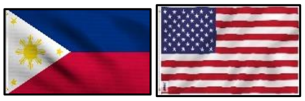
NETWORK DATA SHEET
SPECIAL INSTRUCTIONS (SPINS) SUPPLEMENT
BI-LATERAL OPERATIONS
at
PHILIPPINE ISLANDS



MSN: 25-1-BALIKATAN

06 January 2025

Prepared By:

USINDOPACOM

DISCLAIMER: The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. This document may not be cited for purposes of advertisement.

Table of Contents

(U) SPINS OVERVIEW

(U) These special instructions (SPINS) codify procedures and processes for the BALIKATAN 2025-1 mission executed by the USFPI and AFP cyber defenders.

(U) Commanders will ensure unit leadership, planning staffs, and crews are thoroughly familiar with the procedures and processes listed in the USINDOPACOM MNF Standard Operating Procedures and these SPINS prior to executing BALIKATAN Defensive Cyber Operations (DCO) missions. SPINS review shall be an integral part of training for all members assigned/attached to the MNF DCO teams.

(U) Readers will ensure the most recent version of this document is used.

(U) These standing SPINS are in effect from release into the field, until superseded or at the conclusion of the mission.

(U) MISSION

(U) The Combined Force Commander has tasked the DCO units to provide unique cyberspace capabilities to the defense of the PHILIPPINE ISLANDS against hostile acts from PANGEA (PNG) and allied actors.

(U) PNG claims rights to the Philippine Islands due to real estate acquisitions they have made within Luzon and Palawan. PNG has a long-standing and advanced cyberspace operations program. PNG military strategists grasped the advantages of using cyberspace operations to support kinetic operations. For the past three decades, the PNG military has been developing cyber operators. Some of their early pioneers were educated in Western computer science programs. They brought their knowledge back to PNG and established training programs at many of the post-secondary schools in the country. PNG has expanded its development and recruitment into its elementary school system.

(U) In attempts to escalate the situation in the Philippine Islands, PNG forces have continued to perform harassment operations, performing fly-overs of Philippine territory, harassing mariners in the South China Sea, and increasing cyber operations. The PNG Navy has continued to perform unauthorized boardings and confiscation of merchant vessels.

(U) Because of PNG's recent cyber actions on port facilities, it is assessed that the cyber campaign will attempt to induce confusion and loss of services to commercial and military ship movements.

(U) In response to sanctions and failed diplomatic efforts to deescalate tensions between PNG and the Philippines, the combined force commanders have been requested by the Philippine government to protect Critical Infrastructure systems affecting the Luzon and Palawan regions.

(U) COMMAND RELATIONSHIP

(U) As a DCO team, you will report to, and receive information/ direction from, the Bi-Lateral Cyber Defense Operations Center (CDOC). Direction, guidance, and information will flow from external organizations (Operational Units, Law Enforcement, Intel) to the DCO Cell and down to the DCO teams. The CyberCENTS Knowledge Center ("Learning Management System (LMS)") will be used to manage the flow of information.

(U) COMMUNICATIONS

(U) It is important for both DCO teams and CDOC to have a common understanding of the threat(s) and which pre-approved actions (PAA)/pre-coordinated actions (PCA) will be employed during mission execution. This intent will allow the appropriate PAA/PCA to be executed/incorporated at the right level and right time during mission operations. This should allow the operators to execute the PAA's/PCA's without excessive time delay.

(U) Communication for investigations involving potential insider threat or sensitive Defensive Counter Cyber (DCC) operations will be reported to trusted agents within law enforcement. The mission partner Commander and DCO Team Lead will maintain a current POC list.

(U) Communication/Collaboration methods tables are listed in **Table A**.

(U) Table A. Communication/Collaboration Methods (See Appendix)

(U) Given the limited availability, Voice Over Secure Internet Protocol (VOSIP) contact information is listed for organizations only.

(U) The following organizations in **Table B** represent Friendly Network Forces (FNF) and mission partner forces responsible and/or vested in the execution of the DCO operations. In the event that obfuscated communications are a necessary defensive tactic, the following call signs will be utilized to execute and facilitate operations.

(U) Table B. Call Signs (See Appendix)

(U) Communication Contracts

(U) Teams will submit Requests for Services (RFSs), Requests for Information (RFIs), and Situational Reports (SITREPs) using the Reporting Tool within the Learning Management system by selecting which type of report you are trying to file and filling in the pertinent information. A courtesy message should be sent using the Command

Channel chat at http://www.portal.com in the range, as discussed in the following paragraphs.

(U) Required Friendly Force Information Requests (FFIRs) and Requests for Information (RFIs) fields in the LMS Reporting Tools:

- Report Type
- Report Number (i.e., Naming Convention – CLB-001)
- Team
- Subject and/or Condition
- PAA or PCA Reference
- Authorized Duration
- Description for RFI/RFF/RFS, IOCs for SITREP
- Add Artifacts
- Needs and/or Requests

NOTE: If submitting an RFI, BE VERY SPECIFIC on what it is you are requesting.

(U) Teams will submit RFSs to the CDOC using Command Channel chat at http://www.portal.com in the range. The required fields for RFSs is as follows:

- Report Type
- Report Number (i.e., Naming Convention – CLB-001)
- Team
- Subject and/or Condition
- PAA or PCA Reference
- Authorized Duration
- Description for RFI/RFF/RFS, IOCs for SITREP
- Add Artifacts
- Needs and/or Requests

(U) Stakeholders, listed in **Table C**, will respond as soon as possible.

(U) Table C. Points-of-Contact (See Appendix)

(U) Situational Reports (SITREPs) will be submitted using the Command Chat at http://www.portal.com in the range. The format for SITREPs is as follows:

- Report Type
- Report Number (i.e., Naming Convention – CLB-001)
- Team
- Subject and/or Condition
- PAA or PCA Reference
- Authorized Duration
- Description for RFI/RFF/RFS, IOCs for SITREP
- Add Artifacts
- Needs and/or Requests
- Observed Tactics, Techniques and Procedures
- Attack Vector Used
- Assets Affected
- Expected Impact
- Priority Level
- Actions Taken
- Mitigations Used
- Time of Mitigation
- Restoral Procedure Used
- Time Restored
- Additional Comments

(U) DO NOT wait to submit reports after having all information submitted. This is a living document. In the initial report, put as much information as known and submit to the CDOC.

(U) Table D determines reporting criteria.

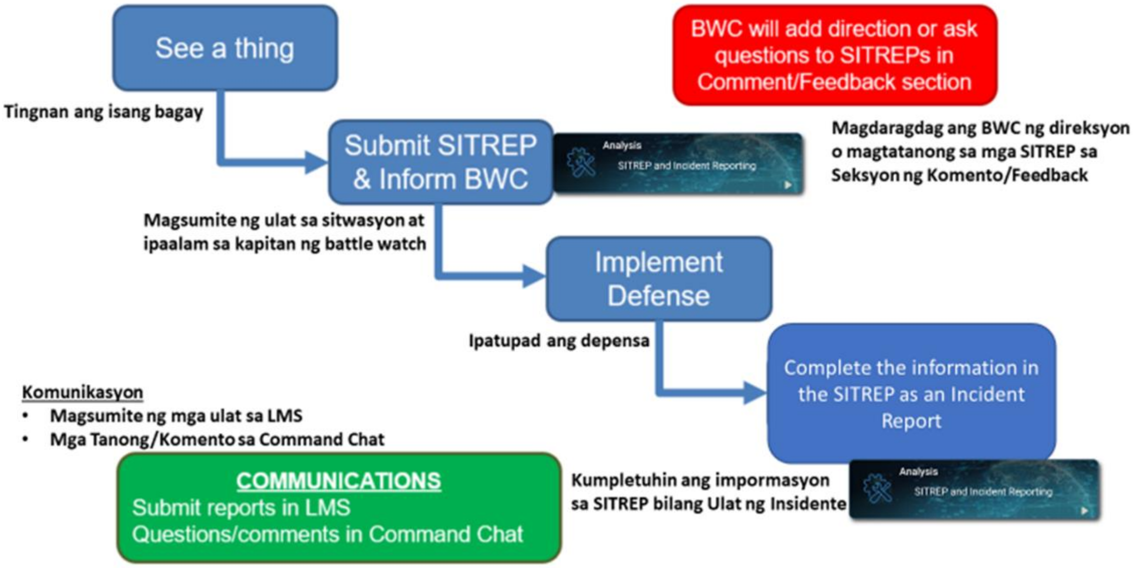
(U) Table D. Contracts (See Appendix)

(U) Threat Collaboration and Reporting will be performed using the following process:

1. Submit initial general discussion and initial reports via the https://www.*portal.com Rocket Chat Command Chat* in-range.
2. Submit the detailed information for initial contacts to the CDOC using the SITREP in the Learning Management System Reporting Tool.
3. After the teams verify activity as malicious, the CDOC will submit the formal incident report.
4. Acknowledgements will be made using all three of the above reporting tools.
5. New information and alerts will be disseminated to DCO teams using the Intelligence Database tool in the CyberCENTS Knowledge Center.

(U) The diagrams below (**Figures 1-3**) display the work flow for reporting.

Situation Reports (SITREPs) and Incident Reporting



See a thing

Tingnan ang isang bagay

BWC will add direction or ask questions to SITREPs in Comment/Feedback section

Submit SITREP & Inform BWC

Magdaragdag ang BWC ng direksyon o magtatanong sa mga SITREP sa Seksyon ng Komento/Feedback

Magsumite ng ulat sa sitwasyon at ipaalam sa kapitan ng battle watch

Implement Defense

Ipatupad ang depensa

Complete the information in the SITREP as an Incident Report

Komunikasyon
- Magsumite ng mga ulat sa LMS
- Mga Tanong/Komento sa Command Chat

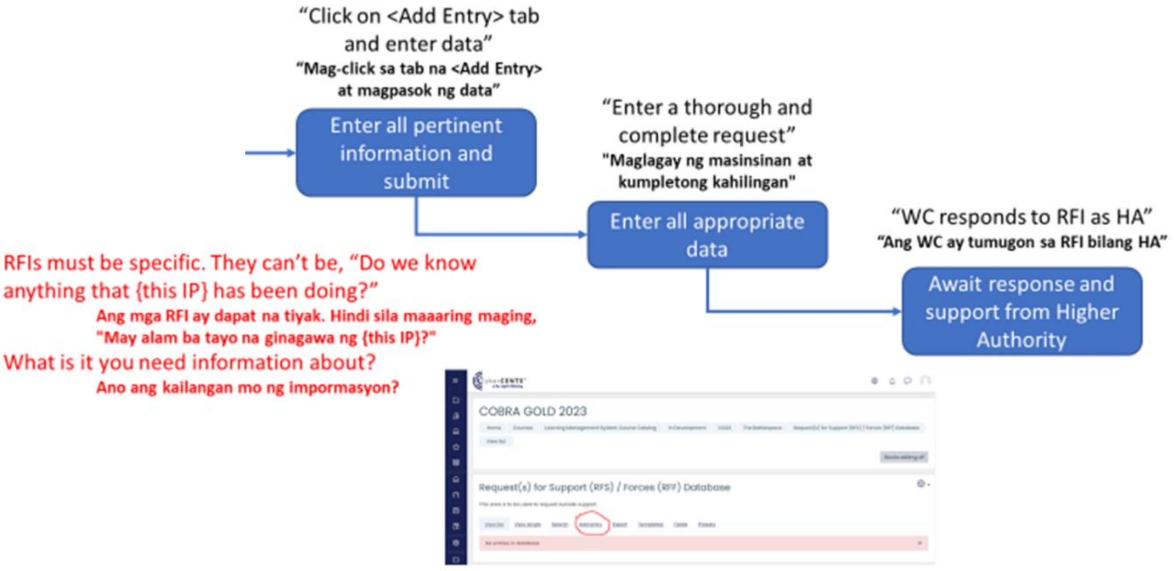
COMMUNICATIONS
Submit reports in LMS
Questions/comments in Command Chat

Kumpletuhin ang impormasyon sa SITREP bilang Ulat ng Insidente

Figure 1. Incident Report Work Flow

Request for Information (RFI) Process

Kahilingan para sa Proseso ng Impormasyon



"Click on <Add Entry> tab and enter data"
"Mag-click sa tab na <Add Entry> at magpasok ng data"

Enter all pertinent information and submit

"Enter a thorough and complete request"
"Maglagay ng masinsinan at kumpletong kahilingan"

Enter all appropriate data

"WC responds to RFI as HA"
"Ang WC ay tumugon sa RFI bilang HA"

Await response and support from Higher Authority

RFIs must be specific. They can't be, "Do we know anything that {this IP} has been doing?"
Ang mga RFI ay dapat na tiyak. Hindi sila maaaring maging, "May alam ba tayo na ginagawa ng {this IP}?"

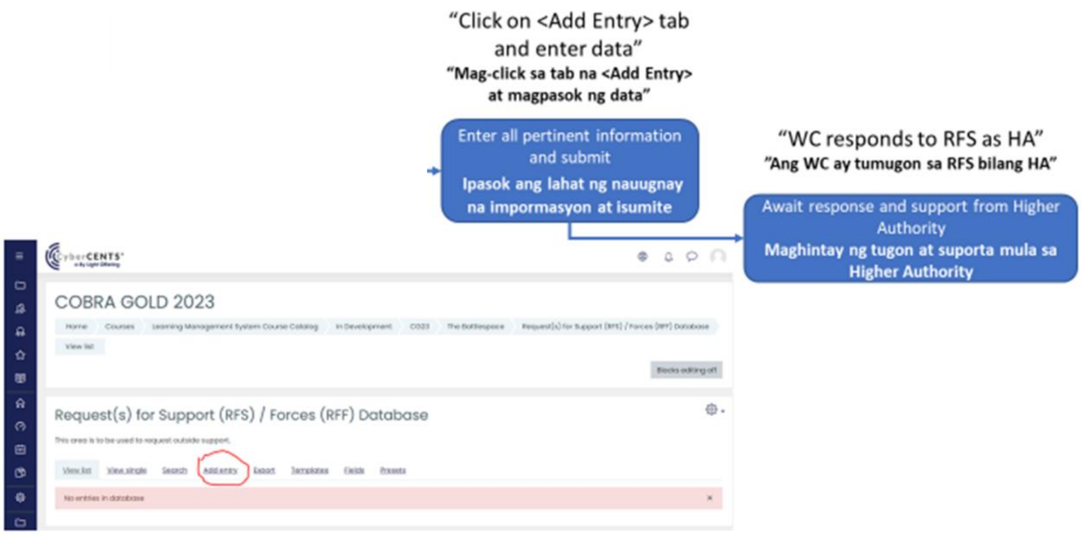
What is it you need information about?
Ano ang kailangan mo ng impormasyon?

COBRA GOLD 2023

Request(s) for Support (RFS) / Forces (RFF) Database

Figure 2. RFI / CCIR Work Flow

Request for Services (RFS)/Request for Forces (RFF) Process
Kahilingan para sa Mga Serbisyo/Kahilingan para sa Forces Proseso



"Click on <Add Entry> tab and enter data"
"Mag-click sa tab na <Add Entry> at magpasok ng data"

Enter all pertinent information and submit
Ipasok ang lahat ng nauugnay na impormasyon at isumite

"WC responds to RFS as HA"
"Ang WC ay tumugon sa RFS bilang HA"

Await response and support from Higher Authority
Maghintay ng tugon at suporta mula sa Higher Authority

COBRA GOLD 2023

Home
Courses
Learning Management System Course Catalog
In Development
CG23
The Battlespace
Request(s) for Support (RFS) / Forces (RFF) Database
View list
Blocks editing off

Request(s) for Support (RFS) / Forces (RFF) Database

This area is to be used to request outside support.

No entries in database

Figure 3. RFS / RFF Work Flow

(U) The CDOC will keep an open dialogue with law enforcement agencies. The CDOC will disseminate intelligence/threat related information regarding activity associated with the DCO team operation.

(U) NETWORK TOPOLOGY

(U) The following pictures and diagrams are an example of the various network devices (servers, routers, workstations, defensive structures) contained in the mission partner network (**Figure 4**). DCO team sensors will monitor network activity within the network. The DCO team will concentrate efforts on Mission Key Terrain – Cyber (MKT-C) shown in **Figure 5** and **Figure 6**. Refer to the Mission Owner Network Diagrams in the Learning Management System for specific topology diagrams.

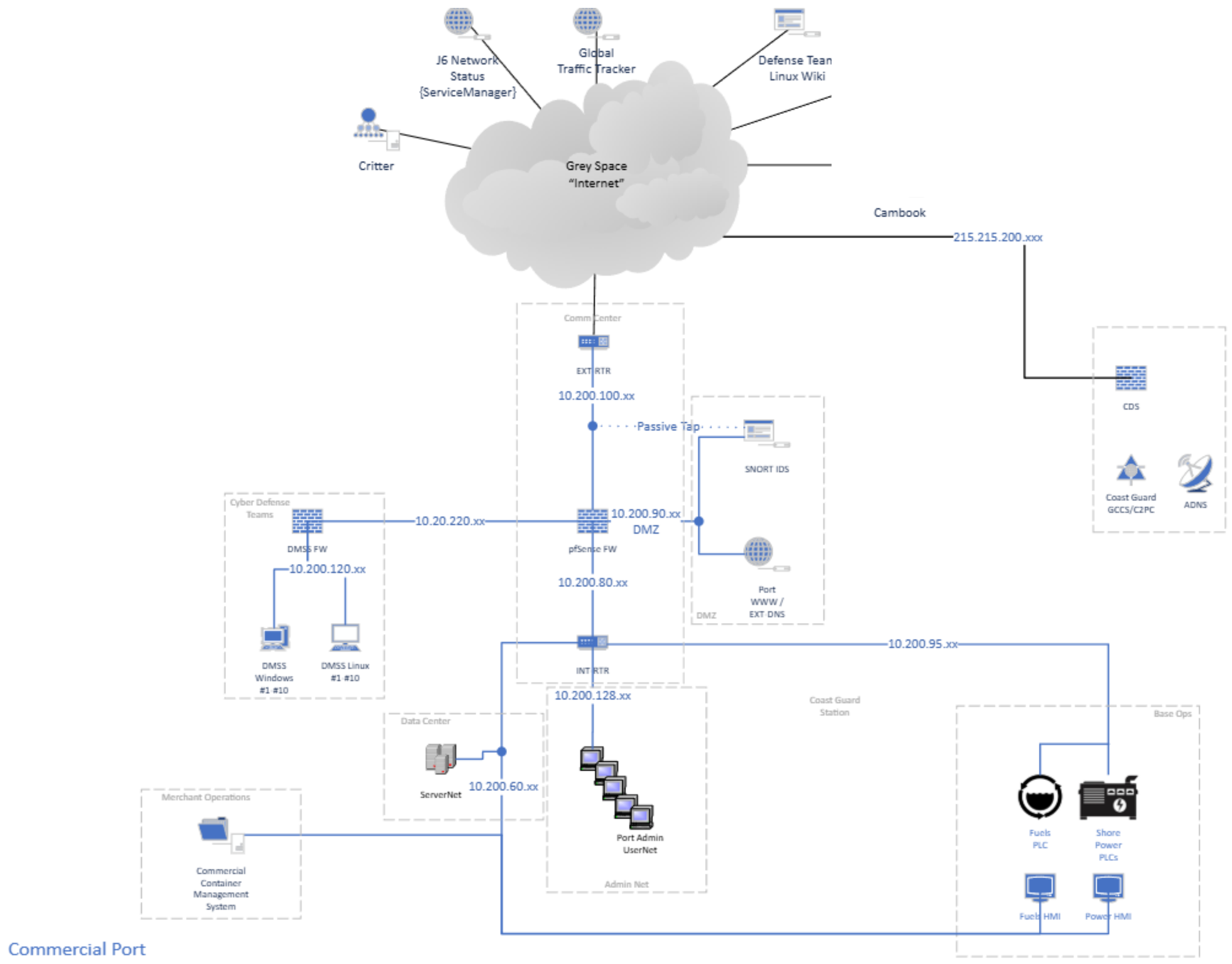


Figure 4. BALIKATAN Mission Owner Network Architecture

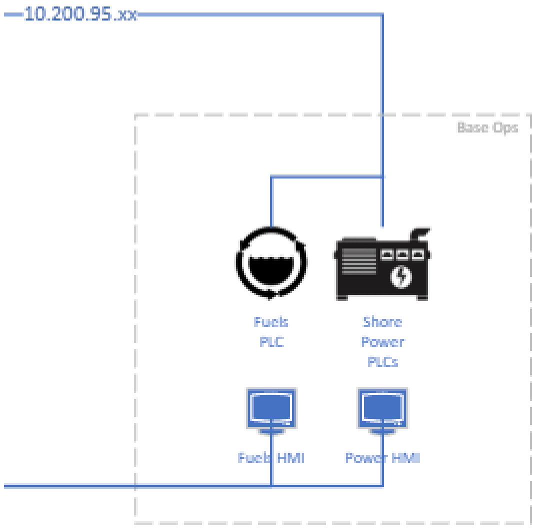


Figure 5. Mission Key Terrain - Cyber (MKT-C)

(U) C6 NETWORK STATUS REPORTING

(U) During operations, C6 will maintain the CYDEX network statuses via http://www.cybex.com (in-range) or using the link provided in the BALIKATAN Theater in the LMS.

(U) SITUATIONAL AWARENESS INFORMATION GRID

(U) **Table E** defines three defensive Areas of Responsibility (AOR) for Friendly Network Forces (FNF) and mission partners, as well as collateral units. It is not uncommon for FNF to identify reportable information that is not in the Defended Asset List (DAL), so this table summarizes the systems in each network AOR. **Table F** provides credentials for major systems on the network. **Table G** provides a Situational Awareness Grid providing FNF force responsibilities.

(U) Teams will also be responsible for securing the **Global Control and Command System (GCCS)** which provides situational awareness to commanders for ongoing military operations.

(U) ROE/PAA/PCA DECISION CHART

(U) Rules of Engagement (ROE) are defined in **Table H**.

(U) PAA (shown in **Table I**) execution authority lies with the DCO team, if in accordance with ROEs. DCO Team Leads will utilize the decision chart (**Figure 7**) to execute their delegated PAA. When used with the ROEs and PAAs/PCAs, the decision matrix chart provides the DCO team with the flexibility to operate without constant communication with the mission partner.

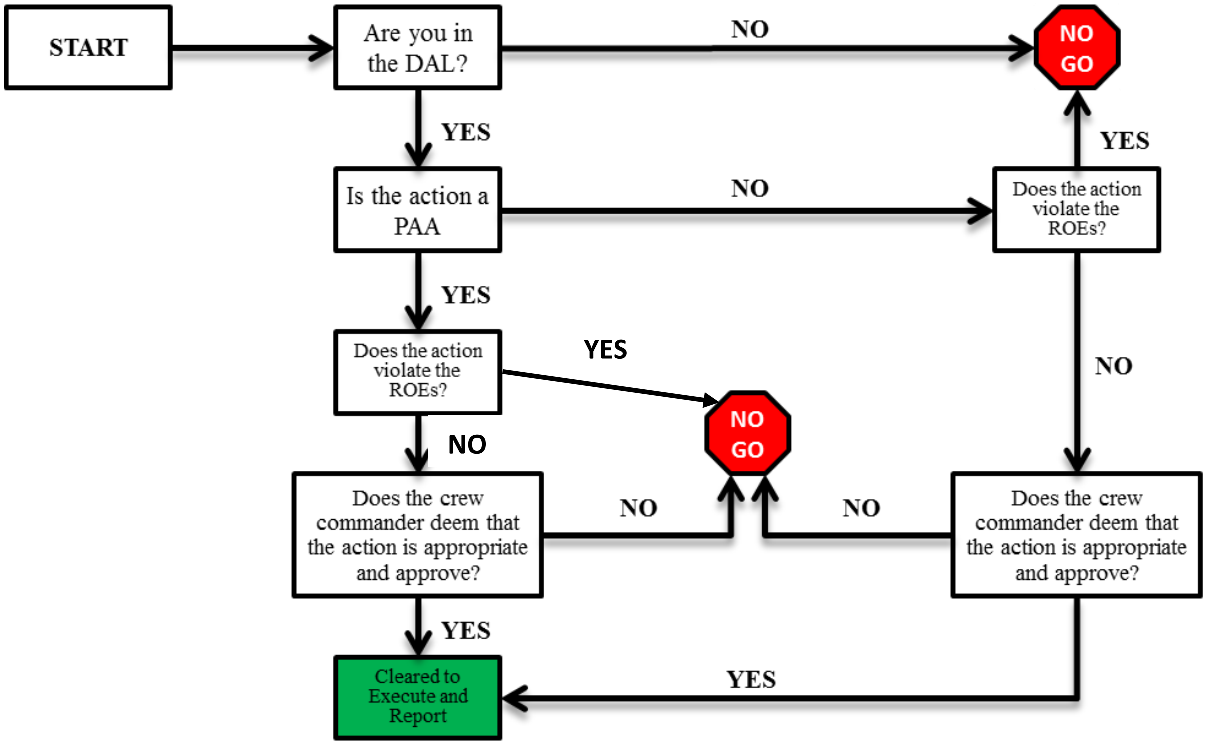

START
Are you in the DAL?
NO
NO GO
YES
Is the action a PAA
NO
YES
Does the action violate the ROEs?
YES
Does the action violate the ROEs?
YES
NO
NO GO
NO
Does the crew commander deem that the action is appropriate and approve?
NO
NO
Does the crew commander deem that the action is appropriate and approve?
YES
Cleared to Execute and Report
YES

Figure 6. Decision Chart

(U) PRE-COORDINATED ACTIONS

(U) Pre-coordinated actions (shown in **Table J**) must be approved by the CDOC and mission partner before execution. Once approved, the DCO team is required to notify both the CDOC and mission partner 10 minutes prior to execution.

(U) No Strike Zones are listed in **Table K**.

(U) REMOTE OPERATIONS INFORMATION

(U) To facilitate rapid response and effective operations, the DCO team will need a network connection facilitating two-way, IP-based communication from the toolkits on the mission network.

(U) The mission partner primary and alternate POCs supporting this operation have been identified in **Table C**.

Appendices

Table A. Communication/Collaboration Methods

Priority	Method	Details
Primary External	Rocket Command Chat	Internal Team Communication Chats and initial reporting using www.portal.com.
Primary External	LMS Reporting Tool	Details on Incident Reporting, RFS/RFF, RFI/FFIR.
Secondary	VoIP Phone	Each domain contains at least one VoIP user workstation.
Teritary	Phone	All communications.

Table B. Organization Call Signs

ORGANIZATION	CALLSIGN
CDOC	OVERWATCH
Team 1 – AFP Camp A-1	CAA
Team 2 – AFP Basa	BAA
Team 3 – AFP Clark	CLA
Team 4 – US Clark	CLB
Team 5 – US Basa	BAB
Team 6 – US Camp A-1	CAB1
Team 7 – US Palawan	PLB
Team 8 – US Subic Bay	SBB
Team 9 – US Camp A-3	CAB3
Team 10 – US Camp A-2	CAB2
Team 11 – AFP Palawan	PLA

Table C. Mission Partner Points-of-Contact (Individuals)

Name	Office	DSN	NIPR E-mail
MAJ Gilber Torres	AFP Planner		mightythors53@gmail.com
MAJ Plamin Rabino	Exercise Director		plamin.rabino@army.mil
Sean McDermott	EXCON		sean.mcdermott@pwc.pacom.mil
Greg Smith	EXCON Range Int		gregory.smith@bylight.com

Table D. Contracts

Activity	Content	Frequency	Initiator	Recipient
Notification of Routine PAA Execution (PAA 1-8)	Day, Time, IP, Host, Effect, Unit, Who Authorized	As Needed	DCO Team	CDOC
Notification of Non-Routine PAA Execution (PAA 9)	Day, Time, IP, Host, Effect, Unit, Who Authorized	Within 5 minutes of execution	DCO Team	CDOC
Traffic Validation/Query	Date, Time, Source IP, Destination IP, Service	Within 2 hours of discovery	DCO Team	CDOC
Weapon System Maintenance Activity	Weapon System Component, Timeframe	24 hours prior to event	DCO Team	CDOC
Mission Partner Maintenance Activity	System Component, Timeframe	24 hours prior to event	Mission Owner	DCO Team
Notification of Suspicious Activity	Date, Time, Description of Behavior, Affected Systems, Impact (Cyber Incident Report Fields)	Within 10 minutes of identification	DCO Team	CDOC

Table E. Defended Asset List (DAL)

IP RANGE	TEAM	AREA/DOMAIN	GATEWAY
10.2XX.0.0/16	ALL	cybexX.mil	10.2XX.0.1
10.2XX.90.0/24	ALL	DMZ	10.2XX.90.1
10.2XX.60.0/24	ALL	Domain Servers / ICS HMIs	10.2XX.60.1
10.2XX.128.0/24	ALL	User Net (Network Owner Workstations)	10.2XX.128.1
10.2XX.120.0/24	ALL	DMSS (DCO Workstations)	10.2XX.120.1
215.216.200.xxx/24	ALL	Mission Systems (FCCS, BC)	215.216.220.1
10.2xx.95.xx/24	ALL	ICS PLCs	10.2xx.95.1

Table F. Network Credentials

USERNAME	PASSWORD	Device/System	NOTES
admin	P@55w0rd!	PFSense Web GUI	
root	P@55w0rd!	PFSense CLI	
snort	P@55w0rd!	Snort Web GUI	
root	P@55w0rd!	Snort CLI	
{domain}\administrator	P@55w0rd!	Domain Admin	
Request from MP	Request from MP	Help Desk	
{domain}\cents	P@55w0rd!	Domain user	
administrator	P@55w0rd!	WWW/EXT-DNS	
administrator	P@55w0rd!	EWS	
cents	P@55w0rd!	FCCS	
cents	P@55w0rd!	BCCS	
cents	P@55w0rd!	HMI Systems	
root	P@55w0rd!	PLC Systems	
cents	P@55w0rd!	Kali Workstations	
cents	P@55w0rd!	Fuels Simulation	
Request from MP	Request from MP	Local administrators	
Contracted Services			
Denis Hotaki		denis.hotaki	Domain Administrator
Olaf Gustavson		olaf.gustavson	Domain Administrator
Tod Wettach		tod.wettach	Domain Administrator
Kenneth Gleason		kenneth.gleason	Domain Administrator
Cherise Elkstrand		cherise.elkstrand	Domain Administrator

Table G. Situational Awareness Information Grid

NETWORK AOR	RANGES / ID (if available)	DEFENSE PRIMARIES
Internet	Non-DoD Net Ranges	OVERWATCH
Server Net	10.2xx.60.xx	
User Net	10.2xx.128.xx	
CPT/DCO Net	10.2xx.120.xx	
ICS/SCADA PLCs Net	10.2xx.95.xx	
Mission System Net	215.216.220.xxx	
DMZ	10.2xx.90.xx	
LAN Switch	10.2xx.80.xx	
LAN-to-WAN Switch	10.2xx.100.xx	
WAN Router Net	10.2xx.0.xx	OVERWATCH

Table H. Rules of Engagement

ROE #	DESCRIPTIONS
1	DCO operations on DAL systems are approved per PAA 1-9
2	DCO activities not included in PAAs/PCAs 1-9 require prior authorization and coordination with mission partner
3	Engagement of adversary on DAL systems requires PRIOR approval and coordination with the CDOC and mission partner.
4	If a classified message incident (CMI) occurs, investigation will be coordinated by the mission partner and the CDOC. The mission partner commander has the authority to eliminate data spillage on network systems and devices, to include DCO Team weapon system components as applicable. The mission partner commander has authority to direct appropriate sanitation actions for DCO Team systems.
5	No Strike List - off limits (no pinging, scanning, enumeration, changing passwords, blocking IPS, or Disabling) for this exercise.
6	Plan Brief Execute Debrief (PBED) - must be done daily (more frequently, if warranted)
7	Configuration changes – Approval by the team NCOIC/OIC, Mission Partner, and CDOC must occur prior to making configuration changes. Changes must be documented and a risk / impact analysis should be done.
8	Crew Discipline and Professionalism a) Communication and Deconfliction – strong communication/team-work must occur in all directions (between crew members, up to the leadership, and from leadership down). b) Take the time to listen to others and be respectful of others thoughts and opinions. c) Speak up if you have an idea or feel strongly about something. d) Provide constructive feedback to team lead and MNF J6 POCs.
9	Physical infrastructure for exercise is OFF-LIMITS (ie workstations, wireless router, etc)

Table I. Pre-Approved Action (PAA) Description

PAA #	PAA DESCRIPTIONS
PAA1	Conduct credentialed and non-credentialed scanning of the network (example: port/service discovery, banner grabbing, host discovery, vulnerability scanning, enumeration of the network)
PAA2	Generate remote interactive sessions (example: ssh, vnc, rdp, winrm, PowerShell).
PAA3	Colledt operating system, service, and/or application logs from devices.
PAA4	Terminate/manage processes spawned as part of CPT actions.
PAA5	Collect known malicious files from targeted devices.
PAA6	Remove files created by CPT actions (example: prefetch, uploaded scripts, etc.)
PAA7	Use (not modify) mission owner services (firewalls, IDS, proxy, NAT devices, DNS) for true source identification of suspicious activity.
PAA8	Secure/manage CPT assets installed on mission owner network (CPT sensors, routers, switches, etc.) within rules of engagement.
PAA9	Collect volatile memory scrapes on targeted devices.
PAA10	Create/implement indicator of compromise (IOC)

Table J. Pre-Coordinated Action (PCA) Description

PCA #	PCA DESCRIPTIONS
PCA1	Manipulate access of specific IPs/ports/protocols on mission owner router/firewall without affecting critical mission system services as identified in DAL (example: manipulate/block internal and external traffic to and from domains/IPs.
PCA2	Execute proxy block of addresses on mission owner proxy (example: block internal to external traffic to domains/IPs.
PCA3	Implement operating system and network hardening on scoped network systems to include file shares without affecting critical services as identified in DAL (example: GPO modification, STIG / Patch enforcement)
PCA4	Bring a device offline / shutdown and collect forensics hard drive image.
PCA5	Deploy/manage weapon system VMs on the mission owner’s virtual environments.
PCA6	Implement permission/encryption on mission owner files without affecting critical services identified in DAL.
PCA7	Connect weapon system components to mission owner provided network drop locations.

Table K. No Strike List

IP Address	AOR	Device
192.168.XX.XX/24	Out of boundary device	Physical Laptops
172.16.XX.XX/16	CENTS Mgmt	Range Control
172.31.XX.XX/16	CENTS Mgmt	Range Control
10.xx.90.1/24	PFSense Rules	Rules set by POR systems should be left alone.