet Society Foundation

Outputs	Outcomes	Objective
Output 1.1: Increased provision of Internet security services that directly maintain and protect critical infrastructure Output 1.2: Regular security monitoring performed by grantees Output 1.3: Sharing of threat intelligence and best practices among cybersecurity ecosystem actors	Outcome 1: More secure critical infrastructure maintained by a diverse ecosystem of trusted operators	Strengthened cybersecurity ecosystem of non-profit providers that more effectively deliver cybersecurity support, advance enabling conditions, and respond to threats including digital transnational repression (DTNR)
Output 2.1: High-risk users receive cybersecurity support Output 2.2: Practical guidance and tools for preventing, responding to, and recovering from attacks are tailored to and shared with specific groups of high-risk users	Outcome 2: Greater protection and resilience of users exposed to targeted threats, including Digital Transnational Repression (DTNR) and technology-facilitated gender-based violence	Highest-level change the Fund can help 'move the needle' on
Output 3.1: Increased knowledge-sharing and coordination among grantees and ecosystem partners Output 3.2: Development of ecosystem-level resources, policies, and recommendations designed to strengthen the enabling conditions for a safer Internet for all	Outcome 3: Strengthened collaborative networks and global partnerships engaged in advancing a safer Internet for all, including vulnerable groups and high-risk communities	**Goal**
Output 4.1: Multiyear and flexible grants issued to CSOs working in cybersecurity Output 4.2: Grantee capacity-building workshops or gatherings on strategy, financial management, data collection, technical best practices, and other topics relevant to organizational development	Outcome 4: Improved organizational capacity and financial stability among grantees	Improved online safety for all and greater protection of high-risk Internet users
Deliverables immediately produced from Fund-supported activities	Changes beyond the Fund's control but we hope to help influence	Big-picture, systemic change we hope to see one day that our project is a small part of

Theory of Change:

IF the Internet Society Foundation, in collaboration with Global Cyber Alliance, runs a well-resourced, five-year grant program that provides multi-year, flexible funding to non-profit organizations working in cybersecurity—particularly in the Global Majority—and complements this funding with technical and organizational capacity building, expert advocacy support, and opportunities for peer learning and knowledge exchange,

THEN these non-profit organizations (Internet Society Foundation grantees) will maintain more secure critical infrastructure, better support high-risk users facing cybersecurity threats, and strengthen collaborative networks and global partnerships that work to advance safety and security initiatives—ultimately resulting in a stronger cybersecurity ecosystem that creates a safer Internet for all.

Critical Assumptions:

- Multi-year, flexible funding provides organizations with sufficient agility to adapt to evolving digital threats, shifts in political or high-risk environments, and changes in the funding landscape.
- Robust organizational capacity-strengthening support that is tailored to grantees' specific needs will lead to ongoing implementation of improved operational practices, ultimately enabling organizations to better sustain their technical programming.
- Building a diverse network of cybersecurity-focused organizations will foster peer-to-peer learning and ongoing collaboration beyond the grant period, contributing to a stronger global support ecosystem in the long term.

CGCF Indicator Guidance

When reporting on indicators, grantees should consider the portfolio of programming that CGCF funding is contributing to or supporting, then include results from those programs/initiatives when reporting indicator data to CGCF. As CGCF can either directly or indirectly support programs, grantees should use their best judgment when deciding what data to include in CGCF reporting. Grantees should also make sure to report only on results achieved during the reporting period and should not include results achieved outside of the date range covered in their report. If ever unsure of what data to include in reporting, grantees should reach out to their CGCF contacts.

Organizational Capacity and Sustainability Indicators (Applicable to All Grantees)

The Organizational Capacity and Sustainability Indicators apply to all CGCF grantees, regardless of the programming area. They are intended to capture changes in organizational capacity, sustainability, and operational effectiveness during the grant period.

Organizational Capacity and Sustainability Indicators (Applicable to All Grantees)	
Indicator	**Guidance**
Number of grantees reporting a higher number of active funding sources at the end of the grant as compared to the start of the grant	Number of grantees who self-report having a greater number of active total funding sources at the end of the grant (or at the time of reporting, for interim reports) compared to the start. 'Funding sources' can include grants, contracts, donations, sponsorships, earned income, etc. This indicator is not meant to definitively prove that the Fund alone is responsible for improving a grantee's financial situation; rather, it is designed to capture any changes in financial situation that CGCF may have helped contribute to

	through either direct funding or organizational capacity building support.
Number of specific operational improvements or other organizational strengthening actions taken by grantees over the course of the grant	Grantees self-report whether they have made any concrete financial, administrative, operational, or other organizational improvements after having received CGCF funding and/or participating in capacity-building activities organized by the ISOC Foundation for CGCF grantees. Grantees should be able to point to specific examples of improvements they believe CGCF funding or capacity-building helped contribute to, such as new or updated protocols/policies, financial systems, strategies, or governance processes; staffing changes; new communication strategies; or organizational use/adoption of new tools.
Number of grantees reporting greater confidence in managing funds for cybersecurity support over the course of the grant	Grantees self-report whether they feel more confident in managing financial resources related to cybersecurity work after having received CGCF funding and/or participating in capacity-building activities organized by the ISOC Foundation for CGCF grantees.

Indicators by Program Focus

For grants focusing on maintaining critical cybersecurity infrastructure (Report Only on Applicable Indicators)	
Indicator	**Guidance**
Estimated number of end-users benefiting from cybersecurity infrastructure	Total number of people who directly or indirectly benefit from grant-supported infrastructure services provided by grantees during the

services that are improved or maintained by grantees	reporting period. Includes users of networks, platforms, or systems that are made more secure through grantee activities. This is a reasoned estimate used to illustrate the scale of the benefits resulting from grantee protection or support of cybersecurity infrastructure services. It may be imprecise because these services often operate at shared, upstream, or Internet-wide levels – resulting in benefits that may extend to large numbers of users indirectly. 'Infrastructure services' include shared operational services that help secure, sustain, and strengthen the availability, integrity, and trustworthiness of core Internet systems – such as by identifying threats, enabling remediation, supporting incident response, and providing trust-enabling functions such as secure certificate infrastructure.
Number of infrastructure-related exposures identified by grantees that are detected prior to exploitation	This counts the number of distinct, significant security weaknesses affecting relevant infrastructure that are identified by granteesduring the reporting period ***before*** there is confirmed evidence of malicious exploitation. 'Exposures' are significant security weaknesses, including vulnerabilities, misconfigurations, insecure defaults, weak access control, or other conditions that could enable unauthorized access, compromise, disruption, or abuse. Grantees should use their technical expertise and internal criteria to determine if an identified exposure should be counted under this indicator as a meaningful security weakness that could lead to harm if not addressed.
Percent of identified exposures successfully	This measures the proportion of exposures identified by grantees that are successfully mitigated by grantees before impacting users.

mitigated by grantees or officially acknowledged for remediation by the responsible infrastructure operator, before impacting users, disaggregated by numerator/ denominator	'Exposures' are significant security weaknesses, including vulnerabilities, misconfigurations, insecure defaults, weak access control, or other conditions that could enable unauthorized access, compromise, disruption, or abuse. An exposure is considered 'successfully mitigated' if it was addressed or reduced before causing harm to users or systems. An exposure is considered officially acknowledged for remediation if the responsible infrastructure operator communicates it is aware of and intends to address the exposure following coordinated disclosure. For the denominator, grantees will report the total # of exposures identified according to the indicator above. For the numerator, grantees will report the total number of exposures (out of those identified) that were successfully mitigated. The Fluxxreporting system will use these two numbers to calculate the resulting percentage.
Number of organizations (e.g., national or sectoral CSIRTs, infrastructure operators, service providers, and civil society organizations) responding to or remediating cybersecurity threats based on reports or intelligence shared with grant support	This counts how many organizations took actionduring the reporting period after receiving cybersecurity threat information, reports, alerts, or intelligence shared through grant-supported work. 'Responding' to threats includes taking action to manage or contain a detected threat or incident, such as blocking malicious traffic, taking down malicious infrastructure, alerting affected users or members, escalating to an incident response team, issuing advisories, initiating containment measures, or sharing the information onward for operational action. 'Remediating' threats includes taking actions taken to fix, reduce, or eliminate the underlying risk or exposure, such as by patching vulnerable systems, correcting misconfigurations, disabling exposed services, rotating credentials, updating rules or controls, or otherwise removing the condition that enabled the threat.

	This is a contribution, not attribution, indicator. Grantees are not expected to prove they alone caused the response. Instead, grantees should show a reasonable link between the information shared and the action taken by the organization. Potential data sources for this indicator include follow-up emails, calls, or meetings with those who received reports/ intelligence to discuss or confirm actions taken, either through new or existing communication channels.
Number of grantees providing new or expanded Internet security services to users, providers, or authorities	Grantees are asked (Y/N) whether they are offering new cybersecurity services or expanding existing ones as part of their grant. If applicable (Y), grantees are then asked to further describe the service(s) provided. Examples of services include monitoring, incident response, advisory support, new or enhanced reporting protocols and data sharing mechanisms. 'Expanded' services includes changes made to grantees' existing services that produce broader coverage or improved quality. Small routine adjustments should not automatically count as an expansion in services unless they are substantial in scope.
Number of distinct threat monitoring activities regularly conducted by grantees	'Distinct threat monitoring activities' are specific types of monitoring including but are not limited to analyzing Indicators of Compromise (IoCs) (technical artifacts or observables that may show malicious activity, such as suspicious IP addresses, domains, files hashes, registry keys, process names, certificates, or other warning signs that may indicate compromise or attempted compromise); identifying distinct adversary campaigns; investigating novel Tactics, Techniques, and Procedures (TTPs); and/or documenting critical vulnerability clusters documented. This includes only grant-supported monitoring activities conducted during the reporting period. Given the nature of this technical activity,

	conducting a higher number of threat monitoring activities does not necessarily mean better performance, as some activities are more complex than others. As appropriate, grantees should include in narrative reporting a brief description of their threat monitoring activities to provide context for the number reported.
Number of public interest reports with high-confidence findings developed and shared by grantees	This counts reports produced by grantees during the reporting period that present strong, evidence-based findings on threats, risks, incidents, or security practices, and that are shared publicly or with relevant partners. 'High-confidence findings' means the information is well-supported by evidence and considered reliable enough to inform action or decision-making. Publicly shared means the report is made accessible beyond the organization (e.g., published on a website, shared with partners, policymakers, or relevant stakeholders, or disseminated through events or networks).
Number of infrastructure-focused operational tools, platforms, or coordination mechanisms developed or strengthened with Fund support and actively used by multiple ecosystem actors	This counts tools, platforms, or coordination mechanisms that are supported by the Fund during the reporting period and help organizations work together to monitor, share information, or respond to cybersecurity threats affecting infrastructure. 'Actively used' means the tool, platform, or mechanism is being used on an ongoing basis after being created or improved, for example through regular data sharing, coordination, or collaborative contributions. To be counted, grantees must have evidence that it is being used by multiple organizations or other actors who are part of the cybersecurity ecosystem, such as CSOs, CSIRTs, platforms, networks, or other actors.

For grants focusing on the delivery of scalable support to secure Internet users from digital harm, including state-directed cyber activity and digital transnational repression (Report Only on Applicable Indicators)	
Indicator	**Guidance**
Percentage of high-risk users who report applying new practices or tools after receiving cybersecurity support, disaggregated by numerator/ denominator	This indicator is assessed among the portion of high-risk users who agree at the conclusion of the support engagement to provide safe, anonymous feedback to the grantee. New practices or tools include secure communication tools, two-factor authentication, safer password practices, threat detection or reporting practices. 'Successfully' means the user correctly engages in a practice or uses a tool as part of their daily activities to improve their security. For the denominator, grantees will report the total # of individuals who received cybersecurity support through the grant and who the grantee followed up with. For the numerator, grantees will report the total # individuals who reported during follow-up that they used a new tool or practice in their daily activities to improve their security. The Fluxxreporting system will use these two numbers to calculate the resulting percentage. While grantees are encouraged to follow up with as many users as is feasible, response rates are unlikely to be 100%, and follow-up may be conducted with a sample. Potential data sources for this indicator include grantee follow-up surveys, calls, or interviews with the users they support. However, grantees are not required to report specific details about high-risk users' practices that could compromise those users' security.

Percentage of Internet users who report feeling safer from digital harm after receiving cybersecurity support from grantees, disaggregated by numerator/ denominator	Percentage of high-risk users who say they feel safer online after receiving support from grantees. This is a perception indicator and not a direct measure of safety. Feeling safer online includes feeling more confident in their ability to protect themselves, recognize risks (e.g., scams, surveillance, harassment), and respond to threats if they occur. For the denominator, grantees will report the total # of individuals who received cybersecurity support through the grant and who the grantee followed up with. For the numerator, grantees will report the total # individuals who reported during follow-up that they feel safer online after receiving support. The Fluxx reporting system will use these two numbers to calculate the resulting percentage. While grantees are encouraged to follow up with as many users as is feasible, response rates are unlikely to be 100%, and follow-up may be conducted with a sample. Potential data sources include grantee follow-up surveys, calls, or interviews with the users they support.
Number of cybersecurity support providers reporting positive changes in incident trends among supported high-risk users	Cybersecurity support providers are defined as grantees who offer training, services, or other types of support to high-risk users designed to increase these users' safety and security. Grantees report whether they have directly observed or received reports of changes in how the high-risk users they support are experiencing or responding to cybersecurity incidents. Positive changes in incident trends may be changes directly observed by grantees that indicate improvements in the security and safety of the users they support, such as less frequent requests for support or changes in the demographics of those requesting support. Changes may also be the grantee receiving from the users they support reports of quicker response, reduced impact, reduced downtime, fewer lost communications or files, faster restoration of access or functionality, or less interference with routine professional activities.

	Grantees should develop a clear internal definition of what 'positive change' means in their context and organize data collection and analysis accordingly.
Qualitative indicator: Examples of individuals or organizations more effectively responding to technology-facilitated gender-based violence after receiving cybersecurity support from grantees	This indicator captures real examples showing how individuals or organizations are better able to prevent, respond to, or recover from online gender-based violence after receiving support from grantees. As with all data collected, grantees should adhere to principles of confidentiality, informed consent, and Do No Harm when collecting examples for this indicator.
Number of high-risk users provided with cybersecurity support, disaggregated by Gender (Male, Female, Other, Unknown, Total) Type of support (Training, Incident response engagement, Other) User profile (Journalists, Human	This counts how many individuals at higher risk of experiencing cybersecurity incidents (e.g., journalists, activists, women leaders, civil society actors, and others, including those targeted by digital transnational repression) received direct cybersecurity support from grantees. Support includes training (defined as a formal session with a clear learning objective that is skills or competency-oriented), incident response engagement (such as operating a hotline), or any other relevant interventions. Grantees are encouraged to count the number of unique individuals who received support during the reporting period when feasible; if the same person receives support multiple times, ideally, they are counted only once. Potential data sources include grantee records, databases, or training sign-in sheets.

Rights Defenders, Civil Society Organizations, Other)	
Number of cybersecurity support sessions conducted by grantees, disaggregated by, Type of support [training, incident response engagement, other] User country (self-identified) [including 'not specified']	This counts the volume of cybersecurity support activities conducted by grantees during the reporting period. 'Sessions' are defined within the context of each grantee's activities and may include training sessions, incident phone calls/chats/tickets, etc. Potential data sources include grantee records, databases, or training sign-in sheets.
Number of cybersecurity guidance materials, tools, or resources delivered to high-risk users with Fund support	This counts the materials or tools the grantees provide during the reporting period to help users prevent, respond to, or recover from cyber threats or incidents. Examples include guides, toolkits, checklists, digital tools, and secure communication tools. Each material or tool is counted once, regardless of the number of users who receive it.

For grants focusing on advancing a safer Internet for vulnerable groups and high-risk communities, including civil society and journalists (Report Only on Applicable Indicators)	
Indicator	**Guidance**
Number of cybersecurity-related policy discussions or official government statements that incorporate recommendations or evidence from grantees or the communities they support	Number of policy discussions or statements during the reporting period that use, discuss, or otherwise reflect data, analysis/research findings, guidelines, or recommendations produced by grantees (or the communities grantees work with) as part of this grant. 'Policy discussions' are consultations, workshops, roundtables, parliamentary sessions, or other discussions in which policymakers are involved. 'Official government statements' are spoken public declarations or written policies, strategies, press releases, or other documents related to cybersecurity policy. Potential data sources for this indicator include follow-up calls or interviews with stakeholders – or reviews of government websites, policy documents, and credible media sources – after dissemination of evidence/ recommendations.
Number of ecosystem-level changes in platform practices or standards resulting from ecosystem actors' coordinated safety and security efforts	Ecosystem-level changes are system-level changes rather than changes implemented by a single organization, company, or individual. Changes in 'platform practices or standards' include the adoption of new or strengthened safety and security practices/protocols, platform policies, or technical standards that reflect a wider ecosystem response to issues surfaced, evidenced, or advanced through coordinated efforts that include grantees. "Ecosystem actors" include grantees and other relevant stakeholders such as civil society organizations, technical

	community actors, platforms, policymakers, service providers, and private sector actors. This is a contribution, not attribution, indicator. Grantees are not expected to prove they alone caused the change. Instead, grantees should show a reasonable link between their efforts and the changes that occurred in the cybersecurity ecosystem during the reporting period.
Number of new or improved coordinated practices or collaborative efforts regularly implemented by multiple ecosystem actors as part of safety and security initiatives	Grantees report the number of coordinated practices or collaborative efforts that begin taking place ***after*** their implementation of safety/security activities supported by the Fund. This is meant to capture any strengthening in collaborative networks or global partnerships that grantees reasonably believe their activities helped contribute to. 'Coordinated practices or collaborative efforts' include cross-organizational arrangements such as shared threat-information exchange, coordinated alerting or notification procedures, joint incident triage or escalation workflows, coordinated vulnerability disclosure processes, referral pathways for support, shared playbooks or operating procedures, and other recurring mechanisms that help multiple actors act in a more aligned and timely way. 'New or improved' means the practice was created or strengthened during the project through grantee activities.
Number of activities organized by grantees that bring together ecosystem actors to promote knowledge sharing and coordination related	Grantees report the number of activities they have organized during the reporting period with Fund support that bring together different actors in the cybersecurity ecosystem (e.g., CSOs, CSIRTs, platforms, networks) to share knowledge, discuss challenges, and coordinate actions Activities include workshops, seminars, gatherings, and joint planning sessions.

to advancing a safer Internet for all	
Qualitative indicator: Examples of safer Internet activities organized by grantees that include technology-facilitated gender-based violence as a key topic and/or incorporate perspectives from women-led organizations	Grantees report and briefly describe any activities they have supported during the reporting period that address gender-related risks (e.g., online harassment, abuse) or include perspectives from women-led organizations. Potential data sources for this indicator include agenda, notes, or other relevant materials from the grantee-organized activity.
Number of written products outlining recommendations and guidelines for cybersecurity policies or standards that are developed and publicly disseminated by grantees	This counts reports, guidelines, or policy documents developed by grantees during the reporting period that aim to improve cybersecurity policies, standards, or practices and are shared publicly or with relevant stakeholders 'Publicly disseminated' means the product is shared beyond the organization (e.g., via a website, with policymakers or stakeholders, or through events or networks). Sharing on social media alone does not count as dissemination unless accompanied by another form of dissemination. A higher number of products is not necessarily better; relevance and quality of products are equally important.
Qualitative indicator: Examples of gender-sensitive	This indicator captures real examples of how grantees include gender considerations (e.g., risks faced by women, inclusive design, protection

recommendations and guidelines included in grantee-developed cybersecurity policy products	measures) in their policy recommendations or guidelines during the reporting period. Potential data sources for this indicator include excerpts from grantee reports/ products showing gender-sensitive recommendations.