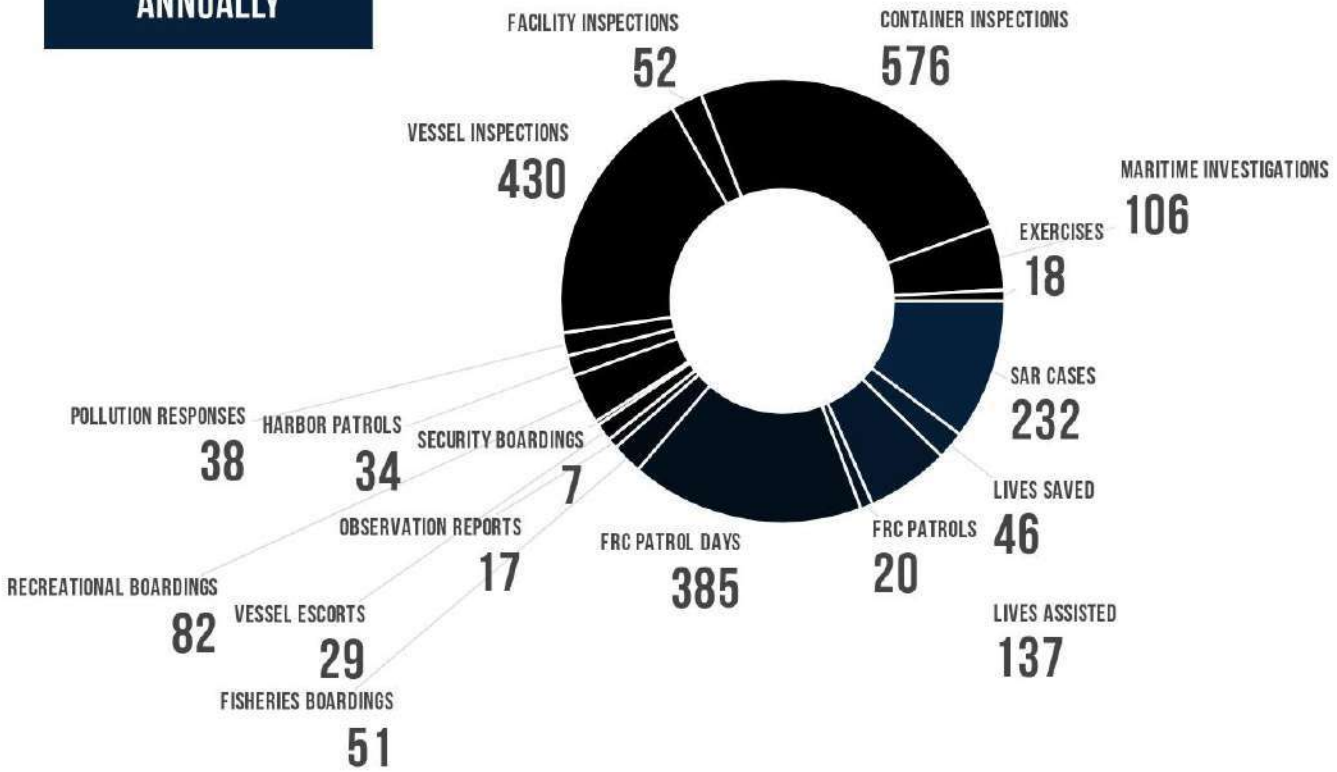
FY23 BY THE NUMBERS

USCG FORCES MICRONESIA SECTOR GUAM

2M TONS IN CARGO MOVE THROUGH GUAM MTS ANNUALLY

$675K PROPERTY SAVED



STRENGTHENING RESILIENCE: HEAVY WEATHER PREPAREDNESS & CYBERSECURITY IN PORT OPERATIONS

Presented by *CDR Greg Sickels, Deputy Commander*
November 2023

COMMANDER'S INTENT

PEOPLE FUNDAMENTALLY

Empowering Local Communities: Prioritize training and engaging local personnel in maritime safety practices, ensuring a deep-rooted understanding of regional challenges and fostering a culture of safety and security within the community.

UNIT RESOLUTELY

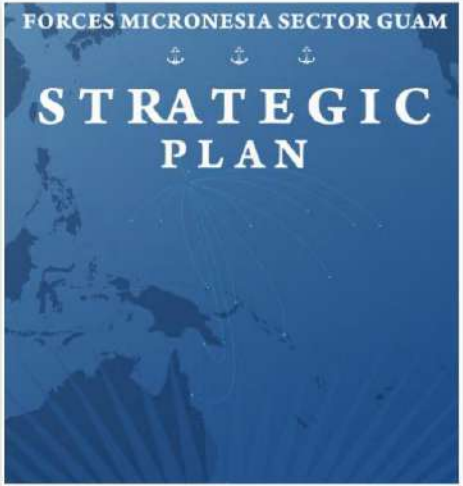
Strengthening Interagency Collaboration: Leverage the synergy of U.S. Coast Guard units with regional port authorities and other maritime agencies to build a cohesive and resilient front against maritime threats and emergencies.

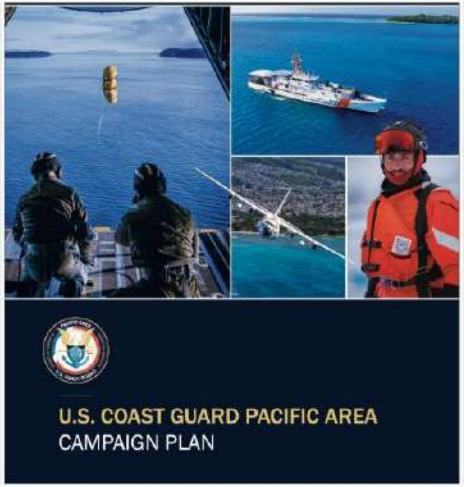
MISSION RELENTLESSLY

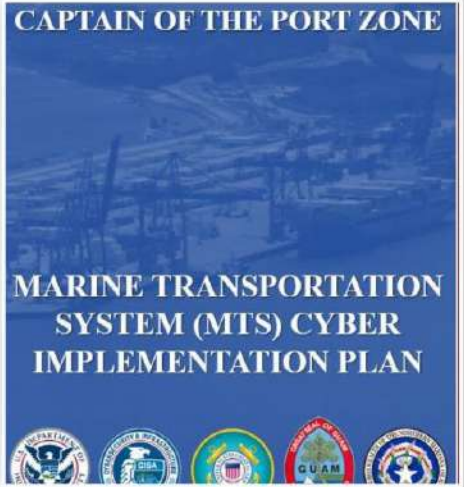
Remain committed to our mission in Micronesia: strengthening partnerships, rigorous patrols and monitoring to prevent illicit maritime activities, mitigating environmental hazards, and ensuring readiness to respond to emergent maritime threats.

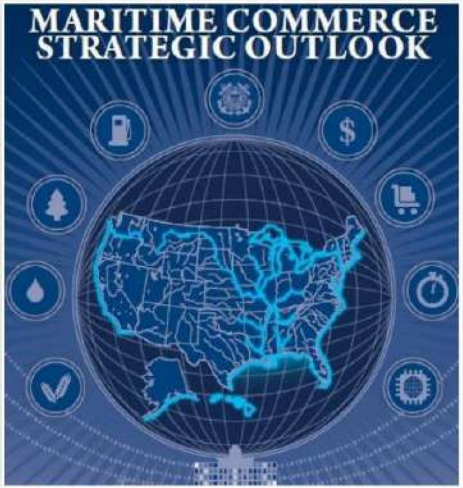
POLICY

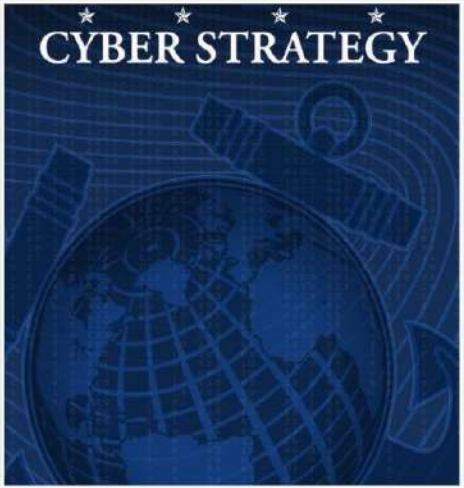
DOCUMENTS
and
PLANS

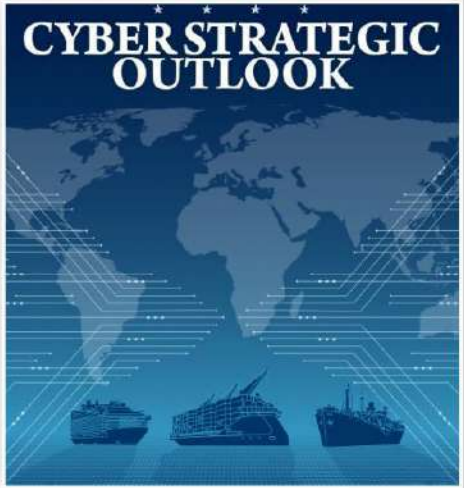




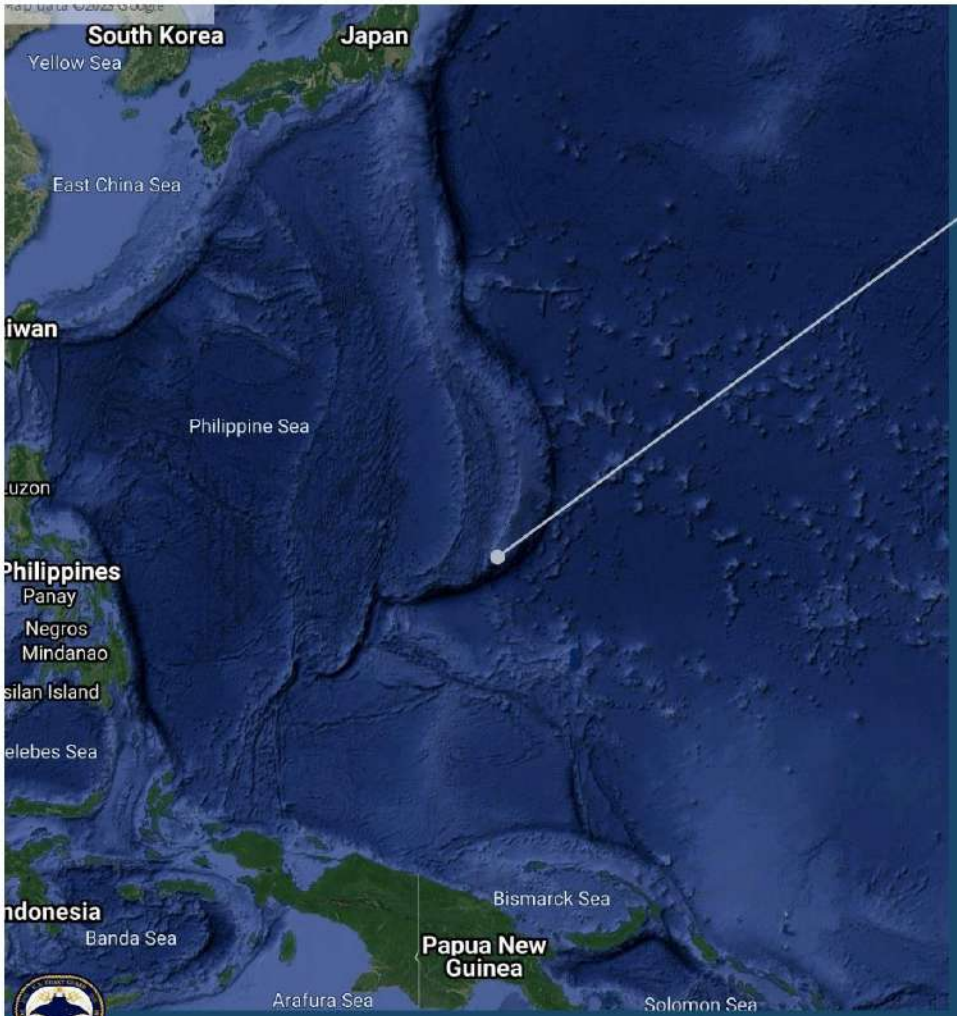








OUR RESIDENT TEAM AND CAPABILITIES



GUAM

US Naval Base, Guam

FM/SG

FORCES - DIVISIONS

JOINT RESCUE SUB-CENTER GUAM

STATION APRA HARBOR

MSD SAIPAN

CUTTERS

USCGC MYRTLE HAZARD

USCGC OLIVER HENRY

USCGC FREDERICK HATCH

MARINE TRANSPORTATION SYSTEM CRITICALITY

"The sea, the great unifier, is man's only hope. Now, as never before, the old phrase has a literal meaning: we are all in the same boat." - Jacques Yves Cousteau (French naval officer, oceanographer, filmmaker, and author)

THE MARINE TRANSPORTATION SYSTEM (MTS) IS VITAL TO REGIONAL NATIONAL SECURITY EFFORTS/OPERATIONS AND ECONOMIC PROSPERITY.

90% OF WORLD TRADE IS CONDUCTED VIA THE NETWORK OF PORTS, VESSELS, AND WATERWAYS THAT COMPRISE THE MTS.

COAST GUARD FORCES MICRONESIA –SECTOR GUAM'S AOR IS EXTREMELY MTS DEPENDENT. PUBLIC HEALTH, SAFETY, AND WELL-BEING ARE INEXTRICABLY LINKED TO MARITIME ENABLED FLOW OF GOODS AND SERVICES.

ANY SIGNIFICANT MTS DISRUPTION (CYBER OR OTHERWISE) WILL HAVE CASCADING AND DETRIMENTAL IMPACTS ACROSS THE WESTERN PACIFIC.

“THE COAST GUARD RELIED ON THREE PILLARS TO TAKE ON TYPHOON MAWAR. FIRST, THE ORGANIZATION RECOGNIZED GUAM’S METEOROLOGICAL AND GEOGRAPHICAL CHALLENGES, MAKING STRATEGIC—AND RELATIVELY LOW COST—INVESTMENTS TO POSITION THE COAST GUARD FOR SUCCESS IN ADDRESSING A WIDE RANGE OF LIKELY SCENARIOS. SECOND, IT RELIED ON THE ORGANIZATION’S BIAS—AND FREEDOM—FOR ACTION, POSITIONING ASSETS EARLY TO ADDRESS POTENTIAL RECOVERY CHALLENGES. AND THIRD, IT GOT TO WORK, COMPLETING DISASTER RESPONSE MISSIONS AN EFFICIENT, NO-NONSENSE MANNER.”

CRAIG HOOPER, FORBES MAGAZINE

HEAVY WEATHER PLAN - PRE-STORM PREPARATIONS

Our efforts prior to landfall from Typhoon Mawar

THE PLAN

The process of implementing the Heavy Weather Plan in Guam and CNMI

THE TEAM

Collaboration with port partners for storm preparation

THE STRATEGY

Strategies for container management to minimize vulnerabilities

COMMUNICATION DURING THE STORM

- Methods of maintaining constant communication with port partners
- Sharing critical operational updates during the storm

> “THE U.S. COAST GUARD’S DELIBERATE INVESTMENTS IN PRACTICAL, LOW-PROFILE CAPABILITIES, WHEN COUPLED WITH THE COAST GUARD’S LONGSTANDING “BIAS FOR ACTION,” IS A PERFECT RECIPE FOR GETTING THINGS DONE IN A PINCH.”

> “LEANING INTO AN ACTIVE RESPONSE PAID OFF. PLANNING DOCUMENTS DETAILING GUAM’S RESPONSE TO A CATASTROPHIC TYPHOON ASSUME STRONG CYCLONES WOULD CLOSE THE ISLAND’S SEAPORT—THE HEART OF THE ISLAND—FOR SEVEN TO TEN DAYS. INSTEAD, THE COAST GUARD NEEDED ONLY ABOUT 72 HOURS, OPENING GUAM’S PORT TO MILITARY, COMMERCIAL AND CARGO TRAFFIC ON MAY 28.”

POST-STORM ACTIONS AND PORT REOPENING

INITIAL ACTIONS

Steps taken in port damage assessment and collaborative efforts
(e.g., DPS in Rota, U.S. Navy's sonar usage, divers' involvement)

MAKING AN IMPACT

The role of port partnership in reopening the port within 72 hours

LESSONS LEARNED

1. KEY TAKEAWAYS
2. POTENTIAL IMPROVEMENTS
3. STRATEGIES FOR FUTURE HEAVY WEATHER EVENTS


Logistics
Section Chief


USCG


U.S.
COAST
GUARD


U.S.
COAST GUARD
DIVER
EOD MOBILE UNIT 5
DIVE LOCKER


45753
IMAGES OF MAWAR

PHYSICAL AND CYBER

PORT SECURITY

The importance of port security in the context of physical and cyber threats

PHYSICAL SECURITY (DOMESTIC)

According to the Code of Federal Regulations, 33 CFR Part 105, regulated maritime facilities in the United States are required to implement security measures to deter the unauthorized introduction of dangerous substances and devices into the facility.

ESTABLISHMENT OF SECURITY MEASURES

Facility owners must ensure unauthorized access is prevented.

INTEGRATION WITH SECURITY PLAN

Facility security plans should include measures to deter TSIs. Complementary measures are key.

IMPLEMENTATION AT VARYING MARSEC LEVELS

MARSEC levels require different security measures.

ACCESS CONTROL IN THE FACILITY SECURITY PLAN (FSP)

Authorized individuals and organizations only for vessel business; defined access control in FSP.

SCREENING AND SECURITY OF UNACCOMPANIED BAGGAGE OR CARGO

Owner/operator must screen cargo and unaccompanied baggage, ensure security in restricted area, and maintain control for transfers to or from vessel.

PHYSICAL SECURITY (INTERNATIONAL PORT SECURITY PROGRAM)

The U.S. Coast Guard IPS Program, established in 2003, is dedicated to supporting nations in improving their port security and ensuring the implementation of the ISPS Code. By working together, the U.S. Coast Guard and our partners aim to enhance maritime safety and security in the Blue Pacific region, benefiting all nations and the global maritime transport system.

RISK REDUCTION GOALS

The IPS Program focuses on reducing risks to U.S. ports, ships, and the global maritime transport system by evaluating anti-terrorism security measures in foreign ports.

BILATERAL SECURITY PRACTICE ALIGNMENT

Through assessments and discussions, the program aims to align and share port security practices internationally, offering mutual benefits.

IMPLEMENTATION AND COMPLIANCE WITH ISPS CODE

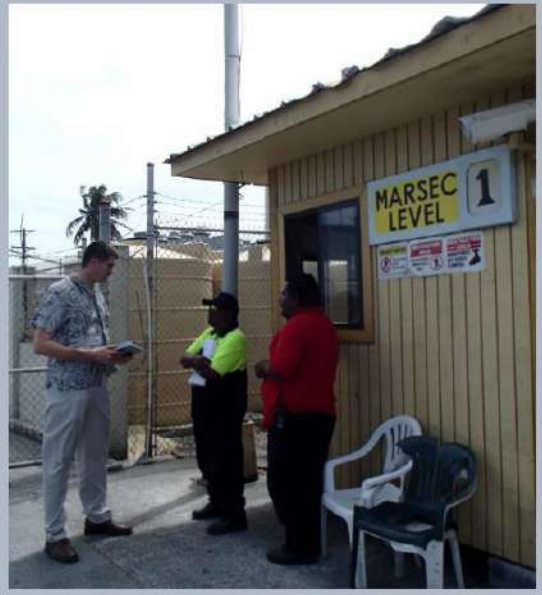
IPS Program ensures foreign ports adhere to ISPS Code and promotes improved security above minimum requirements.

PORT SECURITY ADVISORY AND COMPLIANCE MONITORING

The Coast Guard publishes a Port Security Advisory for foreign states that fail to maintain effective anti-terrorism measures, and continuously monitors compliance.

IMPACT ON U.S. PORT OPERATIONS

Adequate security measures in foreign ports lead to reduced targeting of vessels for port state control actions when arriving in the United States, streamlining maritime operations.



U.S. COAST GUARD CYBER LEGAL AUTHORITIES (REGULATORY)

PRESIDENTIAL POLICY DIRECTIVE 21 DESIGNATES THE U.S. COAST GUARD AS THE **SECTOR RISK MANAGEMENT AGENCY (SRMA) FOR THE MARITIME TRANSPORTATION SECTOR.**

THE U.S. COAST GUARD HAS BROAD LEGAL AUTHORITY UNDER THE MARITIME TRANSPORTATION SECURITY ACT (MTSA) TO REQUIRE PHYSICAL AND CYBER PLANNING FOR FACILITIES AND VESSELS.

TITLE 33 CODE OF FEDERAL REGULATIONS (CFR) SECTIONS 104, 105, AND 106 REQUIRE REGULATED FACILITIES AND VESSELS TO ADDRESS PHYSICAL AND CYBER VULNERABILITIES WITHIN ASSESSMENTS & PLANS.

THE INTERNATIONAL MARITIME ORGANIZATION (IMO) REQUIRES VESSELS SUBJECT TO THE IMO CODE TO INTEGRATE CYBER RISK MANAGEMENT INTO THEIR ONBOARD SAFETY MANAGEMENT SYSTEMS (SMS).

U.S. COAST GUARD CYBER LEGAL AUTHORITIES (PREVENTION AND RESPONSE)

46 U.S.C. 70116 -PORT, HARBOR, AND COASTAL FACILITY SECURITY

(A)GENERAL AUTHORITY. THE SECRETARY MAY TAKE ACTIONS DESCRIBED IN SUBSECTION (B) TO PREVENT OR RESPOND TO AN ACT OF TERRORISM, CYBER INCIDENTS, TRANSNATIONAL ORGANIZED CRIME, AND FOREIGN STATE THREATS AGAINST—

(1) AN INDIVIDUAL, VESSEL, OR PUBLIC OR COMMERCIAL STRUCTURE THAT IS -

(A) SUBJECT TO THE JURISDICTION OF THE UNITED STATES AND

(B) LOCATED WITHIN OR ADJACENT TO THE MARINE ENVIRONMENT; OR

(2) A VESSEL OF THE UNITED STATES OR AN INDIVIDUAL ON BOARD THAT VESSEL.

(B) SPECIFIC AUTHORITY. UNDER SUBSECTION (A), THE SECRETARY MAY…

46 U.S.C. 70116 -PORT, HARBOR, AND COASTAL FACILITY SECURITY

(B) SPECIFIC AUTHORITY. UNDER SUBSECTION (A), THE SECRETARY MAY…

(1) CARRY OUT OR REQUIRE MEASURES, INCLUDING INSPECTIONS, PORT AND HARBOR PATROLS, THE ESTABLISHMENT OF SECURITY AND SAFETY ZONES, AND THE DEVELOPMENT OF CONTINGENCY PLANS AND PROCEDURES, TO PREVENT OR RESPOND TO ACTS OF TERRORISM, CYBERINCIDENTS, TRANSNATIONAL ORGANIZED CRIME, AND FOREIGN STATE THREATS;…

46 U.S.C. 70116 -PORT, HARBOR, AND COASTAL FACILITY SECURITY

(3) DISPATCH PROPERLY TRAINED AND QUALIFIED, ARMED (AS NEEDED), COAST GUARD PERSONNEL ON VESSELS AND PUBLIC OR COMMERCIAL STRUCTURES ON OR ADJACENT TO WATERS SUBJECT TO UNITED STATES JURISDICTION TO DETER OR RESPOND TO ACTS OF TERRORISM, CYBER INCIDENTS, TRANSNATIONAL ORGANIZED CRIME, FOREIGN STATE THREATS, OR TRANSPORTATION SECURITY INCIDENTS, AS DEFINED IN SECTION 70101 OF TITLE 46, UNITED STATES CODE.

U.S. COAST GUARD CYBER LEGAL AUTHORITIES (AGENCY ASSISTANCE)

14 U.S.C. 701. COOPERATION WITH OTHER AGENCIES, STATES, TERRITORIES, AND POLITICAL SUBDIVISIONS

(A) THE COAST GUARD MAY, WHEN SO REQUESTED BY PROPER AUTHORITY, UTILIZE ITS PERSONNEL AND FACILITIES

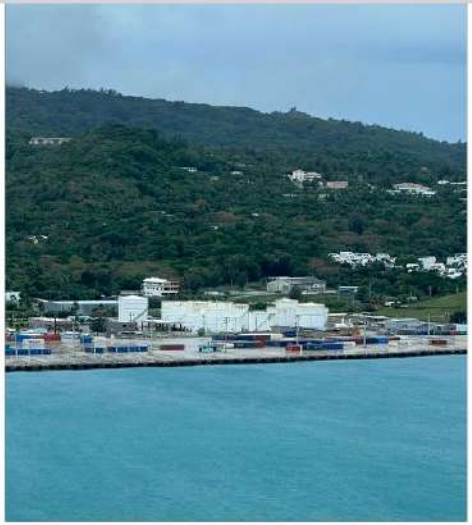
(INCLUDING MEMBERS OF THE AUXILIARY AND FACILITIES GOVERNED UNDER CHAPTER 39)

TO ASSIST ANY FEDERAL AGENCY, STATE, TERRITORY, POSSESSION, OR POLITICAL SUBDIVISION THEREOF, OR THE DISTRICT OF COLUMBIA, TO PERFORM ANY ACTIVITY FOR WHICH SUCH PERSONNEL AND FACILITIES ARE ESPECIALLY QUALIFIED.

THE COMMANDANT MAY PRESCRIBE CONDITIONS, INCLUDING REIMBURSEMENT, UNDER WHICH PERSONNEL AND FACILITIES MAY BE PROVIDED UNDER THIS SUBSECTION.

(B) THE COAST GUARD, WITH THE CONSENT OF THE HEAD OF THE AGENCY CONCERNED, MAY AVAIL ITSELF OF SUCH OFFICERS AND EMPLOYEES, ADVICE, INFORMATION, AND FACILITIES OF ANY FEDERAL AGENCY, STATE, TERRITORY, POSSESSION, OR POLITICAL SUBDIVISION THEREOF, OR THE DISTRICT OF COLUMBIA AS MAY BE HELPFUL IN THE PERFORMANCE OF ITS DUTIES.

IN CONNECTION WITH THE UTILIZATION OF PERSONAL SERVICES OF EMPLOYEES OF STATE OR LOCAL GOVERNMENTS, THE COAST GUARD MAY MAKE PAYMENTS FOR NECESSARY TRAVELING AND PER DIEM EXPENSES AS PRESCRIBED FOR FEDERAL EMPLOYEES BY THE STANDARDIZED GOVERNMENT TRAVEL REGULATIONS.



COOPERATION RANGING FROM THE CNMI ACROSS MICRONESIA TO THE RMI

USCG CYBER OPS IN THE MARIANAS

APRIL 2022

Release of Guam COTP Zone MTS Cyber Implementation Plan

SEPT 2022

Incorporation of cyber scenario in annual USCG-led Port Security Exercise

NOV 2022

Kick-off to DHS CISA Regional Resiliency Assessment Program

(Cyber component for Guam & CNMI)

DEC 2022

Submission date for Facility Security Plans (FSP) annexes; all facilities have submitted plans

JAN 2023

Marine Transportation System Specialist - Cyber (MTSS-C) civilian hire onboarded at Sector Guam

MARCH-APRIL 2023

Cyber technical assist mission (14 USCG 701) to Marianas Regional Fusion Center

JULY 2023

Participation in first Guam cyber summit alongside 100 cyber stakeholders, at a gathering hosted by the Guam National Guard, prompted by cyber attacks and Typhoon Mawar.

AUGUST 2023

First OT-specific discussion-based exercise scenario during AMSTEP full-scale eercise

OCT 2023

Cyber Risk Plan drafted and submitted to Captain of the Port for approval (Guam & CNMI)

NOV 2023

Presented USCG equities to local, federal and regional cyber disaster preparedness partners gathered for a two-day Central Pacific Cybersecurity Summit 2024.

OCT 2023

Development of cyber risk plans for Guam and CNMI and required reporting requirements

~JAN 2024

Locally-developed cyber tech specialist job aid to aid cyber and IT professionals during ICS driven events or in a UC stand up scenaio

2024

Potential cyber technical assist mission (14 USCG 701) to Pacific Island Country partners

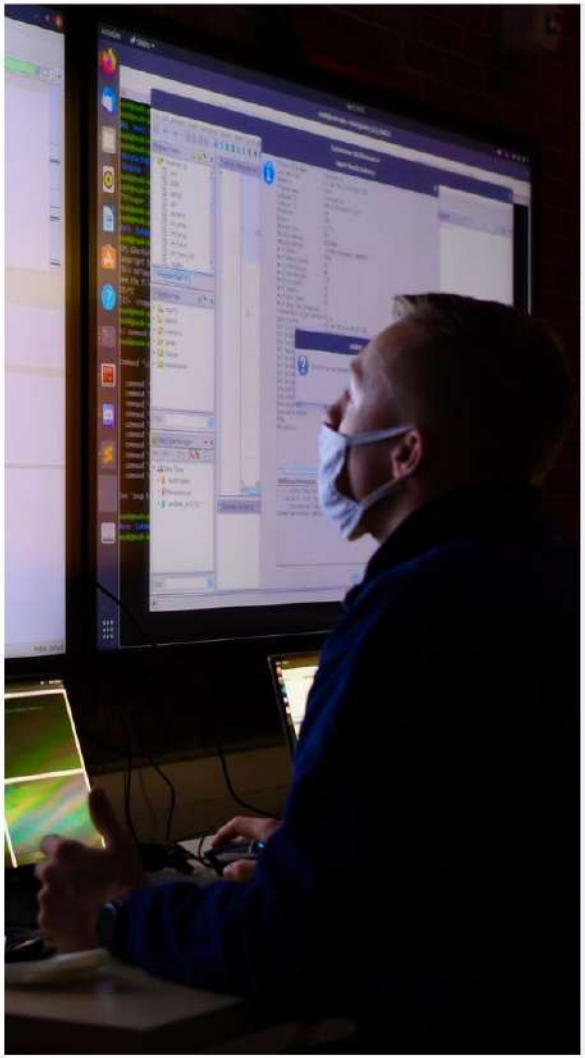
CYBER CASE STUDY

VOLT TYPHOON

Origin & Intent: People's Republic of China (PRC) threat actor "Volt Typhoon" targeted critical U.S. infrastructure, including Guam, focusing on information gathering and potential future attacks.

Stealth & Impact: Utilized "living-off-the-land" tactics for hard-to-detect intrusions, showing a relentless adaptation in espionage, particularly against military and critical networks.

Strategic Implications: This represents a significant shift in PRC cyber operations from economic espionage to targeting strategic assets, underlining the criticality of robust cyber defense mechanisms.



METHODS OF DETECTION

NETWORK TRAFFIC MONITORING

Identification of suspicious communications with known Volt Typhoon IP addresses, indicating unauthorized network access.

ANOMALY DETECTION

Employing advanced cybersecurity tools to detect unusual activities and patterns, indicative of a breach or espionage activities.

THREAT INTELLIGENCE SHARING

Collaboration with external cybersecurity agencies and private sector firms like Microsoft, which provided insights into the group's tactics and targets.

SYSTEM AUDITS AND FORENSICS

In-depth analysis of system logs and forensic investigation to trace the source and methods of the attacks, revealing stealthy "living-off-the-land" techniques.

IMPACTS

ESPIONAGE AND INFORMATION GATHERING

The primary intent seemed to be espionage, gathering sensitive data on U.S. military capabilities and critical infrastructure.

THREAT TO CRITICAL INFRASTRUCTURE

Targeting of essential services like power grids, water systems, and communications networks, posing a risk to national security and public safety.

STRATEGIC SECURITY CONCERNS

The involvement of a People's Repuublic of China state-backed group indicates a geopolitical dimension, raising concerns about the vulnerability of strategic assets in the event of a diplomatic or military conflict.

ADAPTIVE THREAT TACTICS

Demonstrates the evolving nature of cyber threats, with adversaries constantly adapting their methods to evade detection and maximize impact.

STRATEGIES AND MITIGATIONS

1. RISK ASSESSMENT AND MANAGEMENT
2. CYBERSECURITY TRAINING AND AWARENESS PROGRAMS
3. INFORMATION SHARING AND COLLABORATION
4. GUIDANCE AND BEST PRACTICES
5. INCIDENT RESPONSE PLANNING
6. CYBERSECURITY ASSESSMENTS AND AUDITS
7. TECHNOLOGY AND INFRASTRUCTURE UPGRADES
8. REGULATORY COMPLIANCE AND ENFORCEMENT
9. VULNERABILITY IDENTIFICATION AND MITIGATION
10. ENAGEMENT IN CYBER EXERCISES

CONTACT US

1 Victor Pier, Naval Base Guam, Santa Rita Guam 96915

+1 (671) 355-4800

@USCGForcesMicronesia

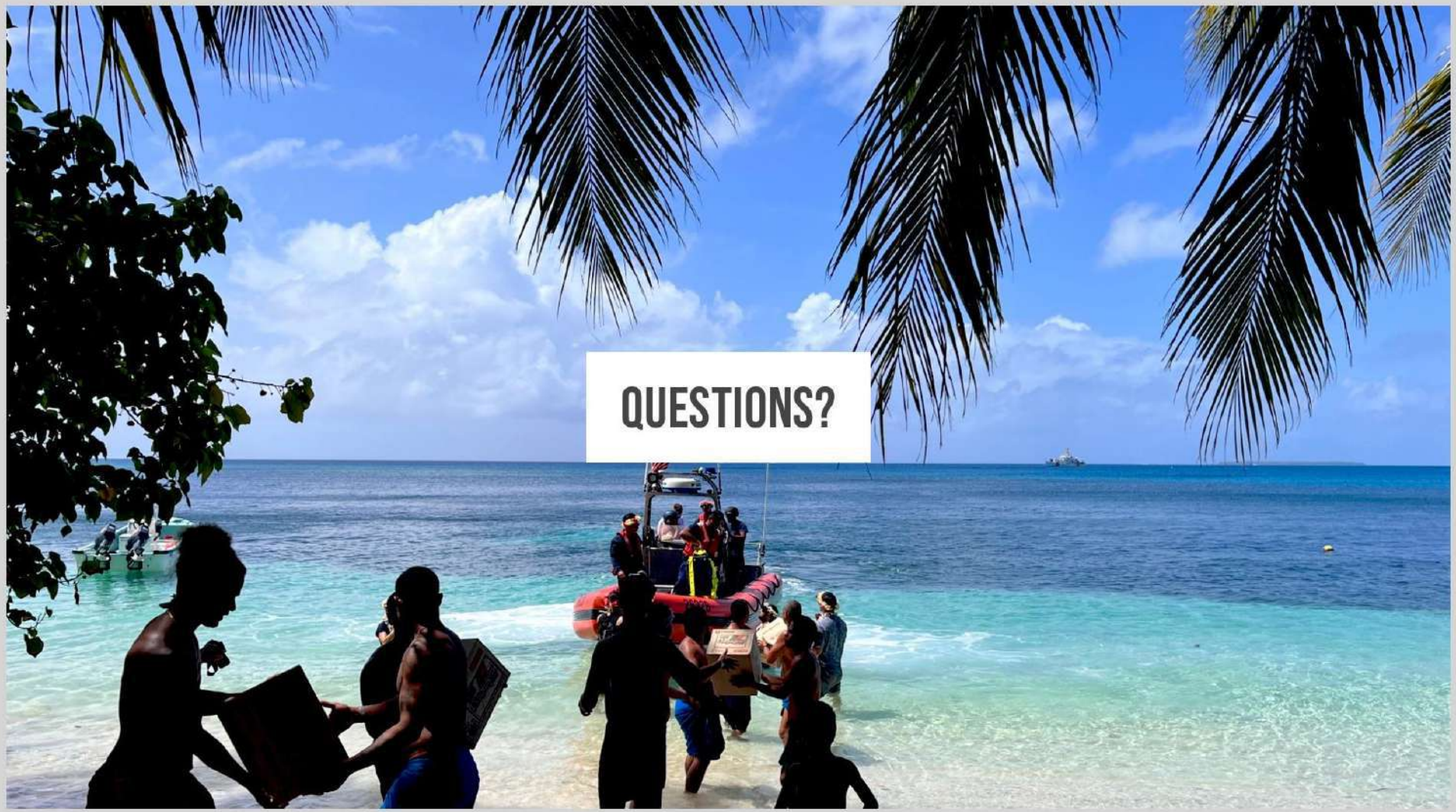
@USCGForcesMiconesia

@USCGFMSG

http://bit.ly/USCGForcesMicronesia

https://www.dvidshub.net/unit/USCG-FMSG

#FORCE4GOOD
#BLUEPACIFIC


QUESTIONS?