



UNITED STATES MARINE CORPS
MARINE CORPS AIR STATION
BEAUFORT, SOUTH CAROLINA 29904

ASO 5239.1C
S6
15 Aug 24

AIR STATION ORDER 5239.1C

From: Commanding Officer
To: Distribution List

Subj: CYBER SECURITY PROGRAM

Ref: (a) MCO 5239.2B
(b) MCO 5400.52
(c) USMC ECSM 001, Computer Security Incident Handling
(d) USMC ECSM 004, Remote Access Systems
(e) USMC ECSM 005, Portable Electronic Devices and Wireless Local Area Network Technologies
(f) USMC ECSM 006, Virtual Private Networks
(g) USMC ECSM 008, Cross-Domain Solutions and Secure Data Transfer
(h) USMC ECSM 010, Unauthorized Disclosure of Classified Information and Electronic Spillage
(i) USMC ECSM 011, Personally Identifiable Information
(j) USMC ECSM 017, Information Operations Conditions in the Marine Corps
(k) USMC ECSM 020, Marine Corps Information Assurance Vulnerability Management Program
(l) USMC ECSM 024, Marine Corps Cyberspace Information Technology/Cybersecurity Workforce Qualification Program
(m) DoD 8570.01-M
(n) DoD Directive 8140.01-03
(o) CJCS Manual 6510.01B
(p) SECNAV Instruction 5239.19
(q) DoD Instruction 8500.01
(r) SECNAV Instruction 5211.5F
(s) CJCS Instruction 6510.01F
(t) SECNAV Instruction 5239.3C
(u) SECNAV Manual 5239.2
(v) SECNAV Instruction 1543.2
(w) SECNAV Manual 5239.1
(x) DoD Manual 5200.01, Volume 3
(y) DoD Manual 5200.01, Volume 4
(z) DoD Manual 5200.01, Volume 2
(aa) DoD 5500.7-R
(ab) DoD Instruction 8520.03
(ac) DoD Manual 5205.02
(ad) MARADMIN 258/16
(ae) MCIEast CG Policy Letter 10-19, Removable Storage Devices
(af) USCYBERCOM TASKORD 13-0651, Insider Threat Mitigation Amplifying Direction
(ag) USCYBERCOM TASKORD 14-0185, Insider Threat Mitigation
(ah) DoD Instruction 5200.48

Encl: (1) Cyber Security Program

1. Situation. This order and all references provide requirements and guidance for Commanding Officers (COs), department heads, Officers in Charge (OICs), supervisors, managers, and Marine Corps Air Station (MCAS) Beaufort Cyber

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

Security professionals to identify and manage cyber risks and meet mission requirements.

2. Cancellation. ASO 5239.1B

3. Mission.

a. To provide guidance regarding Department of Defense (DoD) Cyber Security orders and directives in order to mitigate Cyber Security incidents aboard MCAS Beaufort and ensure mission accomplishment.

b. This Order has been revised and should be reviewed in its entirety.

4. Execution. COs, department heads, OICs, supervisors, and managers shall ensure all military, federal civilians, and contract personnel comply with and implement the references as it pertains to their requirements and in the conduct of operations relating to all Cyber Security functions.

5. Administration and Logistics.

a. Conflicts regarding the contents of this order or recommendations for changes shall be forwarded to the Commanding Officer Marine Corps Air Station Beaufort (Attention: S-6 department, Cyber Security Section).

b. Controlled Unclassified Information (CUI).

(1) Unless specifically marked as classified (e.g. Confidential, Secret, and Top Secret) the following are categories are subsets of Controlled Unclassified Information (CUI) and are to be protected in accordance with 32 CFR Part 2002: Agriculture, Critical Infrastructure, Emergency Management, Export Control, Financial, Geodetic Product Information, Immigration, Information Systems Vulnerability Information, Intelligence International Agreements, Law Enforcement, Legal, Natural and Cultural Resources, NATO Controlled, Nuclear, Patent, Privacy, Procurement and Acquisition, Proprietary Business Information, SAFETY Act Information, Statistical and Tax.

(2) All individuals handling this information are required to protect it from unauthorized disclosure. Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.

(3) Access to and dissemination of Controlled Unclassified Information shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

c. Records Management. Records created as a result of this Plan shall be managed according to national archives and records administration (NARA) approved dispositions per SECNAV Notice 5210 Implementation of New Department of the Navy Bucket Records Schedules and MCO 5215.1K Marine Corps Directives, to ensure proper maintenance, use, accessibility and preservation, regardless of format or medium. Refer to SECNAV M-5210.1 Records Management Manual and MCO 5210.11F Marine Corps Records Management Program for Marine Corps records management policy and procedures.

6. Command and Signal

a. Command. This Order is applicable to all personnel aboard MCAS Beaufort.

b. Signal. This order is effective the date signed.



M. D. BORTNEM

DISTRIBUTION: A

Chapter 1

Introduction

1. General. This Order provides the security requirements and technical/operational controls for information systems (IS) within Marine Corps Air Station (MCAS) Beaufort. This Order represents the Command's plan to manage risks, implement safeguards, audit, report, and document information to ensure physical and personal security.
2. Background. Reference (a) formally establishes the responsibilities for protecting Marine Corps IS as well as delineating Department of Defense (DoD) directives, DoD Instructions, and guidance governing cybersecurity. Per reference (b), detailed cybersecurity practices and procedures supporting the Marine Corps Cybersecurity Program have been published by Headquarters Marine Corps (HQMC) Deputy Commandant for Information (DC I) Command, Control, Communications, and Computers (IC4) through supplemental cybersecurity guidance, updates, or revisions to Enterprise Cybersecurity Manuals (references (c) through (ah)).
3. Purpose. This Order establishes the Command's policies for maintaining compliance with the DoD, Department of the Navy (DoN), and Marine Corps orders, directives, and other governing documents (references (m) through (ag)) for the secure use and safeguarding of IS.
4. Applicability and Scope
 - a. Applicability. This Order applies to all personnel assigned to, or operating in support of, MCAS Beaufort that access Marine Corps IS. This includes any networks that process Marine Corps data, whether stand alone, contractor provided, or directly connected to the Marine Corps Enterprise Network (MCEN).
 - b. Scope. All DoD owned or controlled IS that receive, process, store, display, or transmit information, regardless of mission assurance category, classification, or sensitivity are applicable. This includes but is not limited to:
 - (1) Stand-alone IS.
 - (2) Mobile computing devices such as laptops, tablets, handhelds, and smartphones operating in a wired or wireless capacity and other information technologies that may be developed.
 - (3) Contracted third parties who use commercial devices, services, networks, and technologies.
 - (4) Cybersecurity Policy. This section mandates the actions of all administrators and users who develop, access, and maintain IS.

Chapter 2

Roles and Responsibilities

1. Commanding Officer (CO). The CO's responsibilities, as derived from paragraph 4.a.(3)(j) of reference (a), are listed below with additional responsibilities for special programs or functions as noted:

a. Appoint in writing an Information Systems Security Manager (ISSM) for the installation. Ensure the ISSM receives applicable certifications in accordance with (IAW) reference (m) and can perform required duties.

b. Ensure that all applicable U.S. Cyber Command Tasking Orders are applied to the portion of the MCEN that falls under their area of responsibility per references (c), (h), and (e).

c. Responsibilities listed for incident reporting, unauthorized disclosure, and wireless networks according to references (c), (h), and (e).

d. Assign manpower, personnel, and training responsibilities to local human resources, administrative, and training officers to carry out the Cybersecurity Workforce Improvement Plan (CWIP).

2. Information Systems Security Manager (ISSM). ISSMs are privileged users, who are defined as individuals who have access to system control, monitoring, or administration function. Individuals having privileged access require training and certification to Information Assurance (IA) Technical levels I, II, or III depending on the functions they perform. They should be a U.S. citizen and must hold local access approvals commensurate with the level of information processed on the system, network, or enclave. They must have an IT-I security designation and a Tier 3 (T3) and/or an initiated Tier 5 (T5) Background Investigation per reference (u). The ISSM functions as the command focal point and principal advisor for all cybersecurity matters on behalf of the CO. The ISSM reports to the CO or appointed representative and implements the overall cybersecurity program within their area of responsibility (AOR). The ISSM is appointed in writing by the CO and endorsed by the Authorizing Official (AO). ISSM responsibilities as derived from paragraph 4.a.(3)(k) of reference (a) and paragraph 18 to enclosure (3) of reference (q). Listed below are additional responsibilities for special programs or functions as noted:

a. Establish and manage the cybersecurity program within the command, site, system, or enclave per DoD, DoN, and Marine Corps cybersecurity guidance and policies.

b. Manage the command, site, system, or enclave Risk Management Framework process to ensure that IS within their purview are approved, operated, and maintained throughout its life cycle per the IS accreditation package. This may be done in conjunction with other MCEN stakeholders, such as, but not limited to, the applicable Network Battalions that support the installation.

c. Serve as the principal advisor to the CO for site, system, or enclave cybersecurity matters on behalf of the USMC AO IAW reference (q).

d. Assess the cybersecurity program effectiveness and mitigate deficiencies IAW references (b), (q), (t), and (w).

e. Assess IS for compliance with the Information Assurance Vulnerability Management (IAVM) Program and all applicable Security Technical Implementation Guide (STIG) in addition to accurate compliance information reporting IAW references (q) and (s).

f. Ensure cybersecurity workforce (CSWF) personnel receive required security training commensurate with their security duties IAW reference (n).

g. Report all issues/concerns regarding Programs of Record to the appropriate Marine Corps Systems Command program office or Marine Corps Cyberspace Operations Group (MCCOG) Vulnerability Management Team (VMT).

h. Ensure security incidents (e.g., malicious code, attacks, intrusions, violations, spillages, etc.) are reported to local network battalion cyber security sections, the MCCOG Defensive Cyber Operations Section (DCOS) and the responsible parent command in a timely manner IAW references (p), (s), and (x).

i. Ensure MCCOG DCOS directed protective/corrective actions are implemented for security incident remediation or mitigation IAW the timelines provided, regardless of overtime costs or issues IAW references (o), (p), and (r).

j. Monitor compliance with cybersecurity policy, as appropriate, and review the results of such monitoring.


k. Ensure implementation of IS security measures and procedures, including reporting incidents to the AO and appropriate reporting chains and coordinating system-level responses to unauthorized disclosures IAW reference (x) for classified information or reference (y) for Controlled Unclassified Information (CUI), respectively.

l. Responsibilities listed with regard to **remote access systems** IAW reference (d) are:

(1) Establish and manage the cybersecurity program within a command, site, system, or enclave IAW DoD, DoN, and Marine Corps cybersecurity guidance and policies.

(2) Verify that personnel requesting access to Marine Corps Information Technology (IT) have completed all required Marine Corps Cyber Awareness training for active duty and reserve DoD service members and civilian cyber awareness training for DoD civilians, contractors, and others with unclassified and classified MCEN accounts, and meet all DoD personnel security requirements.

(3) Validate that the DD Form 2875, System Authorization Access Request (SAAR) is completed in its entirety and retained per current directive retention policies.

 m. Secure Data Transfer. Ensure unit/organizational personnel follow the guidelines, processes, and procedures outlined in reference (g) when manually transferring data between security domains.

n. Responsibilities listed regarding **unauthorized disclosures** IAW reference (h) are:

(1) Serve as the first level in the reporting process for unauthorized disclosure or electronic spillage.

(2) Report all unauthorized disclosures or electronic spillages to the Installation S6 Officer, local Network Battalion Cyber Security sections, and the Command Security Manager.

(3) Notify the MCCOG Battle Captain of any action taken on an unauthorized disclosure or spillage.

(4) Support the Naval Criminal Investigative Service (NCIS) in the investigation of any unauthorized disclosure or spillage.

(5) Ensure local network and technical support personnel support NCIS in the investigation as needed.

(6) Coordinate the removal and troubleshooting of devices involved in the unauthorized disclosure or spillage with local personnel.

(7) Coordinate with the Security Manager to send classified materials (e.g., a classified hard drive) to the MCCOG in support of an investigation.

o. Responsibilities listed regarding **Personally Identifiable Information (PII)** IAW reference (i) are:

(1) Report all breaches of PII and make notifications to affected person(s) IAW section 6.0 of reference (i).

(2) Advocate PII policies and procedures.

(3) Initiate and coordinate collaborative efforts within the command for actions required following the initial PII breach report IAW reference (i).

p. Responsibilities listed regarding the **IAVM program** IAW reference (k) are:

(1) Monitor vulnerability management notification Operation Directives and ensure reporting compliance to MCCOG VMT.

(2) Coordinate with systems administrators (SA) on any issue regarding vulnerabilities on Marine Corps systems in their AOR.

3. Information System Security Officer (ISSO). ISSOs are privileged users who have access to system controls, monitoring, or administration functions. Individuals having privileged access require training and certification to IA Technical levels I, II, or III, depending on the functions they perform. They must also be trained and certified on the operating system or computing environment they are required to maintain. They should be a U.S. citizen and must hold local access approvals commensurate with the level of information processed on the system, network, or enclave. They must have an IT-I security designation and a T3 and/or an initiated T5 background investigation per reference (u). ISSOs are appointed in writing by the ISSM, and their

responsibilities as derived from paragraph 4.a.(3)(1) of reference (a) and paragraph 19 to enclosure 3 of reference (q), are listed below with additional responsibilities for special programs or functions as noted:

- a. Provide direct support to the ISSM for all cybersecurity matters.
- b. Enforce system-level cybersecurity controls IAW the proper program and policy guidance per references (b), (n), (q), (t), and (w).
- c. Evaluate risks, threats, and vulnerabilities to determine if additional safeguards are needed to protect the command, site, system, or enclave.
- d. Develop and issue any additional specific cybersecurity policies, guidance, and instructions as needed.
- e. Assist the ISSM in monitoring, reporting, and enforcing the command, site, system, or enclave IAVM program.
- f. Ensure that all users have the requisite security clearances and access authorization and are aware of their cybersecurity responsibilities for DoD IS and IT systems under their purview before being granted access to those systems.
- g. In coordination with the ISSM, initiate protective or corrective measures when a cybersecurity incident or vulnerability is discovered. Ensure that a process is in place for authorized users to report all cybersecurity-related events and potential threats and vulnerabilities to the ISSO.
- h. Assist the ISSM in all aspects regarding unauthorized disclosure IAW reference (h).
- i. Submit requests to Marines Corps Operations Group (MCCOG) for Cryptographic Log On (CLO) exemptions. Ensuring no exemptions will be granted without MCCOG approval.
- j. Ensure all requests to conduct secure data transfer write exemptions are routed through II Mef to the Marine Corps Operations Group (MCCOG).
- k. Cyber IT/CSWF Program Manager (PM). Cyberspace IT/CSWF PMs are personnel appointed in writing who are responsible for serving as the technical Cyber IT/CSWF advisor. Responsibilities listed regarding the CWIP IAW reference (l) are:
 1. Identify all positions performing IS management, specialized, or privileged access cybersecurity functions by category, specialty, and level as described in reference (n). This applies to all positions with cybersecurity duties, whether performed as primary or additional/embedded duties. This requirement applies to military, civilian, and contractor positions.
- m. Identify all cybersecurity function requirements to be performed by contractors in their statement of work/contract. Ensure contractors are appropriately certified and have the appropriate background investigation to perform those cybersecurity functions per reference (m).

n. Train, certify, and obtain the proper background investigation for all military and civilian personnel identified as part of the CSWF to accomplish their cybersecurity duties per reference (m) and ensure contracted companies adhere to the same regulations for contractor personnel.

o. Ensure cybersecurity personnel performing cybersecurity functions obtain/maintain a commercial certification corresponding to the highest-level function(s) required by their position per reference (m).

p. Obtain the appropriate background investigation, per reference (m), prior to granting unsupervised privileged access or management responsibilities to any DoD system.

q. Identify, track, and monitor cybersecurity personnel performing IA functions, per reference (m), to ensure that cybersecurity positions are staffed with trained and commercially certified personnel.

r. Ensure that all CSWF personnel within their command understand and comply with requirements directed in references (a), (b), (m), (n), and (t) through (v) by establishing awareness of individual commercial certification requirements of the position assigned and developing individual training and certification compliance requirements.

s. Track all CSWF personnel, training, and certifications within the command and reporting compliance.

4. Privileged Users. Privileged users (system and network administrators) are defined as individuals who have access to system controls, monitoring, or administration functions. Individuals having privileged access require training and certification to IA Technical levels I, II, or III depending on the functions they perform. They must also be trained and certified on the operating system (OS) or computing environment they are required to maintain. They should be a U.S. citizen and must hold local access approvals commensurate with the level of information processed on the system, network, or enclave. They must have an IT-I security designation and a T3 and/or an initiated T5 background investigation per reference (u). Privileged users are appointed in writing by the ISSM, and their responsibilities are derived from paragraph 4.a.(3)(m) of reference (a) and paragraph 20 to enclosure (3) of reference (q).

a. Monitor user account activity and establish procedures investigating, deactivating, and deleting accounts that do not show activity over time and report these actions and findings to the ISSM.

b. Provide cybersecurity safeguards and assurances to the data under their control as well as their personal authentication and authorization mechanisms, reporting to the ISSM.

c. Analyze patterns of non-compliance or unauthorized activity and take appropriate administrative or programmatic actions to minimize security risks and insider threats, reporting to the ISSM.

d. Recognize potential security violations, take appropriate action to report the incident as required by regulation, and remediate or mitigate any adverse impact.

e. Implement applicable patches and critical security updates in a timely manner to avoid potential compromise or loss of functionality.

f. Manage accounts, network rights, and access to information systems and equipment.

g. Configure, optimize, and test hosts (e.g., servers and workstations) and network devices (e.g., hubs, routers, and switches) to ensure compliance with security policy, procedures, and technical requirements.

h. Install, test, maintain, and upgrade operating systems, software, and hardware to comply with prescribed cybersecurity requirements.

i. Ensure that hardware, software, data, and facility resources are archived, sanitized, or disposed of in a manner compliant with system security plans, requirements, and regulations.

j. Perform audit log review on network, systems, and applications in accordance with the applicable STIGs.

5. Authorized Users. Authorized users (Information Owners and System/Data Users) are defined as any military, government civilian, or contractor who has authorized access to the MCEN or Marine Corps IT resources. Authorized user responsibilities as derived from paragraph 4.a.(3)(n) of reference (a) and paragraph 21 to enclosure (3) of reference (q) are listed below with additional responsibilities for special programs or functions as noted:

a. Obtain a favorable background investigation and hold security clearance or access approvals commensurate with the level of information processed or available on the system.

b. Comply with the guidelines established IAW reference (a) and submit a SAAR for access to government owned IS. A separate SAAR is required for Non-Classified Internet Protocol Router (NIPR) and Secret Internet Protocol Router (SIPR). Each SAAR is valid for three years.

c. Receive initial and annual cybersecurity training IAW references (m) and (n). Training is to be taken via MarineNet or Total Workforce Management System (TWMS) only.

d. Mark, label, and safeguard all media, devices, peripherals, and IS at the security level for which they are intended IAW DoD, DoN, and Marine Corps policies and procedures. Dissemination shall only be made to individuals with a valid need to know and clearance level at or above the classification level of the shared media, device, or peripheral IAW reference (z).

e. Protect all media, devices, peripherals, and IS in their respective area of responsibility IAW physical security and data protection requirements.

f. Practice safe internet and intranet operating principles and take no actions that threaten the integrity of the system or network IAW references (a), (f), and (aa).

15 Aug 24

g. Report incidents or suspicious events regarding suspected intrusions or unauthorized access; circumvention of security procedures; presence of suspicious files or programs; receipt of suspicious email attachment, files, or links; spillage incidents; and malicious logic (e.g., viruses, trojan horses, worms spamming, phishing, chain letters, etc.) to the ISSM, ISSO, or SA IAW references (a) and (p).

h. Report the receipt or discovery of unfamiliar or unauthorized removable media (e.g., CD-ROM, floppy disk, thumb drives, external hard drives, etc.) to the ISSM/system or network administrator IAW applicable directives.

i. Use anti-virus (AV) products on all files, attachments, and media before opening or introducing them into the IS.

j. Report suspicious, erratic, or anomalous IS operations; missing or added files; and non-approved services or programs to the system or network administrator IAW local policy and cease operations on the affected IS until authorized to start operations again by higher authority IAW references (a) and (p).

k. Comply with cryptographic login requirements and password or passphrase policy directives and protect IS from unauthorized access IAW references (a) and (ab).

l. Logoff and secure the IS and work environment (i.e., secure For Official Use Only (FOUO)/CUI media, remove Common Access Card (CAC), etc.) at the end of each workday or when out of the immediate area IAW references (a) and (y).

m. Access only data, controlled information, software, hardware, and firmware for which they are authorized access and have a need to know. Assume only authorized roles and privileges.

n. Install and update of authorized Government-provided products (e.g., AV, Virtual Private Network (VPN), personal firewalls, etc.) is encouraged on personal systems as required by the AO for approved remote access.

o. Digitally sign and encrypt all sensitive information on external media or in email exchanges, using FIPS 140-2 validated encryption (e.g., DoD CAC, DoD Alternate Token). Such information includes items marked FOUO/CUI, financial data, contract related information, health information, PII, network or technical diagrams with identifiable labels (e.g., IP addresses), or other information that may have an operational security impact if compromised.

p. Protect authenticators commensurate with the classification or sensitivity of the information accessed and report any compromise or suspected compromise of an authenticator to the appropriate ISSO.

q. Inform the appropriate system owner when access to a particular DoD IS or IT system is no longer required (e.g., completion of project, transfer, retirement, resignation).

r. Observe policies and procedures governing the secure operation and authorized use of DoD IT, including operations security IAW reference (ac).

s. Use DoD IT/IS only for official or authorized purposes.

t. Notify the appropriate system owner if they are unable to log into their account(s) in excess of 30 days due to deployment, temporary assigned duty, or any other valid reason to prevent them from being disabled or deleted.

u. Report any breach of PII to the ISSM.

v. Responsibilities listed regarding **remote access systems** IAW reference (d) are:

(1) Ensure only authorized programs or applications are used in the performance of official duties.

(2) Restrict the use of Marine Corps IT to official use or authorized purposes only.

(3) Report any misuse, abuse, or other prohibited actions on Marine Corps IT systems through their chain of command.

(4) Have a signed copy on file of the user telework agreement.

w. Responsibilities listed regarding **IT resource access** IAW reference (1) are:

(1) Restrict use of Marine Corps IS and equipment (including computers, electronic mail, and Internet systems) for official use or authorized purposes only.

(2) Report any misuse, as defined in the standards contained in reference (1), of Marine Corps systems to their CO or supervisor.

x. Responsibilities listed regarding **secure data transfers** IAW reference (g) are:

(1) Follow the guidelines, processes, and procedures outlined in reference (g) when transferring data from different security domains.

(2) Ensure proper classification markings and proper handling of classified material.

(3) Act as a reliable human reviewer.

(4) Ensure all Media is marked appropriately with classification markings or labels during quarterly Consolidated Memorandum Report (CMR) checks. Each IT system shall be marked to indicate the highest classification level of the information processed by the IT system and the network to which it is connected.

(5) Ensure no unauthorized Portable Electronic Devices (PED's) to include all privately owned, contractor owned computers, Cellular phones, or any electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo is connected to the Marine Corps network at any time.

Chapter 3

Cybersecurity Policy

1. General. This chapter defines the security policies for the Command's IS and IT assets. It addresses all directed requirements and local policies to ensure the secure use and safeguarding of IS throughout MCAS Beaufort.
2. System Management. MARADMIN 304/15 (reference (ad)) provides guidance on the OS authorized for use on the MCEN. The following additional policies are applicable to MCAS Beaufort.
 - a. MCEN assets will be disabled if not utilized for more than 90 days based off last logon time stamp. Systems requesting to be enabled after this time will require a reimage with current MCEN baseline image before being able to logon to the MCEN again.
 - b. Systems will be maintained by 2nd Network Battalion, MCAS Beaufort S6, and MCCOG to meet STIG and IAVM program requirements.
 - c. Once added to the network, group policy will be applied to configure additional security settings (if required).
 - d. Contractor provided IS are authorized for use on the NIPR MCEN with the current approved MCEN image. Once the IS are no longer required to be on the MCEN, the IS will be reimaged to wipe all potential government information.
 - e. Public Key Infrastructure (PKI). PKI and Public Key Enablement (PKE) are implemented and enforced across the MCEN. Any requests to waive this policy shall be made in writing by the ISSM to the USMC AO. The ISSM will validate such requests and keep a list of any account that is approved for exemption. The following additional policies are applicable for MCAS Beaufort:
 - f. All alternate token and certificate requests are processed by the local Trusted Agents (TA). These are utilized for privileged users, functional accounts, and SIPRNet accounts.
 - g. Tokens and certificates are provided by the MCCOG. Distribution, tracking, and accounting are provided by the local TA.
3. Account Management. Account management controls and policies will be implemented IAW references (q), as updated by the most recent OS, application, or database STIGs. Under the supervision of the ISSM, the following additional account policies will be implemented:
 - a. Maintaining Accounts. NIPR and SIPR SAARs are to be maintained by the S6 Cyber Security section on every account associated to MCAS Beaufort. Each SAAR will be verified and signed by the ISSO to ensure accuracy and completeness. Once the SAAR is signed by the ISSO, they will be filed alphabetically in the SAAR Database folder located on the S6 SharePoint. This folder is locked down to only the personnel who have a need to know as well as the administrators.

b. Destruction of SAARs. SAARs are to be kept on file for one year after the departure of the individual. SAARs will be pulled from the active folders and placed in the destruction folders, separated by month. At the one-year mark, the SAARs are to be permanently deleted.

4. Authorized User Accounts

a. Prior to accessing any system, the required IA Awareness and PII training must be completed. Derivative Classification training is required for SIPR access. Certificates of completion, dated within 365 days, will accompany the completed SAAR form.

b. The Security Manager must validate that a T3 or T5 background investigation has been conducted for all user account requests.

c. One hundred percent verification of credentials and need-to-know is required prior to access being granted by the ISSM.

d. In situations where single sign-on PKE and PKI cannot be used, strong password/phrases of at least 15 characters will be used containing at least two special characters, numbers, uppercase, and lowercase letters. Application/service accounts must be at least 15 characters, meet complexity requirements, and passwords manually generated and entered by a SA must be changed at least annually or whenever a SA that has knowledge of the password leaves the organization.

e. Users who executed a permanent change of station will be deactivated after 60 days if a logical move did not occur (verified through Active Directory). Users that have retired, reached their end of active service date, or are no longer employed aboard MCS Beaufort will have their accounts deactivated when they check out with the S6.

f. Management of inactive authorized user accounts will be as follows:

(1) Accounts that have been inactive for more than 90 days, based off last logon time stamp attribute, will be disabled, and annotated in the description field. Accounts will be moved from their Organizational Unit (OU) to the deletion OU.

(2) The owner of the disabled account is required to contact the enterprise service desk or S6 office to have the account re-enabled. At which time, validation of current documentation will occur.

(3) Guidance on account deletion and mailbox retention will be directed by HQMC. Situations for exemption include extended leave due to illness, contractors or civilians activated on reserve duty, or individuals in a temporary duty status, such as Individual Augment billet requirements. The latter require prior notification of the situation to prevent deletion of the account.

(4) Any account through which unauthorized user activity has been detected will be disabled immediately and appropriate disciplinary actions taken.

5. Privileged Accounts

a. Users requesting a privileged access account will be screened to ensure a T5 background investigation is complete and favorable.

b. All privileged accounts will have a privileged user agreement form on file and updated on a yearly basis.

c. Requests for privileged access will be processed via the ISSM and approved prior to submission for creation via Remedy.

d. The ISSM will maintain a list of privileged users, their roles, and assigned administrative access.

e. Accounts are audited continuously for activity by MCCOG and disabled for inactivity.

f. Management of inactive privileged accounts will be as follows:

(1) Accounts that have been inactive for more than 30 days, based off last logon time stamp attribute, will be disabled, and annotated in the description field.

(2) Accounts that have been disabled for more than 30 days will be deleted.

(3) Once an account has been deleted, if the privileged user requires access, they must complete the request process as a new account.

6. Functional Accounts. Accounts that require multiple users to log in (e.g. watch standers) may have a functional account created. The following requirements must be met:

a. Complete a SAAR, which includes the computer name in the justification.

b. A Sponsor and an ISSO for the functional account.

c. An alternate token will be requested by the local TA and issued to the sponsor of the functional account for access to the MCEN.

7. Wireless Controls. Wireless technologies have specific controls as deemed IAW the references.

a. Per reference (e), wireless peripherals are not authorized for use within the Marine Corps. This includes, but is not limited to: mice, keyboards, headsets, printers, or other devices capable of operating on a radio frequency (RF), or utilizing Wireless Personal Area Network 802.15 protocols (i.e. Bluetooth, Infrared Data Association, Ultra-wideband, Z-Wave, ZigBee, etc.).

b. All wireless local area networks (WLAN) operated by MCAS Beaufort organizations must be approved by the MCEN AO and MCAS Beaufort S6 prior to activation and operation.

c. All WLANs must meet the technical, administrative, and physical security requirements specified in Section 4 of reference (e). All waivers

of the specified requirements must be approved by the MCEN AO via MCAS Beaufort S6.

d. As directed by reference (e), an Authorization to Operate and Authorization to Connect must be granted prior to installation of any commercial wireless technologies.

8. Remote Access. Remote access is an essential means for authorized users located outside the physically secured MCEN boundary to access internal MCEN resources via secure remote connectivity. Reference (d) establishes remote access policies for the MCEN.

9. Remote Access Devices. The following are approved remote connection methods:

a. Government issued cellular devices (hot spot) with a government issued laptop/tablet.

b. Government issued cell phone.

c. Wired connection to a government issued laptop.

d. Personally owned computers may be used to access NIPRNet email and Microsoft Teams via enterprise Office 365 tools using a CAC.

10. Remote Access Controls

a. Authorized users will request Wi-Fi capabilities through the enterprise service desk.

b. Government devices used for remote access will be safeguarded at all times while connected to MCEN resources.

c. Remote access devices will only be enabled during times of use.

d. Laptops may connect to the MCEN through Wi-Fi hotspots in homes, hotels, travel conference sites, and airports (domestic and international) when utilizing the Pulse Secure VPN.

e. Laptops may not be used to connect to the internet for any purpose other than connecting to the MCEN.

f. Personal or Government issued wireless/cellular hot spots are not authorized in areas that are processing or discussing classified information.

g. Wireless/cellular hot spots are not to be used to send, receive, store, or process classified information.

h. All internet browsing will be done after connecting via AppGate VPN.

i. Personal or non-MCEN connection approved contractor owned laptops/desktops are not authorized for remote access.

11. Removable External Storage Devices. Removable secondary storage media devices are addressed in reference (ae). Reference (g) is the current Marine Corps directive for the secure transfer of data. As per these references,

the following will be strictly adhered to when procuring, installing, and/or using a removable external storage device:

a. Prior to use, users must complete a Removable External Storage Device User Agreement.

b. All new hard drives and those transferred between prior commands require initial approval, scanning, and tracking by the S6 Cybersecurity section.

c. Unclassified removable external storage media is authorized up to FOUO. They will be encrypted with BitLocker and not contain any information that is of a personal nature.

d. Removable external storage devices must be Government owned and procured. Personal or contractor owned external storage devices are not authorized for connection to Government information technology assets.

e. All removable storage devices connecting to classified networks shall be treated as controlled items and handled according to local command physical security policy.

f. The Government owned removable external storage device will never be attached to a personal or contractor owned computer.

g. Flash media is not authorized for use in any Marine Corps IS.

h. Storage devices that are disguised to look like common items such as pens, or bracelets are not authorized in MCAS Beaufort spaces.

i. Theft, loss, or compromise of a removable external storage device will be reported immediately to the ISSM.

j. Removable external storage devices will be properly marked and labeled IAW the classification of the information they process.

k. Destruction of classified storage devices is handled by the Command Security Manager.

l. Destruction of unclassified storage devices is handled by the S6 Cybersecurity section. Specific policy on destruction is available from the ISSM.

12. Insider Threat Mitigation. References (af) and (ag) directed DoD components to implement several technical and procedural safeguards to prevent, deter, and detect the insider threat. They are only applicable to SIPRNet with the following controls:

a. Ensure all devices can install the Data Loss Prevention component of HBSS or have an alternate means to disable data transfer activity (DTA).

b. Ensure all users that require DTA are approved in writing by the unit CO.

c. Ensure the procedures to identify, report, and investigate violations of DTA are documented in the Command's incident handling program.

d. Ensure acceptable use and approval processes for use of removable media devices is included in the Command's User Training Program.

e. Ensure all removable media devices are properly labeled.

f. Ensure all approved DTA users maintain data transfer records for all data removed from a SIPRNet machine.

g. Conduct quarterly reviews of privileged users IAW reference (ag) to ensure a continuing need for their capabilities and access (See paragraph 4.b(5)).

13. Information Operations Condition (INFOCON). Reference (j), addresses the implementation of INFOCON in the Marine Corps.

a. Implementation. Meeting INFOCON requirements is the responsibility of network administrator and SA, with validation audits conducted by cybersecurity professionals. This implies INFOCON measures should, to the greatest extent possible, be transparent to users. Maintaining a baseline configuration, running appropriate comparisons, and restoring systems to a known good baseline are part of the processes required to ensure networks are free of malicious activity.

b. Responsibility. The ISSM is responsible for the notification and subsequent compliance with INFOCON procedures as well as the return to normal network activity. The ISSM will periodically check the integrity of the Command INFOCON elevation plan to ensure a smooth transition into an elevated security posture. These responsibilities will be managed by MARFORCYBER, MCI East G6 and coordinated with MCAS Beaufort personnel for any actions that may be required.

c. Disaster Recovery/Contingency Plan. In the event of an outage, emergency, or disaster, the S6 will provide continuity of communication services to support various contingencies with the aid of MITSC East.

14. Incident Handling. Reference (c) provides the techniques and procedures for the proper response to computer security incidents within the Marine Corps, reference (h) is the governing directive for classified spillage handling, and reference (i) addresses the disclosure of PII.

a. Types of Incidents or Events. Paragraph 3.3 of reference (c) defines the types of computer security incidents or events and their categories as established by the Chairman of the Joint Chiefs of Staff, National Institute of Standards and Technology, and DoN.

b. Response. Users of the Command's IS are required to report incidents, suspicious activity, or possible incidents to the S6 Cybersecurity section within 15 minutes through the most expedient means.

c. Report Procedures. The Command's Incident Handling Procedures will provide specific guidance on reporting:

(1) Computer security incidents or events.

(2) Classified spillages.

(3) PII spillages.

15. Incident Storage and Analysis. All incident reports and related data must be preserved by the ISSM for three years from the resolution of the incident to enable possible criminal prosecution. Storage of incident reports and related information will be properly safeguarded (chain of custody if required) to prevent exposure to unauthorized individuals and preserve its integrity as evidence.

16. Protected Distribution System (PDS). The PDS is used to transmit unencrypted national security information, in lieu of a National Security Agency approved Type 1 cryptographic device, through an area controlled at a lesser classification level. As required by DoD regulations, the PDS must provide adequate electrical, electromagnetic, and physical safeguards to deter exploitation. IAW reference (cp), the S6 Cybersecurity section will:

a. Maintain accreditation documents for all MCAS Beaufort Station PDS's.

b. Ensure daily visual inspections of the PDS are conducted by the respective unit and report any evidence of tampering, penetration, or unauthorized interception to the PDS Certification Authority for assessment and the Command Security Manager for review and initiation of an investigation.

c. Supervise PDS modifications to ensure changes adhere to the guidelines in reference (cp).

17. PA Data and PII Data Protection. Reference (r) provides current DoN and Marine Corps policy concerning the PA compliance and PII and establishes policy and procedures for safeguarding PII. The following provides MCAS Beaufort procedures and responsibilities for implementing Marine Corps policy concerning the storage and disposal of documents and media containing PII.

a. No part of the social security number shall be included as part of printed documents, computer document files of any format, computer databases, personnel reports, rosters, award certificates, any other correspondence, or local forms.

b. No PA Data will be resident or accessible via publicly accessible web sites.

c. All PA Data on internal Marine Corps Websites must be secured using Secure Socket Layer and PKI protocols.

d. All files and documents containing PA Data will be marked in accordance with applicable instruction DODI 5200.48 Controlled Unclassified Information "CUI".

e. Any printed documents containing PA Data will be covered with a PA Data Cover Sheet (DD Form 2923).

f. All printed forms of PA Data shall be shredded by a National Security Agency approved crosscut shredder, which produces particles that are 1 x 5 millimeters in size.

18. Secure Data Transfer. The transfer of data from one system to another system of a different classification or releasable level will be conducted IAW reference (g). Failure to follow the procedures in reference (g) is punishable pursuant to Article 92 of the Uniform Code of Military Justice and will be reported as a security incident through the Defense Information System for Security.

19. Unauthorized Dissemination of Classified Information. Electronic spillage is defined as the inadvertent or accidental contamination of electronic storage media by information classified above the accredited level of the device (e.g. secret information being stored to an unclassified hard drive). If a secure data transfer results in a spillage, it will be reported and handled IAW reference (h).

20. Inspections and Audits. The command representative will conduct random inspections of data transfer procedures and logs IAW reference (ag). A system audit will be conducted to verify documented data transfers, identify any unauthorized activity, or activity that exceeds designated threshold for that agent or asset.

21. Cyberspace IT/CSWF. Per reference (a), commands are required to develop a CWIP that compels both training managers and the ISSM to meet shared CSWF tracking, training, certification, and reporting responsibilities. The MCAS Beaufort CWIP details the procedures and responsibilities of the involved units aboard the installation to comply with HQMC guidance.

a. Certification

(1) Per reference (a), all CSWF personnel must obtain and maintain the certification that satisfies the requirements of their designated level and billet code. The CSWF PM will ensure that individuals are assigned the proper level according to duties and following the guidelines of the reference.

(2) It is the responsibility of the individual to ensure that any fees and/or continuing education credits required to retain certification are maintained. Individuals who allow a certification to expire and do not make an effort to re-certify are subject to removal of privileges.

b. Training

(1) The CSWF PM is responsible for determining individual's CSWF level and billet code as detailed in reference (a). Upon determination of billet code and level, the CSWF PM will ensure the appropriate certification training and testing is completed and verified.

(2) The CSWF PM will ensure personnel who have been designated as part of the CSWF are registered within the Defense Manpower Data Center and accounted for in TWMS.

c. Tracking. The CSWF PM will maintain electronic records on all personnel assigned to the CSWF. These records will be maintained for the duration of the individual's employment and/or while the individual maintains a CSWF level status. Personnel will be tracked via local compliancy spreadsheet as well as documented in TWMS.

d. Reporting. The CSWF PM will be responsible for reporting compliancy and annual training to higher headquarters. The CSWF PM will utilize training offices who maintain such records in accordance with this policy. Requests for training and certification records may come with little notice; therefore, it is imperative that training offices ensure records are properly maintained.

22. Prohibited Activities. The following activities are strictly prohibited IAW reference (a), paragraph 4.a(3)(1)18 and users shall not:

a. Use official government IS for commercial gain or to conduct illegal activities.

b. Use IS in any manner that interferes with official duties, undermines readiness, reflects adversely on the Marine Corps, or violates standards of ethical conduct.

c. Intentionally send, store, or propagate sexually explicit, threatening, harassing, prohibited, partisan, political, or unofficial public (e.g., "spam") communications.

d. Participate in on-line gambling or other activities inconsistent with public service.

e. Participate in, install, configure, or use unauthorized peer-to-peer technologies.

f. Release, disclose, or alter information without consent of the data owner, the original classification authority, the individual's supervisory chain of command, Freedom of Information Act official, Communication Strategy and Operations Officer, or the disclosure officer's approval.

g. Attempt to strain, test, circumvent, or bypass security mechanisms; perform network line monitoring; or keystroke monitoring IAW reference (q), enclosure (3) paragraph 21. If cybersecurity mechanisms must be bypassed, users will coordinate the procedure with the ISSO and receive written approval from the ISSM.

h. Modify system or software, use it in any manner other than its intended purpose, introduce malicious software or code, or add user-configurable or unauthorized software (e.g., unauthorized instant messaging, P2P applications).

i. Introduce or use software, firmware, or hardware that has not been approved by the USMC AO IAW reference (q), enclosure (3) paragraph 21.

j. Share personal accounts and passwords or allow remote access to non-privileged users.

k. Alter, circumvent, disable, or remove Government-provided and installed cybersecurity products, protective software, or mechanisms (e.g., AV, VPNs, personal firewalls, etc.) on Marine Corps IS.

l. Acquire commercial or unauthorized internet service provider (ISP) network access into Marine Corps operational facilities without approval from the Marine Corps AO.

m. Implement commercial wireless components (e.g., access points, base stations, clients, etc.) without approval from the Marine Corps AO.

n. Use wireless technologies for storing, processing, and transmitting unclassified information in areas where classified information is discussed, stored, processed, or transmitted without the expressed written consent of the Marine Corps AO.

o. Auto forward email from government accounts to commercial ISP email services, engage in the creation or forwarding of chain mail, or open email attachments or internet links received from unknown sources.

p. Attempt to access files or data, or use OS programs, except those specifically designed or authorized for performance of official duties.

Chapter 4

Acronyms

Anti-Virus	AV
Area of Responsibility	AOR
Authorizing Official	AO
Command, Control, Communications, and Computers	IC4
Commanding Officer	CO
Common Access Card	CAC
Controlled Unclassified Information	CUI
Cybersecurity Workforce	CSWF
Cybersecurity Workforce Improvement Program	CWIP
Data Transfer Activity	DTA
Defensive Cyber Operations Section	DCOS
Department of Defense	DoD
Department of the Navy	DoN
Deputy Commandant for Information	DC I
For Official Use Only	FOUO
Headquarters Marine Corps	HQMC
In Accordance With	IAW
Information Assurance	IA
Information Assurance Vulnerability Management	IAVM
Information Operations Condition	INFOCON
Information System	IS
Information System Security Officer	ISSO
Information Systems Security Manager	ISSM
Information Technology	IT
Internet Service Provider	ISP
Marine Corps Air Station	MCAS
Marine Corps Cyberspace Operations Group Command	MCCOG
Marine Corps Enterprise Network	MCEN
Marine Corps Information Technology Service Center	MITSC
Naval Criminal Investigative Service	NCIS
Non-Classified Internet Protocol Router	NIPR
Office in Charge	OIC
Official Portable Electronic Devices	OPED
Operating System	OS
Organizational Unit	OU
Personally Identifiable Information	PII
Personal Portable Electronic Devices	PPED
Portable Electronic Devices	PED
Privacy Act	PA
Program Manager	PM
Protected Distribution System	PDS
Public Key Enablement	PKE
Public Key Infrastructure	PKI

Radio Frequency	RF
Secret Internet Protocol Router	SIPR
Security Technical Implementation Guidelines	STIG
System Administrator	SA
System Authorization Access Request	SAAR
Telephone and Information Services Department	TISD
Tier 3	T3
Tier 5	T5
Total Workforce Management System	TWMS
Trusted Agent	TA
Virtual Private Network	VPN