PUBLIC

DOCUMENT OF THE INTER-AMERICAN DEVELOPMENT BANK

JAMAICA

STRENGTHENING CYBERSECURITY IN JAMAICA

(JA-L1093)

PROJECT PROFILE

This document was prepared by the project team consisting of: Benjamin Roseth (IFD/ICS), Team Leader; Ariel Nowersztern, (IFD/ICS), Alternate Team Leader; Cynthia Hobbs (SCL/EDU), Alternate Team Leader; Miguel Porrúa, Julieth Santamaría, Florencia Aguirre, Pablo Libedinsky, Santiago Paz, Laura Rodriguez, Ynty Martínez, María José Martínez, (IFD/ICS); Jodi Ho Lung, Sudaney Blair (CCB/CJA); Kayla Grant (IFD/CTI); Shirley Foronda, Verónica Benedettelli (VPC/FMP); Paola Pedroza (ORP/REM); Henry Mooney (CCB/CCB); Gastón Pierri (SPD/SDV); Gerard, P. Alleng (CSD/CCS), María Sofia Greco (LEG/SGO).

PROJECT PROFILE

JAMAICA

I. BASIC DATA

Project Name:	Strengthening Cybersecurity in Jamaica		
Project Number:	JA-L1093		
Project Team:	Benjamin Roseth (IFD/ICS), Team Leader; Ariel Nowersztern, (IFD/ICS), Alternate Team Leader; Cynthia Hobbs (SCL/EDU), Alternate Team Leader; Miguel Porrúa, Julieth Santamaría, Florencia Aguirre, Pablo Libedinsky, Santiago Paz, Laura Rodriguez, Ynty Martínez, María José Martínez, (IFD/ICS); Jodi Ho Lung, Sudaney Blair (CCB/CJA); Kayla Grant (IFD/CTI); Shirley Foronda, Verónica Benedettelli (VPC/FMP); Paola Pedroza (ORP/REM); Henry Mooney (CCB/CCB); Gastón Pierri (SPD/SDV); Gerard, P. Alleng (CSD/CCS), María Sofia Greco (LEG/SGO).		
Borrower:	Jamaica		
Loan Modality:	Specific Investment Loan		
Executing Agency: (Co-executing Agency or/sub-executing Agency if applicable):	Jamaica-MSET - Ministry of Science Energy and Technology		
Financial Plan:	IDB (source):	US$	6.5 million
	Co-financing[1]	US$	0
	Total:	**US$**	**6.5 million**
Safeguards:	Risk Classification:		Low
	Impact classification:		''C''
Processing track:	☐ Standard		☒ Special
Country Strategic Alignment:	GN-3138; Strategic Objective 5.1		
Strategic Alignment:			
Challenges:	☐ Social Inclusion ☒ Productivity and Innovation ☐ Economic Integration		
Crosscutting:	☒ Gender Equality ☐ Diversity ☐ Environmental sustainability ☐ Climate Change ☒ Institutional Capacity and Rule of Law		

II. GENERAL JUSTIFICATION AND PROGRAM STRATEGY

2.1 **Background and justification.** Jamaica is gradually becoming a digital society. In the last decade, the percentage of the population using the internet doubled, reaching 82% in 2021.[2] Although at a slower pace, there was also an increase in

[1] The project team is exploring the possibility of co-financing this loan with grant funding from other donors.
[2] ITU, ICT Development Dashboard.

the Government of Jamaica's online presence and availability of online services.[3] One out of five Jamaicans use the internet for digital transactions, such as online banking and shopping.[4]

2.2 As use of digital services rises, so do the risks of suffering cyberattacks because of an expansion of what experts call the "attack surface" - society's dependency on digital systems, and the value cybercriminals can extract.[5] The consequences of cyberattacks fall into dozens of categories,[6] including: financial harm through response and mitigation costs, direct theft or fraud, lost productivity, stolen or published intellectual property, and even adverse psychological and health consequences, among others.[7] It is estimated that the LAC region suffered 137 billion cyberattack attempts during the first semester of 2022, a 50% increase compared to the same period in 2021.[8] Consequently, organizations across various sectors perceive cybercrime among the top 10 risks they face.[9] Driven by the increasing awareness of risks, revenue in the cybersecurity goods and services market is projected to reach US$173.50 billion in 2023.[10]

2.3 Jamaica's vulnerability to cyberattacks is high. An estimated 12 million cyberattacks were attempted on Jamaican targets in 2022.[11] Between January and September 2018, there were 62 reported counts of internet banking fraud, with an estimated loss of US$38.2 million.[12] Twice as many cyberattacks were reported to the Jamaica Cyber Incident Response Team (JaCIRT) between October 2021 and October 2022 as compared to the year before. In the first two months of 2023, at least two government entities suffered cyberattacks: the Office of the Prime Minister and the Southeast Regional Health Authority.

2.4 The Government of Jamaica has taken steps towards protecting its cyberspace in the past decade. In 2015, it released a National Cybersecurity Strategy, which focuses on four areas: technical measures, human resource and capacity building, legal and regulatory framework, and public education and awareness. The Strategy established the creation of JaCIRT, a division of the Ministry of Science, Energy and Technology (MSET), and is responsible for coordinating incident response, prevention, and mitigation across government.[13] In 2010 Parliament passed the Cybercrime Act, which was updated in 2015[14] and is currently under review for further updates, and in 2020 it passed a Data Protection Act.[15] However,

---

3 UN, UN E-Government Survey 2022. Jamaica's score for the subcomponent Online Service Index increased form 0.38 in 2003 to 0.49 in 2022.

4 Survey of 2,000 Jamaicans conducted by the Project Execution Unit of the National Identification System for Economic Growth Project (4437/OC-JA) during 2022. Unpublished.

5 Cybercrime Magazine.

6 Agrafiotis, I., Nurse, J.R., Goldsmith, M., Creese, S. and Upton, D., 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1), p. tyy006.

7 Ex: a 2021 data breach on the application JamCOVID19 exposed the personal data of 500,000 travelers. Source: TechCrunch.

8 Our Today.

9 WEF 2023.

10 Statista.

11 The Gleaner, 2022.

12 Bank of Jamaica, 2018.

13 Jamaica Cyber Incident Response Team.

14 2015 Cybercrime Act.

15 2020 Data Protection Act.

Jamaica has seen little progress in key areas since 2016, namely: critical infrastructure protection, crisis management, and cyber defense. In the private sector, many companies lack cyber incident response plans.[16]

2.5 **Main problem.** There is a high vulnerability to cyberattacks in public and private sectors.[17] The specific problems related to the general problem are as follows:

2.6 **Lack of government capacity to protect government digital systems and national critical infrastructure against cyberattacks.** For example, comparative statistics reveal a limited monitoring capability: JaCIRT in 2022 registered 86 cyber incidents (one per 32,558), whereas in Uruguay and Chile, the authorities responded to 2,798 (one per 1,215 people) and 15,321, respectively (one per 1,272 people), in 2020.[18] This problem is linked to the following causal factors: (i) government institutions that have cybersecurity responsibilities are underequipped and understaffed;[19] (ii) the cybersecurity legal, regulatory, and policy framework is nonexistent; (iii) implementation capacity for cybersecurity regulation is limited; (iv) there are limited coordination mechanisms in place between the different government institutions that deal with cybersecurity; (v) there are limited measures in place specifically to protect national critical infrastructure; and (vi) there is a lack of awareness of cybersecurity risks among public sector employees.[20]

2.7 **Limited availability and skills of trained cybersecurity professionals and service offerings from the private sector.** Between 2016 and 2020, Jamaica's capabilities in cybersecurity training, education and awareness remained practically stagnant.[21] This problem is linked to the following causal factors: (i) limited foundational technical skills and awareness of career opportunities of potential cybersecurity professionals; (ii) available courses in cybersecurity are limited and lack specialization;[22] (iii) there are not enough educators in this field to meet the demand for training cybersecurity professionals;[23] (iv) there is limited awareness of cybersecurity risks among the private sector and the general population; and (v) local cybersecurity companies offer limited products and services to serve the local economy. Cybersecurity students and professionals are predominantly men, consistent with global trends.

---

16 IDB-OAS, 2020.

17 In the 2020 IDB-OAS measurement of national cybersecurity maturity, Jamaica scored 106 out of a possible 265 points, in comparison to 185 points scored by Uruguay.

18 A lack of detection capability allows cyberattacks to increase in severity before they are noticed, increasing their negative impacts and remediation costs.

19 Considering only JaCIRT, the Major Organized Crime and Anticorruption Agency (MOCA), the Jamaica Constabulary Force (JCF), the Ministry of National Security (MNS), and eGovJamaica Limited, there are at least 35 unfilled cybersecurity positions. Furthermore, there is no malware analysis lab for use by government institutions in Jamaica.

20 Globally, two-thirds of cyberattacks on organizations occur as a result of employee negligence. Source: *Cybint*. In Jamaica, there have been no government-wide efforts to reduce such potential negligence.

21 IDB-OAS, 2020.

22 The Office of the National Security Advisor (2022) found that the market offering of cybersecurity training is insufficient, and for some job roles it was inexistent.

23 At the two largest public universities, University of the West Indies – Mona and the University of Technology, there are approximately ten professors that teach cybersecurity courses, whose classes are consistently oversubscribed.

2.8 **Objectives.** The general objective of the program is to contribute to the reduction of vulnerabilities to cyberattacks in the public and private sectors. The specific objectives are: (i) increase the coverage of cybersecurity protection extended to public institutions; and (ii) increase the production of specialized cybersecurity professionals.

2.9 **Component 1. Strengthening the government's ability to protect against cyberattacks (US$4,600,000).** The following activities will be carried out: (i) draft organizational design and workplans for a national cyber authority; (ii) draft legislation, regulations, and policies for cybersecurity; (iii) enhance JaCIRT's operational capabilities, including incident response and threat intelligence; (iv) improve the cyber resiliency of government digital assets via: (a) controls for prevention, protection, and monitoring; and (b) periodic audits; (v) improve the cyber resiliency of public and private critical infrastructure via: (a) drafting of a critical infrastructure protection strategy; (b) identification and cataloging of critical infrastructure and systems; (c) capacity building for cybersecurity of regulatory bodies; and (d) sectorial monitoring and collaboration initiatives; (vi) establish a national incident information exchange service; (vii) upgrade skills for government cyber professionals; and (viii) raise cyber-awareness among public servants.

2.10 **Component 2. Strengthening the national educational and private sector cybersecurity ecosystem (US$1,400,000).** The following activities will be carried out: (i) support cybersecurity curriculum development, career orientation and outreach activities for secondary school students, and career orientation and outreach activities for tertiary students in computer science programs or similar, with a gender perspective; (ii) support the development and/or enhancement of cybersecurity vocational programs, with a gender perspective; (iii) establish a (gender-sensitive) post-secondary scholarship program and associated outreach activities for future public service cybersecurity positions such as government, local academic institutions and NGOs; (iv) develop and disseminate cybersecurity guidance, standards and alerts for public and private sector organizations; (v) foster the development of a cybersecurity cluster, encompassing the private sector, government, NGOs and academia; and (vi) conduct cybersecurity awareness raising activities with different population segments, including minors and seniors.

2.11 The initial project administration budget allocation will be US$500,000 that will be used for covering PEU salaries, audit, and monitoring and evaluation.

2.12 **Expected results and beneficiaries.** The program will reduce the country's vulnerability to cyberattacks in the public and private sectors by: (i) increasing the government's capacity to prevent, detect and respond to cybersecurity incidents; and (ii) strengthening the capacity of educational institutions to train cybersecurity professionals. The beneficiaries of the program will be government institutions whose digital assets will be better protected, the academic sector whose cybersecurity training offer will be expanded, the private sector which will have easier access to qualified cybersecurity professionals, and citizens in general, through the greater awareness and protection from cyberattacks of public and private services.

2.13 **Strategic alignment.** The program is aligned with the Second Update of the Institutional Strategy (AB-3190-2) and is aligned with the Productivity and Innovation challenge by promoting technology and innovation. It is aligned with the IDB Country Strategy with Jamaica 2022-2026 (GN-3138), which includes Accelerating Digital Transformation, including via cybersecurity, in its pillar on Productive Sector Reactivation for Sustainable Growth and is aligned with the strategic objective 5.1 enhancing the effectiveness of public administration. It is also aligned with the Sector Strategy on Institutions for Growth and Social Welfare (GN-2587-2) for contributing to the theme of Institutions for Innovation and Technological Development, specifically to the objectives: (i) improve government policies and action in the ICT sector; (ii) develop advanced human capital; and (iii) strengthen institutions and networks. The operation aligns with the cross-cutting challenges of (i) Institutional capacity and rule of law by building the capacity of the lead government institution responsible for protecting the country's cyberspace; and (ii) Gender equality, by improving women and girl's participation in cybersecurity through the training courses. It is aligned with the Gender and Diversity Sector Framework Document (GN-2800-13) and with the Joint MDB Assessment Framework for Paris Alignment and the IDB Group Paris Alignment Implementation Approach (PAIA) (GN-3142-1). Furthermore, it will contribute toward Jamaica's long-term development plan, Vision 2030,[24] in particular to outcome 2 (World-class education and training), outcome 5 (Security and safety), outcome 8 (an enabling business environment), and outcome 11 (A technology-enabled society). Lastly, it contributes to the Government of Jamaica's national security strategy, Plan Secure Jamaica, which includes Cyber[25] as a strategic subject area.

2.14 **Financial Instrument.** The operation will be an investment loan of ordinary capital with a four-year disbursement period, executed by the Government of Jamaica through the Ministry of Science, Energy, and Technology (MSET). This execution period, one year shorter than most IDB loans in Jamaica, is justified due to its relatively small amount. This loan modality will allow for specific investments in hardware, software, and training, the hiring of a Project Execution Unit to support implementation, and for continuous IDB technical and fiduciary support.

III. SECTOR KNOWLEDGE AND PREPARATION PLAN

3.1 **Bank experience.** The Bank has experience in the design and implementation of projects to support the digital transformation of the public sector, encompassing cybersecurity, including Government Digital Transformation to Strengthen Competitiveness (4549/OC-BH), Panama Online (3683/OC-PN), and Program to Support the Digital Government Strategy (4867/OC-UR), among others. The Bank also has experience in supporting the modernization of the Jamaican public administration, including through the Support to the Public Sector Transformation Programme (4374/OC-JA), the Implementation of the National Identification System for Economic Growth (4437/OC-JA), and the Security Strengthening Project (4400/OC-JA). This project would be the third IDB loan operation focused exclusively on cybersecurity, following Strengthening Cybersecurity in Uruguay

[24] PIOJ, Vision 2030 Jamaica.
[25] MSET, National Cybersecurity Strategy.

(4843/OC-UR) and Cybersecurity for Critical Information Infrastructure Program (5735/OC-AR).

3.2 **Lessons learned.** Lessons learned from the aforementioned IDB operations in the region that inform program design include the importance of: (i) a national ecosystem approach to building cybersecurity capability, encompassing legal, strategic and policy measures, government capacity for prevention, detection and response to cyberattacks, protecting critical infrastructure, talent generation and retention, and private sector capacity building in collaboration with government; (ii) a strong lead institution with sufficient mandate and resources to provide cybersecurity services to both government and the private sector, as well as to lead coordination with academic institutions and international partners; (iii) a pipeline approach to talent development, encompassing awareness and skill building for primary and secondary students, certificate and degree opportunities for post-secondary students, and ongoing training opportunities for working professionals; and (iv) use of international standards to inform strategies, operating plans, procurements and training programs. Lessons learned from the ongoing execution of an IDB loan operation with the same executing agency that will be incorporated in project design include the importance of: (i) ensuring strong buy-in with project design at both the political and technical levels of the institution; (ii) designing the project operations manual to maximize efficiency, considering the EA's own procedures; and (iii) embedding project execution capability building activities in project design.

IV. TECHNICAL ASPECTS, ENVIRONMENTAL RISKS AND EXECUTION AND FIDUCIARY ASPECTS

4.1 **Execution.** The operation will be executed by the Ministry of Science, Energy, and Technology (MSET). MSET has prior experience executing IDB-financed programs. Its capacity to undertake execution of this program will be assessed through the Institutional Capacity Assessment Platform (ICAP) prior to completion of the Proposal for Operations Development (POD). Results of the ICAP will inform project design and the composition of the Project Executing Unit (PEU).

4.2 **Fiduciary aspects.** It is intended that the MSET be responsible for overall project fiduciary oversight including procurement, financial management and disbursement arrangements through a Project Executing Unit (PEU). The PEU would be responsible for procurement, budgeting and planning, accounting, and reporting, ensuring flow of funds, internal controls, procurement and financial management staffing and external audits for the whole project. While the MSET has recent experience managing EMEP, an IDB-financed project, the PEU will be new and not familiar with IDB fiduciary policies and procedures. Furthermore, it might be a challenge to find staff to be part of the PEU familiarized with IDB procurement, disbursement, and financial management procedures. A financial management and procurement capacity assessment will be conducted to determine the areas that require to be strengthened to have robust financial management and procurement arrangements in full compliance with the Bank's requirements. The overall fiduciary risk of the project at this stage is medium-high.

4.3 **Safeguards.** In accordance with the Environmental and Social Policy Framework (ESPF), the operation was classified as low risk/Category “C” as it is expected to cause minimal or no negative environmental or social impacts.

4.4 **Coordination.** The program will require coordination both within government and with the private sector. The intra-government coordination will be led by MSET; other actors tentatively include eGovJamaica Limited, the Office of the National Security Adviser, Major Organized Crime and Anti-Corruption Agency, Jamaica Constabulary Force, and Jamaica Defense Force for technical cybersecurity issues, and the Ministry of Education and Youth, and HEART/NSTA Trust for education issues. MSET will lead coordination with the private sector via dialogue with one or more technology-focused professional associations, potentially including the Private Sector Organization of Jamaica and/or the Jamaica Technology and Digital Alliance. Private sector coordination will be necessary for the following activities: (i) drafting a critical infrastructure protection strategy; (ii) the identification and cataloguing of critical infrastructure; (iii) sectoral cyber threat monitoring; (iv) the design of a cyber incident alert service; and (v) the design and implementation of a national incident information exchange service.

4.5 **Sustainability.** The program primarily supports capacity building efforts of permanent government institutions that have the mandate, strategic framework, and capability necessary to continue the initiatives that will be executed under the program once its resources are fully executed.

4.6 **Risks.** The following risks to project execution have been preliminarily identified: (i) delays in inter-institutional agreements with educational and training institutions (medium-low); (ii) challenges in recruiting and retaining specialized staff to support the implementation of project activities (high); and (iii) a change of government because of elections that may occur anytime, as is inherent to the parliamentary system (high). The corresponding mitigation measures are: (i) create a project steering committee including the Ministry of Education to facilitate inter-institutional agreements with educational and training institutions; (ii) offer flexible and competitive contracts (e.g. open to both local and international specialists); and (iii) front-load the major procurements and institutional agreements.

V. RESOURCES AND TIMETABLE

5.1 The distribution of the Operation Development Proposal (POD) to the Quality and Risk Review (QRR) is expected on July 06, 2023: for the Operating Policy Committee on July 28, 2023, and consideration by the Executive Board on September 27, 2023. Total transactional resources required for preparation are estimated at US$60,178 (US$27,500 for consultant fees and US$32,678 for missions). The staff time required for loan preparation will be 1.54 FTE.

Annexes

I. Summary of the Environmental and Social Review
II. Timetable and Preparation Resources
III. Filters for determining the processing track.

SUMMARY OF THE ENVIRONMENTAL AND SOCIAL REVIEW

A. Environmental impact

1.1 In accordance with the Environmental and Social Policy Framework (ESPF), the operation was classified as Category "C" as it is expected to cause minimal or no negative environmental or social impacts.

1.2 In order to comply with the requirements of the ESPF and especially those of the Environmental and Social Performance Standards 1, 2 and 10, during preparation any existing environmental and social management instrument in the Executing Unit and/or in the applicable local regulations will be reviewed.

B. Environmental and Social Performance Standards (ESPSs)

2.1 **ESPS 1 -** The Executing Agency will not prepare and maintain an Environmental and Social Management System (ESMS) for the operation as defined under ESPS 1.

2.2 **ESPS 2 -** The Executing Agency will prepare and maintain an Environmental and Social Management System (ESMS) for the operation with specific elements related to Labor and Working Conditions under ESPS 2.

2.3 **ESPS 10 –** The Borrower will operate a Grievance Redress Mechanism at the Project level (direct and contracted).

CONFIDENTIAL

[1] The information contained in this Annex is confidential and will not be disclosed. This is in accordance with the "Deliberative Information" exception referred to in paragraph 4.1 (g) of the Access to Information Policy (GN-1831-28) at the Inter-American Development Bank.

CONFIDENTIAL

[1] The information contained in this Annex is confidential and will not be disclosed. This is in accordance with the "Deliberative Information" exception referred to in paragraph 4.1 (g) of the Access to Information Policy (GN-1831-28) at the Inter-American Development Bank.