# I MINA'TRENTAI SIETTE NA LIHESLATURAN GUÅHAN 2024 (SECOND) Regular Session VOTING RECORD

Bill No. 190-37 (COR) As amended by the Committee on General	Speaker Antonio R. Unpingco Legislative Session Ha Guam Congress Buildin					
Government Operations and Appropriations; and further amended on the Floor.						July 10, 202
NAME	Aye	Nay	Not Voting/ Abstained	Out During Roll Call	Absent	Excused
Senator Chris Barnett	J					
Senator Frank Blas, Jr.	J					
Senator Joanne Brown	J					
Senator Christopher M. Dueñas	J					
Senator Thomas J. Fisher	J					
Senator Jesse A. Lujan	J					
Vice Speaker Tina Rose Muña Barnes	J					
Senator William A. Parkinson	J					
Senator Sabina Flores Perez				7	J	1
Senator Roy A. B. Quinata	J					
Senator Joe S. San Agustin	J					
Senator Dwayne T. D. San Nicolas	J					
Senator Amanda L. Shelton	J					
Senator Telo T. Taitague	J					
Speaker Therese M. Terlaje	J					
TOTAL	14	0			1	1
	Aye	Nay	Not Voting/ Abstained	Out During Roll Call	Absent	Excused

I = Pass

Clerk of the Legislature

# I MINA'TRENTAI SIETTE NA LIHESLATURAN GUÅHAN 2023 (FIRST) Regular Session

## Bill No. 190-37 (COR)

As amended by the Committee on General Government Operations and Appropriations; and further amended on the Floor.

\*

Introduced by:

Tina Rose Muña Barnes
Dwayne T.D. San Nicolas
Chris Barnett
Frank Blas, Jr.
Christopher M. Duenas
Jesse A. Lujan
William A. Parkinson
Joe S. San Agustin
Roy A. B. Quinata
Thomas J. Fisher
Joanne M. Brown
Telo T. Taitague
Sabina Flores Perez
Therese M. Terlaje
Amanada L. Shelton

AN ACT TO *ADD* A NEW CHAPTER 15 TO DIVISION 1 OF TITLE 5, GUAM CODE ANNOTATED, RELATIVE TO CREATING THE MARIANAS CYBER SECURITY WORKING GROUP.

#### 1 BE IT ENACTED BY THE PEOPLE OF GUAM:

- 2 Section 1. Legislative Findings and Intent. I Liheslaturan Guåhan finds
- 3 that the monitoring of potential cyber-threats has been an ongoing task for many
- 4 years, but it has now come out of the shadows and into the limelight with the catchall
- 5 term "cyber security." In Guam's case, whether the end goal is data smuggling or

interrupting critical communications for the island, its neighbors or its allies – the mere fact that as much as seventy-five percent (75%) or more of information relayed over the internet transitions through one of the island's undersea cables should be enough reason for the local and federal governments to make and fund drastic improvements of Guam's efforts to combat these bad actors. To set the stage for these efforts, there is a pronounced need to become familiar and conversant with this method of tracking the attempts to access systems by those who would do harm to the island's online systems and programs.

Therefore, the establishment of the Marianas Cyber Security Working Group provides a platform to discuss these issues, to be informed of threats that have been detected, and learn of measures taken to mitigate the harm caused by the threats. The collaboration that can result from the issues discussed at the Working Group briefings can generate legislative measures or administrative policies that will help the government of Guam refocus toward capacity building, strategic planning and protection protocols for its management information systems government-wide.

**Section 2.** A new Chapter 15 is *added* to Division 1 of Title 5, Guam Code Annotated, to read:

18 "CHAPTER 15

## MARIANAS CYBER SECURITY WORKING GROUP

- § 15100. Creation of Working Group.
- § 15101. Purpose of Working Group.
- § 15102. Membership.

- § 15103. Information Dissemination.
- § 15100. Creation of Working Group.

There is created within the Office of the Governor the Marianas Cyber Security Working Group (Group) which shall be headed by *I Maga'håga/Maga'låhi*, with administrative support provided by the Mariana Regional Fusion Center.

## § 15101. Purpose of Working Group.

The Group shall meet on a monthly basis to discuss issues involving cyber security and its heightened priority within Guam. It shall receive periodic briefings from the Mariana Regional Fusion Center on best practices available to implement cyber security measures and secure management information systems and minimize threats to commerce and government operations. The briefings may also include a recap on any recent threats to government of Guam entities, the outcomes of such threats, and any recommendations to avoid future threats. To the extent practicable, the briefing information shall also be disseminated to the general public as a means to assist them in their individual needs to safeguard their own access to various sites on the internet. The Group may recommend legislation and administrative policy to safeguard and enhance system and software security and eliminate vulnerabilities resulting from threats, and engage in public awareness campaigns and outreach events to support the above goals.

# § 15102. Membership.

The Group's membership shall include *I Maga'håga/Maga'låhi*, or her/his designee; the Speaker of *I Liheslaturan Guåhan*, or her/his designee; the Chief Justice of Guam, or his/her designee; the General Manager, Guam Power Authority, or his/her designee; the General Manager, Guam Waterworks Authority, or his/her designee; the General Manager, Port Authority of Guam, or his/her designee; the Executive Manager, Guam Airport Authority, or his/her designee; the Director of Administration, or his/her designee; the Director, Department of Military Affairs, or his/her designee; the Chief Technology Officer, Office of Technology; one (1) representative from each of Guam's telecommunication companies, to be appointed by *I Maga'håga/Maga'låhi*; a representative recommended by the Guam Bankers Association, to be appointed by *I Maga'håga/Maga'låhi*; a member of the business

- 1 community with background and experience in computer operations and analytics,
- 2 to be appointed by *I Maga'håga/Maga'låhi*, and the Attorney General of Guam.
- **§ 15103.** Information Dissemination.
- 4 Select information presented by the Mariana Regional Fusion Center shall be
- 5 disseminated to the general public by no less than ninety (90) business days to allow
- 6 the information given to go through vulnerability patching before being shared. The
- 7 reporting of information disseminated to the public shall be anonymized and/or
- 8 redacted for the general overview of cyberthreats and trends that were discussed
- 9 during the meeting."