-----OFFICIAL INFORMATION DISPATCH FOLLOWS----- RAAUZYUW RUOIBBB9168 3612012-UUUU--RHCRNAD RUOISSA RUOISTA.
ZNR UUUUU
R 261805Z DEC 18
FM CNO WASHINGTON DC
TO NAVADMIN
BT
UNCLAS
NAVADMIN 315/18
PASS TO OFFICE CODES:
FM CNO WASHINGTON DC//N2N6//
INFO CNO WASHINGTON DC//N2N6//
MSGID/GENADMIN/CNO WASHINGTON DC/N2N6/DEC// SUBJ/TRANSFORMING OUR END-TO-END INFORMATION ENVIRONMENT - COMPILE TO COMBAT IN 24 HOURS IMPLEMENTATION FRAMEWORK (CORRECTED COPY)// REF/A/DOC/CNO WASHINGTON DC/DEC18//
REF/B/DOC/NAVAUDSVC/09MAR2018/NOTAL//
REF/C/DOC/JCS/31AUG2018//
REF/D/LTR/SECDEF CIO/28MAR13//
REF/E/DOC/SECDEF CIO/05DEC17//
REF/F/LTR/CNO N2N6 WASHINGTON DC/01FEB17// REF/G/LTR/CNO N2N6 WASHINGTON DC/19DEC17// REF/H/DOC/SPAWAR SAN DIEGO CA/14SEP18// REF/I/MTG/INFORMATION ASSURANCE TECHNICAL ADVISORY BOARD/19SEP18// REF/J/DOC/SECDEF/21MAY14// NARR/ REF A IS THE CHIEF OF NAVAL OPERATIONS DESIGN FOR MAINTAINING MARITIME SUPERIORITY V2.0. REF B IS NAVAL AUDIT SERVICE (NAVAUDSVC) AUDIT REPORT N2018-00 21 - NAVY DATA STRATEGY DETAILING NAVYS INABILITY TO MEET DATA MANAGEMENT AND DATA SHARING REQUIREMENTS AS SET FORTH IN WHITE HOUSE AND DEPARTMENT OF DEFENSE (DOD) MANDATES.
REF C IS THE CHARTER OF THE JOINT REQUIREMENTS OVERSIGHT COUNCIL
(JROC) AND IMPLEMENTATION OF THE JOINT CAPABILITIES INTEGRATION AND DEVELOPMENT SYSTEM (JCIDS) MANUAL GOVERNING ASSESSMENTS OF JOINT MILITARY CAPABILITIES, IDENTIFICATION, APPROVAL, AND PRIORITIZATION GAPS IN OPERATIONAL CAPABILITIES, AND MANDATES SPECIFIC ADHERENCE TO DOD ARCHITECTURE FRAMEWORK (DODAF) REQUIREMENTS AND PERFORMANCE PARAMETERS FOR COVERED SYSTEMS. REF D IS THE DOD MEMO FOR ADOPTION OF THE NATIONAL INFORMATION EXCHANGE MODEL (NIEM) WITHIN THE DOD, AND ESTABLISHING THAT MODEL AS THE DOD MANDATED DATA SHARING MODEL. REF E SETS THE SHARING OF DATA, INFORMATION, AND INFORMATION TECHNOLOGY (IT) SERVICES IN THE DOD AND ESTABLISHES DOD POLICY, ASSIGNS RESPONSIBILITIES, AND PRESCRIBES PROCEDURES TO ENABLE A SECURE DATA SHARING ENVIRONMENT THAT SUPPORTS THE WARFIGHTING, BUSINESS, DOD INTELLIGENCE, AND ENTERPRISE INFORMATION ENVIRONMENT MISSION AREAS. REF F IS THE NAVY CLOUD FIRST POLICY AND PROVIDES POLICY FOR PROMOTION, ACQUISITION, AND CONSUMPTION OF COMMERCIAL CLOUD SERVICES AS PART OF THE NAVY CLOUD COMPUTING STRATEGY. REF G, THE NAVY COMMERCIAL CLOUD BROKERAGE POLICY, IMPLEMENTS NAVY COMMERCIAL CLOUD BROKERAGE GOVERNANCE AND DEFINES REQUIREMENT TO ACCELERATE NAVY ADOPTION OF COMMERCIAL CLOUD TECHNOLOGIES AND SERVICES WHILE PROTECTING NAVY INFORMATION IN THE CLOUD. REF H, THE SPAWAR C2C24 IMPLEMENTATION STANDARD, DOCUMENTS APPLICATION AND SYSTEM DEVELOPMENT REQUIREMENTS FOR SOFTWARE APPLICATIONS TO TRANSITION TO A MODERN SOFTWARE DELIVERY LIFECYLE THAT SUPPORTS WARFIGHTING,BUSINESS, NAVY INTELLIGENCE, AND ENTERPRISE INFORMATION ENVIRONMENT MISSION AREAS, AND PROVIDES DATA STANDARDIZATION VIA THE EXTENSIBLE MARKUP LANGUAGE(XML)

STANDARD. REF I WAS THE INFORMATION ASSURANCE TECHNICAL ADVISORY BOARD (IA TAB) DECISION ON ADOPTION OF EXTENSIBLE MARKUP LANGUAGE (XML) AS THE NAVY DATA STANDARD. REF J IS THE DOD INSTRUCTION, INTEROPERABILITY OF INFORMATION TECHNOLOGY (IT),INCLUDING NATIONAL SECURITY SYSTEMS (NSS), GOVERNING INTEROPERABILITY CERTIFICATION OF SYSTEMS.//POC/WALKER/GG -15/ OPNAV N2N6G32/-/TEL: (571) 256-8543/TEL: DSN 260-8543// RMKS/1. This NAVADMIN establishes the way ahead for transforming our enterprise information environment and architecture from shore through to the tactical edge. It describes key fundamental changes to how we move, secure, and prioritize information exchange in the Compile to Combat in 24 Hours (C2C24) framework and its supporting four pillars. The C2C24 Implementation Framework puts the Navy on the path to modernizing our data and transport architecture, to include using commercial industry best practices for software modernization.

Successful implementation of this data centric approach will provide information in context for decision making to the tactical edge, and will improve how data are move and used across the enterprise.

It also provides the foundation to leverage future capabilities like artificial intelligence and machine learning to increase warfighting lethality and improve readiness (references (a) through (h)).

C2C24 supports the Chief of Naval Operations vision to use commercial technology and open standards for maximum agility, speed of capability delivery and joint/coalition interoperability. C2C24, successfully piloted by SPAWAR for the past year, provides the standardized way forward to transforming the Navys information environment through the adoption of a service oriented application architecture and common standards for data formats and interfaces.

Implementation of the C2C24 Framework will also enable program managers to significantly reduce Risk Management Framework accreditation timelines, and will enable improved cybersecurity monitoring.

2. Information from resource sponsors and program offices for implementation of a common software delivery lifecycle and data environment using the C2C24 framework is requested and detailed below. The Navy will build upon C2C24 piloting to enable enterprise adoption for appropriate system owners. Successful adoption and integration of this capability hinges on receiving detailed feedback from resource sponsors and acquisition components related to the technical approach piloted by C2C24.

3. C2C24s Implementation Framework Consists of Four Key Pillars:

a. Data Standardization. Establishing a standard way for authoritative data to be stored once and reused by many allowing for more efficient transport, and accessibility of data by all decision makers.

b. Use of Shared Infrastructure Afloat and Ashore.

Decomposition of legacy applications, systems and portals into agile, secure and streamlined web services using industry standards and best practices similar to how content is delivered to smartphones. These services will be hosted on shared infrastructure.

c. Automation. Maximizing automation of development, security authorization and approval processes to speed capability delivery.

d. Commercial Cloud. Implementing cloud technologies afloat and ashore to provide the platform for leveraging advanced data analytics and synchronization of content. Each of these pillars is described in more detail in paragraph 7 below.

4. All application owners and content providers are subject to the data call reflected in this NAVADMIN, including Combat Systems, Weapons Systems, portal owners and Operational Technology/Control Systems. Feedback related to C2C24 is requested from all resource sponsors, Functional Area Managers, and program executive officers responsible for the development and integration of software applications. Application owners and program managers are specifically requested to address information requested in paragraph 9. C2C24 adoption will initially focus on systems hosted by the Consolidated Afloat Networks and Enterprise Services (CANES) and Agile Core Services (ACS) however, the technical approach is anticipated to be applicable to Combat Systems, Weapons Systems, and Operational Technology/Control Systems. Responses to this NAVADMIN are requested as follows:

a. Category I. Applications/systems (to include portals) that are already web based and using shared infrastructure (such as those applications already hosted on CANES) are best positioned to transition to the C2C24 framework first. Application owners for these systems are directed to provide a Plan of Actions and Milestones (POAM) to DASN C4I and OPNAV N2N6G by 15 March 2019.
This POAM should reflect a plan to sustain current applications while implementing applications in the C2C24 framework within
24 months. Resource sponsors and program offices shall identify where existing funding could be used to support refactoring and modernization. If migration to C2C24 is not possible within 24 months using existing funding, application owners should identify what additional support and/or resources are needed.
b. Category II. Applications and systems not covered under category I are directed to provide to DASN C4I and OPNAV N2N6G by 15 March
2019 an assessment of required actions to implement C2C24.
Application and system owners should specifically address their plans to expose their data and share data for reuse per the C2C24 framework and relevant policy specific to the use of the subject data. Identify potential barriers to implementation to be removed (may be technical, policy, architectural, contractual, financial, or other).
If implementation is feasible, provide a POAM for modernization and identify what additional support and/or resources are needed.
5. OPNAV will organize systems into mission capability areas and review the POAMs to ensure system IT architecture, cybersecurity /Authority to Operate (ATO) Accreditation, and data management compliance with the Net Ready Key Performance Parameters (NR-KPPs) per reference (c), coordinate a prioritized mission-based allocation of requirements, costs, dependencies, risks and timelines in phases, and remove barriers necessary to implement C2C24. The results of the reviews will be used to inform program requirements, POM planning, and other priorities.
6. For service oriented architecture used in the afloat environment, application and system owners will also identify their requirements for use of the shared infrastructure (described below), to include information exchange requirements for ships in port and those underway so satellite and pier infrastructure bandwidth can be properly scoped. To assist content/application owners with producing their POAMs:
a. Detailed C2C24 Implementation Standard developers guidance is provided in reference (h), and PMW160 is promulgating the CANES Agile Core Services (ACS) Developers Guide in December 2018 (draft is available now at https://confluence.di2e.net/display/ACS3ext/) to help capability developers understand how to build in this environment.
b. A C2C24 Developers Working Group meeting was held 16-18 October
2018 for all Navy Program Management Offices (PMO), system owners, application developers, and content providers to go through the development process in detail. Another Developers Working Group is being scheduled for Spring 2019. The details of the second event will be announced via a separate NAVADMIN.
c. Subject Matter Experts are available to meet with application owners and program offices to provide advice on refactoring applications to align with the C2C24 framework.
7. C2C24 Implementation Framework and Four Pillars in Detail.
a. Data Standardization. Data will be standardized using Extensible Markup Language (XML) IAW references (h) and (i). Exceptions will be made when it is demonstrated that there is an operational requirement for use of a different data format (i.e., a legacy combat or control system). XML is a leading industry data standard format that provides many benefits in one format in addition to the meeting inter-agency data exchange requirements directed in references (b) through (d).
As a leading industry open standard for describing data, XML benefits

include:
(1) Enables maximum use of commercial products built to this standard for improved interoperability and easy of meta-tagging data
(2) Improves cybersecurity at the data element layer by using the XML Security Assertion Markup Language (SAML) protocol
(3) Improves Quality of Service for precision prioritization of data transfer to the tactical edge
(4) Enables compression of data using the XML EXI specification for efficient bandwidth usage over limited satellite communication channels
(5) Mitigates data communication satellite based-latencies
(6) Enables use of National Security Agency approved cross-domain XML data guards for movement of data between networks of different classifications. References (b) through (e), require the movement and transformation of data through distributed, automated data exchange and brokerage mechanisms that is durable, resilient, and fault tolerant. XML meets those requirements. Additionally, to enable more robust data analytics, even systems that cannot use XML for their primary function (i.e., a legacy weapon or control system) can still provide an EXI compressed XML archival record of the non -XML data for integration into the DON cloud-based Data Enterprise per reference (f).
b. Shared Infrastructure Pillar. This pillar establishes a drop code, not boxes IT development and delivery model for accelerated capability delivery. In Phase I of C2C24, shared infrastructure afloat will be provided by the CANES program and ashore via the approved cloud offerings coordinated through Navy authorized cloud brokers (reference (g)). Shore based web services will be hosted in commercial cloud. Focus of effort from content providers is on delivering software code for new capabilities quickly and securely rather than delivering hardware and systems. For content/application owners providing services afloat, use of the CANES shared infrastructure alleviates the need for costly and time consuming processes for systems authorization and approvals for integrating hardware afloat that slow speed to capability for the Fleet. Full use of the CANES environment afloat, including CANES Agile Core Services (ACS) defined in reference (h), as the baseline development target has the following benefits: Reduces the cybersecurity attack surface and maximizes use of afloat enterprise security services, enables improved defense in depth and cybersecurity monitoring, and maximizes availability and integrity of operational data in a denied environment. Content owners that currently provide their own hardware and could transition to CANES will stop new development of their application in the legacy construct and supporting hardware as they transition to this C2C24 Framework, and will sustain their current infrastructure only until all afloat platforms that use their services can access them via CANES. CANES ACS provides the needed data analytics services for the data centric approach as well as the Platform as a Service
(PaaS) to enable rapid development and deployment of applications.
This will significantly reduce workload and complexity for systems administrators and Sailors afloat. Follow on phases of C2C24 will address non-CANES platforms that are unable to migrate to CANES.
c. Automated Security Authorization and Functional Testing Pillar. Implementation of the automation pillar drives standardized processes, reduces development, testing, fielding and authorization costs, eliminates duplicative hardware, software and other physical infrastructure, and re-engineers or eliminates existing costly and time consuming processes for fielding capability. C2C24 has established a cloud-enabled CANES DevelopmentSecurityOperations
(DevSecOps) environment for all content providers to use, adopting commercial industry best-practices for software development by implementing secure coding methodologies into development and deployment code. The DevSecOps environment for shore based applications to be hosted in the cloud is under development with operations to commence in Spring 2019. Through automation of our core business processes, there are anticipated cost and time gains of up to 15 percent or more as we commence effort to full execution. By standardizing the development, data and fielding, existing

processes can be eliminated or streamlined and automated. For example, existing security accreditation and authorization processes have been adapted by the Program Offices and Navy Authorizing Official (NAO) to leverage this new framework for process reform, automating functional and security testing. The NAO approved a Rapid Assess and Incorporate Software Engineering in a Day (RAISED) process that enables applications owners compliant with references
(h) to use automated security authorization testing to significantly reduce the cost and time associated with fielding their capability. It provides an automated fast lane to obtain a Risk Management Framework
(RMF) authorization decision for the modern cloud-based containerized code developed in accordance with reference (g), and using CANES ACS services. A software security tool chain is available in the cloud as a fee for service model as part of the RAISED process and more information about it can be found in reference (h).

d. Use of Commercial Cloud Pillar. References (f) and
(g) establish Navy policy for the use and acceleration for promotion, acquisition and consumption of cloud technologies and services. This pillar provides Program Management Offices
(PMOs) the ability to leverage the benefits of using cloud technologies and best practices to develop capability, store, use, and move data. C2C24 recognizes that current cloud offerings and implementations have technical limitations, and vary across classification domains. Adoption of C2C24 will ensure that Navy can quickly and seamlessly integrate cloud capabilities as they become available. The Navy will be able to leverage cutting edge commercially provided tools in the cloud for big data analytics and reuse of authoritative data for multiple purposes across the enterprise. In the C2C24 framework, the commercial cloud is used for hosting and production, application development, and as a test and integration environment. The C2C24 team in coordination with the CANES program office established a CANES development and test environment in the cloud for PMOs to reduce the cost and complexity associated with current development and test processes. The development environment for development and operations of shore based web services in the cloud will be available in Spring 2019. PMOs will use cloud for data storage and to maximize data sharing for the purpose of data analytics and artificial intelligence.

8. Applicability. This NAVADMIN applies to all Navy systems, including business, warfighting, control systems and portals that move data between shore sites and Navy platforms on, under, and above the sea. While C2C24 is primarily focused on unclassified and secret General Service (GENSER) networks, commonality across the enterprise is the goal, and the Navy will leverage existing, Intelligence Community (IC)-provided Top Secret/Sensitive Compartmented Information (SCI) infrastructure to get to a common solution across all classification domains as quickly and seamlessly as possible.

a. Warfighting and Combat Systems. Warfighting systems are NSS, as defined by 40 USC 11103 (a)(1)(B), (C), (D), or (E). The intent is for combat and warfighting systems to adopt the C2C24 Implementation Framework for better integration into the overarching network and the data analytic environment. At a minimum, system owners are expected to expose their data and share it for reuse as previously described, in accordance with relevant policy concerning the use and rights to specified data. Follow on guidance will be provided after the NR-KPP review based on the information provided by these systems in response to this NAVADMIN.

b. For CANES hosted systems/applications, ensure system new starts or modernization efforts develop new capabilities in accordance with the C2C24 Framework articulated in references (b) through (i). Non-CANES systems that are hosted by or interfaced with another afloat network shall develop a plan to migrate to CANES.

c. All manned and unmanned (UX) warfighting systems deployed as sensor platforms, shall provide modernization plans that allow for collected sensor data to be to be transmitted, post mission, to an enterprise data lake IAW C2C24 data standards.

d. All systems currently in development are subject to the C2C24 data call to meet the same timeline for execution of their capability in the C2C24 framework. Systems currently in development or in sustainment will identify changes that would be required make such systems compatible with the C2C24 construct and timeline. Current systems with joint information exchange requirements and/or joint information exchange interfaces need to verify their certification status (four years from the date of issue) per reference (j), and apply for certification and/or re-certification as required. Systems under development if it is determined that they will have joint information exchange requirements will follow the same referenced instructions. Systems under development that will not have joint information exchange requirements may apply for a waiver to policy per reference (j).

9. Required Actions. Application owners will provide the following information for each system under their resource control, including a POAM that describes their plan to decompose their existing application or portal within 24 months in accordance with the C2C24 Framework specifications in reference (h). In support of the NR-KPP review, within 90 days, all program managers and application owners shall provide the following information to OPNAV N2N6 via this tasker link https://portal.secnav.navy.mil/orgs/OPNAV/N2N6 /DDCION/C2C24/SitePages/Home.aspx.

a. For Category I systems, provide POAM to migrate systems/applications/portals to the C2C24 framework within the next 24 months. PMs should show how they will reallocate existing FY19-20 fundingto cease development in non-compliant frameworks and migrate to the C2C24 Framework. If the program cannot meet the 24-month timeline, provide an alternative POAM based on the existing BES-20 resource profile. Identify risks, if any, under this approach.

b. For Category II systems, provide an assessment of what would be required to implement C2C24, specifically addressing the ability to expose data and share it for reuse per the C2C24 framework. Identify risks, if any, under this approach.

c. Identify any barriers to migration and what help is needed across DOTMLPF to overcome them. Specifically, identify any resources required in the POM-21 FYDP to meet or accelerate migration. These resources may include identification of specific knowledge, skills, and expertise in the form of identified training requirements as well as resources required for the refactoring of software codebase and retooling of development, and hosting environments.

d. Subject Matter Expert (SME) Point of Contact (POC) capable of responding to resourcing and technical specification questions on the system/application/portal.

e. System/application/portal name, and if the system used both afloat and ashore.

f. System Department of the Navy Applications and Database Management (DADMS) registration number, if the system is registered, or DADMS placeholder identifier X9999, if the system is not registered. Additional guidance on registration of systems in DADMS for C2C24 purposes will be provided via NAVADMIN.

g. Data formats currently generated or received by the system.

h. Communication requirements of the system, specifically for afloat applications anticipated amount of data that would be exchanged /synchronized between the afloat and ashore clouds while the unit is in port and what would need to be exchanged/synchronized over satellite links. This will enable engineers to properly scope afloat and pier bandwidth connectivity services.

i. Mandatory connectivity latency or computational latency factors KPPs (Quality of Service requirements).

j. Software language, including the current and future software development environment approach used for the system.

k. For afloat capability, identify required shared infrastructure capacity to support the processing and storage of data.

Content providers should estimate this based on their user requirements over the next 3-5 years.
l. Resource expenditures on sustaining the current as-is (non-C2C24) code for the system while executing a transition to C2C24.
m. An estimate of resource requirements for sustaining the system after it has transitioned to the C2C24 Framework. Resource requirements may include identification of specific knowledge, skills, and expertise in the form of identified training requirements.
n. System related requirements that will be eliminated from the PMO once transitioned to C2C24 (i.e., standalone or unique application testing labs).
o. Additional technical data reporting requirements will be identified by the technical developers community of interest and data collection clarifications will be addressed at the Spring 2019 Developers Working Group Meeting.
10. Understanding that this is a significant transformation effort across Navy, and will require iteration to accelerate adoption, N2N6G will lead monthly retrospectives that will seek to clarify feedback and adoption. Initial sources for this first phase of identifying transition plans:
a. The SPAWAR C2C24 Implementation Standard can be downloaded from https://go.intelink.gov/d8X1R2g.
b. Contact Ms. Delores Washburn for advice or questions related to transitioning existing applications to the C2C24 framework.
Commands may contact Mr. Rick Jack to arrange for one-on-one assistance and to discuss options best suited to program needs from a cadre of software subject matter experts on a fee for service basis.
11. Additional points of contact:
a. C2C24 Policy: RDML Danelle Barrett, Navy Cyber Security Division Director, Office of the Chief of Naval Operations, at comm: (571)
256-8505 or email: danelle.barrett(at)navy.mil.
b. C2C24 Execution and Implementation: Mr. Joseph T. Walker, C2C24 Executive Lead, at comm: (571) 256-8543, DSN: 260-8543, or
email: joe.t.walker(at)navy.mil.
c. C2C24 Technical Requirements and advice: Ms. Delores Washburn,
C2C24 Implementation Executive, at comm: (619)553-6798, or
email: delores.washburn(at)navy.mil.
d. C2C24 Developers Implementation Framework: Ms. Delores Washburn, C2C24 Implementation Executive, at comm: (619) 553-6798, or email: delores.washburn(at)navy.mil.
e. C2C24 Cadre of Software Experts: Mr. Rick Jack, SSC PAC Software Senior Scientific Technical Manager, at comm: (619) 553 -3840, or email: richard.jack(at)navy.mil.
f. NAVADMIN Data Reporting Clarification: Mr. Joseph T. Walker,
C2C24 Executive Lead, at comm: (571) 256-8543, DSN: 260-8543, or
email: joe.t.walker(at)navy.mil.
g. DADMS Registration Clarification: Ms. Brooke Zimmerman, OPNAV N2N6G31 Portfolio Management, at comm: (571) 256-8521,
DSN: 260-8521, or email: brooke.zimmerman(at)navy.mil.
h. C2C24 RMF Raised: CAPT Vincent Augelli, OPNAV N2N6G5 Cybersecurity Director, at comm: (571) 256-8422, DSN: 260-8422, or
email: vincent.a.augelli(at)navy.mil.
i. Application Integration: Mr. Brian Miller, PEO C4I, PMW-160 CANES Application Integration Support APM, at comm: (619) 524-7592 or
email: brian.miller5(at)navy.mil.

12. Released by VADM Matthew J. Kohler, Deputy Chief of Naval Operations for Information Warfare, OPNAV N2N6 and VADM Michael T. Moran, Principal Military Deputy to Assistant Secretary of the Navy for Research, Development and Acquisition.
BT
#9168
NNNN
<DmdsSecurity>UNCLASSIFIED//</DmdsSecurity>

CLASSIFICATION: UNCLASSIFIED//
Classification: UNCLASSIFIED