DEPARTMENT OF THE AIR FORCE
HEADQUARTERS 7TH BOMB WING (AFGSC)
DYESS AIR FORCE BASE TEXAS

24 June 2024

MEMORANDUM FOR 7TH BOMB WING PERSONNEL

FROM: 7 BW/CD

SUBJECT: 7 BW Critical Information and Indicators List (CIIL) and Countermeasures (CM)

1. Information on sensitive 7 BW activities, intentions, capabilities, and limitations is considered Critical Information and Indicators. Personnel will make every effort to protect Critical Information and Indicators and practice ideal Operations Security (OPSEC) to prevent threats (e.g. foreign adversaries, violent extremist organizations, insider threats) from gaining information they could use to disrupt, degrade or deny force generation and U.S. and allied operational and technological advantages.

2. The 7 BW CIIL includes the following topics:

Deployment/Mobilization/TDY Details	Recalls, staging/processing areas, chalk times, planning procedures, leave cancellations, mission objectives/purpose, deployment locations, personnel/equipment involved, dates/times of execution or phases, operation duration, mobility readiness status, combat generation & force composition, concept of operations (CONOPS)
Force Readiness	Mission capability rates, medical/vaccine preparedness, number/location of aircrew, fleet-wide aircraft maintenance status
Capabilities/Limitations	Capabilities/limitations of: aircraft, personnel, supplies, communication networks, sensors, intelligence, command/control, operations support, weapons/physical security, stock levels of critical supplies (POL, MREs, attack response gear), resources required/available, inventories, inspection results, usage statistics, design information
Personnel Training/Qualifications	Skill levels, special experience identifiers, special qualifications, combat mission ready/basic mission capable ratings, training

Codes/Call Signs/Passwords/PINs	Authentication codes, duress words, usernames, PINs, associating callsigns with specific functional areas, door/safe combinations
AFFORGEN Cycle Information	Association of units to AFFORGEN phases
Schedules	Daily flying/range/deployment/exercise/ combat schedules/mission related weather products
Radio	Frequencies/settings
Contingency Procedures	Force Protection (FPCON) measures, nuclear biological and chemical (NBC) attack preparedness, random anti-terrorism measures, planned reaction times to crisis, contingency tasks, Information Operations Condition (INFOCON), Health Protection Condition (HPCON), Cyberspace Protection Conditions (CPCON)
Base Infrastructure Critical Nodes	Diagrams/blueprints/imagery that identify potential points of failure for the following: electricity, water, sewage, unclassified and classified communication networks, petroleum oil and lubricants, and security, control, and communication measures taken to protect such assets
Exercises	Details concerning simulated deployed location(s), simulated adversarial country, units involved, overall scenario, daily scripts, final exercise report, special instructions (SPINS), Crisis Action Team (CAT) Directives
Key Personnel	VIP/DV/Sr Officer schedules/itineraries/billeting/personal contact information
Personal Identifiable Information (PII)	SSNs, addresses, dependent(s) information, recall/alpha/access rosters
Government Purchase Card (GPC)	Purchase list(s), receipts listing sensitive equipment, logs/records

* This CIIL is not all-inclusive. Additionally, avoid grouping CIIL content together in the same document and/or correspondence, as the combined information may reach classified levels. Practice OPSEC at all times and protect classified information in accordance with all governing requirements.

3. 7 BW OPSEC Countermeasures safeguard Critical Information and Indicators; thus the following actions must be taken regarding Critical Information and Indicators content:

a. Know and protect 7 BW's CIIL content
b. Use CAC encrypted emails, government issued telephones and radios, and government approved communication applications during such correspondence
c. Mark documents and emails with CIIL content as containing CUI
d. Discuss OPSEC importance with family members (both immediate and extended)
e. Avoid discussing CIIL content in public areas where conversations can't be monitored
f. Destroy respective documents by using an authorized shredder
g. Lock documents to physically protect access when not in use by authorized personnel
h. Do not archive nor post CIIL content on social networking sites, nor on non-government web-pages and non-government electronic devices
i. Limit distribution to those with need-to-know

4. This document is to be posted in each work center. The responsibility to safeguard Critical Information and Indicators rests with each teammate of the 7 BW (military, civilian, contractor and family). Carefully consider if your actions ideally support OPSEC. Unauthorized disclosure of Critical Information and Indicators and/or failure to abide by OPSEC Countermeasures may result in disciplinary action. Violations must be reported to the 7 BW/ OPSEC office at DSN 461-4808 and 7 BW/IP office at DSN 461-3105. Lastly, report suspicious information gathering activity to Air Force Office of Special Investigations (AFOSI) at DSN 461-2296.

5. If you have any questions or concerns regarding this memorandum, please contact the 7 BW/OPSEC office at DSN 461-4808.

FRIEND.SAMUEL.ADAM.1158368621

Digitally signed by FRIEND.SAMUEL.ADAM.1158368621
Date: 2024.07.11 16:23:54 -05'00'

SAMUEL A. FRIEND, Colonel, USAF
Deputy Commander