Marine Corps

Commercial Mobile Device Strategy

April 2013

THIS PAGE INTENTIONALLY LEFT BLANK

FOREWORD

The currently constrained budget environment requires us to balance fiscal responsibility and mission accomplishment. To align with DOD strategies and initiatives and in accordance with the Marine Corps Information Enterprise (MCIENT) Strategy, the Marine Corps has begun consolidating data centers and published a private cloud computing environment strategy. With increasing mobile device capabilities, the Marine Corps recognizes the trend of evolving information needs within garrison and tactical environments and the need to provide an agile method of meeting those needs. The user requirement to access and share information from non-traditional workspaces will enable more efficient mission accomplishment. The ability to access, share and manipulate data and information from non-traditional workspaces will afford users with additional freedom of movement across an expanding information environment. The flexible and ubiquitous ability to share information effectively will reduce the orientation and decision-making timelines, thereby affecting more rapid mission accomplishment.

Through this strategy, I am establishing a secure mobile framework that will enable the Marine Corps to identify mobile device capability requirements, leverage existing resources to include approved personally owned mobile devices and classified mobile device capabilities.

Kevin J. Nally

Brigadier General, United States Marine Corps

Director, Command, Control, Communications, and Computers Department (C4)

Department of the Navy Deputy Chief Information Officer

Deputy Commanding General, MARFORCYBER

THIS PAGE INTENTIONALL LEFT BLANK

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

The demand for and use of mobile devices in the United States Marine Corps has significantly increased in recent years primarily due to their convenience, ease of use, and productivity benefits. Currently, the use of mobile devices on the Marine Corps Enterprise Network (MCEN) is limited to privileged users[1]; however, the Department of Defense (DOD) is shifting to an environment where mobile access to networks and information is no longer limited by this parameter. An example of this shift is evidenced by DOD Instruction 1035.01, which addresses using personally owned computers on unclassified DOD systems and networks. With personnel in garrison increasingly working in non-traditional workspaces, the DOD recognizes the need to access enterprise resources for performing tasks, such as delivering information or decision briefs (through development of presentations), face-to-face conversations over distance (through VTC systems), information sharing (through file and web services), and messaging, which facilitates information sharing (through email, chat, real time presence, and social media).

The increased use and functionality of mobile devices introduces new security threats to the MCEN. The requirement of incorporating standardized information assurance tactics, techniques, and procedures for mobile devices within the MCEN directly relates to the importance of implementing a secure mobile framework (SMF), which will ultimately support the Marine Corps way ahead. To achieve the overall Commercial Mobile Device Strategy, the Marine Corps will strive to attain the following four goals: 1) Establish a Secure Mobile Framework; 2) Transition the Unclassified Mobile Device Infrastructure to a Cost Effective and Platform Agnostic Environment; 3) Collaborate with DOD and Industry Partners to Develop a Classified Mobile Device Capability; and 4) Incorporate Personally Owned Mobile Devices.

NOTE: The use of personally owned mobile devices, as outlined in this strategy, is applicable only within the garrison environment, not in the tactical environment.

[1] A privileged user is an individual that the Command identifies as being mission critical or mission essential and is provided mobile government furnished equipment (GFE) or a reimbursement for using their commercial mobile device to gain access to their personal organizational data.

2 INTRODUCTION

Traditionally, the use of mobile devices within the Marine Corps has been limited to privileged users with a requirement to access Marine Corps data outside the traditional workspace. Moving forward, in accordance with senior organizational strategies and in recognition of the increasing mobile workforce requirements for IT consumerization across the DOD, this document identifies four goals for mobile device implementation across the Marine Corps: 1) Establish a Secure Mobile Framework; 2) Transition the Unclassified Mobile Device Infrastructure to a Cost Effective and Platform Agnostic Environment; 3) Collaborate with DOD and Industry Partners to Develop a Classified Mobile Device Capability; and 4) Incorporate Personally Owned Mobile Devices.

3 FOUNDED ON USER REQUIREMENTS

As the Deputy Department of the Navy Chief Information Officer (CIO) (Marine Corps), one of the C4 Director's responsibilities is to "identify IT investment opportunities for the Marine Corps and those that would result in shared benefits or cost avoidance/savings" (MCO 5400.52, 2010). Basing decisions on user requirements and validated needs is essential in avoiding the cost of acquiring technology based on industry trends.

4 MOBILE DEVICE DEFINITION

In order to ensure alignment with the DOD Mobile Device Strategy, this document will use the same mobile device definition. A mobile device is a handheld computing device with a display screen that allows for user input (e.g., touch screen, keyboard). When connected to a network, it enables the sharing of information in formats specially designed to maximize the use of information given device limitations (i.e., screen size, computing power). Mobile devices provide the conveniences of conventional desktops or laptop computers in a more portable package. Examples of popular mobile devices include smart phones and tablets.

5 CURRENT STRATEGIES

Both the Federal and DOD CIO have published strategies that deal with the incorporation of mobile devices into public sector networks. The Marine Corps has also published a strategy to influence enterprise Force Development priorities. Aligning this document with their objectives and goals is essential for efficient implementation and overall interoperability.

5.1 DIGITAL GOVERNMENT STRATEGY

The Digital Government Strategy focuses on improving Federal Government processes to enable the rapid adoption and acquisition of emerging technologies, to include mobile and wireless related capabilities. It highlights the need to securely architect systems for interoperability and openness from conception. In addition, it promotes common standards and methods to share lessons learned by early adopters. The Digital Government Strategy will adopt a coordinated approach to ensure privacy and security in a digital age by achieving the following objectives:

I. Enable the American people and an increasingly mobile workforce to access high-quality digital government information and services anywhere, anytime, on any device.

II. Ensure that as the government adjusts to this new digital world, we seize the opportunity to procure and manage devices, applications, and data in smart, secure and affordable ways.

III. Unlock the power of government data to spur innovation across our Nation and improve the quality of services for the American people.

5.2 DEPARTMENT OF DEFENSE MOBILE DEVICE STRATEGY

The DOD Mobile Device Strategy identifies IT goals and objectives to capitalize on the full potential of mobile devices. It focuses on improving three areas critical to mobility: wireless infrastructure; the end device; and mobile applications. It provides a framework which will facilitate the Department to converge towards a common vision and approach. The Marine Corps Commercial Mobile Device Strategy will align with the following DOD Mobile Device goals:

I. Advance and evolve the DOD Information Enterprise infrastructure to support mobile devices.

II. Institute mobile device policies and standards.

III. Promote the development and use of DOD mobile and web-enabled applications.

5.3 MARINE CORPS INFORMATION ENTERPRISE STRATEGY (MCIENT)

The purpose of the MCIENT strategy is to influence enterprise Force Development priorities by providing the Marine Corps' single, top level Information Enterprise objectives that inform future capability decisions, supporting plans, concepts, and programming initiatives. As such, it serves as Appendix 1 of Annex K to the Marine Corps Service Campaign Plan. The MCIENT strategic objectives relevant to this strategy are shown in Figure 1.

Figure 1. Relevant MCIENT strategy objectives

6 GOALS AND OBJECTIVES[2]

The Marine Corps Commercial Mobile Device Strategy identifies and defines four distinct goals. Each goal includes a number of objectives that will work to achieve the respective goal.

6.1 GOAL 1: ESTABLISH A SECURE MOBILE FRAMEWORK (SMF)

The Marine Corps Commercial Mobile Device Strategy establishes the SMF, depicted in Figure 2. In direct support of MCIENT strategy objective 13, Field Systems with Inherent IA controls, the SMF will facilitate the integration of IA requirements into the mobile systems design life cycle process. In addition, the SMF will enable the Marine Corps to identify mobile device capability gaps, leverage existing resources, and fill capability gaps in a cost effective manner. This will better ensure that mobile devices are properly developed, procured, and tested, while also influencing industry to build in appropriate IA requirements at the same time internal IA policies are being modified. As a result, the SMF will facilitate streamlining of the procurement process.

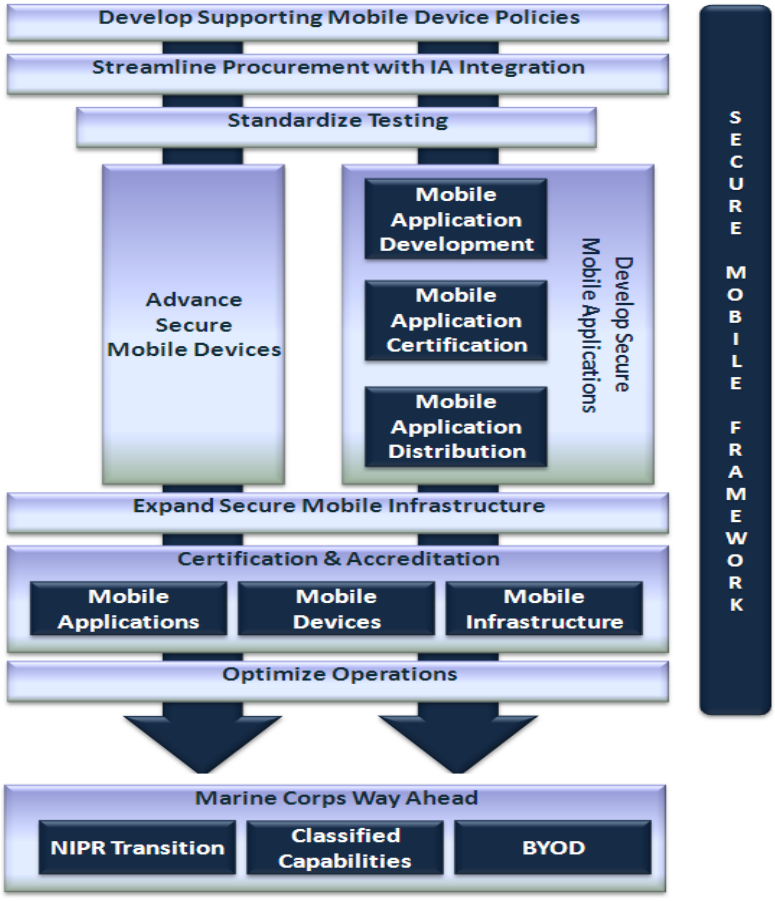


Figure 2. Secure Mobile Framework

[2] An implementation plan will be developed in order to execute the objectives identified within the Secure Mobile Framework.

6.1.1 OBJECTIVE 1.1: DEVELOP MOBILE DEVICE POLICY

(Supports MCIENT Objectives 1, 2, 4, 8, and 13) Policies related to mobile device incorporation will be developed and maintained to reflect and support Marine Corps requirements. MARADMINs, USMC Enterprise Cybersecurity Directives (ECSDs), and Naval Messages will address all mandated guidance for the procurement, testing, and fielding of mobile technologies and their associated transmissions. ECSDs define the IA parameters for different technologies and protocols used within the MCEN.

6.1.2 OBJECTIVE 1.2: EXPEDITE PROCUREMENT

(Supports MCIENT Objectives 4 and 13) Efficient procurement of mobile capabilities is essential in order to satisfy user requirements. The current IT procurement request review and approval processes need to continue to be enhanced to expedite the overall procurement process. This includes utilizing an approved mobility products list similar to the Marine Corps Common Hardware Suite (MCHS) service catalog construct, and an approved mobile application list similar to the Marine Corps Software Enterprise License Management System (MCSELMS) construct.

6.1.3 OBJECTIVE 1.3: ADVANCE SECURE MOBILE DEVICES

(Supports MCIENT Objectives 2, 3, 4, 9, 10, and 13) With an abundance of dynamic and complex mission requirements across the Marine Corps, there are advantages for adopting a variety of mobile operating systems and form factors. By working with and influencing industry, different hardware components will be enhanced in order to satisfy Marine Corps needs.

6.1.4 OBJECTIVE 1.4: DEVELOP SECURE MOBILE APPLICATIONS

(Supports MCIENT Objectives 2, 3, 4, 9, 10, and 13) The unique capabilities of secure mobile applications can provide distinct advantages for the Marine Corps; however, the potential security concerns associated need to be evaluated and controlled appropriately.

6.1.4.1 Mobile Application Development

The Marine Corps will leverage the DOD CIO common mobile application development framework, which will consist of developer tools, documentation, and automated processes to help build and test mobile applications. This will ensure efficiencies and interoperability across mobile platforms and between the Services.

6.1.4.2 Mobile Application Attestation

The Marine Corps will treat every application, whether developed commercially or by the government, as untrusted until proper Marine Corps attestation is completed, per ECSD 018: Marine Corps Certification and Accreditation Process. Attestation tools and processes will ensure the application is doing what it is supposed to do. Tightly integrated with the Marine Corps C&A process, mobile application attestation will look for elevated permissions, embedded malware, and irregular access of data stores and memory from outside applications. Results and documentation from the attestation process will provide the MCEN AO/DAA with the necessary information to make an educated risk management decision.

6.1.4.3 Mobile Application Distribution

The Marine Corps will leverage approved existing investments, as well as external resources (e.g., DISA Mobile Application Store) for application distribution, where applicable.

6.1.5 OBJECTIVE 1.5: STANDARDIZE TESTING

(Supports MCIENT Objectives 2, 8, 12, and 13) The Marine Corps will leverage current operational testing procedures (e.g., Joint Interoperability Test Command [JITC]), DOD facilities (e.g., DOD IA Range), and policies and configuration documents to standardize a mobile and wireless technology testing process.

6.1.6 OBJECTIVE 1.6: EXPAND SECURE INFRASTRUCTURE

(Supports MCIENT Objectives 1, 2, 3, 4, 9, 10 and 13) A diverse wireless infrastructure introduces a number of spectrum and security concerns due to the inherent characteristics of radio frequency (RF); therefore, applicable IA controls need to be implemented. By strategically placing and expanding mobile device management (MDM) capabilities, the Marine Corps will offer an enterprise infrastructure that supports device and platform agnostic capabilities. The provisioning of MDM platforms must be incorporated into an engineering effort in support of the MCEN.

The Marine Corps provides enterprise-wide access to the MCEN. In the garrison environment, the Marine Corps leverages commercial networks for privileged mobile communications users; however, for forward deployed forces we will need to continue to evolve our MAGTF communications and devices. In addition, wireless network/personnel authentication and encryption controls will continue to advance in order to support a mobile environment.

An additional capability that is being considered for mobile users is the ability to gain access to the individual's workspace via an external form of media. Using the same enterprise configurations for desktops and laptops will ensure security requirements are being met regardless of the operating system the external media is using for network and display access. This platform is not intended to replace desktops, laptops, or other mobility offerings. Rather, it provides support for efficient use of resources for alternative workplace environments.

6.1.7 OBJECTIVE 1.7: CERTIFICATION & ACCREDITATION

In alignment with the DOD Mobile Device Strategy, the Marine Corps will continue to find ways to expedite the current C&A process (e.g., approved products list, approved mobile application list, etc.) and leverage approved cross department/agency DIACAP packages for reciprocity.

6.1.8 OBJECTIVE 1.8: OPTIMIZE OPERATIONS

(Supports MCIENT Objectives 1, 2, 3, and 10)The mobile workforce's ability to access information and computing power can optimize information sharing, communication, and action response time for greater mission effectiveness. The Marine Corps will ensure the SMF continuously evolves in alignment with DOD and DoN strategies and policies, MCIENT objectives, and industry advancements.

6.2 GOAL 2: TRANSITION THE UNCLASSIFIED MOBILE DEVICE INFRASTRUCTURE TO A COST EFFECTIVE AND PLATFORM AGNOSTIC ENVIRONMENT

(Supports MCIENT Objectives 1, 3, 4, 12, and 13) As the MCEN regionalization efforts continue to move forward, the Marine Corps will modify the current mobile device management infrastructure to support platform agnostic unclassified devices and capabilities. This includes, but is not limited to, advancing virtualization and mobile device management capabilities. In addition, the Marine Corps will continue to enhance its telecommunication expense management (TEM) services to establish more cost efficient commercial service plans.

6.2.1 OBJECTIVE 2.1: CONTINUE CURRENT MOBILITY OPERATIONS AND MAINTENANCE SUPPORT

The Marine Corps will continue to provide operational and maintenance support to current mobile solutions. This includes current MCEN portable electronic devices, telework capabilities, and basic cellular and Wi-Fi capabilities. In addition, the Marine Corps will continue to provide emerging technologies, where possible, to satisfy urgent mission requirements.

6.2.2 OBJECTIVE 2.2: IDENTIFY MOBILE SOLUTIONS WHICH SUPPORT PLATFORM AGNOSTIC DEVICES

In order to expand operational capabilities, the Marine Corps must expand its infrastructure to support a variety of platforms and devices. The Marine Corps will evaluate a number of options, both externally and internally, to assess, select, and implement platform agnostic mobile device management and virtualization capabilities for unclassified devices.

6.2.3 OBJECTIVE 2.3: MANDATE AND PROMOTE THE USE OF TELECOMUNICATION EXPENSE MANAGEMENT SOLUTIONS

By leveraging current resources, the Marine Corps will develop training and awareness initiatives to promote TEM solutions. By mandating the use of TEM solutions, the Marine Corps will realize an instant return on investment by managing costs and streamlining savings across the entire Marine Corps enterprise.

6.3 GOAL 3: COLLABORATE WITH DOD AND INDUSTRY PARTNERS TO DEVELOP A CLASSIFIED MOBILE DEVICE CAPABILITY

(Supports MCIENT Objectives 1, 3, 4, 12, and 13) In addition to traditional Type 1 Government Off-The-Shelf products, the DOD is progressing towards leveraging Commercial Off-The-Shelf products to handle classified services. This is a paradigm shift in the way the DOD has handled Cryptographic Controlled Items/Type 1 devices and classified services. The Marine Corps currently relies on capabilities like the Secure Mobile Environment Portable Electronic Device (SME PED) to provide mobile classified voice and data capabilities. However, the carrier's technology which provides these services is nearing end of life and the Marine Corps will have a capability gap for mobile classified voice services. The Marine Corps will continue to collaborate with the National Security Agency regarding their Commercial Solutions for Classified process to develop DISA classified mobile services, and transmission capabilities for both the Garrison Base Post Camp Station (G/B/P/C/S) environment and forward deployed forces.

6.3.1 OBJECTIVE 3.1: COORDINATE WITH OTHER SERVICES

Collaborating with other military Services will be necessary for understanding the current environments that each face. Additionally, knowing where potential gaps and overlaps exist will provide opportunities to promote information sharing, as well as exchanging best-practices.

6.3.2 OBJECTIVE 3.2: LEVERAGE EXISTING TECHNOLOGIES

Given the current economic landscape and DOD-wide efforts to decrease spending, the Marine Corps will work with other Services, Agencies, and industry partners to identify existing technology, rather than using constrained funds to develop new solutions.

6.4 GOAL 4: INCORPORATE PERSONALLY OWNED MOBILE DEVICES

(Supports MCIENT Objectives 1, 3, 4, 12, and 13) The Marine Corps will establish a mobile environment that allows the workforce to leverage approved personally owned mobile devices to access MCEN NIPRNet controlled unclassified information (CUI). This concept, commonly known as Bring Your Own Device (BYOD), offers a number of advantages, including cost efficiency and increased worker effectiveness; however, it also introduces a number of challenges, such as legal ownership rights and security validation. The key tenet to implementing a BYOD environment is ensuring the security of the MCEN is maintained. As previously mentioned, inclusion into tactical networks will not be feasible.

For G/B/P/C/S, the Telework Enhancement Act of 2010 (DOD I, OMB memo, and MCO) has set precedence for telework and encourages federal employees to do so. Authorized users gain remote access to personal organizational data (e.g., mail, calendar, tasks, contacts, and notes) that resides within the MCEN infrastructure via authentication and authorization technology on personally owned devices. Remote access to security enabled, organizational collaboration sites that reside on the MCEN further enhances telework capabilities and multiple worksite environments.

Participation in a BYOD environment is completely voluntary and no command, organization, or office may make it otherwise.

6.4.1 OBJECTIVE 4.1: DEVELOP PERSONALLY OWNED MOBILE DEVICE POLICY

Current policy exists for privileged mobile users and telework users; however, with modification, this policy can be expanded to encompass all individuals (i.e., privileged and non-privileged users[3]) that desire using authorized personally owned mobile devices to access their personal organizational data. Coordination with USMC and DoN legal teams is required to modify this policy. Additionally, coordination with DOD CIO pertaining to the use of personally owned commercial mobile devices will have to occur in order to address the DOD CIO Commercial Mobile Device Interim Policy.

6.4.2 OBJECTIVE 4.2: DEVELOP PROCEDURES TO IDENTIFY AUTHORIZED PERSONALLY OWNED MOBILE DEVICES

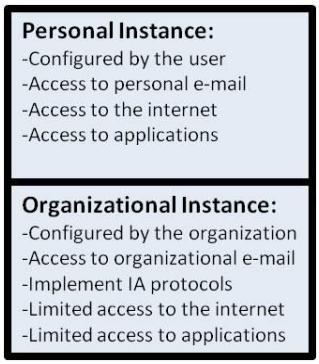
The Marine Corps Commercial Mobile Device Strategy for BYOD relies heavily on separation technology within the end node terminal device to support multiple domains. This can be accomplished either through hardware separation (e.g., multiple hardware abstraction layers [HAL] based on a chipset that

[3] A non-privileged user is an individual that is not provided GFE, nor reimbursed for the use of a commercial mobile device to gain access to their personal organizational data.

can run multiple instances of an operating system), or software separation (e.g., virtualization, bootable non-persistent operating systems, remote desktop platforms, etc.). Each of these methods can enhance the Marine Corps BYOD environment. This will incorporate IA requirements to ensure users are selecting mobile services, devices, and products that are in accordance with DOD and Marine Corps IA policies.

Only those devices that can be configured to support multiple domains will be considered as candidates for inclusion to the authorized list.

6.4.3 OBJECTIVE 4.3: STANDARDIZE SECURITY CONTROL PROCEDURES



The Marine Corps will employ authentication and authorization technology on the organizational instance of approved personally owned mobile devices to provide an additional layer of information security, as well as a function for ensuring adherence to mandated policies. Access to the individual's personal instance will be based on their personal security parameters and will not be mandated nor controlled by the Marine Corps.

The separation technology and implementation of organizational security policies ensures that personal organizational data and personal data are not compromised nor commingled on a single commercial mobile device. This provides an aspect of personal privacy and organizational privacy not seen on traditional commercial and government implementations of BYOD.

6.4.4 OBJECTIVE 4.4: PRIVILEGED USERS AND NON-PRIVILIGED USERS

In order to realize a reduction in Operations and Maintenance (O&M) costs, as they pertain to our mobile workforce, Commands must identify those individuals it deems as privileged users and non-privileged users. As Command O&M budgets decrease, it is anticipated that the number of privileged users will also decrease; however, it is the responsibility of the Command to determine what constitutes mission critical or mission essential personnel.

As previously mentioned, privileged users are those individuals that a Command identifies as being mission critical or mission essential. These individuals are provided mobile GFE or a reimbursement for using their commercial mobile device to access their personal organizational data in support of their daily functions and tasks. For example, a Command would expect privileged users to be able to return phone calls, answer e-mails, or initiate some type of recall 24 hours a day, 7 days a week.

Also previously mentioned, non-privileged users are individuals that are not provided GFE, nor are they reimbursed for using a commercial mobile device to access their personal organizational data. Again, it is the Command's responsibility to determine whether an individual is considered mission critical or mission essential. There are no expectations for Marines, Sailors, civilian Marines, or contractors supporting Marine commands and organizations to participate in a BYOD environment if they are deemed to be non-privileged users. Participation in a BYOD environment is completely voluntary.

7 WAY AHEAD

The Marine Corps will continue participating in the DOD CIO Commercial Mobile Device Working Group, the DoN Enterprise Mobility Integrated Product Team, and working with other Federal Agencies and industry partners. This will better position the Marine Corps to eliminate duplication of efforts and will ensure Marine Corps mobility requirements are identified in mobile device capability development. An implementation plan with a plan of action and milestones, driven by achievable dates, is being developed in order to execute the goals identified within the Marine Corps Commercial Mobile Device Strategy.

APPENDIX I – REFERENCES

- Telework Enhancement Act of 2010 (Public Law 111 – 292). 2010
- Digital Government Strategy. 2012
- Department of Defense (DOD) Instruction 1035.01. 2012
- Department of Defense (DOD) Chief Information Officer (CIO) Memo: Commercial Mobile Device (CMD) Interim Policy. 2012
- Department of Defense (DOD) Mobile Device Strategy. 2012
- Marine Corps Order (MCO) 5400.52. 2010
- United States Marine Corps (USMC) Service Campaign Plan 2012 – 2020. 2012
- Marine Corps Information Enterprise (MCIENT) Strategy. 2010
- Marine Corps Enterprise Cybersecurity Directive (ECSD) 018. 2012
- Marine Corps Certification and Accreditation Process. 2012

PLEASE PROVIDE FEEDBACK TO HQMC C4 VISION AND STRATEGY (CV) DIVISION

Mr. Rob Anderson
Robert.L.Anderson@usmc.mil
CV Division Chief

The mission of the HQMC C4 Strategy and Vision Division is to serve as the primary and dedicated support staff to assist the Director in developing, communicating, implementing, and assessing his vision and priorities for the Marine Corps Information Enterprise across all war fighting domains.

THIS PAGE INTENTIONALLY LEFT BLANK


COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS
Headquarters, U.S. Marine Corps, Washington, DC
C4