I MINA'TRENTAI SIETTE NA LIHESLATURAN GUÅHAN
RESOLUTIONS

Resolution No.	Sponsor	Title	Date Intro	Date of Presentation	Date Adopted	Date Referred	Referred to	PUBLIC HEARING DATE	DATE AUTHORS REPORT FILED	NOTES
237-37 (LS)	Tina Rose Muña Barnes Jesse A. Lujan Frank Blas, Jr.	Relative to recognizing Cyber Security Awareness Month 2023; and commending the collaborative efforts in demonstrating its importance of promoting cybersecurity awareness and preparedness to protect critical infrastructure.	10/27/23 4:15 p.m.	11/6/23 1:30 p.m.						

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

Resolution No. 237-37 (LS)

Introduced by: Tina Rose Muña Barnes
Jesse A. Lujan
Frank Blas, Jr.

Relative to recognizing Cyber Security Awareness Month 2023; and commending the collaborative efforts in demonstrating its importance of promoting cybersecurity awareness and preparedness to protect critical infrastructure.

BE IT RESOLVED BY *I MINA'TRENTAI SIETTE NA LIHESLATURAN GUÅHAN*:

WHEREAS, in commemoration of its 20th year, the Cybersecurity & Infrastructure Security Agency (CISA) has introduced an enduring cybersecurity awareness initiative known as "Secure Our World," which serves as a lasting message to be seamlessly incorporated into the various awareness campaigns and programs of (CISA), urging all individuals to remain vigilant in safeguarding themselves while online or when using connected devices; and

WHEREAS, the geographic isolation of Guam necessitates vital interconnection through physical infrastructure, thereby concentrating potential attack surfaces and increasing vulnerability to cyber threats across interconnected digital and physical systems; in addition, the geopolitical tensions underscore Guam's strategic significance, making it a potential target for influencing responses during regional crises; and

WHEREAS, foreign government-backed hackers have demonstrated the capability and intent to disrupt crucial communications between the United States and Asia by targeting utilities in Guam, necessitating the utmost coordination of defensive efforts among civilian, military, federal, and private partners; as critical utilities underpin both civilian services and military functions, it is imperative to prioritize the protection of operational technology; and

WHEREAS, the rapid pace of digitization has outstripped security adaptations, demanding workforce training to instill resilience, with emerging threats evolving faster than legal authorities can respond, necessitating flexible remediation capabilities and near real-time shared awareness to facilitate coordinated incident response among military, government, and National Guard Units; and

WHEREAS, previous weather disasters, including Typhoon Mawar, have exposed infrastructure weaknesses that could compound the potential cascading impacts of cyber disruptions on health, safety, and economic prosperity; and

WHEREAS, to truly achieve resilience, we must shift our perspective on networked infrastructure. Rather than viewing it as a single, interconnected system, we must see it as a collection of distributed "islands" to allow better assessment of threats and proactively address risks that emerge over time. By continuously reviewing our approach, we can ensure the safety and security of our infrastructure for years to come; and

WHEREAS, evaluating interdependencies across physical and digital infrastructure is critical for identifying the potential for cascading failures originating from single points of disruption; considering risk-informed segmentation options that allow critical utilities to isolate operations if necessary while balancing integration benefits; modeling the impacts of disruptive cyberattacks or combined cyber-physical scenarios to inform continuity of operations planning; and

WHEREAS, expanding the availability of cyber range and simulation facilities enhances training for critical infrastructure operators; partnering with federal

laboratories on tailored threat intelligence and detection tools for OT/ICS networking strengthens local defenses; testing multi-agency response playbooks through exercises enhances preparedness for integrated incident management; leveraging automated indicator sharing, where possible, through technologies like STIX/TAXII scales up protections against emerging tactics regionally; and

WHEREAS, establishing clear policies and procedures among stakeholders is essential for coordinated security and incident response; determining optimal centralization-decentralization constructs for local cyber coordination aligns with specialized requirements and assets; continuous benchmarking against peers and standards bolsters Guam's combined cyber and physical security posture and resilience over the long term, considering the increasing risks posed by disruptive ransomware and malware spreading through interconnected systems; and

WHEREAS, Guam's reliance on imports, including water, which relies partly on international systems and partners beyond local control, highlights the need for stronger protections for the Port Authority of Guam, utilities, and other essential services, including updated policies, standards, information sharing, and resources to uphold national security responsibilities alongside civil services; and

WHEREAS, long-term espionage conducted by foreign government-backed hackers has revealed their capabilities in targeting critical communications infrastructure on Guam, further complicated by the dependence on imported and third-party sourced equipment and software, introducing unmanaged vulnerabilities and insider threats due to concentrated expertise and access within Guam's utilities sector; workforce limitations and geographic isolation exacerbate phishing and social engineering risks, with credential theft posing a significant threat given the operational interdependencies across Guam's utilities; and

WHEREAS, the Government of Guam Cybersecurity Working Group (CWG) developed the Pacific CyberGuard: Kontra I Pligru Island-wide Cybersecurity Plan (PCG) as an Incident Annex to the Guam Emergency Response Plan, recognizing the

urgent need to bolster the security and resiliency of our island's digital environment, and to improve the accessibility and efficiency of digital systems; and

WHEREAS, the CWG engaged a diverse group of experts and stakeholders within our government agencies, local organizations and our federal partners to include the offices of Guam Homeland Security and Civil Defense (GHS/OCD), Mariana Region Fusion Center (MRFC), Office of Technology (OTECH), CISA, Guam Army National Guard, FBI, and the Coast Guard, to ensure a collaborative and inclusive process in the PCG's development; and

WHEREAS, the "whole of government" efforts culminated in the PCG and and is a "living document" that will assist all sectors of local government, including critical infrastructure and private sector partners, as well as communications providers, higher education institutions, finance health, election, transportation, commissions, boards and councils in the development of strategic processes and implementation of mature cybersecurity systems; and

WHEREAS, the PCG represents a significant measure in safeguarding our island's digital infrastructure to ensure the safety and security of our community, and in bridging gaps in technical assistance and support for cyber plan development and maturity; and

WHEREAS, the GHS/OCD and the OTECH are the administrators of the PCG and the designated cyber or information technology experts for the MRFC; as a division of the GHS/OCD, the MRFC collects, evaluates, and disseminates intelligence relating to criminal and terrorist activity in the Marianas and protects information networks and telecommunications networks from cyber attacks; and

WHEREAS, GHS/OCD will leverage technology and industry resources to enhance the security and efficiency of our digital systems, and improve the resilience of our digital environment. As our community grows and progresses, our people will continue to rely on the efficiency and security of digital engagement with our

government agencies and with each other setting a course toward ensuring a safe and reliable digital environment that meets the needs of our people in the days to come; and

WHEREAS, Guam's unique isolation and concentrated infrastructure necessitate consideration of the potential impacts of cyber or hybrid attacks, which could have far-reaching consequences, including disruptions to utility websites or data systems potentially compromising public health protections, especially during crises; the potential strategic advantages adversaries could gain through covert data collection from Guam's networks must also be addressed, and vital control interfaces supporting Guam's facilities and services should be safeguarded against misconfigurations; given the growing global threats of ransomware, data theft, and infrastructure sabotage, coordinated defenses are vital to mitigate these risks; now, therefore, be it

RESOLVED, that the Government of Guam places a high priority on developing a comprehensive cybersecurity strategy, which includes, Conducting of audits of critical infrastructure operators to identify and remediate high-risk vulnerabilities, with regular evaluations of controls using frameworks like National Institute Standards Training CSF; Mandating multi-factor authentication, access logging, patching, vulnerability scanning, and other fundamental security practices across government networks and essential services; Encourage coordination between relevant agencies, the private sector, and federal partners for detecting, containing, and learning from cyber incidents; Promoting awareness training to cultivate a culture of digital defense through workforce development initiatives; Assessing risks associated with supply chain dependencies, including mandatory testing of water imports, while securing and supporting local sources and contingency preparations; Reviewing authorities, response plans, and joint exercises to prepare for escalating or destructive cyber and hybrid threats; Modernizing critical infrastructure with network segmentation, monitoring, security-by-design principles, and the ability to isolate compromised systems; Allocating resources to prioritize long-term security improvements alongside short-term remediation, including budgeting for emerging challenges through technology upgrades; and Providing regular

reports to the Legislature on strategy implementation and emerging risks necessitating additional authorities or investments in the public interest; and be it further

RESOLVED, that *I Mina'trentai Siette Na Liheslaturan Guåhan,* does hereby, on behalf of the people of Guam, recognize Cyber Security Awareness Month 2023; and commend the collaborative efforts in demonstrating its importance of promoting cybersecurity awareness and preparedness to protect critical infrastructure; and be it further

RESOLVED, that the Speaker certify, and the Legislative Secretary attest to, the adoption hereof, and that copies of the same be thereafter transmitted to Frank L.G. Lujan, Jr., Chief Technology Officer; Major General Esther J.C. Aguigui, Guam Homeland Security Advisor; Charles V. Esteves, Administrator for the Office of Civil Defense; John M. Benavente, P.E., General Manager, Guam Power Authority; Miguel C. Bordallo, P.E., General Manager, Guam Waterworks; Joseph "Joey" T. Duenas, Chairman, Consolidated Commission on Utilities; Jeffrey C. Johnson, Chairman, Public Utilities Commission; Guam Chamber of Commerce, Guam Korean Chamber of Commerce, Chinese Chamber of Commerce Guam, Taiwanese Business Association of Guam; Rear Admiral Gregory C. Huffman, Commander, Joint Region Marianas; and to the Honorable Lourdes A. Leon Guerrero, *I Maga'hågan Guåhan*.

DULY AND REGULARLY ADOPTED BY *I MINA'TRENTAI SIETTE NA LIHESLATURAN GUÅHAN* ON THE DAY OF 2023.

THERESE M. TERLAJE **Speaker**	**AMANDA L. SHELTON** **Legislative Secretary**