DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON DC 20350-3000

Canc: Jan 2022

MCBul 3967
MCCDC (C 16)
12 Jan 2021

MARINE CORPS BULLETIN 3967

From: Commandant of the Marine Corps
To: Distribution List

Subj: INTERIM GUIDANCE FOR THE FY21 MISSION FOCUSED CYBER HARDENING OF MARINE CORPS WEAPON SYSTEMS, SUPPORTING ASSETS, AND INFRASTRUCTURE

Ref: (a) National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2016 §1647 (Public Law 114-92)
(b) NDAA for FY 2017 §1650 (Pub. L. 114-328)
(c) John S. McCain NDAA for FY 2019 §1637 (Pub. L. 115-232)
(d) NDAA for FY 2018 § 1640 (Pub. L. 115-91)
(e) NDAA for FY 2018 §1639 (Pub. L. 115-91)
(f) NDAA for FY 2020 §5726 (Pub. L. 116-92)
(g) 10 U.S.C. §2223
(h) 40 U.S.C. §111
(i) E.O. 13800
(j) DoD Instruction 8510.01 of July 28, 2017
(k) ECSM 018, Marine Corps Assessment and Authorization Process (MCCAP), June 4, 2020
(l) MCO 3058.1
(m) SECNAVINST 5000.2F
(n) SECNAV M-5210.1
(o) MCO 5210.11F
(p) 5 U.S.C. §552a
(q) SECNAVINST 5211.5F

Encl: (1) Definitions
(2) Mission Focused Cyber Hardening (MFCH) Flow Chart

1. Situation

a. Purpose. In accordance with references (a) through (q) this Marine Corps Bulletin (MCBUL) establishes a codified, standardized, and repeatable process to identify, assess, prioritize, and reduce cyber-related risk in weapon systems and their critical supporting infrastructure.

b. Background. The Marine Corps has completed the evaluations of cyber vulnerabilities on 23 weapon systems, including aircraft, ground vehicles, radars, command and control systems, intelligence systems, and artillery systems in accordance with reference (a). In a separate effort, the service has evaluated installation infrastructure and Supervisory Control and Data Acquisition (SCADA) systems and identified the criticality of those assets based on their support to Marine Corps missions, including support to weapon systems, to meet the requirements of reference (b). Multiple Marine Corps

entities conduct cyber-related risk analysis of specific assets – infrastructures - and mission chains. To maximize use of resources appropriated by the Marine Corps to accomplish the requirements reference (c), the Marine Corps requires a process to unify efforts to systematically conduct cyber evaluations on critical capabilities and implement mitigations in a prioritized manner. Given the expansive nature of the attack surface, a cohesive process is vital to ensure limited resources are effectively targeted to address exploitable cyber vulnerabilities that directly impact mission success and combat preparedness in a cyber-contested environment.

2. Mission. To effectively conduct Mission-Focused Cyber Hardening (MFCH) efforts in response to reference (d) through a comprehensive, effectively coordinated, end-to-end kill chain risk assessment of critical weapon systems that includes mission chain analysis, cyber threat and vulnerability pairing, enterprise-wide risk mitigation prioritization, risk reduction recommendations, and strategies to increase the cyber survivability of critical weapon systems.

3. Execution

a. Commander's Intent and Concept of Operations

(1) Commander's Intent. Maintain the readiness, survivability, and cyber resilience of critical Marine Corps weapon systems and supporting capabilities by identifying and mitigating cyberspace vulnerabilities.

(2) Concept of Operations. This Bulletin integrates cyber evaluation efforts across the Marine Corps to effectively identify and prioritize cyber-related risk to weapon systems. The Marine Corps employs a systematic, repeatable, and rapidly executable process to target risk reduction strategies to potential sources of mission failure. This approach enables the Marine Corps to invest in increasing the cyber survivability of our warfighting capability, ensuring our ability to continue the fight and accomplish the mission in all circumstances and operating conditions.

b. Subordinate Element Missions

(1) Deputy Commandant for Plans, Policies, and Operations (DC PP&O) shall:

(a) Lead the Mission Focused Weapons System cyber assessment process to support cyber hardening and operational resiliency.

(b) Lead development and coordinate additional requirements of a TS//SCI MFCH data repository for mission chain analyses, kill chain analyses, cyber survivability plans, and risk reduction strategies.

(c) In conjunction with identified commanders, leverage a systematic process to determine priority missions for weapon systems requiring cyber survivability hardening in accordance with FY21 MFCH of weapon systems.

(d) Lead the conduct of end-to-end mission and kill chain analyses with all stakeholders IAW priority missions to identify risk of mission failure or severe compromise of critical capabilities.

(e) Integrate with Marine Corps Tactical Systems Support Activity (MCTSSA), Deputy Commandant for Information (DC I), Deputy Commandant for Combat Development and Integration (DC CD&I), and Marine Corps Systems Command (MCSC) to identify mission critical systems or Programs of Record (POR) in order to establish a specified target system for Red and Blue Team assessment.

(f) Collaborate with stakeholders to provide MFCH risk remediation recommendations for incorporation into actionable strategies that enhance a commander's ability to conduct missions in a cyber-contested environment.

(g) Support the MFCH process to address mission priorities until funding has expired for FY21.

(2) Deputy Commandant for Information (DC I) per the authorities outlined in references (g), (h), (i), and (j) shall:

(a) Develop and update applicable policies to reflect the MFCH requirement for critical capabilities and infrastructure per the direction and authorities as assigned in reference (i).

(b) Develop workflows in the Marine Corps Compliance and Authorization Support Tool (MCCAST) for the Risk Management Framework (RMF) Assessment & Authorization (A&A) process of applicable weapon systems and infrastructure associated to the MFCH process.

(c) In collaboration with DC CD&I and MCSC, coordinate Blue Team assessments consistent with prioritization coordinated by DC PP&O through all supported stakeholders.

(d) Coordinate with stakeholders and ensure they program funding to address their cyber risks identified by the risk assessments. Risk plans and assessments will be programmed under Cyber Engineering Analysis (CEA). Stakeholders are responsible for programming their remediation costs under their POR. DC I will develop and implement a cost reporting process that captures risk assessments and mitigation actions invested.

(e) Incorporate enterprise assessments of RMF A&A standards and processes for cybersecurity, information technology, and operational technology products and services as applicable per references (i), (j), and (k).

(f) Review MFCH reports related to Marine Corps systems and assets and develop risk reduction plans for prioritized vulnerabilities in accordance with the RMF A&A process per references (j) and (k).

(g) In collaboration with DC PP&O, support the analysis of the operational and mission impacts of cyber vulnerabilities related to evaluated weapon systems and infrastructure per reference (i).

(h) In collaboration with MARFORCYBER, provide intelligence support to MFCH that includes analyses, threat vulnerability assessments, and risk reduction mitigation strategies.

(i) Collaborate with stakeholders to develop investment strategies based on risk assessment findings and recommendations and advocate for program and policy solutions for MFCH activities.

(j) Lead and manage Marine Corps network information technology and operational technology remediation activities identified by MFCH in accordance with the RMF A&A process per references (i), (j), and (k).

(3) Deputy Commandant Combat Development & Integration (DC CD&I) shall:

(a) In collaboration with DC I, coordinate Red and Blue Team system-of-system adversarial assessments consistent with prioritization coordinated by DC PP&O through all supported commanders.

(b) If a non-materiel solution is required, integrate with the appropriate Program Manager (PM) to develop and implement a risk reduction solution.

(c) If a materiel solution is required, integrate with MCSC to begin cost risk analysis and implement necessary requirement change for development of materiel solution.

(4) Marine Corps Tactical Systems Support Activity (MCTSSA) shall:

(a) Execute Blue and Red Team adversarial assessments for each specified target system IAW the priority assessment budget.

(b) If an acquisition change is required, develop vulnerability reduction recommendations for discovered exploits of specified systems that could affect the weapons system's ability to execute the required mission functions.

(c) Utilize vulnerability reduction recommendations and integrate with the PM for CEA and the target POR PM to evaluate existing solutions and strategies already developed and planned for execution.

(d) Integrate with DC PP&O, DC CD&I, DC I, MCSC, Marine Forces Cyberspace Command (MARFORCYBER), and other applicable MARFORS to develop a strategy for cyber hardening in order to determine the most expedient method (without new development) to defend the target system and harden the capability against cyber-attack.

(e) Integrate with MCSC, DC PP&O, and DC CD&I to identify DOTMLPF-P solutions that most significantly reduce the cyber vulnerabilities of cyber-attack against discovered vulnerabilities and cost.

(f) Implement the cyber survivability strategy and conduct Blue Team adversarial assessments in order to validate the risk reduction solution.

(5) Marine Corps Operational Test and Evaluation Activity (MCOTEA) shall:

(a) Validate response metrics for target system to determine the time to failure, time to detect, time to respond and time to recover in order to inform DC PP&O of impact to mission, readiness, and operational resilience of force in response to cyber-attacks on specified target system.

(b) Integrate with DC PP&O, DC I, and MARFORCYBER to communicate risk and readiness via the MFCH repository to ensure Defensive Cyberspace Operations (DCO) are effectively prepared for defense of critical system.

(6) Marine Corps Systems Command (MCSC) shall:

(a) If an acquisition program change is required, integrate with MCTSSA to conduct Blue Team adversarial assessments for specified target system and architecture.

(b) Provide Blue and Red Team adversarial assessment results to stakeholders to support the Cyber Survivability Strategy Development.

(c) Coordinate with POR and Functional Area Managers (FAMs) to develop an implementation strategy that minimizes operational impacts to the FMF.

(7) Commanders, geographic MARFORS, functional MARFORS, and Supporting Establishment (SE) Commands shall:

(a) Participate and inform the end-to-end kill chain analysis of priority missions to identify risk of failure or severe compromise to critical assets / capabilities.

(b) Provide inputs to the MFCH process to DC PP&O for inclusion in the TS//SCI MFCH data repository.

(8) Coordinating Instructions

(a) Commanders will share cybersecurity assessment results with stakeholders to ensure applicable weapon systems/capabilities deployed and tactical, allied, or other command and control systems are protected to the fullest extent possible.

(b) All PORs PMs shall report to DC I their MFCH costs. MFCH cost reports shall include the risk assessment findings and recommendations; and cost to remediate POR risks. DC I shall develop the report's design and establish the reporting frequency.

(c) Cyber survivability measures provided by the MCSC program office will be integrated into the maintenance and sustainment POR management system(s).

(d) Systems evaluated in response to reference (a) will be tracked in Marine Corps Critical Asset Management Systems (MC-CAMS), MCCAST, and all other applicable repositories to support risk reduction activities.

(e) Supply Chain Risk Management will be conducted in accordance with reference (l) to inform the MFCH process and meet Department of Defense Chief Information Officer guidelines.

(f) During POR gate reviews, ensure cyber vulnerabilities are identified along with risk acceptance and mitigation, in order to assist early identification and mitigation of intelligence-informed vulnerabilities.

(g) Distribute MFCH findings to the FAMs, PMs, and Capability Integration Officers (CIOs) to inform future capability development and gate reviews in accordance with reference (m) and facilitate mitigation of cyber vulnerabilities.

4. Administration and Logistics

a. Records Management. Records created as a result of this directive shall be managed according to National Archives and Records Administration (NARA)-approved dispositions per reference (o) to ensure proper maintenance, use, accessibility and preservation, regardless of format or medium. Records disposition schedules are located on the Department of the Navy/Assistant for Administration (DON/AA), Directives and Records Management Division (DRMD) portal page at: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx. Refer to reference (o) for Marine Corps records management policy and procedures.

b. Privacy Act. Any misuse or unauthorized disclosure of Personally Identifiable Information (PII) may result in both civil and criminal penalties. The Department of the Navy (DON) recognizes that the privacy of an individual is a personal and fundamental right that shall be respected and protected. The DON's need to collect, use, maintain, or disseminate PII about individuals for purposes of discharging its statutory responsibilities shall be balanced against the individuals' right to be protected against unwarranted invasion of privacy. All collection, use, maintenance, or dissemination of PII shall be in accordance with the Privacy Act of 1974, as amended (reference (p)) and implemented per reference (q).

c. Recommendations. Recommendations to this Bulletin may be sent to Deputy Commandant Combat Development and Integration via richard.swihart@usmc.mil.

5. Command and Signal

a. Command. This Bulletin is applicable to the Marine Corps Total Force.

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

G. P. OLSON
Staff Director,
Marine Corps Staff

DISTRIBUTION: PCN 10200396700

Definitions
(These definitions are for the purpose of this MCBUL only)

Blue Team: A group of individuals that conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cybersecurity readiness posture. Often times a Blue Team is employed by itself or prior to a Red Team employment to ensure that the customer's networks are as secure as possible before having the Red Team test the systems. The group responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team).

Criticality: Defined measurement of the strategic value of a given asset and its mission that includes impact type, time to impact, and time to restore.

Cyber Survivability: The ability of a system or infrastructure to prevent, mitigate, and recover from cyber events. Cyber Survivability focuses on detectable cyberattacks.

Cyber Resiliency: The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber Resiliency efforts assume the presence of undetectable potential disruptions.

Hazard: A condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degredation. .

Mission Focused Cyber Hardening (MFCH): The application of standards, processes, and procedures across the DOTMLPF-P spectrum to achieve operational resilience through cyber survivability such that weapons systems, supporting assets, and infrastructure are able to execute defense critical missions throughout their life cycle in a contested cyber environment.

Mitigation: A solution set, whether materiel or process, that contains, reduces, or resolves a risk.

Operational Resilience: The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions.

Red Team: A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture.

Remediation: The act of correcting or reducing the impact to a vulnerability or eliminating a threat through mitigation.

Risk: Probability and severity of loss [mission failure or severe degradation] linked to threats or hazards.

Threat: Human-caused intentional actions that can impact the viability of an asset or mission.

Vulnerability: 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (JP 3-01) 2. The characteristics of a system that can cause it to be degraded (incapability to perform the designated function or mission) as a result of being subjected to a certain level of effects in an unnatural (man-made) hostile environment. (JP 3-60) 3. In information operations, a weakness in information system security design procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. (JP 3-13)

Mission Focused Cyber Hardening (MFCH) Flowchart