International Civil Aviation Organization
North American, Central American and Caribbean Office

INFORMATION PAPER

NACC/DCA/11 — IP/26
09/06/23

Eleventh North American, Central American and Caribbean Directors of Civil Aviation Meeting (NACC/DCA/11)
Varadero, Cuba, 28-30 June 2023

Agenda Item 5: **NAM/CAR Regional Aviation Security/Facilitation Implementation**

PROGRESS ON CYBERSECURITY OF CIVIL AVIATION

(Presented by Dominican Republic)

EXECUTIVE SUMMARY	
This note summarizes the ongoing initiatives and progress made in cybersecurity by the Dominican State, whose goal is to safeguard critical infrastructures in a safe and reliable manner. This informative note presents the situation regarding the cybersecurity law, the updating of policies, the continuous training of the Organization's human resources, as well as future measures to continue improving.	
Strategic Objectives:	• Strategic Objective 3 – Security & Facilitation

1. Introduction

1.1 The State's mission is to establish the appropriate cybersecurity mechanisms that protect it, as well as the productive sectors and citizens, all with the aim of guaranteeing a favorable cybersecurity ecosystem for national economic development, within the framework of digital transformation. and on a safe, resilient and trustworthy cyberspace.

2. Development

2.1 Decree 230-18 Creates the National Cybersecurity Strategy 2018-2021 that establishes the appropriate cybersecurity mechanisms for the protection of the State, its inhabitants and, in general, development and national security to create a safer and more secure cyberspace in the Dominican Republic. reliable. Special emphasis is placed on Article 6 of the Decree referring to pillar 2 of the Strategy on Protection of National Critical Infrastructures and State Infrastructures of Information and Comunication Tecnology (ICT). In this same decree, the National Cybersecurity Center is created as a dependency of the Ministry of the Presidency of the Dominican Republic.

2.2. It should be noted that the National Cybersecurity Center is the body authorized by the State dedicated to the development of cybersecurity, the strengthening of the digital trust of the Dominican user and the protection of the critical and technological infrastructure of the Dominican State.

23 The aforementioned decree was updated on June 14, 2022, thus promulgating decree 313-22, which establishes the National Cybersecurity Strategy 2022-2030, outlines the objectives and lines of action that the Dominican State has as its primary responsibility during this period, achieve and develop, to promote and strengthen the cybersecurity ecosystem, taking into account the sustainable development goals and international development indicators and good practices in cybersecurity.

2.4 The Cybersecurity Strategy of the Dominican Republic 2030 establishes the objectives and lines of action that guarantee a favorable environment for the development of all the productive sectors of the country, guaranteeing a safe cybersecurity ecosystem, reducing the impact of cyber threats and protecting the information systems and with special attention to national critical infrastructures and relevant Government IT infrastructures. All this facilitating as a State, that citizens can use the services offered through ICT, confident in their security.

2.5 The Strategy has four pillars: 1) Legal Framework and Institutional Strengthening, 2) Protection of National Critical Infrastructures and Government ICT Infrastructures, 3) Education and National Cybersecurity Culture, and 4) National and International Alliances, whose purpose is to establish a mechanism for dialogue and cooperation between all sectors of society to promote best practices, identify common problems and develop appropriate solutions to deal with cyber threats.

2.6 It is important to note that the Dominican Republic advanced 30 positions in the National Cybersecurity Index (NCSI), which measures the preparation of countries to prevent threats and manage cyber incidents. According to the report, the country reached a level of development of 71% between 2022 and 2023, for which it went from position 58 to 28, in the ranking that measures e-Governance Academy Foundation of the Republic of Estonia.

3. Regulatory Framework

3.1. The Dominican State has in force Law no. 53-07 on Misdemeanors and High Technology Crimes: Its purpose is the comprehensive protection of systems that use information and communication technologies and their content, as well as the prevention and punishment of crimes committed against these or any of their components or the committed through the use of said technologies to the detriment of natural or legal persons under the terms provided in this law. The integrity of the information systems and their components, the information or the data, that are stored or transmitted through them, the transactions and commercial agreements or of any other nature that are carried out by their means and the confidentiality of these, are all protected legal assets.

3.2. Law no. 172-13 whose purpose is the comprehensive protection of personal data stored in files, public records, data banks or other technical means of data processing intended to provide reports, whether public or private.

3.3. Currently, a Cybersecurity bill is in the Dominican Senate for approval, which aims to strengthen the regulatory framework for the management of cybersecurity of information and communication technology infrastructures of the Public Administration and critical state infrastructures.

4. Training

4.1 CESAC, as an entity belonging to the Ministry of Defense, through the CSIRT-Defense of the C5i, carries out continuous training in cybersecurity aspects through its talent recruitment platform.

4.2 The National Cybersecurity Center, which is the competent entity in the field of cybersecurity in the Dominican Republic, was recently summoned to the civil aviation sector to participate in a Risk Analysis session for Critical Information Infrastructures, this in cooperation with the CyberNet project of the European Union, in order to identify the critical infrastructures of the civil aviation sector and know how to defend them against any cyberattack.

5. Conclusion

5.1 The adoption of the Cybersecurity Strategy of the Dominican Republic marks a milestone for the development of Dominican cyberspace. The challenges associated with cybersecurity are of a varied and complex nature, one of the main ones being the definition of the applicable legal framework. It is for this reason that the Dominican State is committed to establishing and periodically reviewing the legal framework. As a priority, criminal law and procedures must be reviewed to ensure the prevention, investigation and prosecution of all forms of cybercrime.

5.2 The main focus, with regard to the cybersecurity of critical infrastructures and relevant ICT infrastructures of the Government, is to establish mechanisms for prevention, detection, response and mitigation of cyber threats. The State is currently identifying which infrastructures are criticism in the civil aviation sector, which demonstrates the commitment to achieve a safer cyberspace.

— END —