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

2300-19
IC4/ICC
APR 24 2023

From: Director, Information, Command, Control, Communications, and Computers (IC4) Division, Deputy Commandant for Information (DC I)

Subj: MARINE CORPS INFORMATION TECHNOLOGY (IT) REGISTRATION

Ref: (a) SECNAV Memo, Designation of the DON Deputy CIO (Navy) and the DON Deputy CIO (Marine Corps)
(b) MCO 5400.52
(c) MCO 5230.21
(d) SECNAVINST 5230.14
(e) DODI 5000.85

Encl: IRM 2300-19 Marine Corps IT Registration Policy

1. Purpose. To establish policy and standard processes for all Marine Corps components to register Marine Corps IT applications, mobile apps, and systems; regardless of network connectivity (i.e., whether stand- alone, or operating on a Marine Corps, commercial, cloud or other network). This includes as-a-Service (aaS) offerings (i.e., software (SaaS), platform (PaaS), infrastructure (IaaS), other (XaaS)).

2. Cancellation. This document is the first issuance and will supersede all previous policies and messages on the topic. In accordance with applicable Marine Corps Orders (MCOs) and National Institute of Standards and Technology (NIST) Controls, this document will be reviewed at least once annually and updated when necessary to account for emerging technologies.

3. Authority. The information promulgated in this publication is based upon policy and guidance contained in references (a) through (e).

4. Applicability. This publication is applicable to the Marine Corps information systems, applications, and aaS offerings, regardless of network connectivity.

5. Scope.

a. Compliance. Compliance with the provisions of this publication is required unless a specific waiver is authorized.

b. Waivers. Waivers to the provisions of this publication will be authorized by the DC I.

6. Sponsor. The sponsor of this technical publication is DCI IC4 ICC.

W. H. SEELY III
Acting

MARINE CORPS

INFORMATION RESOURCES MANAGEMENT (IRM)

2300-19

MARINE CORPS INFORMATION TECHNOLOGY (IT)

REGISTRATION POLICY

April 24, 2023

Version 1.0

This page intentionally left blank

Document Approval / Major Revision Change History Record

This table is used for initial release and subsequent revisions. Major revisions are indicated by the number to the left of the decimal point while minor revisions are indicated by the number to the right. Major revisions are required when the intent or process is changed, rendering the prior version obsolete or when the number of minor releases total twenty (20). Changes to this document shall be recorded, described, and approved using the table below:

Release Date (MM/DD/YY)	Release No.	Approvals		Change Description
		Author	Process Owner/Approver	
4/24/23	1.0	IC4 / ICC	IC4 / ICC-CIO	Initial policy
		Printed Name	Printed Name	
		Printed Name	Printed Name	
		Printed Name	Printed Name	
		Printed Name	Printed Name	

This page intentionally left blank

TABLE OF CONTENTS

EXECUTIVE SUMMARY **8**
SECTION 1.0: INTRODUCTION **10**
1.1 Background 10
1.2 Purpose 10
1.3 Applicability and Scope 10
1.3.1 Applicability 10
1.3.2 Scope 11
1.3.3 Objectives 11
1.4 Cancellation 12
1.5 Distribution 12
1.6 Structure 12
1.7 Recommendations 12
1.8 Effective Date 12
SECTION 2.0: ROLES AND RESPONSIBILITIES **12**
2.1 Director, IC4 12
2.2 Marine Corps IC4 Authorizing Official (AO 13
2.3 IC4 Compliance Branch/Cybersecurity 13
2.4 Commanding Generals (CG)/ Commanding Officers (CO) 13
2.5 Functional Area Manager (FAM) Leads 13
2.6 Program Managers (PMs), Application/System Owners (A/SOs) 14
SECTION 3.0 IT SOLUTION REGISTRATION **14**
3.1 Definitions: 14
3.2 General 16
3.3 DON Application and Database Management System (DADMS) 17
3.4 DoD Information Technology Portfolio Repository – Department of Navy (DITPR-DON) 19
APPENDIX A: GLOSSARY (ACRONYMS & ABBREVIATIONS) **A1**
APPENDIX B: REFERENCES **B1**
APPENDIX C: EXCEPTION/WAIVER REQUEST TEMPLATE (DISAPPROVED AND/OR UNSUPPORTED SOFTWARE) **C1**

List of Figures

Figure 1: Registration Decision Flow (DADMS or DITPR-DON) 17

List of Tables

None.

This page intentionally left blank

EXECUTIVE SUMMARY

This Marine Corps manual documents the formal process for registering Marine Corps Information Technology (IT) applications, mobile apps, and systems; regardless of network connectivity (i.e., whether stand-alone or; operating on a Marine Corps, commercial, cloud or other network). This includes as-a-service (aaS) offerings (i.e., software (SaaS), platform (PaaS), infrastructure (IaaS), and other (XaaS)).

This manual supports the Department of Defense (DoD) and Department of Navy (DON) directives, instructions, and policies governing information technology governance. The IRM's primary purpose is to promulgate detailed direction to the IM/IT communities in accordance with the Marine Corps Chief Information Officer's (CIO) strategic vision and priorities. They are to be followed by Marine Corps commands, organizations, and detachments and provide a policy mechanism to communicate, coordinate, collaborate, and keep pace with Marine Corps Information Environment Enterprise (MCIEE).

This page intentionally left blank

SECTION 1.0: INTRODUCTION

Marine Corps Order (MCO) 5230.21, Information Technology (IT) Portfolio Management (PfM), established USMC IT PfM policy and guidance. Among the responsibilities listed in the MCO are the requirements to register IT solutions in the applicable authoritative data source (ADS): applications and mobile apps are to be registered in the Department of the Navy (DON) Application and Database Management System (DADMS); and IT systems are to be registered in the DON instance of the Department of Defense (DoD) Information Technology Portfolio Repository (DITPR-DON) module of DADMS. Registration of IT solutions in the applicable ADS does not allow approval to operate the solution on the Marine Corps Enterprise Network (MCEN). The Enterprise Cybersecurity Manual (ECSM) 018, Marine Corps Assessment and Authorization Process (MCAAP), established policy and procedures to obtain authority to operate IT solutions on the MCEN. This manual will address the requirement for registration of all Marine Corps IT solutions per established business processes.

1.1 Background

On 30 April 2020, the Deputy Commandant for Information (DC I) was appointed by the Secretary of the Navy (SECNAV) as the DON Deputy Chief Information Officer, Marine Corps (DDCIO(MC)), reference (a). Director, Information Command, Control, Communications, and Computers (IC4) was designated to provide leadership and governance of Marine Corps Information Management (IM) and IT activities for the Marine Corps. On behalf of DC I, the Director IC4 oversees all planning, directing, and coordinating of IT capabilities that support Marine Corps warfighting and business functions.

DoDI 8115.02, SECNAVINST 5230.14, and MCO 5230.21 require the registration and periodic review of IT solutions (e.g., systems, applications, services, etc.) in designated ADS' for the purpose of IT PfM, accountability, and reporting. MCO 5230.21 requires annual review of IT solutions. Based on a 2018 DoD Inspector General (IG) report, the IG determined "The Marine Corps [and others] did not consistently rationalize their software applications…As a result, the DoD and its Components are exposing the DoD Information Network to unnecessary cybersecurity risks…"

1.2 Purpose

To document the formal requirements for registering Marine Corps IT applications, mobile apps, and systems; regardless of network connectivity (i.e., whether stand-alone or; operating on a Marine Corps, commercial, cloud, or other network). This includes as-a-service (aaS) offerings (i.e., software (SaaS), platform (PaaS), infrastructure (IaaS), and other (XaaS) to include, but not limited to, low/no-code solutions).

1.3 Applicability and Scope

1.3.1 Applicability

This manual applies to:

- Marine Corps components, organizations, and personnel (government and non-government employees) that operate aboard Marine Corps facilities or access Marine Corps IT. This includes, but is not limited to, any Marine Corps applications, mobile apps, systems, or networks that process, store, or transmit any Marine Corps data whether

stand-alone, contractor provided, as a service, or directly connected to the MCEN backbone.

1.3.2 Scope

This document is applicable to the Marine Corps total force. The standards identified in this manual will be used as a resource by all Marine Corps organizations and departments that acquire, develop, use, and maintain IT. This includes contracted third parties who use commercial devices, services, networks, and technologies in both ashore and afloat environments accessing/utilizing Marine Corps data. This manual will not alter or supersede the existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence. The Intelligence Community (IC) is encouraged to respond to areas not specifically addressed by existing IC directives.

1.3.3 Objectives

- Any IT solution, for which the Marine Corps allocates funding or resources towards, requiring Marine Corps Risk Management Framework (RMF) actions (i.e., not currently fully leveraging an existing Authority to Operate (ATO) or Marine Corps application authorization letter), or if RMF actions are not required but the solution is categorized as Mission Critical or Mission Essential must be registered in DADMS/DITPR-DON.
- IT solutions registered in DADMS are those that only need an operating system (OS) to deliver the intended capability. These solutions are typically referred to as an application.
    - Example: Can be installed and fully operated as intended on any desktop computer or mobile device.

IT solutions registered in the DITPR-DON module of DADMS are those that require hardware and/or software components beyond the OS, and/or deemed mission critical or mission essential.

Example: If the IT solution requires the use of interfaces, and/or multiple applications; and/or platforms; and/or infrastructure to meet the required capability - it is a system. Additionally, if the IT solution is deemed Mission Critical or Mission Essential (by either the Functional Area Manager (FAM) or IC4), but does not specifically meet the definition of a “traditional” system, it is to be registered in DITPR-DON.

Software as a Service supporting a defense business function must be registered in DITPR-DON regardless of hardware/software requirements.

Non-compliance will result in a Denied Authorization to Operate (DATO) (and/or revocation of application authorization letter); and/or IT Procurement (ITPR) request disapproval; and/or failure to obtain DBS certification as required.

IC4 will monitor compliance and provide periodic reporting to DC I.

** Note: New applications and mobile apps must be compatible with Microsoft Windows version 11 (Win 11) if operating on or within a Windows environment, and be IPv6 capable. IT Portfolio Lead approval in DADMS does not equate to approval for an application, mobile app,

etc. to be installed on a Marine Corps owned end user computing device, server, or other Marine Corps IT equipment. Approval to install and use on any computing device within the Marine Corps requires authorization and accreditation (A&A) from DCI-IC4-ICC-Cybersecurity via the Application Authorization process, or, when applicable, the full system ATO A&A process as per refs (c) and (h).

1.4 Cancellation

This policy is the first issuance for IRM 2300.19 Marine Corps Information Technology (IT) Registration Policy. Subsequent released versions will supersede this IRM as applicable. This manual will be reviewed annually or on an as needed basis to facilitate the implementation of Access Control Policy and associated Access Controls.

1.5 Distribution

Approved for public release; distribution is unlimited.

1.6 Structure

This manual is organized into three major sections: (1) Introduction, (2) Roles and Responsibilities, and (3) Information Technology (IT) Solution Registration.

1.7 Recommendations

Recommendations for changes or amendments to this manual will be submitted in writing via formal task management systems through the DC I IC4-ICC-CIO Branch at: USMC_HQMC_DCI_IC4_ICC_CIO.

1.8 Effective Date

This IRM is effective upon signature.

SECTION 2.0: ROLES AND RESPONSIBILITIES

The registration of aaS, applications, mobile apps, and systems in DADMS/DITPR-DON is a coordinated effort between:

1) The end user and their representative command information office (e.g., G-6), together hereafter referred to as the application/system sponsor;
2) If assigned, the Program Manager (PM) and/or Program Portfolio Manager (PPM); and
3) The applicable IT FAM Lead and/or IT PfM support.

The positions named in this section have the responsibilities identified below:

2.1 Director, IC4

Director IC4 responsibilities:

- On behalf of DC I, serves as DDCIO(MC) pursuant to ref (a), overseeing all planning, directing, and coordinating of IT capabilities that support Marine Corps warfighting and business functions, to include but is not limited to
  - o providing leadership and governance of Marine Corps Information Management (IM) and IT activities;
  - o serving as the Marine Corps lead for IT PfM;

- serving as the Marine Corps IT Expenditure Approval Authority (ITEAA) per ref (g); and
- facilitating Marine Corps IT Audit/General Controls and Remediation.

2.2 Marine Corps IC4 Authorizing Official (AO)

AO responsibilities:

- Reviews and approves all Enterprise level Information System Security Managers (ISSM) appointments.
- Serves as RMF oversight authority for all IT processing, storing, and/or transmitting Marine Corps data.

2.3 IC4 Compliance Branch/Cybersecurity

IC4-ICC-CY responsibilities:

- Provides guidance and policy on the proper access and use of Marine Corps IT.
- Provides risk assessment authority for the introduction or use of Marine Corps IT.
- Provides policy on the proper access and use of cybersecurity and information assurance policy and standards.
- Incorporates DoD and DON policies as necessary.
- Addresses access and appropriate use issues of emerging products.

2.4 Commanding Generals (CG)/ Commanding Officers (CO)

CG/CO responsibilities:

- Implements local procedures to comply with this manual as the final authority for access to Marine Corps IT.
- Ensures coordination with the applicable FAM Lead(s) prior to the development of any IT solution.
- Ensure IT procurement submission and approval via ITPRAS prior to executing resources in support of IT services and solutions.
- Ensures all IT solutions in use are registered within the Marine Corps ADS or other Service ADS.
- Coordinate the registration of IT via the applicable FAM Lead.

2.5 Functional Area Manager (FAM) Leads

FAM Lead and FAM Lead support responsibilities are as follows:

- As it pertains to this IRM, register all IT within their area of responsibility (AOR) (i.e., IT portfolio alignment) in the applicable ADS.
- Set the last date allowed for IT registered in DADMS as follows:
  - Commercial-off-the-shelf (COTS) – to the vendor end-of-support (EOS) date or sooner; or to the contract period-of-performance (POP) or sooner if third party support is procured.
  - Government-off-the-shelf (GOTS) – to the contract POP or sooner if contractor supported; or no longer than one year from the date of request if not contractor supported.
  - Open Source Software (OSS) – no longer than one year from the date of request.
  - Mobile app – treated as COTS if developed by a third party vendor; treated as GOTS if developed by a government entity; or OSS as applicable.

- In coordination with DCI-IC4-CIO, categorize IT solutions within respective portfolios as Mission Critical, Mission Essential, or Mission Support.
- In coordination with DCI-IC4-CIO, register all capitalized internal use software (IUS) in DPAS with required key supporting documentation.
- For additional FAM Lead roles and responsibilities see ref (C).

2.6 Program Managers (PMs), Application/System Owners (A/SOs)

PM and/or A/SO (where a PM is not assigned) responsibilities:

- Ensure coordination with FAM Lead(s) prior to, as well as during, development or procurement of IT, to include initiation of an ITPR prior to procurement of IT solutions.
- Ensure all IT in use within their AOR are registered in an ADS and have the applicable RMF accreditation (i.e., ATO or Application Authorization (formally Marine Corps Certified Application (MCCA) letter).
- Ensure IT within their AOR maintain compliance with applicable laws, regulations, policy, and guidance (LRPG) (e.g., Clinger-Cohen Act (CCA), RMF, IUS, etc.)
- Coordinate the registration of IT via the applicable FAM Lead.
- Maintain DITPR-DON records after creation by the FAM Lead.
- After creation of a DPAS record in accordance with USMC IUS policy and or procedures, maintain IUS DPAS records for accountability and audit reporting. Provide all key supporting documentation (KSD) as required by policy.
- Initiate annual review of IT within their AOR (e.g., DITPR-DON annual reviews, Last Date Allowed (LDAs), etc.)
- Assist FAM Leads with portfolio reviews (e.g., provide financial information, capability requirements, etc.).
- Provide lifecycle management functions for respective IT solutions.

SECTION 3.0 IT SOLUTION REGISTRATION

3.1 Definitions:

- **Application**: Any software that uses an existing operating system program to provide the user with a specific capability or function that is independent of other "applications." If it is dependent on other applications and/or specific hardware (i.e., a server) beyond an end user device (e.g., desktop computer, smart phone, etc.), it becomes a system. (MCO 5230.21).

- **Defense Business System**: An information system that is operated by, for, or on behalf of the DoD, including any of the following: Financial system; Financial data feeder system; Contracting system; Logistics system; Planning and Budgeting system; Installations Management system; Human Resources Management system; Training system; and Readiness system. [National security systems (NSS) and Morale, Welfare and Recreation (MWR)-related Non-appropriated Funds (NAF) systems are excluded]. (DBS Investment Cert. Manual, DON OMCO DON OMCO)

- **Infrastructure as a Service (IaaS)**: The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources

where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). (NIST SP 800-145)

- **IT Service**: A capability provided to one or more DoD entities by an internal or external provider based on the use of IT and supports a DoD mission or business process. An IT Service consists of a combination of people, processes, and technology. (DITPR guidance; DoDI 8500.01)

- **Mission Critical IT Solution**: The loss of which would cause stoppage of warfighter operations and/or direct mission support of warfighter operations.

- **Mission Essential IT solution**: Necessary for the accomplishment of the organizational mission, the loss of which would cause work stoppage to mission essential or mission critical functions within the organization. This includes IT solutions deemed authoritative and/or mandated by laws, regulations, and/or policies, but do not meet the definition of mission critical.

- **Other as a Service (XaaS)**: A service, other than SaaS, PaaS, or IaaS, procured by the Marine Corps to meet an IT need, capability, and/or functionality.

- **Platform as a Service (PaaS)**: The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. (NIST SP 800-145)

- **Resources:** The forces, materiel, funds, and other assets or capabilities apportioned or allocated to a program or the commander of a unified or specified command. Consists of military and civilian personnel, material on hand and on order, and the entitlement to procure or use material, utilities, and services as required for performance of the basic mission of the responsibility center, as well as work performed for others (MCO 7000.1)

- **Risk Management Framework (RMF):** The Risk Management Framework provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. The risk-based approach to control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations. Managing organizational risk is paramount to effective information security and privacy programs; the RMF approach can be applied to new and legacy systems, any type of system or technology (e.g., IoT, control systems), and within any type of organization regardless of size or sector. (NIST)

- **Software as a Service (SaaS)**: The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. (NIST SP 800-145)

- **System**: Any solution that requires a combination of two or more interacting, interdependent, and/or interoperable hardware, software, and/or firmware to satisfy a requirement or capability. (MCO 5230.21)

- **System of Systems (SoS)**: A set of interdependent systems that are related or connected and provide a given capability. The loss of any individual system element or system could significantly degrade the performance or capabilities of the entire system (of systems). The development of a SoS solution will involve trade space between the systems as well as within an individual system performance. (DITPR guidance; CJCSI 3170.01F)

3.2 General

Regardless of IT solution type (application, system, network, etc.) and connectivity (e.g. networked, stand-alone, virtual, etc.), the first steps will always be for the application/system sponsor/owner, and when applicable the PM/PPM, to develop, document, and validate the requirements and assess potential solutions prior to solution selection. In all cases some form of a business case analysis needs to be conducted before moving forward to solution analysis.

Designated IT FAM Leads and/or IT PfM support (collectively, IT Portfolio Lead) shall be informed and included early in the analysis of potential solutions. Reduction of unnecessarily redundant capabilities, alignment to strategy, and alignment with the portfolio-specific IT portfolio roadmap shall be the focus of the applicable IT Portfolio Lead when determining whether to accept new IT solutions into the portfolio. Registration of IT solutions into the applicable ADS is required prior to obligation of funds. In all cases coordination with the applicable FAM Lead(s) must take place prior to development and/or procurement of IT.

If at any point during the analysis of solutions the IT Portfolio Lead determines another solution can likely meet the capability/functionality requirements, they shall disapprove the request to develop, procure, and register a new solution, and provide the application/system sponsor/owner with at least one alternative solution.

If the initially contacted IT Portfolio Lead determines the request may be better aligned to another portfolio based on the primary capability of the solution, that IT Portfolio Lead shall immediately facilitate additional coordination with the proposed IT Portfolio Lead. If agreed, the other IT Portfolio Lead will proceed with assisting in the solution analysis and/or with adding the solution into the portfolio. When concurrence about portfolio alignment cannot be reached, DCI-IC4-ICC-CIO shall be consulted.

DCI-IC4-ICC-CIO will periodically review IT portfolios to ensure solutions are properly registered and aligned to the correct IT portfolio and mission area, based on the solution's primary capability. DCI-IC4-ICC-CIO is the final disposition and decision authority for approval, determination of mission area (MA) alignment, functional area/portfolio alignment, and record type (e.g., application or system) determination. Funding and/or IT procurement requests will not be approved for obligation to procure, develop, modernize, or maintain any IT solution that is not registered and compliant in DADMS/DITPR-DON and compliant with any other applicable LRPG (e.g., CCA compliance, certification of defense business systems, IUS, etc.). Additionally, IT solutions using USMC data will not be allowed to operate, on or off the MCEN, other Marine Corps, commercial, or cloud network(s), without such registration and compliance. Refer to Figure 1 below for assistance in determining registration requirement.

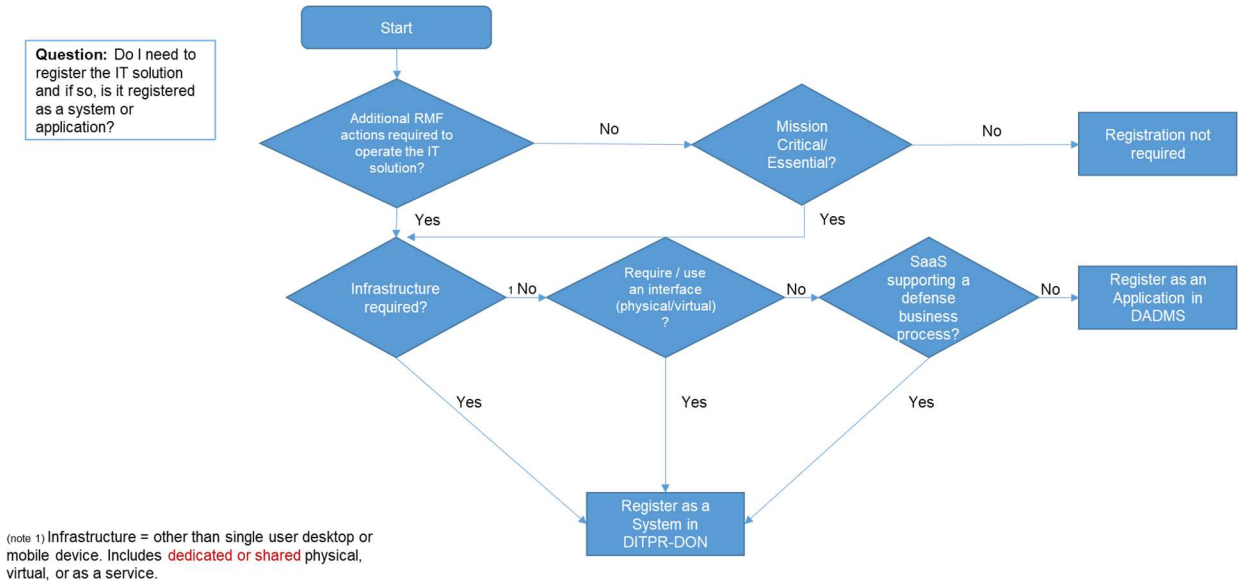

Figure 1. Registration Decision Flow (DADMS or DITPR-DON)

In coordination with the application/system sponsor/owner and/or the PM/PPM, the IT Portfolio Lead will be responsible to register all IT in DADMS/DITPR-DON regardless of network/connectivity status. The PM/PPM will be responsible for maintaining DITPR-DON records, and when assigned for applications, mobile apps, etc. will assist IT Portfolio Leads in the maintenance (i.e., updating capability descriptions and providing proof of vendor support to justify last dates allowed) of DADMS records. When there is no PM/PPM assigned to an application, database or mobile app, the application sponsor/owner will be responsible to assist the IT Portfolio Lead in maintaining the DADMS record(s).

3.3 DON Application and Database Management System (DADMS)

Registration of applications, aaS, and mobile apps is initiated by the application sponsor with the completion of an IT procurement request (ITPR) pursuant to current ITPR policy and processes, as well as the completion of a DADMS Questionnaire (DQ) . If a PM/PPM is assigned in support of the solution, the application sponsor /owner will coordinate with the PM/PPM. Once validated, the DQ will be forward to the applicable IT Portfolio Lead, determined by the primary

capability/functionality of the IT solution (i.e., not the requesting or funding organization). If it cannot be determined which portfolio the IT solution should fall under, the application sponsor must contact DCI-IC4-ICC-CIO for further guidance.

Upon receipt, the IT Portfolio Lead will review the DQ:

1) To ensure no other solution already exists in the DON IT portfolio, and
2) To ensure the request is in alignment with their portfolio strategy and five-year IT roadmap.

Following validation and acceptance, the IT Portfolio Lead will create the new DADMS record(s) and provide final approval disposition in the record. The IT Portfolio Lead will subsequently update their IT roadmap to account for the new solution.

If a solution already exists in DADMS, the IT Portfolio Lead will recommend and provide the DADMS ID of a product that delivers the requested capability/functionality, whether approved by USMC, Navy or at the Secretariat level. If the recommended solution is not currently approved within the USMC and the application does not fall within a SECNAV/OPNAV portfolio (i.e., Acquisition, Civilian Personnel, Financial Management, Legal, Medical, METOC), the IT Portfolio Lead will provide USMC disposition and Unit Identification Code (UIC) association to the existing record. If the solutions falls within a SECNAV or OPNAV portfolio, the IT Portfolio Lead will coordinate the addition of the applicable Marine Corps UICs to the DADMS record; USMC-specific approval is not required.

New applications, aaS, and mobile apps regardless of connectivity status (stand alone, cloud, MCEN, commercial, etc.) shall be registered in DADMS as follows:

- Naming Convention: DADMS registration shall consist of the vendor (or organization, if GOTS) name, followed by the full application name (as identified by the vendor, owning contractor, or program). The acronym shall consist of the first letter of each word contained in the full application name.
    - For example, if the Marine Corps developed an application called Portfolio Management Tracking Tool, the application shall be registered as "Marine Corps Portfolio Management (PfM) Tracking Tool." The acronym would be "MCPfMTT."
- Versioning: All USMC DADMS records shall be recorded through the second octet (e.g., 1.0, 1.1, or 1.1.x, NOT 1 or 1.x). The following shall be used for mobile apps or '...as'
    - Mobile apps: "(M)" shall precede the version number (e.g., (M)1.1).
    - as a Service: "([...]aaS)" shall precede the version number (e.g., (SaaS) 1.1)
- Last Date Allowed: All DADMS records are required to have a last date allowed (LDA). The LDA identifies when applications, mobile apps, etc. are no longer authorized for use.
    - COTS: In the case of commercial-off-the-shelf (COTS) the LDA shall coincide with the vendor's EOS date, or contract period of performance (POP) if third party support is procured. The FAM Lead may at their discretion set the LDA for a date sooner than the vendor EOS or POP date, but not later.
    - GOTS: In the case of government-off-the-shelf (GOTS) the LDA shall be set to one year from the date of approval, or the contract POP if the application, mobile app, etc. is contractor supported.

- OSS: If the application is an open source software (OSS) application, the IT Portfolio Lead shall set the LDA to one year from the date of approval. OSS shall only be approved as long as it is the latest version available and is supported via original (community) vendor or third party support.

3.4 DoD Information Technology Portfolio Repository - Department of Navy (DITPR-DON)

Like applications, registration is required regardless of connectivity and/or virtualization status (e.g., virtual systems, stand alone, cloud, MCEN, commercial, etc.). Requests to add new IT systems (to include networks and portals) to the Marine Corps IT portfolio begins with the system sponsor (i.e., organization or program office originating the requirement) first validating the gap and the requirement to fill the gap with an IT solution. Once it is determined the gap solution will entail developing or procuring an IT system, the system sponsor shall coordinate with the applicable IT Portfolio Lead; or DCI-IC4-ICC-CIO if the system sponsor is not sure which IT portfolio the proposed solution should align to. The IT Portfolio Lead will assist in solution selection/analysis. If during rationalization the IT Portfolio Lead identifies an existing IT system to be a potential solution to the gap, whether current Marine Corps, Navy, or other Service, the IT Portfolio Lead will inform the system sponsor and/or PM/PPM.

The IT Portfolio Lead will proceed with accepting the system into the portfolio if:

1) The existing solution recommendation is determined to be insufficient based on a substantial lack of capability and/or functionality, or
2) No solution already exists and there are no other efforts in place to create such a solution.

The next step will be for the IT Portfolio Lead to request from DCI-IC4-ICC-CIO additional permission in DITPR-DON, allowing the creation of a new record. The IT Portfolio Lead will subsequently create the DITPR-DON record shell containing at a minimum the following system information as provided by the PM:

1. Full System Name (without acronyms);
2. System Acronym (as stated for applications);
3. DON Record Type (Initiative, Family of Systems, System of Systems, System, Network, Portal, Sub-system);
4. Primary MA Domain;
5. UII (Unique Investment Identifier);
6. DBS (Yes or No);
7. Acquisition category (ACAT or BCAT);
8. Is the system spectrum dependent? (Yes or No);
9. System operation (e.g. GOGO);
10. Type if IT/NS;
11. Custom Software Development (Yes or No);
12. DevSecOps (Yes or No);
13. CCA Compliant (Yes or No);
14. Mission criticality;
15. Description (concise, but detailed enough to describe the primary capability provided);
16. *Explain (for use of UII 00000990)
17. FAM assigned;

18. Echelon;
19. Budget-Submitting Office (BSO);
20. DON Record type;
21. Resource Sponsor;
22. Mission criticality. Mission criticality will be assessed by the FAM in coordination with IC4-ICC-CIO for applicability to the enterprise. Systems will be categorized as Mission Critical, Mission Essential, or Mission Support. Because one organization has acquired or developed a local system that is integral to its particular operations, does not constitute mission criticality or essentiality. Mission criticality or essentiality may be established to necessitate compliance with local operational or regulatory requirements (e.g., Status of Forces Agreement compliance, etc.). Mission Support applies to systems which are not categorized as Mission Critical or Mission Essential.
23. Proposed Joint Capability Area mapping and business enterprise architecture (BEA) mapping if the system is a DBS; and
24. Lifecycle phases and dates (current and future

As stated previously, the PM is subsequently responsible for ensuring the completion of the remaining data fields in the entire DITPR-DON record. The PM shall also maintain accuracy and completeness of the record throughout the system's life cycle. Any registered system record with incomplete or non-compliant information at any time will be subject to recommendation for rejection of future IT procurement requests and/or funding deferral until compliance requirements are met. If records are habitually (i.e., for more than one calendar year) non-compliant and/or incomplete the systems will be recommended for termination.

This page intentionally left blank

Appendix A: Glossary (Acronyms & Abbreviations)

aaS	as-a-Service
A&A	Authorization and Accreditation
AOR	Area of Responsibility
ADS	Authoritative Data Source
AO	Authorizing Official
ATO	Authority to Operate
BEA	Business Enterprise Architecture
CCA	Clinger-Cohen Act
COTS	Commercial-Off-the-Shelf
DADMS	DON Application and Database Management System
DATO	Denial of Authority to Operate
DBS	Defense Business System
DCI	Deputy Commandant Information
DNI	Director of National Intelligence
DITPR-DON	DoD Information Technology Portfolio Repository – Department of Navy
DQ	DADMS Questionnaire
DoD	Department of Defense
DON	Department of the Navy
DDCIO(MC)	DON Deputy Chief Information Officer, Marine Corps
EOS	End of support
ECSM	Enterprise Cybersecurity Manual
FAM	Functional Area Manager
GOTS	Government-Off-the-Shelf
IC4	Information Command, Control, Communications, and Computers
IM	Information Management
IRM	Information Resources Management
ISSM	Information System Security Managers
IaaS	Infrastructure-as-a-Service
IT	Information Technology
ITPR	Information Technology Procurement
IG	Inspector General
IC	Intelligence Community
IRB	Investment Review Board
LDA	Last Date Allowed
LRPG	Laws, Regulations, Policy and Guidance
MCAAP	Marine Corps Assessment and Authorization Process
MCCA	Marine Corps Certified Application
MCEN	Marine Corps Enterprise Network
MCO	Marine Corps Order
MA	Mission Area
MWR	Morale, Welfare and Recreation
NAF	Nonappropriated Funds
NIST	National Institute of Standards and Technology
NSS	National Security System
OSS	Open Source Software

OS	Operating System
POP	Period of Performance
PaaS	Platform-as-a-Service
PfM	Portfolio Manager
PM	Program Manager
PPM	Program Portfolio Manager
RMF	Risk Management Framework
SECNAV	Secretary of the Navy
SCI	Sensitive Compartmented Information
SaaS	Software-as-a-Service
SoS	System of Systems
UIC	Unit Identification Code
XaaS	Other-as-a-Service

This page intentionally left blank

Appendix B: References

This appendix includes references cited in this document as well as other references germane to the topic. Although it is not a comprehensive collection of IT related references and authorities, it is sufficiently detailed to facilitate the reader's use of this IRM.

A. SECNAV Memo, Designation of the Department of the Navy Deputy Chief Information Officer (Navy) and the Department of the Navy Deputy Chief Information Officer (Marine Corps), 30 April 2020
B. MCO 5400.52, Department of the Navy (DON) Deputy Chief Information Officer Marine Corps Roles and Responsibilities, 5 January 2010
C. MCO 5230.21, Information Technology Portfolio Management, 3 October 2012
D. GENADMIN message, Marine Corps Policy on Last Date Allowed for Software, 12 May 2014
E. DON OCMO Manual, Defense Business System (DBS) Investment Certification Manual, 8 February 2019
F. GENADMIN message, Business Capability Management, Business Process Reengineering, Defense Business System (DBS) Investment Review Board (IRB), and Business Enterprise Architecture (BEA) Process, 25 April 2018
G. DON CIO Memo, Department of the Navy (DON) Information Technology Expenditure Approval Authorities (lTEAA), 19 July 2011
H. United States Marine Corps Enterprise Cybersecurity Manual 018, Marine Corps Assessment and Authorization Process (MCAAP), 04 June 2020
I. DoD Instruction 5000.76, Accountability and Management of Internal Use Software (IUS), 07 June 2019
J. MARADMIN 453/21, Update To MARADMIN 375/11 Information Technology (IT) Funding, Approval, and Procurement, 27 august 2021
K. DoD Instruction 8115.02, Information Technology Portfolio Management Implementation, 30 October 2006
L. SECNAV Instruction 5230.14, Information Technology Portfolio Management Implementation, 09 November 2009
M. DoD Information Technology Portfolio Repository (DITPR) Guidance, May 2018
N. MCO 5239.2B, Marine Corps Cybersecurity, 05 November 2015
O. MARADMIN 685/12, Marine Corps Clinger-Cohen Act (CCA) Compliance Policy and Procedures, 03 December 2012

This page intentionally left blank

Appendix C: Exception/Waiver Request Template (Disapproved and/or Unsupported Software)

Application Name and Version:
<Include Vendor, full application name, and exact version.>

DADMS ID:
<Provide system-generated ID.>

Associated System/Program Name (if applicable):
<Include, using a table, full system name(s), system acronym(s), DITPR-DON ID(s), applicable program name(s) and Marine Corps Programming Code (MCPC). If not applicable, state "Standalone application and include applicable MCPC".>

Justification:
1. **Who is requesting the exception/waiver to use the unsupported software application/version?**
<Applicable USMC Organization(s), UIC(s), and number of users at each organization.>

2. What is the functional description of the application and what capabilities does it provide?
<Provide a detailed description of what the application does/will do and how the application is/will be used within the Marine Corps to fill what specific capability requirements.>

3. When did vendor (or 3rd party) support end, and when is the last date you are going to need the software application/version?
<Provide the date vendor/3rd party support ended. If support was previously via a contract, indicate why the contract was not renewed. Also provide the actual date when this specific version will no longer be needed. Note: exception requests will only be granted for one year. If needed beyond one year, resubmission will be required.>

4. Where will the software application/version be used?
<List all applicable organizations and networks.>

5. Why is continued, unsupported use of this specific software application/version needed, instead of migrating to a supported version of this application or a supported competitor's product?
<List the detailed justification and mission impact if the waiver request is disapproved. Specify for each system impacted. Include the mission area(s) and strategic goals supported by this application.>

6. Point of Contact for this specific software application/version request.
<Primary POC, FAM Lead, and FAM: Name, Title, Email, Phone and signature.>

<The PM will submit the above information to the designated FAM Lead for submission to the FAM (GOFOSES) for further consideration by Dir IC4 on behalf of DC I. Approved waiver documentation will be provided to the FAM Lead by HQMC DCI-IC4-ICC-CIO.>

This page intentionally left blank. Last page of IRM.