



USAID
FROM THE AMERICAN PEOPLE

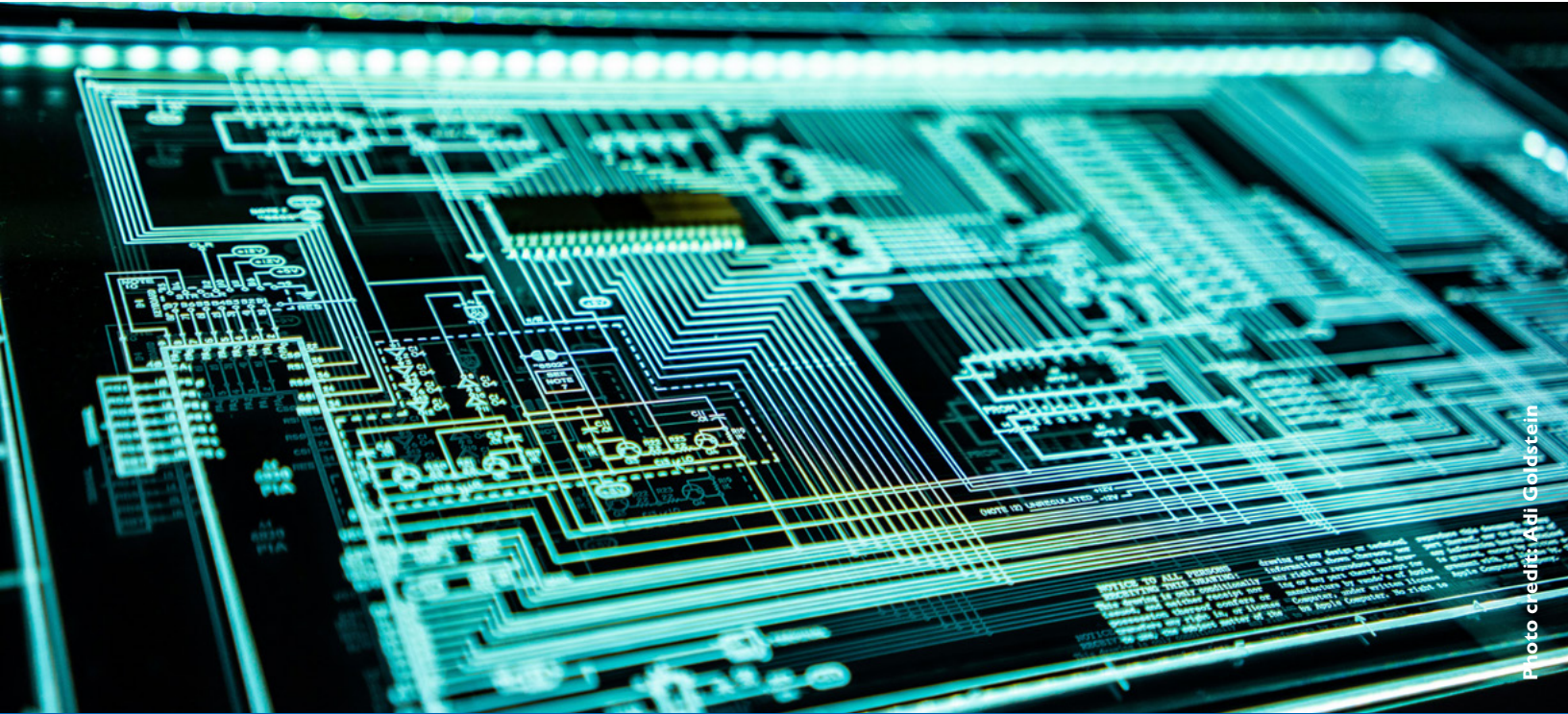


Photo credit: Avi Goldstein

DIGITAL ECOSYSTEM COUNTRY ASSESSMENT (DECA) TOOLKIT

Cybersecurity Addendum

APRIL 2024



ACKNOWLEDGEMENTS

The Cybersecurity Addendum to the Digital Ecosystem Country Assessment (DECA) Toolkit was produced by the Cybersecurity Team within USAID's Technology Division in the Innovation, Technology, and Research Hub of the Bureau for Inclusive Growth, Partnerships, and Innovation (IPI/ITR/T) in collaboration with the DAI Digital Frontiers Project. The Addendum was authored by Timothy Dubel with notable contributions from Rachel Chang, Susannah Horton, and Priya Sethi. Copy edits were provided by Ann J. Procter and report design and graphics were provided by Stefan Peterson. The authors extend their appreciation to all USAID staff who participated in internal discussions and review, especially the dedicated guidance and review provided by Stan Byers, Siobhan Green, Craig Jolley, Hank Nelson, and Maurice Kent.

The authors also extend sincere thanks to all external stakeholders who participated in content consultations including from the International Telecommunication Union (ITU), the MITRE Corporation, and the e-Governance Academy National Cybersecurity Index (NCSI).

The authors accept responsibility for any errors or inaccuracies in this report.

This publication was produced by the Digital Frontiers Project under Cooperative Agreement AID-OAA-17-00033 at the request of the United States Agency for International Development (USAID). This report is made possible by the generous support of USAID under the Digital Strategy. The contents are the responsibility of the author or authors and do not necessarily reflect the views of USAID or the United States Government.

TABLE OF CONTENTS

Acknowledgements	2
Acronyms	4
Section 1: Context for a DECA Cybersecurity Addendum	5
1.1 Cybersecurity as a Digital Development Priority	6
1.2. Cybersecurity is a Complex Topic	7
Section 2: Cybersecurity in the DECA Process	10
2.1 Phase 1: Desk Research and Planning	11
2.2 Phase 2: Interviews	13
2.3 Phase 3: Analysis and Report Writing	14
Section 3: Tools and Resources	24
3.1. Having a Cybersecurity Conversation	25
3.2. Additional Questions and the DECA Research Checklist	26
Appendix A: Key Supplemental Questions by DECA Pillar	28
Appendix B: Cybersecurity Links and Resources	31
Appendix C: Updates to Glossary (Abbreviations and Definitions)	34

LIST OF BOXES, TABLES, AND FIGURES

Boxes

Box 1. Global Cybersecurity Reports and Trends:	6
Box 2. Data Governance Explained	6
Box 3. The important relationship between data protection, data privacy, and cybersecurity	14

Tables

Table 1. Four cybersecurity focus areas and sub-topics for DECA research	7
Table 2. Cybersecurity measures by stakeholder level	9
Table 3. DECA Team roles and opportunities to focus on cybersecurity	11
Table 4. Key points to be communicated by the DECA Research Team to interviewees about cybersecurity	13
Table 5. Cybersecurity indices and frameworks	16
Table 6. Elements of a DECA Cybersecurity Summary	19
Table 7. Cybersecurity links and resources	32
Table 8. Glossary update	35

Figures

Figure 1. Information on specific strategic areas and sub-topics for DECA Research Teams	17
Figure 2. Example of a graphic cyber summary for Country X	21


ACRONYMS

CaaS	Cyber crime as a Service
CBM	Confidence Building Measure
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency
CISSP	Certified Information Systems Security Professional
CMM	Cybersecurity Capacity Maturity Model
CoE	Cyber Center of Excellence
CSDI	MITRE Cyber Strategy Development and Implementation Framework
CSF	NIST Cybersecurity Framework
CSIRT	Computer Security Incident Response Team
CSO	Civil society organization
CTA	Cyber Threat Alliance
DPG	Digital Public Goods
DPI	Digital Public Infrastructure
eGA	e-Governance Academy
ENISA	European Union Agency for Cybersecurity
FIRST	(Global) Forum of Incident Response and Security Teams
GCA	Global Cyber Alliance
GCI	Global Cybersecurity Index
GFCE	Global Forum for Cyber Expertise
ISAC	Information Sharing and Analysis Center
ISACA	Information Systems Audit and Control Association
KI	Key informant
NCAF	ENISA National Capabilities Assessment Framework
NCCOE	National Cybersecurity Center of Excellence
NCSC	National Cyber Security Centre (UK)
NCSI	National Cyber Security Index
NGO	Non-governmental Organization
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
OES	Operators of Essential Services
SME	Small and Medium-sized Enterprises
SOC	Security Operations Center
TLP	Traffic Light Protocol
TTX	Table Top Exercises
V-DEM	Varieties of Democracy

SECTION 1:

Context for a DECA Cybersecurity Addendum





Cybersecurity has quickly emerged as a priority for the international development sector. The [USAID Digital Strategy](#) identifies cybersecurity as a cross-cutting topic, noting that development programs must make every effort to understand risks and design programs to strengthen cybersecurity and build resilience. Public institutions, private sector companies, and civil society organizations are incorporating digital technologies into all aspects of life, which leads to an ever expanding data environment. Positive benefits such as improved connectivity and service delivery are abundant, but the use of digital technologies without adequate cybersecurity leaves critical infrastructure and public and private data vulnerable to threats. A deeper understanding and thorough review of cybersecurity is an essential part of a Digital Ecosystem Country Assessment (DECA).

This DECA Toolkit Addendum provides DECA Research Teams with supplemental guidance and resources to assess cybersecurity in a more cross-cutting manner, to explore specific cybersecurity issues in greater depth, and to develop detailed and actionable recommendations. Most DECA researchers are not cybersecurity specialists. This resource aims to increase researchers' familiarity with a range of cybersecurity topics and promote learning and information exchange. The addendum builds on other key documents including USAID's Digital Strategy, the [Cybersecurity Primer](#), [Cybersecurity Briefers](#), [DECA Toolkit](#), and [DECA Research Checklist](#).

1.1 CYBERSECURITY AS A DIGITAL DEVELOPMENT PRIORITY

Digital technologies are an ever present aspect of modern life including in international development programs. This invites both opportunities and risks and an urgent need for more robust cybersecurity systems and capabilities. Critical infrastructure is increasingly vulnerable to cyber attacks, which presents significant threats to public safety and essential economic functions. Technology depends on data ranging from publicly available information such as geospatial data to sensitive private data such as individual health records. Data environments

are unsecured in many countries, which presents countless risks to the economy, national security, and the safety of individual citizens. Unsecured data offers malicious actors an opportunity to exploit digital development programs.

BOX 1. GLOBAL CYBERSECURITY REPORTS AND TRENDS:

[Digital Defense Report 2023](#): Comprehensive annual report on the state of cybersecurity by Microsoft.

[Cyber Outlook for 2023](#): Overall trends, risk areas, and geopolitical issues from World Economic Forum

[State of Humanitarian and Development Cybersecurity Report \(2023\)](#): Prepared by NetHope, covers challenges and mitigation efforts in the development sector.

BOX 2. DATA GOVERNANCE EXPLAINED

[Data governance](#) is a significant component of cybersecurity and defines what data is captured, why, how it is meant to be used (or not used), and by whom. Strong data governance approaches coupled with cybersecurity legislation build trust among users and digital technologies by creating protocols for data privacy and protection. Data protection cannot be solely addressed through cybersecurity measures. Policies, procedures, institutions, and actors designated to protect sensitive data must be put in place to increase the capacity of stakeholders to prevent and respond to cyber attacks or data breaches that may have detrimental societal and economic consequences if not secured. This is especially true when data governance pertains to government functions, public service delivery, and critical infrastructure sectors.

Despite significant efforts by public, private, and civil society sectors around the world to detect and prevent incidents, the pace and scale of cybersecurity attacks continues to increase as threat actors seek to exploit vulnerabilities for a variety of economic and political reasons. Trends such as a rapidly growing Cyber crime-as-a-Service (CaaS) market and increasing use of artificial intelligence (AI) offer these threat actors ever more powerful and sophisticated tools to expand their attacks. Individuals also face a growing number of cyber threats. These range from phishing and cyber crime to digital repression, surveillance, and access to sensitive personal data for legal profiling. These global trends underscore that while detection and prevention are key, it is no longer a question of *if* an attack will happen but *when*.

DECA Research Teams should take this into consideration and include an assessment of preparedness and response as a foundational aspect of cyber resilience or systemic capacity involving all stakeholders in mitigation and recovery. USAID invests in building [cyber resilience](#) at a global and local level. DECA offers an opportunity to assess the foundational elements of cybersecurity in a country's digital ecosystem. As a cross-cutting development area, cyber resilience must include critical infrastructure, public sector services, humanitarian response, civil society, democratic rights and governance, and other components of social and economic development. A foundation for cyber resilience includes many aspects such as facilitating trust between public, private, and civil society stakeholders in the digital ecosystem. Investments and capacity-building efforts must be localized to ensure that they are sustainable by working with local actors and tailoring cybersecurity solutions to specific contexts. The need for and recognition of cybersecurity as a critical topic in digital development is growing, signified by the release of the November 2023 [Accra Call for Cyber Resilient Development](#). Endorsed by the U.S. government and more than 50 other countries, private sector companies, and large implementing organizations, the Accra Call emphasizes the importance of integrating cyber capacity-building into national and international development agendas.

1.2. CYBERSECURITY IS A COMPLEX TOPIC

Cybersecurity is a cross-cutting topic and DECA Research Teams are tasked with assessing aspects of cybersecurity relevant to each pillar in the [Digital Ecosystem Framework](#). Given this broad scope, researching cybersecurity in the DECA is complex and encompasses multiple subtopics from cyber hygiene to cybercrime. This addendum offers four primary focus areas to help DECA Research Teams frame cybersecurity in each DECA pillar, streamlining research and analysis. These four focus areas can guide the DECA Research Team's use of the [Research Checklist](#) and formulation of cybersecurity recommendations.

TABLE 1: Four cybersecurity focus areas and sub-topics for DECA research

Preparedness and Response	Multi-Stakeholder Engagement	Workforce Development	International Engagement
<ul style="list-style-type: none"> National strategy Incident response plans and capacity Threat intelligence/situational awareness Exercises and drills 	<ul style="list-style-type: none"> Cybersecurity governance Threat analysis and information-sharing Public private partnerships 	<ul style="list-style-type: none"> Education system capacity Cyber professional certifications Non-technical workforce Workforce diversity 	<ul style="list-style-type: none"> International agreements and standards Participation in international organizations, events, exercises

Preparedness and Response: The National Institute of Standards and Technology Cybersecurity Framework ([NIST CSF](#)) includes five core functions: identify, protect, detect, respond, and recover. Many assessments focus more on the first three functions, but it is important to recognize that cyber resilience requires a capacity to respond and recover from an incident. This systemic preparedness must be based on a clear roadmap, such as a National Cybersecurity Strategy or a National Incident Response Plan. A national plan can require that all government ministries or departments as well as key sectors have their own response plans in place. Tabletop exercises (TTX) or cyber drills involving many stakeholders build national level capacity to respond to cyber incidents. National incident response plans may be mandated in a cybersecurity strategy or legislation. Effective national response is ideally led by an entity such as a national Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) with clear authority established in law and sufficient capacity in terms of staff and resources. During desk research, the DECA Research Team should determine whether incident response plans (national or sectoral), strategies, or legislation exist and then explore implementation status with key stakeholders as part of the interview phase.

Multi-Stakeholder Engagement: Effective cyber resilience requires all stakeholders to be engaged in the development and implementation of laws, regulations, and policies including data protection legislation. A CERT or CSIRT serves as a central coordination point and source of information for government, private sector, and civil society stakeholders to identify potential cyber threats and respond quickly to incidents. Information-sharing across sectors is vital to maximize the benefits of a sectoral CERT or Information Sharing and Analysis Center (ISAC). Information-sharing methods vary, but typically include a website, incident reporting mechanism, and push notifications for alerts and response guidance. Understanding the level of multi-stakeholder engagement in a country's cybersecurity efforts allows DECA Research Teams to identify gaps, priorities, and opportunities for development programs. DECA research should verify the existence, utilization, and trust in various communication methods through desk research and stakeholder interviews.

Workforce Development: The cybersecurity workforce gap is estimated at 3.4 million people globally.¹ Many assessments view the cybersecurity workforce primarily in terms of technical talent such as obtaining a Certified Information Systems Security Professional (CISSP) certification or higher education degree. However, the complexity of cybersecurity requires a diverse workforce. The [NIST National Initiative for Cybersecurity Education \(NICE\) website](#) is a valuable resource for understanding more about cybersecurity roles and competencies and preparing for discussions with stakeholders regarding cybersecurity human capacity. Public-private partnerships can fill skill gaps, building short and long-term capacity. DECA Research Teams should consider cybersecurity workforce development beyond building technical talent and aim to understand additional workforce dynamics such as career transition programs for declining industries or veterans, digital upskilling for small businesses, and training on cyber skills, cyber diplomacy, and strategy for public officials. This approach will help DECA Research Teams propose recommendations that highlight the diversity needed to build and maintain cyber resilience.

International Engagement: A country may make significant investments at a national level, but cross-border cybersecurity risks are inherent. A cyber attack on a country's critical infrastructure may affect anything from disruption of regional transportation or financial transactions to a widespread environmental crisis. Improved cybersecurity at the country level can boost local development and international security. These dual objectives are stated in many national cybersecurity strategies and cyber diplomacy efforts, including the U.S. [Cybersecurity and Infrastructure Security Agency \(CISA\)](#) global program. Adoption of international standards ranging from data

1 ("(ISC)2 Cybersecurity Workforce Study," 2022, <https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf>).

protection to industry operational standards is a key component of international engagement. It is essential for DECA Research Teams to understand if and how a country is involved in regional and global efforts to prepare for and withstand cross-border cybersecurity incidents.

DECA researchers may encounter the [concepts](#) of cyberterrorism and cyber war (or cyber warfare). Although these concepts will not be applicable in all contexts, it is important to know that they may arise and are relevant to DECA cybersecurity research. Cyber terrorism refers to the use of technology to cause fear, panic, and disruption among the general public. Cyber war is the use of technology to conduct military operations. Addressing and mitigating these threats is an essential part of a country's threat assessment and intelligence capabilities as well as its national defense capacity.

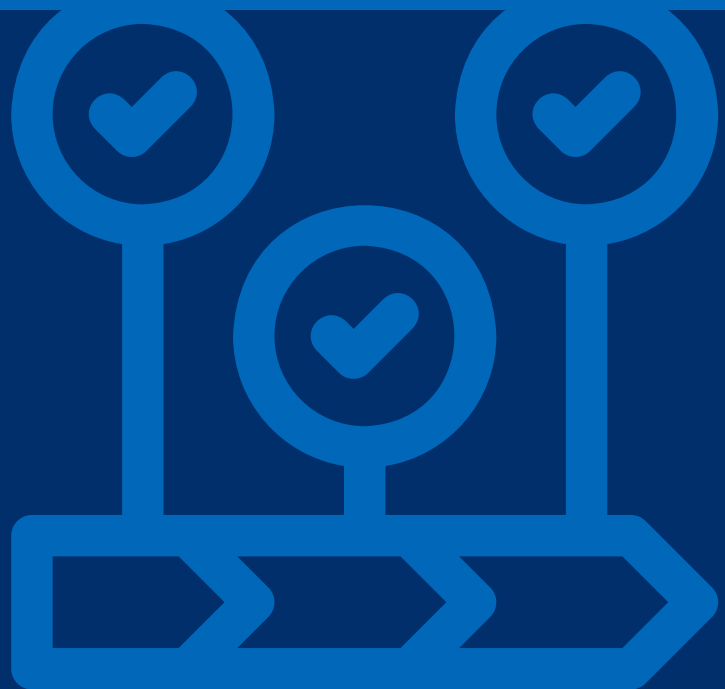
It is important to understand which cybersecurity measures are relevant at different stakeholder levels, from individual to international. The table below provides an overview.

TABLE 2: Cybersecurity measures by stakeholder level

Level	Cybersecurity Measures
Transnational (International)	<ul style="list-style-type: none"> • Threat intelligence and data-sharing • Regional cybersecurity capacity mechanisms such as cyber drills or incident response exercises • International standards
National Level	<ul style="list-style-type: none"> • Cybersecurity strategy, legislation, and policy • National cybersecurity institutions and response mechanisms • National response plan and exercises • Threat intelligence and analysis • Public Private Partnerships • Workforce development
Industry or Sector	<ul style="list-style-type: none"> • Critical infrastructure security • Supply chain security • Sector/industry response mechanisms • Follows international standards and best practices • Workforce development
Organizations	<ul style="list-style-type: none"> • Cybersecurity policies and procedures • Secure technologies and tools • Access to secure infrastructure, including internet infrastructure • Cyber capacity of civil society and non-profit organizations
Individual	<ul style="list-style-type: none"> • Cybersecurity awareness programs • Cyber hygiene and digital skills training • Cybersecurity training and professional certifications

SECTION 2:

Cybersecurity in the DECA Process



The DECA process offers numerous opportunities to focus on cybersecurity. This section provides suggestions and guidance for addressing cybersecurity in each DECA phase. From the outset, specific opportunities for DECA team roles to focus on cybersecurity and cyber resilience are detailed in the table below. It may also be helpful to consult with the [Cybersecurity team](#) at USAID as early as possible. The team can add important global context and help shape additional research and connections to support findings and recommendations.

TABLE 3: DECA Team roles and opportunities to focus on cybersecurity

Mission DECA Lead	DECA Research Team
<ul style="list-style-type: none"> • Engage U.S. government interagency contacts (Regional Security Officer, Embassy Cyber Coordinator, Political/Economic Section). • Consult with the USAID Cybersecurity team and Mission Digital Development Advisor where appropriate. • Ensure discussion of cybersecurity and cyber resilience in the kickoff meeting. • Provide perspective on how the Country Development Cooperation Strategy relates to cybersecurity. • Brief the team on sensitivities regarding DECA cross-cutting themes of inclusion, emerging technologies, and geopolitical positioning. • Assist research team in finding and connecting with individuals who have a cybersecurity perspective (such as CISOs at large companies). 	<ul style="list-style-type: none"> • Include key cybersecurity points in milestone presentations: broader ecosystem questions in the intro meeting; key findings in the post-interview; and recommendations in the final briefing). • Understand local cybersecurity governance, institutional structures, and political economy • Conduct intentional cross-pillar discussion to determine if a cross-cutting cyber summary or pillar summaries are more appropriate. • Ensure additional focus within pillars: <ul style="list-style-type: none"> » Pillar 1 - Review critical infrastructure protection and operators of essential services » Pillar 2 - Review governance and multi-stakeholder engagement for cybersecurity » Pillar 3 - Review private sector partnerships and cyber workforce development.

2.1 PHASE 1: DESK RESEARCH AND PLANNING

Understanding the stage of cybersecurity development in a country or region provides a valuable frame of reference for deeper DECA research. This begins early in the Desk Research and Planning phase of the DECA and will include a review of existing resources (Appendix B), in particular the Global Cybersecurity Index (GCI) and the National Cyber Security Index (NCSI) as well as any available cyber maturity assessments such as the Cybersecurity Maturity Model for Nations (CMM). Section 2.3 below on Phase 3 Analysis and Writing provides further guidance on utilizing these important resources. Another key resource for DECA Research Teams is the [Research Checklist](#) and cybersecurity-specific questions in Appendix A.

DESK RESEARCH

Check for previous assessments. In some cases, the U.S. Government (USG) has engaged research organizations, federal laboratories, implementing partners, or universities to conduct a country or sector assessment, which may be available to the DECA Research Team through the U.S. Embassy interagency team or the cyber working group. The Mission DECA Team Lead and the USAID Cybersecurity Team can help make the necessary connections.

IDENTIFY KEY INFORMANTS (KIs)

Private sector leaders. The Mission Economic Growth team or Economic Section at the Embassy may be helpful in identifying contacts. A simple search on “top industries in COUNTRY/REGION” is a good starting point for possible stakeholders. DECA Teams can consider a mix of international companies and large local firms such as local subsidiaries of international technology, logistics, or manufacturing companies. Global consulting firms are also likely to be valuable sources of information. Speaking with a Chief Information Security Officer (CISO) or equivalent at those entities can be very informative. Larger local companies may also have a CISO or similar role.

Business and professional groups. Chambers of commerce, both international (U.S. or UK chambers) and local, can be a good starting point. Many chambers of commerce have technology or innovation committees with an interest or perspective on cybersecurity. Professional organizations such as the Information Systems Audit and Control Association (ISACA) may have a local chapter, which can be found by searching the [ISACA site](#).

Media and Civil Society. These organizations are often knowledgeable about and have direct experience with cyber resilience and digital surveillance. Media and civil society organizations provide a valuable perspective on the local cybersecurity context, including the legal and regulatory environment, key threat actors, and ongoing or emerging threats. Smaller local non-governmental organizations (NGOs) and USAID grantees can likely speak to local capacity challenges and opportunities. Larger international NGOs and USAID implementing partners can offer insights into national or regional threats as well as into local capacity. USAID Mission Democracy, Human Rights and Governance teams are a good resource for further guidance and interviewee recommendations or referrals.

Academic and cybersecurity certification programs. Universities in many countries either have or are beginning to develop cybersecurity programs. DECA researchers can identify experts in or through the computer science, engineering, business, or other departments. In some contexts, private sector cybersecurity education and certification programs are active, including with international certification programs such as the [Cisco Networking Academy](#). Civil society organizations (CSOs) and NGOs (national and international) may also have cybersecurity training or certificate programs that are relevant for the DECA Research Team. The [TechSoup Global Network](#) is a good source for local NGOs that provide digital capacity building.

2.2 PHASE 2: INTERVIEWS

The Research and Planning phase should produce a key informant (KI) list that includes a diverse range of cybersecurity perspectives, from expert to layperson. Adequately preparing for and conducting those interviews is essential. A basic understanding of the local political economy for cybersecurity is important before carrying out interviews. Researchers should also be aware of potential negative perceptions of a USG-funded activity that may cover sensitive topics such as cybersecurity and be prepared to inform KIs that the objective of the DECA is to better understand context and key issues rather than specific vulnerabilities. It is imperative that researchers follow the interview guidance provided in the [DECA Toolkit](#) (sections 3.6 and 3.7) and where needed explain methods to protect information and the identity of KIs.

It is important to allocate sufficient time to discuss cybersecurity. For some interviews this will mean explicitly including cybersecurity as a topic on the agenda. In other cases, it will mean extending the interview time or requesting a separate meeting focused on cybersecurity.

Interview questions related to cybersecurity can be sent in advance to give the interviewee(s) time to prepare when appropriate. For those less familiar with cybersecurity, a brief reminder that it is a broader topic involving people, process, and technology can set the tone for a more open and constructive dialogue. This is a common paradigm for understanding cybersecurity readiness. Cybersecurity is not only about the hardware or software involved in detecting and responding to cyber threats and risks, it also involves the policies and procedures to manage cyber responses as well as the skills and awareness of the people following (or not following) these processes. Cybersecurity is a sensitive topic. It is important to convey the key points in the table below based on the individual's knowledge of cybersecurity.

TABLE 4: Key points to be communicated by the DECA Research Team to interviewees about cybersecurity

Interviewee	Expert, Leader, Senior Official	Layperson, Non-Technical Program Manager
Key Points	<ul style="list-style-type: none"> • Cybersecurity affects every organization and individual in today's world. • The DECA is not an audit or formal cybersecurity risk assessment. • The focus is less about technical matters and more about process and people. • The objective is to understand the context for cybersecurity and its impact on your organization and its work. 	<ul style="list-style-type: none"> • Everyone has a valuable perspective on cybersecurity. • This discussion is not about reporting an incident or disclosing a vulnerability. • This is not a technical discussion. It is focused more broadly on people and processes related to cybersecurity. • Achieving cybersecurity readiness is an ongoing process.

To better prepare for interviews, see the Cybersecurity Conversation Guide in Section 3 and Key Supplemental Questions in Appendix A. The [DECA Research Checklist](#) also has useful guidance, including an “ideal state” description and questions to be covered.

2.3 PHASE 3: ANALYSIS AND REPORT WRITING

Several primary resources such as global indices and maturity assessments provide additional information and analysis about cybersecurity in a given country's context. These resources are explained in more detail below. The following section proposes the development of a Cyber Summary, a standalone section that synthesizes cybersecurity findings across the three DECA pillars.

2.3.1 A FRAMEWORK FOR CYBERSECURITY INDICES AND FRAMEWORKS

Several well-known cybersecurity frameworks and indices exist, each with a different methodology, perspective, and presentation of data. Analyzing the available information can be overwhelming and understanding how these resources relate to one another is important. Complementarity and overlap across the resources and inconsistencies can usually be attributed to differences in methodology or timing. The primary indices include most countries, although assessments and maturity models are not available for every country.

BOX 3. THE IMPORTANT RELATIONSHIP BETWEEN DATA PROTECTION, DATA PRIVACY, AND CYBERSECURITY

It may be helpful for DECA Research Team members to review key concepts presented in these resources, including [data protection](#), [data privacy](#), and cybersecurity.

Data protection is the practice of safeguarding data from unauthorized access, use, disclosure, disruption, modification, or destruction. It is a broad term that encompasses data privacy.

Data privacy is the practice of protecting personal information from access by unauthorized parties, a subset of data protection that focuses on the confidentiality of personal data.

Cybersecurity refers to protecting computer systems and networks from unauthorized access, theft, damage, or disruption. It is a broad term that encompasses both data protection and data privacy.

Additional resources on data governance (see Box 2 above): the [Global Data Barometer](#), the [Digital Trade and Data Governance Hub](#), and the [United Nations Conference on Trade and Development's](#) page on worldwide data governance legislation.

GLOBAL INDICES: GLOBAL CYBERSECURITY INDEX AND NATIONAL CYBER SECURITY INDEX

The **Global Cybersecurity Index (GCI)** has five pillars supported by 20 indicators, is updated globally for over 190 countries every two to three years and consists of a survey completed by country contacts and verified by the UN International Telecommunication Union (ITU).



The GCI is a good starting point for better understanding strengths and weaknesses across its five pillars (Legal, Technical, Organizational, Capacity Development, and Cooperation), comparative regional ranking, and global standing. The period between updates can result in out-of-date information, but the country profiles provide useful context for further research. The [GCI website](#) also includes valuable resources such as the database of National Cyber Strategies. A discussion with the ITU regional representative could be considered.

The **National Cyber Security Index (NCSI)** covers 175 countries and is refreshed on an ongoing basis as local contacts or e-Governance Academy (eGA) team members update the database with information and supporting evidence. Data is typically more current. Country ranking is subject to the availability of openly published data such as national laws and policies, unlike with GCI. As a result, countries that keep cybersecurity mechanisms and procedures confidential and less available to the public may be ranked lower, which leads to discrepancies in country ranking across multiple indices and makes it challenging to accurately assess national cyber capacity from indices alone.



The NCSI tool is particularly valuable for its ability to drill down on a capacity area to find supporting evidence including documentation and websites. In 2023, eGA launched the new [NCSI methodology 3.0](#) with three pillars— Strategic, Preventive, Responsive—supported by 12 capacity areas. As of January 2024, eGA has used this new methodology to assess 24 countries, with more coming soon. The NCSI should be considered a valuable resource for current data and supporting evidence.

COUNTRY CYBERSECURITY ASSESSMENTS AND MATURITY MODELS

Country cybersecurity assessments are typically more comprehensive and are not available for every country. The Cybersecurity Capacity Maturity Model ([CMM](#)) is the most widely available and may include assessments over time for a [country or region](#), offering a perspective on progress or on persistent issues. The [model](#) has five dimensions (Policy and Strategy, Culture and Society, Knowledge and Capabilities, Legal and Regulatory Frameworks, and Standards and Technologies) supported by 23 factors, providing a broad view of a country's cybersecurity capacity.

Review of the model is highly recommended for a foundational understanding of cybersecurity issues at a national level, and for deeper dives into a wide range of specific subtopics. The model includes five levels of maturity, which can be useful input for developing a cyber summary, as proposed in the next section.

The USG may engage third parties such as MITRE to conduct cybersecurity assessments to share with host governments as part of assistance and coordination programs. These assessments may be available from the Mission DECA Team Lead through U.S. Embassy contacts. The MITRE Cyber Strategy Development and Implementation Framework ([CSDI](#)) includes three categories (Enabling, Operational, and Governance) and eight capacity areas (see Box 4). The DECA Research Team can review the CSDI framework during the research and planning phase to better understand and identify issues for further research. If possible to set up, a briefing with the MITRE team on a given country can be a valuable source of information.

The World Bank also carries out cybersecurity assessments and plans to do so through the [Cybersecurity Multi-Donor Trust Fund](#).

The table below is a summary of the main indices and frameworks in terms of value for DECA Research Teams. It explains considerations that may result in discrepancies between indices, such as frequency of data collection.

TABLE 5: Cybersecurity indices and frameworks

Index, Model, Framework	Primary Value and Considerations for DECA Teams
Global Cybersecurity Index (GCI)	<ul style="list-style-type: none"> • Well researched summary of global cybersecurity issues and trends • Country profiles include strengths and weaknesses, with scores across five key categories, but they are not provided in narrative form • Key weakness: Conducted every 2-3 years, so data may be outdated
National Cyber Security Index (NCSI)	<ul style="list-style-type: none"> • Serves as an archive for supporting evidence in key categories including links to documents and websites <ul style="list-style-type: none"> » Tip: drill down on sub-categories to find evidence • Provides source of evidence as valuable resource for DECA contacts • Updated on an ongoing basis, so data may be more current • Key weakness: Relies on publicly available data, so might not be accurate for countries with confidential cybersecurity mechanisms
Cybersecurity Capacity Maturity Model (CMM)	<ul style="list-style-type: none"> • In-depth country or region reports covering key capacity areas • Identifies primary entities for including in DECA contact list • Key weakness: Not available for every country and may be outdated
Cyber Strategy Development and Implementation Framework (CSDI)	<ul style="list-style-type: none"> • Detailed capacity assessments often linked to USG capacity-building and partnership programs • Key weakness: Not available for every country and only upon request

The figure below provides a quick reference for strategic areas and sub-topics (indicators, factors) across the global indices and country assessment methodologies described above.² Some indices and assessments have more information about specific strategic areas and sub-topics, which can help guide which resource is the most pertinent for a specific line of inquiry.

Each indice or assessment has key pillars, categories, or dimensions as follows:

- **GCI (ITU):** Legal Measures; Technical; Organizational; Capacity; Cooperation
- **NCSI (eGA):** Strategic; Preventive; Responsive
- **CMM (Oxford):** Policy and Strategy; Culture and Society; Knowledge and Capabilities; Legal and Regulatory Standards and Technologies
- **CSDI (MITRE):** Enabling; Operational; Governance

² "Global Overview of Existing Cyber Capacity Assessment Tools," GFCE Policy and Strategy Working Group, 2021, https://cybilportal.org/wp-content/uploads/2021/08/Global-Overview-of-Assessment-Tools_CLEAN_17Aug.pdf

FIGURE 1: Information on specific strategic areas and sub-topics for DECA Research Teams

	GCI (ITU) <i>updated every 2-3 years</i>	NCSI (eGA) <i>updated regularly</i>	CMM (Oxford) <i>on demand</i>	CSDI (MITRE) <i>on demand</i>
Strategic Area	Indice or Assessment Sub-Topic (indicator, factor, capacity area)			
Legal Frameworks, Policy, Standards	National Cybersecurity Strategy	Policy Development and Coordination	National Cybersecurity Strategy	Civil law, regulations, accountability
	Cyber crime Law - (incl IP protection, Online Safety)	Cyber crime		Cyber crime Prevention and Prosecution
	Cybersecurity Regulation - Data Protection, Privacy and Standards	Personal Data Protection	Legal and regulatory provisions and legislative frameworks	
	Online protection strategy and initiatives			
	National framework for cybersecurity standards		Adherence to standards	Policy and Standards
Cybersecurity Awareness and Capacity	Public cybersecurity awareness campaign		Cybersecurity Mindset (incl media and online platforms)	Public awareness - Culture of Cybersecurity
	Government incentive mechanisms		Cybersecurity awareness and education	
			Users understand online privacy	
	Cybersecurity R&D	Research and Development	Research and Innovation	
	Cybersecurity metrics		Trust and confidence in online services	
	Interagency partnerships		Cooperation frameworks to combat cyber crime	
Preparedness and Response	Responsible Cyber Agency	Threat Analysis and Awareness	Legal and regulatory capabilities and capacity	Risk Management and Resourcing
		Critical Information Infrastructure	Communications and internet infrastructure resilience	Resilient Operations
		Cybersecurity of digital enablers	Software quality	
		Incident Response	Security Controls and Responsible Disclosure	Incident Response
		Crisis Management	Reporting Mechanisms	
Workforce Development and Private Sector	Cybersecurity professional training	Education and Professional Development	Cybersecurity Professional Training	Cybersecurity workforce development
	Cyber education as part of national curriculum			
	National cyber industry		Cybersecurity Marketplace	
	Public-private partnerships with private sector			
International Engagement and National Security	International agreements	Global Contribution		
		Military Cyber Defense		

SELF-ASSESSMENT FRAMEWORKS: NIST CYBER SECURITY FRAMEWORK AND ENISA NATIONAL CYBERSECURITY ASSESSMENT FRAMEWORK



Several frameworks have been developed that allow organizations or nations to self-assess their cybersecurity posture to better identify and manage risks. The DECA Research Team may encounter frameworks such as [C2M2](#), originally developed for energy sector entities, or the [CSIRT Maturity Framework](#) developed by Global Forum for Cyber Expertise (GFCE) based on existing frameworks. These tools can be valuable when assessing capacity of individual organizations but are less applicable for a broader country assessment. In discussions with stakeholders and KIs, researchers should ask if assessments have been carried out and have been shared.

Although the **NIST Cybersecurity Framework (CSF)** is a self-assessment framework originally intended for larger critical infrastructure organizations, an updated CSF 2.0 framework is expected to be released in mid-2024 and will be more applicable to small businesses and CSOs. The CSF includes five core functions and 23 categories.

These five functions are commonly seen as the essential pillars of cybersecurity capacity. DECA Research Teams can use this as a framework for research and discussions with stakeholders about how risks are identified and managed including aspects of governance, data security, incident reporting, and mitigation.

The **European Union Agency for Cybersecurity (ENISA) National Capabilities Assessment Framework (NCAF)** is a self-assessment model developed for EU member countries but applicable in any country context. The framework is based on strategic objectives of EU Member States' national cybersecurity strategies and organized into four clusters: Governance and Standards, Capacity Building and Awareness, Legal and Regulatory, and Cooperation and 17 objectives.

As the framework is built around national strategic objectives, it provides a foundation for discussion with national level public sector leaders. The clusters include objectives such as securing the supply chain, securing digital identity, and public-private partnerships, which are valuable to DECA Research Teams across pillars.

The NIST [NICE Framework](#), which outlines competencies for a diverse range of cybersecurity professional tracks, is useful when researching cybersecurity workforce development.

As DECA Research Teams examine the intersection between democracy, digital rights, and cybersecurity, there are a few useful resources to explore. The [Digital Society Project](#) offers indices and a public dataset covering political environments and social media in 179 countries, and Varieties of Democracy, or [V-DEM](#), includes reports, working papers, and datasets that explore democracy and digital security topics. Key indicators include: government cybersecurity capacity; cybersecurity capacity of political parties; privacy protection by law exists; and privacy protection by law content.

2.3.2 DEVELOPING A CYBERSECURITY SUMMARY

DECA Teams should consider developing a cybersecurity summary to be included in the introduction section of the DECA report to emphasize the cross-cutting nature of cybersecurity. At a minimum, a cybersecurity summary should be incorporated into each pillar section, although this could lead to a fragmented understanding of a broader issue. An overarching cybersecurity summary will draw upon the findings under each pillar and identify the stage of cybersecurity development, notable strengths and challenges, and areas of opportunity. This supports a more holistic and systemic understanding of cybersecurity and ultimately can lead to more robust engagement with stakeholders, including other donors, and result in more targeted and effective development programs. A brief overview of the threat landscape facing a country or region, both from internal and external actors, will add additional context to the summary by identifying potential vulnerable areas. DECA Teams can include both a written and graphic cyber summary. See below for basic examples.

Most cybersecurity frameworks and models include an indicator of maturity (e.g., CMM³ and the NCAF). DECA Research Teams can use the simplified approach below, which details four stages of cybersecurity development.

TABLE 6: Elements of a DECA Cybersecurity Summary

Element	Definition and Resources
Stage of Cybersecurity Development	<p>DECA Research Teams do not need to conduct an extensive maturity assessment. This is a qualitative observation drawn from research findings intended as a frame of reference for detailed pillar information and recommendations. The proposed stages are:</p> <ul style="list-style-type: none"> • Early – Limited steps have been taken to address or improve cybersecurity. There is minimal awareness and prioritization of cybersecurity, resulting in low trust and cooperation among sectors and stakeholders. Key segments of the economy and society remain disproportionately vulnerable to cyber risks. • Maturing – Key legislative and policy elements exist but gaps remain such as lack of enforcement or publicly available documents. Some institutions have been formed but have limited capacity in staff and resources, or face significant challenges with operating independently. Stakeholders do not engage effectively. Risks may be known and some mitigation measures are in place. • Advanced – Legal/regulatory and policy frameworks are largely complete. Stakeholders are engaged and there is a common understanding of strategy and implementation. Capacity gaps exist but are closing through investments and partnerships. Some international engagement may be taking place. • Developed – Most legal, policy, and capacity components exist and multi-stakeholder engagement is functioning. Basic legislation and documentation of national cybersecurity strategy is available for public access. Implementation of policy is prioritized and risks are managed. Response and recovery plans and associated capabilities are in place. International engagement is evident and expanding. <p>Sources include:</p> <ul style="list-style-type: none"> • Oxford CMM Reviews • ITU Global Cybersecurity Index • eGA National Cyber Security Index • MITRE country assessments • Key informant interviews • Research and other third-party assessments

3 Cybersecurity Capacity Maturity Model for Nations (CMM), Global Cybersecurity Capacity Centre, 2021, 8, <https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf>.

Element	Definition and Resources
Strengths and Challenges	<p>This is a high level summary of strengths and weaknesses, drawing from information gathered to evaluate the stage of cybersecurity development. This is not a vulnerability assessment but may call out risks or specific gaps, especially those that can be addressed as part of development programs.</p> <p>Examples of strengths include a well-developed legal framework, or active and capable CERT. Examples of challenges include lack of multi-stakeholder engagement or limited partnerships, or limited awareness among key constituencies (businesses, critical infrastructure (CI) operators, CSOs, etc.) of CERT resources.</p> <p>If possible, a brief description of the threat landscape including key actors, most common tactics, and target organizations or sectors, as well as capacity to understand and respond to threats, will provide valuable context.</p>
Areas of Opportunity	<p>Drawing from both the stage of cybersecurity development and the strengths and challenges assessment, this section should summarize at a high level the ways in which challenges can be addressed, in particular through development programs. These areas of opportunity should tie to specific recommendations where possible. Examples include:</p> <ul style="list-style-type: none"> • Development of key legislation and policies • Improved governance through multi-stakeholder engagement • Recognition of best practices to build awareness and trust • Strategic workforce development through partnerships and investment • Technical capacity-building in key institutions

EXAMPLE OF A WRITTEN CYBERSECURITY SUMMARY:

COUNTRY X has made significant progress in recent years and can be considered at the maturing stage of cybersecurity development. In 2018, the Cybersecurity Strategy was launched and the Cybersecurity Law was passed in 2020. However, the Strategy and related policies have been developed in the absence of multi-stakeholder engagement and funding to build the capacity of key public sector entities, including the national CERT, is insufficient. Civil society also remains vulnerable to cyber incidents due to limited capacity to manage and protect data. Weak cyber hygiene practices among small and medium enterprises introduce supply chain risks. Ransomware attacks against businesses and health services organizations have increased significantly and the government has published reports of several attempted attacks on critical infrastructure in the past year. The national CERT has limited capacity to inform stakeholders of key threats and mitigation measures.

To further advance cyber resilience, development programs could support creation of a national incident response plan including adoption of international standards and mandatory response plans for critical infrastructure operators. Support for expanded capacity to act on threat intelligence through technical assistance to the national CERT should be a priority and increased efforts to build awareness of cybersecurity at the consumer and small business level will further strengthen the digital ecosystem.

FIGURE 2: Example of a graphic cyber summary for Country X

Stage of Cybersecurity Development	Strengths and Weaknesses	Areas of Opportunity
<p>Maturing – with regard to legislation, policies, and institutional capacity (CERT). Institutions in place but limited in capacity due to underfunding and workforce shortages.</p>	<ul style="list-style-type: none"> • Cybersecurity Law and National Cyber Strategy are in place. • Lack of multi-stakeholder awareness and engagement. • CSOs have limited capacity to protect data. • CERT has limited capacity for threat analysis and response. 	<ul style="list-style-type: none"> • Developing a National Incident Response Plan. • International standards for public sector and CI entities. • Increased cybersecurity awareness for consumers and small businesses. • Build CERT capacity to analyze and act on threat intelligence.

DECA Research Teams should avoid drafting summaries with limited insight. Insufficient cyber summaries report information from global index rankings or threat intelligence reports without interpreting it or adding nuanced context. Simply listing a country’s ranking on an index does not provide sufficient information about the cybersecurity dynamics at play in the digital ecosystem. The objective of the DECA Cybersecurity Summary is for DECA Research Teams to develop an original analysis using findings from their desk research and interviews.

2.3.3. DEVELOPING RECOMMENDATIONS

The DECA process has a proven approach to developing recommendations, which has resulted in numerous cybersecurity recommendations including assistance to develop laws and policies, capacity-building in public sector and CSOs, and workforce development. DECA Research Teams can draw upon their research findings, interviews, and analysis to make specific and targeted cybersecurity recommendations aligned with the four focus areas and subtopics provided below.

Preparedness and Response indicates whether national or sector-specific policies, strategies, and plans exist to detect potential cyber risks, mitigate cyber threats, and respond to cyber incidents. It also takes into consideration the capacity for stakeholders to act with designated roles and responsibilities.

- Support establishment or capacity-building of cybersecurity centers of excellence. Depending on a country’s stage of cybersecurity development, it may be recommended that the country establish or build the capacity of a Cyber Center of Excellence (CoE) within a responsible ministry/department or CERT/CSIRT, or a trusted independent entity. The cyber CoE model can be scaled based on resources and can be linked to regional centers. Support for a CoE can also be done in partnership with other USG entities or donors given the specialization and resource needs (including technical procurements and training). In Ukraine, USAID funded support to carry out a TTX while the U.S. State Department provides ongoing support to build the capacity of the National Cyber Security Center. The Moldova DECA also recommended that USAID support development of a CoE. Best practices for cybersecurity centers of excellence, such as the [NIST NCCoE](#), are readily available.

Multi-Stakeholder Engagement includes considerations around cybersecurity governance, innovative partnerships between public and private sector institutions, and opportunities to promote information-sharing on cybersecurity among different sectors.

- **Promote whole-of-government/nation approaches.** DECA recommendations should support the development and strengthening of collaboration and connections across stakeholders. Suggested programming efforts may include technical assistance and awareness-raising for implementation of policy across government entities at the national and local levels; encouraging stakeholder dialogue through convening events or supporting mechanisms such as working groups for cybersecurity knowledge exchange; and development of best practices and models that can be extended across sectors and the government.
- **Encourage public and private sector partnerships.** Private sector companies are responsible for managing telecoms, health care delivery, and other critical services, while government systems contain citizen identification data of the individuals receiving these services. To deliver and protect these essential services, governments, public institutions, businesses, and all stakeholders would benefit from greater coordination. Working together, the public and private sectors can leverage their respective strengths to address threats and reduce vulnerabilities through proactive collaboration to gather, share, and analyze available data. A government may benefit by working with private sector partners to develop a solution that addresses a significant increase in attempted hacks on public networks. DECA recommendations can encourage stakeholders to set mechanisms to facilitate greater communication and collaboration so efforts to secure critical infrastructure systems and sensitive data do not happen in siloes. Additional resources DECA Research Teams can use to build effective partnerships for cybersecurity include: a [paper](#) on promoting cybersecurity through collaboration in Africa, a CSIS [report](#) on public-private collaboration for cybersecurity, and a World Economic Forum [report](#) on partnerships for cybersecurity.

Workforce Development explores the cybersecurity talent pool, often highlighting the skills gap. This issue is multifaceted. Training efforts are not keeping up with rapidly evolving cyber threats, where attacks are becoming even more complex globally. Other factors include local constraints to recruiting and retaining cybersecurity professionals especially in public and civil society sectors. Salary caps for civil servants may limit the ability of the government to attract skilled talent, or upon completion of cybersecurity training individuals may pursue more lucrative opportunities in other countries. The relative strengths of local cybersecurity markets are also inextricably linked with the cybersecurity workforce. A strong or growing cybersecurity private sector is essential for encouraging the workforce to contribute to local preparedness. DECA researchers will need to consider market factors and potentially include recommendations for strengthening local markets through investment, mentorship, and other initiatives.

From IT operators to CSOs and public officials, cybersecurity workforce dynamics present significant challenges for many organizations. This includes every organization where employees interact with digital technologies, as a lack of basic cyber hygiene awareness is often one of the greatest vulnerabilities.

- **Promote cybersecurity literacy and cyber hygiene:** As countries become more cyber mature, key features are seen and referenced in multiple global indices and frameworks such as the presence of cybersecurity education courses in higher universities and schools, or cybersecurity awareness and skills training for professionals. DECA recommendations can focus on increasing opportunities for all individuals to gain access to and participate in ways to learn how to stay safe online, secure their private data, identify potential risks and harms, and build skills in cybersecurity strategy and management. Recommendations should include examples of how cybersecurity awareness and good practices can benefit their specific department, industry, or sector.
- **Understand local constraints and opportunities to build a skilled cybersecurity workforce:** Recommendations for workforce development will vary based on local conditions. In some cases the DECA Research Team may not have sufficient resources to explore these dynamics in depth. In cases

where research and KIs provide a clearer understanding, recommendations may include building capacity in higher education institutions, developing programs to attract and retain cyber professionals in the public sector and civil society, or supporting events like capture-the-flag exercises to provide young professionals with practical experience. In other cases DECA Research Teams may recommend a further assessment to better understand local workforce needs and inform future programming. This assessment might need to be expanded to better understand the local cybersecurity market and how USAID can help businesses grow and attract talent.

- **Make internal USAID recommendations:** Most DECAs include recommendations for USAID Missions, some of which are requirements for contract language specific to cybersecurity. Additional suggestions include encouraging implementing partners (IPs) to share and learn from each other in terms of cybersecurity best practices; working with IPs to establish high level sectoral incident response plans (for example, what a USAID-funded health program would do in the event of a wide scale healthcare data breach); and, ensuring that cybersecurity is a standing agenda item during regular IP meetings. DECA Research Teams should refrain from making recommendations on the cybersecurity of USAID Mission's internal IT systems.

International Engagement highlights the need for countries and regions to collaborate on shared efforts to withstand cross-border cyber incidents, such as through the adoption of best practices and platforms for facilitating knowledge exchange to improve threat detection and incident response. Cybersecurity capacity and resilience are relevant on a local or national scale and are a matter of international security.


- **Link to international indices, country assessments, and regional cybersecurity initiatives.** The GCI and NCSI provide information on international best practices and standards for cybersecurity. There is an opportunity to link DECA recommendations back to areas identified as particular risks or capacity gaps, with improved outcomes on index rankings or scores as a clear objective. Cyber capacity assessments may provide similar opportunities to link country-specific recommendations to specific areas of regional or global need.
- **Encourage participation in international events or exercises:** Participation in national and international cyber drills and exercises allows stakeholders to simulate how they would respond to a cyber incident and deepens their understanding of the need for improving cyber threat detection, mitigation, or response. CISA offers a [TTX Handbook](#). An additional indicator of preparedness is demonstrated by participation in cross-border exercises at a regional or global level, such as those organized by the U.S. (Cyber Flag), EU (Cyber Europe), or NATO (Locked Shields) or Confidence Building Measures (CBM) organized by the ITU, Organization of American States (OAS), Organization for Security and Co-operation in Europe (OSCE), and others. DECA recommendations may also encourage countries and regions to participate in international cybersecurity councils or forums to increase information-sharing and promote international collaboration on shared objectives. Exposure to such networks will generate opportunities for participation in regional exercises and capacity-building efforts such as training.



SECTION 3:

Tools and Resources





This section provides guidance and links to tools and resources that DECA Research Teams may find useful throughout the DECA stages, including supplemental guidance for existing resources such as the DECA Research Checklist.

3.1. HAVING A CYBERSECURITY CONVERSATION

As noted in Section 2, key information interviews for DECAs should include individuals with a deeper understanding of cybersecurity based on close coordination with the USAID Mission and the U.S. Embassy. The DECA Research Team should also connect with individuals who have diverse cybersecurity perspectives in USAID implementing partners, local CSOs and businesses, host government ministries, and other donors. One of the main challenges for any interview is conducting a meaningful conversation without intimidating or alienating the other individual.

Important considerations when discussing cybersecurity with key informant interviewees:

- **Cybersecurity is a sensitive subject. Direct questions about specific vulnerabilities or cyber incidents should be avoided.** Instead inquire if and how cybersecurity is affecting an organization or sector: are threats, risks, and vulnerabilities known? What is the level of preparedness to respond in the event of an incident?
- **Frame discussion in terms of costs and impacts.** These include disruption of service (downtime), costs to defend or restore, loss of sensitive information, or reputational and trust costs.
- **Cyber resilience requires trust and cooperation.** It is helpful to determine if there is perceived trust among stakeholders and to ask for examples of cooperation. Avoid assigning blame but attempt to understand whether there is an awareness of the importance of trust among stakeholders and a willingness to engage.
- **Cybersecurity is often considered a national security issue involving defense (military) and law enforcement (cyber crime and investigations).** It is important to have a basic understanding of the responsible government authorities and cybersecurity governance structure in a country before engaging in a conversation with a cybersecurity expert. In many countries, cybersecurity policy can be new and capacity is still developing. As a result, a lack of clear authorities and responsibilities across entities may give rise to power dynamics of which DECA Research Teams should be aware.
- **Understand that data protection and privacy may influence a country's cybersecurity context.** Discussions with stakeholders about cybersecurity may expose concerns about how the public or private sector potentially use or misuse data that is legally obtained for a specific purpose: for example, using biometrics contained in an electoral database for law enforcement purposes, or selling mobile money account details without explicit consent. The misuse of data may not be legally defined and different stakeholders will have different perspectives regarding justification for using data for national security. This could be a sensitive topic and open-ended broad questions should be asked as opposed to leading or accusatory questions.

3.2. ADDITIONAL QUESTIONS AND THE DECA RESEARCH CHECKLIST

The [DECA Research Checklist](#) includes helpful questions for framing a productive conversation about cybersecurity (see [Guiding Questions](#) on page 7). Depending on the individual and context, additional guiding questions within the four focus areas may include:

PREPAREDNESS AND RESPONSE:

- What policies, regulations, and legislation exist to prevent and address cybersecurity threats? Are data protection requirements in place?
- Which government agency is primarily responsible for cybersecurity in your country? Which other agencies are involved in cybersecurity preparedness and response?
- Do you feel that your country, your sector, or your industry and your organization are prepared for a cyber incident?
 - » What are the strengths and weaknesses in terms of preparedness and incident response?
 - » What would be the impacts of an incident on your organization?
- What are the most significant cyber threat trends in the country?
 - » Who are the primary victims or targets? Who are the primary perpetrators?
- Does a national incident response plan or similar guidance exist?
 - » If so, what is the status of implementation?
 - » Are public sector entities required to have an incident response plan in place? Are critical infrastructure sectors required to have an incident response plan in place or are they acting on their own initiative to put incident response plans in place?

MULTI-STAKEHOLDER ENGAGEMENT:

- How do different stakeholders (e.g., private sector, public sector, civil society, media) perceive the importance of cybersecurity?
- Are there opportunities for all stakeholders to participate in developing cybersecurity laws and policies? Are there adequate resources for stakeholders to better understand and implement those policies?
 - » Is there clear guidance and a tool for incident reporting? If not, where are the gaps?

WORKFORCE DEVELOPMENT:

- What steps has your organization taken with regard to cybersecurity?
 - » Is leadership aware of the risks related to inadequate cybersecurity?
 - » At what level is cybersecurity managed in your organization?
 - » Do members of your organization receive cybersecurity training?
 - » Does your organization have a dedicated cybersecurity team?

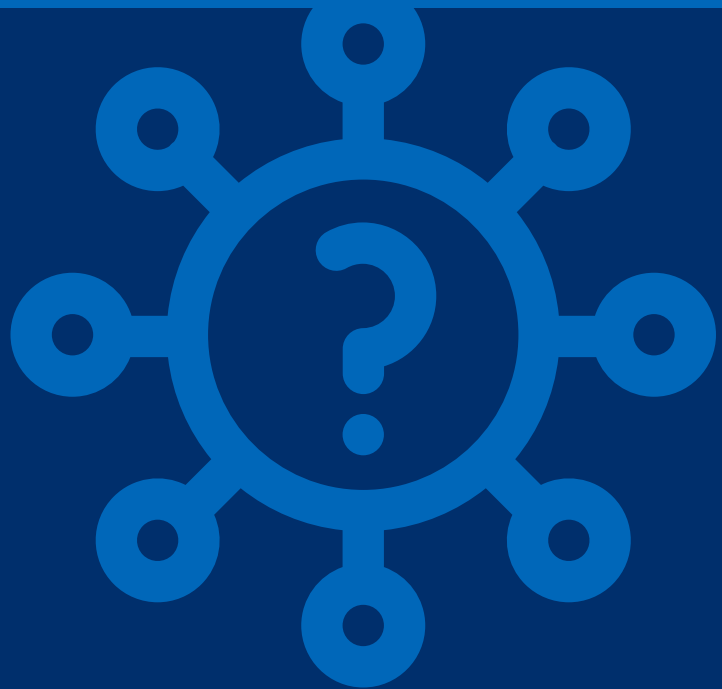
- Are critical infrastructure sectors or operators of essential services defined in legislation or policy?
 - » If so, are these sectors required to address and improve cybersecurity in a specific way, such as through the adoption of international standards?
 - » Have sectoral CERTs, Security Operations Centers (SOCs), or Information Sharing and Analysis Centers (ISACs) been established? Do they coordinate and share information with government CERTs and SOCs? With other sectors?
 - » Do these entities use international standards such as [TLP](#) (Traffic Light Protocol) for sharing threat intelligence?

INTERNATIONAL ENGAGEMENT:

- Does the country conduct regional or international cyber crisis exercises? This may include tabletop exercises (TTX) or emergency response drills.
- Does the country participate in an international cybersecurity hub or council?
- Are there regional policies in place to address cross-border cyber incidents?

APPENDIX A:

Key Supplemental Questions by DECA Pillar



PILLAR 1: DIGITAL INFRASTRUCTURE AND ADOPTION

Preparedness and incident response including critical infrastructure protection (CIP).

- Do key critical infrastructure (CI) sectors and entities have incident response plans in place? What role does the government play, if any, in development of incident response plans (policy, regulation, standards, guidance, response exercises)? Are incident reporting requirements in place (check the national CERT page for guidance or a link to report an incident)?
- Have CI sectors or essential services been formally identified and are CIP cybersecurity policies or practices in place? Are cross-sector or sector-specific information and threat sharing mechanisms in place (sector Computer Emergency Response Teams (CERTs), Security Operations Center (SOCs), Information Sharing and Analysis Centers (ISACs))?
- Have CI stakeholders identified senior staff members responsible for cybersecurity? Are Boards of Directors briefed regularly on cybersecurity? Is investment in cybersecurity a priority?
- Do CI stakeholders play an active role in promoting a culture of cybersecurity among their partners and customers? Do stakeholders have in place supply chain cybersecurity standards or public awareness campaigns?

PILLAR 2: DIGITAL SOCIETY, RIGHTS, AND GOVERNANCE

Trust and cooperation through multi-stakeholder engagement and increased resilience through international cooperation.

- Is the national framework for cybersecurity based on multi-stakeholder engagement? Are there examples of cooperation among stakeholders, such as regular working group meetings, or an advisory committee representing a diverse group of stakeholders?
- Are international standards for cybersecurity recognized and required by the government? Does the national government engage in cybersecurity initiatives on a regional or global level?
- Are key entities such as the national CERT members of international cybersecurity organizations (ex. [FIRST](#))?
- Do public sector budget allocations reflect cybersecurity as a priority?
- What data protection legislation and associated data protection enforcement entities exist? What capacity do these entities have to enforce data protection legislation? Do data protection bodies engage in multi-stakeholder engagement to discuss data protection challenges from different perspectives?

PILLAR 3: DIGITAL ECONOMY

Cooperation between the public and private sectors and small and medium-sized enterprise (SME) capacity building.

- To what extent does the private sector engage in and support cyber resilience, for example, through active incident reporting or sharing of threat intelligence?
- Are public-private partnerships in place to support national cybersecurity? This may include partnerships between academic institutions and private sector entities to build workforce capacity, or SOC services offered to the public sector by private companies.
- Are private sector entities investing in cybersecurity capacity at a systemic level, for example through partnerships with CSOs, public awareness programs, supply chain strengthening, or cyber workforce training?
- Do SMEs have access to resources to build cybersecurity capacity? This may include training, low-cost or free tools, or partnerships with larger companies. Do SMEs understand the risks related to poor cyber practices?

APPENDIX B:

Cybersecurity Links and Resources



TABLE 7: Cybersecurity links and resources

Resource	Source Organization/Program	Related Links
USAID Cybersecurity Primer	USAID	Digital Ecosystem Country Assessment and Toolkit
USAID Cybersecurity Briefers	USAID	The collection includes 11 sectoral briefers: Agriculture and Food Security ; Democracy, Human Rights, and Governance ; Digital Financial Services ; Economic Growth and Trade ; Education ; Environment, Energy, and Infrastructure ; Gender Equality ; Global Health, Humanitarian Assistance ; Youth ; and Conflict Prevention and Stabilization .
Cyber Strategy Development and Implementation Framework	MITRE	
Global Cyber Security Capacity Center	Oxford University	Cyber Maturity Model for Nations (CMM) ; Oceania Cyber Security Centre ; Cybersecurity Capacity Centre for Southern Africa ;
Global Cybersecurity Index	International Telecommunications Union (ITU)	National Cybersecurity Strategies Repository ; ITU Data Hub: Cybersecurity
Global Forum on Cyber Expertise Cybil Portal	GFCE	Catalog of Project Options for the National Cybersecurity Strategy Cycle ; CSIRT Maturity Framework ; Developing Cybersecurity as a Profession ; Global Overview of Cyber Capacity Assessment Tools (GOAT) ; Integrating Cyber Capacity in the Digital Development Agenda ; WG Paper on Confidence Building Measures
National Cybersecurity Assessment Framework	European Cybersecurity Agency (ENISA)	See Topics for additional resources across cyber sub-topics
National Cyber Security Index (NCSI)	eGovernance Academy	NCSI Methodology 3.0
NIST Cybersecurity Framework (CSF)	National Institutes of Standards and Technology	NIST Applied Cybersecurity Division – includes: NICE (Workforce Development) NCCOE (Center of Excellence)
Africa CERT	Africa CERT	
Asia Pacific CERT	Asia Pacific CERT	
Carnegie Mellon CERT Division	Carnegie Mellon University	
CISA Global Overview	Cybersecurity and Infrastructure Security Agency (CISA)	CISA International CISA Cyber Essentials
Cisco Network Academy Locator	Cisco	

Resource	Source Organization/Program	Related Links
Cyber Diplomacy Atlas	EU Cyber Direct	
Cyber Peace Institute	Cyber Peace Institute	Humanitarian Cybersecurity Center CyberPeace Builders
Cyber Threat Alliance (CTA)	Cyber Threat Alliance	See Resources for programs and publications
Global Cyber Alliance (GCA)	Global Cyber Alliance	GCA Toolkits
Global Data Barometer	Global Data Barometer	
Data Protection Laws of the World	DLA Piper	
Digital Defense Report 2023	Microsoft	
FIRST – Improving Security Together	FIRST	FIRST CSIRT Services Framework
Digital Society Project	Digital Society Project	V-DEM
Freedom on the Net	Freedom House	
The Hague Program on International Cybersecurity	The Hague Program	
ISACA Local Chapters	ISACA	ISACA Main Page
Multi-Donor Cyber Trust Fund	World Bank	
National Cyber Security Centre	NCSC UK	
OAS Cybersecurity Program	Organization of American States (OAS)	
Open CSIRT Foundation	Open CSIRT Foundation	Find local CSIRTs via Trusted Introducer SIM3 self-assessment tool
OSCE Cybersecurity Program	Organization for Security and Cooperation in Europe (OSCE)	Emerging Practices in Cybersecurity Public-Private Partnerships
RUSI Cyber Research	Royal United Services Institute	
State of Humanitarian and Development Cybersecurity Report	NetHope	Global Humanitarian ISAC
TechSoup Global Network	TechSoup Global	Find a local Partner
UNCTAD Data Protection and Privacy	United Nations	
UNIDIR Cyber Policy Portal	United Nations	
WEF Centre for Cybersecurity	World Economic Forum	Global Cybersecurity Outlook 2023

APPENDIX C:

Updates to Glossary

(Abbreviations and Definitions)



TABLE 8: Glossary update

Term	Definition
Confidence Building Measure (CBM)	<ul style="list-style-type: none"> Defined as actions and processes designed to reduce or eliminate the causes of mistrust, tensions, and hostilities between and among states that could fuel arms races or lead to escalations and actual conflicts (source: GFCE).
Critical Infrastructure (CI)	<ul style="list-style-type: none"> Assets, systems, and networks, whether physical or virtual, are considered so vital that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof (source: CISA).
Critical Infrastructure Protection (CIP)	<ul style="list-style-type: none"> The process of securing the CI of a region or nation from threats such as cyber attacks, natural disasters, and terrorist activities. These infrastructures include people, systems, and assets that are essential for public safety, economy, and national security.
Cyber Resilience	<ul style="list-style-type: none"> The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resilience is intended to enable mission or business objectives that depend on cyber resources to be achieved in a compromised cyber environment (source: NIST).
Digital Public Infrastructure (DPI)	<ul style="list-style-type: none"> Refers to digital solutions and systems that enable essential functions and services in the public and private sectors, such as digital forms of ID and verification, payment, data exchange, and information systems (source: Digital Public Goods Alliance),
Digital Public Goods (DPG)	<ul style="list-style-type: none"> Open source software, open data, open AI models, open standards and open content that adhere to privacy and other applicable laws and best practices, do no harm, and help attain the SDGs (source: UN).
Operators of Essential Services (OES)	<ul style="list-style-type: none"> Public or private entities providing services essential to the maintenance of critical societal or economic activities (source: EU NIS Directive).

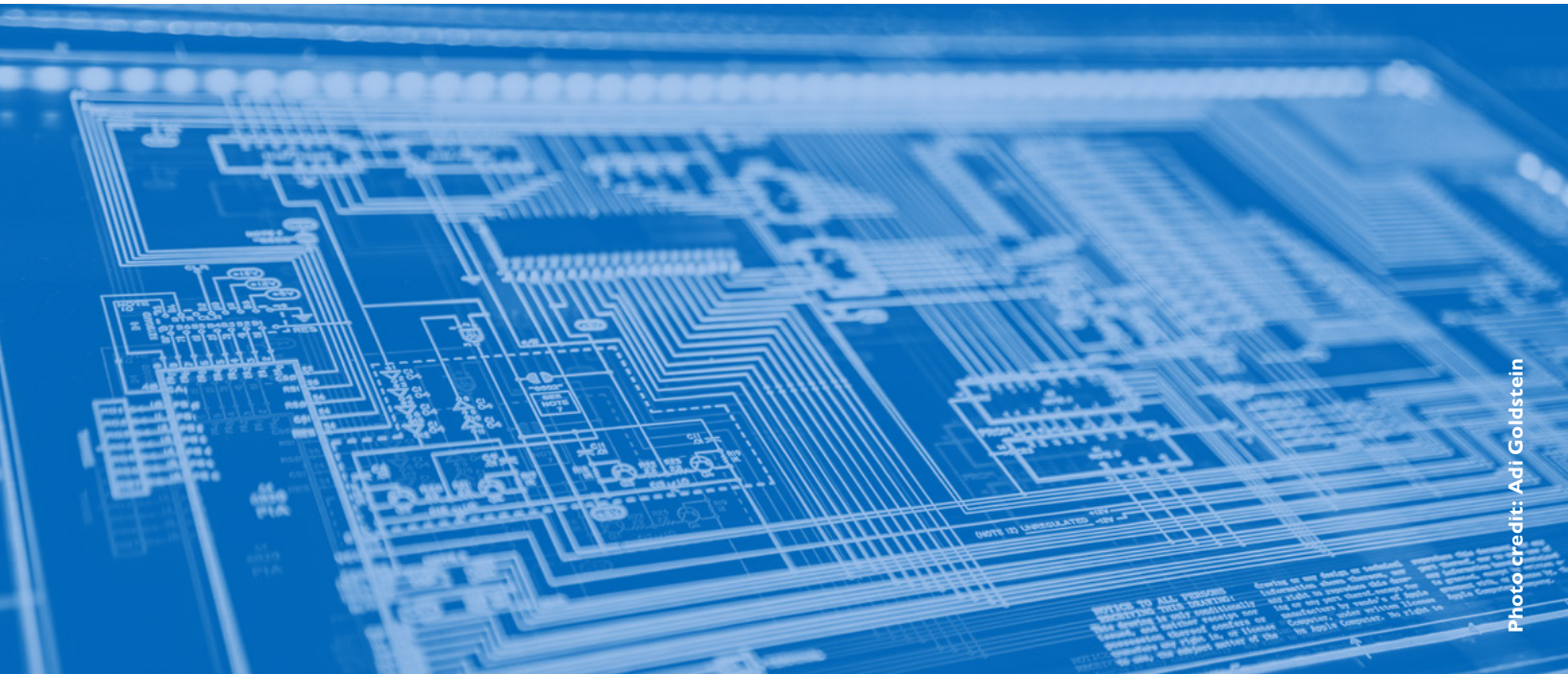


Photo credit: Adi Goldstein



BUREAU FOR INCLUSIVE GROWTH, PARTNERSHIPS, AND INNOVATION (IPI)
INNOVATION, TECHNOLOGY AND RESEARCH HUB (ITR)

[usaid.gov/usaid-digital-strategy](https://www.usaid.gov/usaid-digital-strategy)