NOTICE OF DISCLOSURE

A recent Peer Review of the NAVAUDSVC determined that from 13 March 2013 through 4 December 2017, the NAVAUDSVC experienced a potential threat to audit independence due to the Department of Navy organizational structure in effect during this timeframe. Specifically, instead of reporting to the Secretary of the Navy or Under Secretary of the Navy, the Auditor General of the Navy reported to lower level officials who had not been charged with governance over the entire Department of the Navy to include certain non-delegable statutory functions. This alignment did not comply with generally accepted government auditing standards (GAGAS) and the Department of the Navy policy regarding independence. On 4 December 2017, the Auditor General of the Navy once again reported to the Under Secretary of the Navy in accordance with GAGAS. The Navy policy on independence was revised to clarify that the Auditor General of the Navy reports directly to the Under Secretary of the Navy (or to the Secretary of the Navy whenever the position of the Under Secretary of the Navy is vacant.)

With the exception of the potential structural threat outlined above, we believe that the projects performed from 13 March 2013 through 4 December 2017, complied with all other generally accepted government auditing standards.

~~FOR OFFICIAL USE ONLY~~

NAVAL AUDIT SERVICE

AUDIT REPORT

Navy Data Strategy

The mission of the Naval Audit Service is to provide independent and objective audit services and products to assist Department of the Navy leadership in assessing risk to improve efficiency, accountability, and program effectiveness.

~~Do not release outside the Department of the Navy, post on non-Naval Audit Service websites, or post in Navy Taskers without prior approval of the Auditor General of the Navy.~~

This report contains information exempt from release under the Freedom of Information Act. Exemptions (b)(5) and (b)(6) apply.

N2018-0021
8 March 2018

~~FOR OFFICIAL USE ONLY~~

Executive Summary

Why the Audit was Conducted

The objective of this audit was to verify that the Department of the Navy's (DON's) data strategy was consistent with Department of Defense (DoD) guidance and Joint Information Environment mandates.

What the Audit Found

We determined that the Navy does not have a current enterprise-wide data strategy.

Specifically, we found that 10 of 12 Navy commands we visited were unaware of the DON Chief Information Officer (CIO) November 2000 data strategy. DON CIO and the DON Deputy Chief Information Officer (DDCIO) Navy (N) had not updated this strategy. This condition occurred because DON CIO and DDCIO (N) did not ensure implementation of data strategy that included attributes as required by DoD Instructions 8320.02, "Sharing Data, Information, and IT [information technology] Services in the DoD," and 8320.07, "Implementing the Sharing of Data, Information, and IT Services in the DoD." Further, sufficient communication, alignment of oversight, and communities of interest (COIs) were not present to prevent the stovepipe mentality when procuring new Navy systems.

As a result of not implementing a current enterprise-wide Navy data strategy, the Navy is perpetuating obsolescence by planning new systems that will not conform to current DoD instructions. Potential nonconformances include continuing lack of interoperability, duplication of data and effort, and commercial off-the-shelf (COTS) products that, upon fielding, potentially will not conform to current DoD instruction requirements. Data within the Navy's business systems we audited was not visible, accessible, understandable, trusted, and interoperable throughout the data's lifecycle for all authorized users as required by DoD instructions.

What DON Can Do to Address the Situation

We made recommendations to DON CIO to develop a strategic plan and end goals and to DDCIO (N) to implement a Navy data strategy that is in line with current DoD instructions and Office of Management and Budget Memorandum M-13-13 "Open Data Policy-Managing Information as an Asset," 9 May 2013. DON CIO and DDCIO (N) should establish procedures and provide oversight to ensure that the Navy data management system includes defined goals and benchmarks, and new systems include the necessary data fields and flexibility for new technologies. We also recommend that the Deputy Chief of Naval Operations resource sponsors establish procedures and provide oversight to ensure that new systems include the appropriate data fields. Management responded and took and plans appropriate corrective actions. Both recommendations are considered open pending completion of the corrective actions. Because the target completion date is more than 1 year in the future, we are establishing an interim reporting date of 6 August 2018; we request that the command provide us with an update on the corrective actions at that time.

Ronnie J. Booth

RONNIE J. BOOTH
Assistant Auditor General
Energy, Installations, and Environment Audits

[redacted]

[redacted]
Audit Director

FOIA (b)(6)

Table of Contents

Section A: Finding, Recommendations, and Corrective Actions

Finding: Enterprise-wide Data Strategy

The Navy does not have a current enterprise-wide data strategy. We judgmentally selected 12 Navy business and tactical systems contained within the Department of the Navy (DON) Application and Database Management System (DADMS) and the Department of Defense (DoD) Information Technology Portfolio Repository (DITPR)-DON. We found that none of the business systems selected for review fully enabled the sharing and discovery of data throughout DON, as intended. This occurred because the DON Chief Information Officer (DON CIO) and DON Deputy Chief Information Officer Navy (DDCIO (N)) did not ensure implementation of a data strategy that includes attributes as required by DoD Instructions 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the DoD;" and 8320.07, "Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the DoD." As a result, the Navy is perpetuating obsolescence by planning new systems that will not conform to the DoD data strategy. Potential nonconformances include continuing lack of interoperability, duplication of data and effort, and commercial off-the-shelf (COTS) products that, upon fielding, potentially will not conform to current DoD instruction requirements.

Background

The Secretary of the Navy (SECNAV) established DON CIO in 1997 to provide top-level advocacy in the development and use of information management (IM)/IT and to create a unified IM/IT vision for the Department. DON CIO uses higher-level guidance to establish Navy objectives to develop and implement strategic plans and goals, which are to be implemented by DDCIO (N) and Chief of Naval Operations (CNO) N-Codes.

In Fiscal Year (FY) 2000, DoD CIO provided the "DoD Data Management Strategic Planning Guidance FY 2000" to the services as a framework for their individual IM/IT strategic plans (please see Exhibit A, "Background and Pertinent Guidance" for more information). The most current approved Navy data strategy provided to us during the course of the audit is the 2 November 2000 "DON Data Management and Interoperability Strategic Plan," although it is not listed on the Policy and Guidance section of the public DON CIO Web site.

In subsequent years, DON CIO established the primary instruction the Navy uses to control data strategy, SECNAV Instruction 5000.36A, "Department of the Navy Information Technology Applications and Data Management," dated December 2005. This instruction establishes roles and responsibilities for Functional Area Managers (FAMs) and the development, execution, and maintenance of DON IT processes and tools to transform apps and data into net-centric Naval capabilities consistent with DoD policy for interoperability and data sharing (please see Exhibit A, "Background and Pertinent Guidance" for more information).

In June 2011, DDCIO (N) was established by the Vice Chief of Naval Operations as the FAM authority for the Navy. A key role for DDCIO (N) is to strengthen, align, and integrate Information Technology Portfolio Management (IT PfM) efforts throughout the chain of command via FAM Leads and Echelon II CIOs. Effective and authoritative IT PfM implementation is imperative for Navy to meet long-term objectives. This designation of DDCIO (N) as the single FAM authority for the Navy provides the governance and authority to meet these objectives.

Subsequent to the terrorist attacks on 11 September 2001, a grassroots effort by a handful of organizations supporting state and local government, named the Global Justice Sharing Initiative, set in motion the creation of a seamless, interoperable model for data exchange across Government agencies called the Global Justice XML Data Model. The National Information Exchange Model (NIEM) was formally launched in 2005 by the CIOs of the Department of Homeland Security and the U.S. Department of Justice. NIEM is a community driven, standards-based approach to exchanging information. All 50 states and the majority of Federal agencies are using (at varying levels of maturity) or considering NIEM. In March 2013, DoD CIO issued DoD CIO Memorandum, "Adoption of the National Information Exchange Model within the Department of Defense," requiring the adoption of NIEM as the best suited option for standards-based data exchanges. This adoption involves a series of phased implementations by components and programs using NIEM content, guidance, and tools in an integrated effort to transition current DoD data exchange standards, specifications, and policies to a NIEM-based approach. In addition, DoD is tasked with working with the NIEM Program Management Office to create a Military Operations Domain as part of NIEM.

Shortly thereafter, the Office of Management and Budget (OMB) issued OMB Memorandum M-13-13, "Open Data Policy-Managing Information as an Asset," dated 9 May 2013. It requires agencies to describe information using common core metadata, in consultation with the best practices found in Project Open Data, as it is collected and created. The memorandum also requires that agencies build information systems to support interoperability and information accessibility (please see Exhibit A, "Background and Pertinent Guidance," for more information).

Subsequent to DoD CIO and OMB guidance in early 2013, DoD CIO issued DoD Instruction 8320.02 in August 2013, which establishes policies, assigns responsibilities,

and prescribes procedures for securely sharing electronic data, information, and IT services, and securely enabling the discovery of shared data throughout DoD.

[redacted] With ever changing and emerging technologies, DON CIO issued guidance for acquiring commercial cloud services. It canceled initial Cloud Service Supplemental Guidance and direction concerning cloud pilots and services in previous DON CIO memorandum. The Navy intends to be "Cloud First," with a goal to move 75 percent of Navy IT capabilities (systems, applications, and services) to the commercial cloud by 2022. In February 2017, an update to the Navy Cloud Policy was enacted by DDCIO (N). Highlights of this policy included updated guidance for acquiring commercial cloud services, including: reducing investment in legacy data centers, brokering cloud services through a Managed Service Organization such as Program Executive Office Enterprise Information Systems (PEO EIS), ensuring security requirements are implemented, and ensuring flexibility while avoiding vendor lock.

FOIA (b)(5)

In August 2015, DoD Instruction 8320.07 was published establishing policy, assigning responsibilities, and prescribing procedures to implement DoD Instruction 8320.02; it enables a secure sharing environment in DoD that supports the warfighting, business, DoD intelligence, and information enterprise environment mission areas. This instruction describes or references key enablers necessary for sharing data, information, and IT services, and ensuring data, information, and IT services are visible, accessible, understandable, trustworthy, and interoperable.

[redacted][1]

FOIA (b)(5)

Audit Results

We reviewed 12 Navy business (8) and tactical (4) systems contained within DADMS DITPR-DON. Our review focused on analyzing the systems' supporting documentation to determine compliance with DoD guidance and Joint Information Environment (JIE) mandates. In addition, we reviewed the system design or architecture to determine if any

[1] [redacted]

FOIA (b)(5)

data strategy elements within DoD instructions were included. We also interviewed Program and System Managers to understand the oversight procedures and guidance provided by their respective Functional Area Managers (FAMs), and to obtain corroborating documentation pertaining to data strategy. Table 1 shows a list of the systems reviewed, whether they were business or tactical systems, and who owns the system.

Table 1. DON Systems Selected for Review.

System Number	System Name (abbreviation)	Tactical/Business	Owner/SYSCOM	Resource Sponsor
Benchmark	National Information Exchange Model (NIEM) Core			
1	Distributed Common Ground System-Navy (DCGS-N)	Tactical	PEO C4I	N2/N6
2	Maritime Domain Awareness-Non Classified Enclave	Tactical	Office of Naval Intelligence	N2/N6
3	Airborne Laser Mine Detection System	Tactical	NAVSEA	PMS 495 (ASN RDA)
4	Navy Tactical Cloud-Reference Implementation (NTC-RI)	Tactical	ONR	N2/N6
5	Enterprise Procurement System (EPS)	Business	PEO EIS	N4
6	Navy Maritime Maintenance Enterprise Solution- Technical Refresh (NMMES-TR)	Business	NAVSEA	N9
7	Maritime Shore Environment	Business	NAVSEA	N9
8	Navy Enterprise Resource Planning (ERP)	Business	PEO EIS	N4
9	Enterprise Safety Application Management System (ESAMS)	Business	CNIC	N4
10	Internet Facilities Asset Data Store (iNFADS)	Business	NAVFAC	N4
11	Navy Enlisted System (NES)	Business	CNO N1 (N16) BUPERS	N1
12	Ordnance Inventory System	Business	NAVSUP	N4

Acronym key: ASN (RDA) – Assistant Secretary of the Navy (Research, Development and Acquisition); BUPERS – Bureau of Navy Personnel; PEO – Program Executive Office; PEO C4I –PEO Command, Control, Communications, Computers, and Intelligence; CNIC – Commander, Navy Installations Command; PEO EIS – PEO Enterprise Information Systems; CNO N1 – Office of the Chief of Naval Operations Manpower, Personnel, Education, and Training; CNO N16 – CNO N1-Enterprise; CNO N2/N6 – Navy Cyber Security Division Director, Office of the Chief of Naval Operations; CNO N4 – Fleet Readiness and Logistics; CNO N9 – DCNO for Warfare Systems; NAVFAC – Naval Facilities Engineering Command; NAVSEA – Naval Sea Systems Command; NAVSUP – Naval Supply Systems Command; ONR – Office of Naval Research; SYSCOM – Systems Command.

We found that DON CIO and DDCIO (N) had policies and procedures in place for Navy IM and IT; however, the Navy has not implemented an enterprise-wide data strategy. Of the 12 systems, the 4 tactical systems aligned more closely with applicable guidance, but all 8 business systems did not comply with DoD and DON CIO policies. We determined that not all business systems we audited:

- Stored data as data objects with associated metadata to make the data visible;
- Associated metadata with each respective data asset to make data accessible;
- Used NIEM to transfer data, and the systems in the early planning stages had no documentation that required NIEM to make the data understandable;

- Used metadata and standard data objects to allow other systems to search their system data, making the data interoperable;
- Had interfaces where they were transferring data in an Extensible Markup Language (XML) format with metadata to track the source of the data, making the data trusted; or
- Used data elements for the selected systems that were normalized between systems to make the data understandable.

DoD Data Attributes

DoD Instructions 8320.02, "Sharing Data, Information, and IT Services in the DoD," and 8320.07, "Implementing the Sharing of Data, Information, and IT Services in the DoD," describe or reference key enablers necessary for sharing data, information, and IT services. To confirm compliance with these DoD instructions, we determined whether data, information, and IT services for the selected systems were made:

- **Visible** to authorized users by creating and associating metadata, including discovery metadata, for each asset;
- **Accessible** to authorized users by conforming to DoD-specified publication methods consistent with DoD guidance and policy;
- **Understandable** so authorized users were able to consume them and readily determine how those assets might be used for specific needs;
- **Trusted** so that they provided sufficient pedigree (i.e., enabling consumers to track the source and lineage of an asset) and descriptive metadata for consumers to rely on them as authoritative data sources (ADSs); and
- **Interoperable** such that consumers considered the parameters as specified in the DoD Enterprise registries for a given IT service in order to consume its data.

We used these data attributes to evaluate the data in the 12 systems selected for audit. The intent of DoD Instructions 8320.02 and 8320.07 is not to mandate retrofitting existing systems, services, or capabilities. Changes are only required for data, information, and IT services supporting existing systems to the extent that they receive investment dollars for modernization.

DoD Instruction 8320.07, Enclosure 3, calls for all DoD organizations, data producers, program managers, functional owners and managers, COIs, data producers, data providers, data consumers, and system developers to perform the following procedures for making data, information, and IT services available for all applicable consumers.

Data Visibility

We found that one of the eight business systems we audited was storing data as data objects with associated metadata. Further, within the four tactical systems audited, only the Navy Tactical Cloud-Reference Implementation (NTC-RI) and Distributed Common Ground System-Navy (DCGS-N) were designed to store data as data objects with associated metadata.

The Distributed Common Ground/Surface Systems (DCGS) Test and Evaluation Focus Team assessed the DCGS enterprise during the "Enterprise Challenge 2015, Main Exercise." They determined that DCGS was able to interoperate in a secure federation, while correctly providing and redacting data, based on requestor attributes 97 percent of the time. The data placed in DCGS-N by operators onboard the *USS FITZGERALD* were discovered by all of the other DoD commands involved in the test, including the Army and Air Force. This exercise illustrates the importance of using data objects with standard metadata to make Navy data visible and searchable.

Of the business systems we audited, the best example of making data visible was the Internet Facilities Asset Data Store (iNFADS), which has a published data dictionary[2] that is available on the Internet. This allows other Navy or DoD commands to identify what data within iNFADS is useful for their own business data needs. The worst example of data visibility we found during our audit was within the Enterprise Safety Applications Management System (ESAMS). This system had a data dictionary, but we were told that it could not be provided to us because it was proprietary software. Therefore, the only way for another command to identify useful information within the system would be to become a user of the system.

Data Accessibility

We found that one of the eight Navy business systems we audited associated metadata with each respective data asset. Seven of the eight business systems did not reduce the need for predefined, engineered point-to-point interfaces by using standardized Web-based, machine-readable open formats, which maximize reuse wherever operationally and technically feasible. Of the business systems we audited, only the Enterprise Procurement System (EPS) recognized the importance of reducing point-to-point interfaces.

The best examples we found of systems meeting the DoD criteria were the tactical systems NTC-RI and DCGS-N:

NTC-RI. NTC-RI publishes data to a central data store in a Cloud-like environment on Navy ships. NTC-RI uses open source applications to create a NoSQL data store

[2] A data dictionary is a set of information describing the contents, format, and structure of a database and the relationship between its elements, used to control access to and manipulation of the database.

and allows for associating data using metadata. NTC-RI ingests data from many different systems, which could include DCGS-N, shipboard sensors, and other Fleet systems in the deployed battle group. NTC-RI appends metadata and stores the information in a central data store on ships. The appended metadata can be used to control access to the data. Once the data is in the NTC-RI data store, multiple system applications (apps) can access the same information to facilitate tactical decisions. This illustrates the possible future for Navy systems, where apps are using data stored on a different computer system by accessing the information directly. The metadata allows the system to locate the data, and controls access to the data at the data object level. NTC-RI was a demonstration system and most of its capabilities will be included in the next increment of DCGS-N.

DCGS-N. DCGS-N stores data with metadata that is searchable by other systems. DCGS-N uses metadata standards managed by the DCGS Integrated Backbone. The DCGS metadata standards maintain the pedigree of data, which is critical for targeting. The pedigree of the data includes where the data was produced, when the data was produced, and what system or sensor originated the data. The standard metadata includes the security markup information or classification of the data, which indicates who can see the data (controlled at the data layer). DCGS-N demonstrates how important metadata is in controlling data accessibility.

DCGS-N pushes data to the ships. The system consolidates information from the other services and Government agencies. The information is then sent to the shipboard-part of the system for the ship to use. The ship will then combine the information with local sensor information to make decisions. Ships will also transfer information back to the DCGS-N shore-based system to be used by all the Services and Government agencies.

Data Understandability

To determine whether the selected systems conformed to DoD instructions, the audit team obtained documentation from the cognizant Program and System Managers regarding the systems' data elements, interfaces with systems both inside and outside of their functional areas, and the COIs in which they actively participate.

Data Elements. We found that data elements for the selected systems were not normalized between systems. For example, something as simple as a name was stored differently in every system we audited. Due to the lack of standardization, we found duplication of data in multiple system sources. Currently, systems are overcoming these differences in the standardization of data elements through system interfaces. Each system interface we audited had unique agreements between two systems that required one of the systems to transfer data to another system to be stored on the other system. One of the systems that sign the interface agreement would then be required to translate the data elements so that both systems could use the data. Further, two of the

eight systems audited were found to have used COTS software solutions that have pre-determined element names. The use of COTS will be addressed later in the audit results.

Interfaces. We found that each interface agreement we reviewed was unique and negotiated separately. We found that 7 of the 12 selected systems exchange data using flat files (i.e., each line of the transferred text file holds one record, with fields separated by delimiters, such as commas or tabs) and not in real time, but on scheduled intervals such as daily, weekly, or monthly. This type of technology to transfer files dates back to the early days of computers. We also found that 8 of the 12 systems use XML to exchange data. Using XML allows data to be transferred in a near real time manner and possibly allows data to be transferred on demand. One of the 12 (EPS) selected systems that was in the early planning phases, pre-Acquisition Category (ACAT), has requirements for the use of XML exchanges.

None of the selected systems used NIEM to transfer data. Also, none of the systems in the early planning stages had documentation that required NIEM. Furthermore, of the Program and System Managers of the 12 systems selected for review, six were unaware of NIEM. The best examples we found of systems meeting the DoD criteria were the tactical systems, NTC-RI and DCGS-N.

NTC-RI. NTC-RI ingests data from other systems as it is, appends metadata, and stores the information in a central data store on-ship. NTC-RI does not require systems to modify their data, but accepts it in any format including picture files, movies, sensor data, spreadsheets, and Microsoft Power Point presentations.

DCGS-N. DCGS-N searches other systems' databases using a browser (search engine) to locate and directly pull data from other systems and allows these other systems to browse and pull data from DCGS-N.

Both of these examples go beyond the need for a NIEM interface because they do not use the traditional interface.

Communities of Interest (COIs). We found that the Navy has not developed the necessary COIs, which include users outside of their functional areas, who are required to make a NIEM-first approach for data interfaces work. Some of the systems we reviewed were part of COIs that included:

Defense Manpower Data Center (DMDC). DMDC dictates many of the data element requirements for the Manpower, Personnel, Education, and Training COI. The Navy N1 COI is associated with the Enterprise Information Management Board, which is normalizing personnel data elements.

Naval Facilities Engineering Command (NAVFAC). NAVFAC is involved in a COI that developed the Real Property Inventory Requirements, which defines the data elements and language for real property assets.

The Defense Logistics Management System (DLMS). Naval Supply Systems Command (NAVSUP) is involved in a COI for DLMS, which defines the data exchange elements for all DoD logistics systems. These systems are required to be compliant by 2019. DoD Directive 8190.01E states that the Director, Defense Logistics Agency helps develop domain-relevant industry standards in support of NIEM, such as Accredited Standards Committee (ASC) X12, to support DoD, and incorporates changes to ASC X12 standards into DLMS in accordance with NIEM.

Distributed Common Ground System (DCGS). DCGS has a COI in the intelligence area that defines metadata standards for all data.

All of the functional COIs described above have developed standard data elements and/or metadata standards. They are, therefore, very close to having what they need to create NIEM interfaces. In many cases, all they need to do is group their data elements together in data objects, with the necessary metadata, and publish the results in a NIEM domain. By doing so, they will have achieved what is necessary to produce a NIEM interface. We found two systems under development that failed to address the DoD criteria, NMMES-TR and EPS, which provided no documentation to support the requirement to develop the necessary COIs.

Data Trustworthiness

We found that all eight selected business systems reviewed identified their systems as Authoritative Data Sources (ADSs). We also found that two of the eight business systems did not have interfaces that were transferring data in an XML format. Five of the eight business systems did not have interfaces that were transferring data using metadata. Of the three business systems with metadata, one system had metadata on the header and trailers on flat files to ensure that the file had been transferred, and one system had metadata tagged to unique transactions as shown on their Functional Design Specification. Of the planned business systems we audited, only EPS discussed use of metadata within the XML file exchanges. Coupled with not having a data strategy, we found that the data within the Navy's business systems was not trusted, as defined in DoD Instruction 8320.07.

The best examples we found of systems meeting the DoD criteria were NTC-RI and DCGS-N, which used metadata to document the pedigree of the data.

Data Interoperability

We found that two of the eight selected business systems (NMMES-TR and EPS) were in the early stages of system development. Since their data structure had not been developed or defined yet, we could not evaluate their data. They were still considered the poorest examples we found of systems failing to address the DoD criteria. NMMES-TR's problem statement, dated 19 January 2016, did not discuss interfacing with any system other than the maintenance community, and did not require the consideration of NIEM first or COIs. [redacted]

FOIA (b)(5)

The best examples we found of systems meeting the DoD criteria were the tactical systems NTC-RI and DCGS-N. NTC-RI ingests data from multiple systems and appends metadata and stores the information in a central database on-ship to be shared and accessed by apps that are developed for end-users. DCGS-N uses metadata to allow other systems to search system data.

Secretary of the Navy Instruction 5000.36A

DON CIO requested the audit team review Secretary of the Navy (SECNAV) Instruction 5000.36A, dated 19 December 2005, "Department of the Navy Information Technology Applications and Data Management," which is the primary instruction the Navy uses to control the Navy's data strategy. This instruction designates FAMs, who are responsible for the development and management of system, application, and database portfolios used to support the processes within that functional area. FAMs in turn appoint Functional Data Managers (FDMs). FDMs are organizations designated by the respective FAM to produce and control structuring of data and metadata within functional activities, information systems, and computing and communications infrastructures. The FAMs for the Navy are all designated CNO N-codes, such as N1 Personnel Management, N4 Logistics, etc.

We found that this oversight structure lends itself to those involved placing their emphases on the functional data needs of their own functional area in the Navy. We found that systems were typically developed to meet an organization's unique data needs without regard for how their data may be useful for the needs of others within the Navy who are using different systems, even though most of the business systems we audited had interfaces to systems outside of their functional area. The FAMs we visited were primarily resource sponsors who ensured the systems in their functional areas were funded. Limited guidance with respect to data strategy for their functional systems was issued by the FAMs.

Additionally, we only identified one FDM (CNO N1) that had been appointed prior to our audit commencing. We also identified one who was appointed after the audit began (N9). SECNAV Instruction 5000.36A states that FDM organizations shall:

1. Support FAM organizations in defining requirements for, and optimizing availability of, required data while eliminating unnecessarily redundant data in their functional area;
2. Coordinate and implement standardized DON functional processes to monitor the use of data within and across functional activities, information systems, and computing and communications infrastructures;
3. Coordinate and implement standardized DON guidance and processes for the registration of databases and data exchange formats;
4. Prepare and maintain appropriate functional area data architectures representing the aggregate of functional area data requirements linked to standards, interfaces, and ADSs;
5. Designate ADSs for their respective functional areas and maintain that designation using processes and procedures approved by DON CIO and the DDCIOs; and
6. Identify and manage resources required to execute FDM and Functional Namespace Coordinator (FNC) roles and responsibilities.

The system managers we spoke with during the audit could not provide us with any guidance (with exception of CNO N1) from the FAMs or FDMs that related to data management. Therefore, we determined that SECNAV Instruction 5000.36A was not being followed and was ineffective in shaping the Navy's data strategy.

Data Strategies

The most recent released DON data strategy is the 2 November 2000 "DON Data Management and Interoperability Strategic Plan." The Navy Data Management and Interoperability (DMI) Strategic Plan identifies strategic DMI goals and related performance measures. [redacted][3]

FOIA (b)(5)

[3] [redacted]

FOIA (b)(5)

DON Data Management and Interoperability Strategic Plan (2 November 2000)

During our review, we found that the DMI strategic plan was not published on the DON CIO Web site where other DON CIO instructions and memorandums were located. It also was not provided by DON CIO's office during our first meeting with them. We also found that only the Ordnance Information System (OIS), of the 12 systems' program managers, FAMs, or FDMs reviewed, provided us with this strategic plan or indicated that they were aware of it. At the completion of our fieldwork, DON CIO's office provided us a copy of the plan. Because only one command was aware of the strategic plan, we concluded it was out of date and no longer being used by the Navy.

Even though we concluded that the strategic plan is out of date, we found that it contains a lot of good information and valid concepts. The strategic plan contained strategic goals, defined objectives, planned products, and metrics to measure the success of the strategic plan. We found that this gave the strategy a clear vision of what should be, and allowed the progress and success of the strategy to be measured. Therefore, any updated Navy data strategy should include defined goals and benchmarks. It also identified the reasons why the Navy needs a data strategy by stating, "While hardware and software standards have played a major role in achieving basic interoperability, there has been less success in implementing data standards. Even as database management programs and hardware advance in step with the rest of IT, achieving systems interoperability at the data level has been very difficult. Earlier reasons include a lack of suitable standardization technologies and methodologies, lack of a pragmatic process, few qualified technical personnel, and fewer still high-level managers confronting the issue."

When comparing the strategic plan to current DoD instructions, we concluded that the Navy strategy matched well to the instructions when defining the importance of metadata; however, we found that it did not match well with:

1. DoD Instruction 8320.02, which states, "Data, information, and IT services will be made visible, accessible, understandable, trusted, and interoperable throughout their lifecycles for all authorized users." These attributes are not discussed in the Navy strategy;
2. DoD Instruction 8320.07, which addresses the "consider NIEM first" requirement, because NIEM did not exist in 2000 when the strategy was written; and
3. DoD CIO Cloud Computing Strategy (dated July 2012) that addresses the Cloud, because the Cloud did not exist in 2000, when the strategy was written.

An updated Navy data strategy should include the above items to be in compliance with DoD policy.

Draft Data Strategies Audit Results

[redacted]

FOIA (b)(5)

[redacted][4]

FOIA (b)(5)

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[4] [redacted]

FOIA (b)(5)

FOIA (b)(5)

[redacted]

Use of NIEM

On 28 March 2013, DoD CIO released a memorandum with the subject of "Adoption of the NIEM within the Department of Defense." This memorandum stated that "in order to comply with White House guidance on the adoption of reference information exchanges, DoD will adopt NIEM as the best suited option for standards-based data exchanges … DoD organizations shall first consider NIEM for their information sharing solutions when

deciding which data exchange standards or specifications meet their mission and operational needs. Every effort shall be made to ensure that a rigorous analysis of NIEM be conducted as a part of this consideration."

The memo also states, "The adoption of NIEM as a common standards-based data exchange may present challenges to some DoD stakeholders, particularly when viewed from the perspective of an individual program. In those situations where an organization's design goals and requirements are not fulfilled by NIEM, the organization shall provide justification why the use of NIEM is not feasible; exceptions may be granted by DoD CIO. In such cases, an organization shall use an alternative or complementary data standard that is interoperable with NIEM."

DoD Instruction 8320.07 (dated 3 August 2015) requires the Navy to provide justification of why the use of NIEM is not feasible in those situations where an organization's design goals and requirements are not fulfilled by NIEM. [redacted][5] This confirms that consideration of NIEM first should be a part of any Navy data strategy, and the Navy needs to document the steps taken to consider NIEM first.

FOIA (b)(5)

DoD Instruction 8320.07 states that in accordance with the DoD CIO memorandum, and except as required otherwise by law or DoD policy, the use of NIEM-based exchanges must be considered for all new XML information exchanges created, and for all XML information exchanges being modernized as part of the normal lifecycle management for these information exchanges. There is a coding language (Java Script Object Notation (JSON)) that is more efficient than XML. At the time of our review, XML was the primary language used by NIEM. JSON could be used to produce data objects with associated metadata similar to NIEM, producing a NIEM-like product, and it would be acceptable for the Navy to use in the development of new systems if it is compatible with the NIEM process. Since the time implementation of the instruction, the NIEM program has been revised to support the use of JSON for exchanging data using the NIEM vocabulary.

The NIEM Web site states, "NIEM has a model content for 14 domains, which are community-specific business areas. In addition, several emerging communities are working toward developing data model content, which may lead to the establishment of new domains." The development by the Navy and the United States Department of Homeland Security of the Maritime Domain within NIEM demonstrated that it takes time to develop a COI and then have this COI agree on the data objects, the data elements within these objects, and the metadata attached to these objects. Many of the current Navy systems are already members of a COI within their functional area, such as the Real Property Inventory Requirements, and the Defense Logistics Management Standards

[5] [redacted]

FOIA (b)(5)

(DLMS), which have set data element requirements that could be developed into NIEM interfaces. Also, systems managers can examine their current interfaces to determine what other activities use their data and include these activities in their COI.

The "consider NIEM first" requirement has been in place for 4 years, yet we could not find a single NIEM data exchange in the systems we audited. We concluded that the Navy does not have an internal control in place to ensure that systems follow the "consider NIEM first" requirement. If the Navy required all systems targeted for replacement to update their interfaces with NIEM before funding the new system, in our judgment, the Navy would establish the necessary internal control to ensure commands followed the "consider NIEM first" requirement, which would:

- Allow the COI to be developed before a system redesign begins;
- Define the agreed-upon data objects and metadata to be used in future interfaces for inclusion as a requirement for the development of the proposed system, allowing for these requirements to be placed in any contract used to purchase a new system; and
- Allow the possibility of the new system using the agreed-to data objects with associated metadata to be used in the data layer of the system. This would eliminate the need to translate data for interfaces, saving money.

The Cloud

The Navy does not have a policy that addresses what its data strategy should be within the cloud. Instead, we found that current Navy instructions only have guidance on how to purchase cloud services and what certifications the cloud provider is required to have to store certain impact level data. During the audit, we noted that five of the business systems reviewed were planning to move their systems to a cloud-based service. In each case, the developers of those systems were exploring the use of a commercial cloud. None of these systems have yet moved, but each of the managers for those systems is making plans for this move. This could result in five different cloud systems that continue to use flat file interfaces and store the same data in five different places.

We found two tactical system and one planned business system redesigns that showed a paradigm shift in how systems should be developed. Those systems were NTC-RI, DCGS-N, and the proposed CNO N1 strategy.

NTC-RI. NTC-RI is a central data store in a cloud-like environment aboard ship. It is not a commercial cloud environment, which demonstrates the ability for the Navy to produce cloud-like services on Navy-owned servers, using open source software. NTC-RI ingests data objects from feeder systems, appends metadata, stores the information in an open-source NoSQL database, and uses data analytics. Other computer apps on-ship then use the data within NTC-RI to analyze the data. NTC-RI

represents the potential future of data strategy where NoSQL databases can be leveraged as a service by multiple apps in lieu of major systems.

DCGS-N. DCGS-N stores information using data objects with standardized metadata. The standardized metadata allows other systems to search the data objects with a search engine, similar to searching for Web pages. This allows other systems to directly obtain information (data objects) from DCGS-N on demand without the need for an interface. DCGS-N uses standard metadata to document the pedigree of the data; therefore, the systems that obtain the information will know the source of the data and the date the data was created. The standard metadata also contains the classification of the data, which allows the system to control access to classified data at the data object level. DCGS-N represents the potential future of data strategy, where system databases can be searched, rather than using interfacing, and data can be controlled at the data object level, protecting classified information, personally identifiable information, and other business sensitive information.

[redacted]

FOIA (b)(5)

[redacted] Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource," dated 27 July 2016, which states that agencies shall structure acquisitions for major IT investments into useful segments, with a narrow scope and brief duration, in order to reduce risk, promote flexibility and interoperability, increase accountability, and better match mission needs with current technology and market conditions. The circular also states that agencies shall structure acquisitions to the extent practicable, using modular contracts for IT, including orders for increments or useful segments of work. Such contracts should be awarded within 180 days after the solicitation is issued. If an award cannot be made within 180 days, agencies shall consider cancelling the solicitation. The IT acquired should be delivered within 18 months after the solicitation, resulting in the award of the contract.

FOIA (b)(5)

The examples of NTC-RI, DCGS-N, [redacted], illustrate the importance of getting the data layer of Navy systems correct. The Navy is planning to move many systems to the Cloud where it can take advantage of the NoSQL data environment. Data that is stored in an ADS using data objects with standard metadata agreed to by the COIs would meet the requirements of being visible, accessible,

FOIA (b)(5)

understandable, trusted, and interoperable throughout their lifecycles for all authorized users.

The Navy could realize many benefits if it requires all new system development efforts to use NIEM data objects with metadata as their data dictionary for the systems (or define the data in the systems). This approach would enable data element normalization and normalized data objects, with metadata, across Navy systems. The normalization of metadata would enable a searchable data layer for all new Navy systems similar to what the Navy did with DCGS-N. The Navy could still develop unique data objects as required, using the NIEM construct.

Once the data level of systems has been defined, the Navy could develop apps to perform data entry, data processing, and system reports similar to the proposed CNO N1 strategy. With a standard data structure across the Navy, apps could be reused for new system development efforts, which could save resources such as funding and time. The Navy could use NIEM interfaces to feed legacy systems as the data layer is developed. Then, once the data layer was completed, the Navy could use NIEM interfaces to feed legacy data to the data layer. In our opinion, the Navy should not simply move current systems to the Cloud and recreate all of the current data problems there. The audit reviewed current Navy guidance for the Cloud and found that the Navy gave guidance on how Cloud services should be acquired and approved. The current Navy guidance did not determine what system data should look like in the Cloud.

In our opinion, the Navy should determine if it will use commercial Cloud services, GovCloud (COTS/Government-off-the-Shelf (GOTS)), or an internally-produced Cloud service based on a cost/benefit analysis and risk assessment. It is also our judgment that the Navy should determine if it should place multiple systems in the same Cloud environment based on a cost/benefit analysis and risk assessment. Further, the Navy should require and enforce the use of metadata for all data stored in a Cloud environment.

COTS Software

COTS systems are purchased with predetermined data elements and database design. Three of the systems we reviewed were COTS systems: Navy ERP, ESAMS, and EPS. After being modified, they are now considered modified-off-the-shelf (MOTS) systems.

Navy ERP. Navy ERP was purchased with about 90 percent of the data elements predetermined. The remaining data elements that were added were necessary due to the Navy's use of appropriation accounting and standard document numbers. Customization of ERP software was required to use these elements. We also noted that the system had many interfaces, each of which required a unique interface agreement. Each interface also required custom software, and costs were incurred to maintain these interfaces.

ESAMS. ESAMS was also purchased as a COTS solution, but it too required modification. ESAMS has a data dictionary, but that dictionary is considered proprietary.

Based on the examples of MOTS we audited, it is our judgment that the Navy will face challenges fitting COTS or MOTS into a data strategy.

EPS. The command staff confirmed that the ontology and elements for the future state of EPS will be based on a COTS solution. The COTS solution will not allow for input on a data dictionary, data elements, or data entities. We were told that there would be an option to allow for local fields to be added to the COTS solution. We were also told that customization of COTS will create cost increases due to Change Orders. These modifications would make this a MOTS system.

[redacted] FOIA (b)(5)

Command personnel stated that this would be the largest system moving to the Cloud to-date, and in their opinion, it is easier to start the system in the Cloud environment rather than migrate to the Cloud at a later date. The data structure had not been determined for EPS; therefore, we could not determine if the requirements of the five concepts in DoD Instruction 8320.02 (visible, accessible, understandable, interoperable, and trusted) would be met. [redacted] FOIA (b)(5)

NMMES-TR

DON CIO requested the audit team to review the proposed business system, NMMES-TR. We found that NMMES-TR had limited documentation available. We reviewed the problem statement for the system and determined that it did not discuss interfacing with any system other than the maintenance community. The problem statement also did not include the requirement to "consider NIEM first," therefore, a NIEM-first approach to system interfacing as described by DoD Instruction 8320.02 was not included in the Analysis of Alternatives (AOA). The AOA recommended a solution that combined a future version of a current COTS/MOTS system and modified modules of the current system. At the time of our review, the data structure had not been determined for NMMES-TR; therefore, we could not determine if the requirements of the five concepts from DoD Instruction 8320.02 would be met. Without the requirement to "consider NIEM first," this solution would not meet the DoD requirements.

Why This Occurred

DoD Data Attributes

We found that the Navy data strategy does not meet the DoD Instruction 8320.02 principles that data, information, and IT services be made visible, accessible, understandable, trusted, and interoperable throughout their lifecycles. Some of the systems were designed before the development of metadata. Some systems were COTS, and the designer of the system determined the structure of the data. Also, the Navy did not follow the November 2000 DON "Data Management and Interoperability Strategic Plan," SECNAV Instruction 5000.36A, or DoD Instructions 8320.02 and 8320.07.

Data Strategy

DON CIO and DDCIO (N) did not ensure implementation of a data strategy that includes attributes as required by DoD Instructions 8320.02 and 8320.07. The development of this strategy was required by SECNAV Instruction 5000.36A, which requires DON CIO to "[d]evelop and maintain a DON net-centric data strategy to ensure requisite processes, products, tools, and metrics are in place to resolve system data interoperability and cross-functional issues, including the designation and management of ADS, and the development of integrated Service-level and DON data architectures" in accordance with DoD directives and instructions. The audit concluded that this had not been done from November 2000 until this audit began. After the audit began, DON CIO initiated work on an updated draft data strategy.

Use of NIEM

The policy of "consider NIEM first," has been around since 2013; however, the Navy does not have a single NIEM interface. Based on our review, we found that the Navy personnel we met with do not consider this to be a requirement, and as a result, they are not implementing it. Six of the system managers we spoke to during the audit were not aware of NIEM. In cases where NIEM is not used, an organization shall use an alternative or complementary data standard that is interoperable with NIEM. During our review, we found no evidence that NIEM was considered or an exemption request had been made by the Navy.

Cloud

Based on our review, we concluded that Navy personnel believe that use of the Cloud is cheaper than running their own data centers. As a result, the Navy has focused its attention on how to acquire Cloud services. It was also noted during our review that despite this focus, the Navy has not developed polices on how data should be stored in

the Cloud. While storing data in the Cloud may be a viable solution, a data strategy including the five concepts from DoD Instruction 8320.02 is necessary to ensure optimal communication between systems and reduce redundancy in the Cloud.

COTS

Navy personnel believe that COTS software is cheaper than developing Navy software. They also believe that private business processes that are imbedded in COTS products are more efficient. Therefore, most new Navy systems plan to have COTS software. COTS products come with their own data structure, which may not match any data standards established by the Navy or DoD. Therefore, in our judgment, using COTS and maintaining a data strategy will be a challenge for the Navy.

Impact

Because the Navy lacks an enterprise-wide data strategy, it is perpetuating obsolescence by planning new systems that will not conform to the DoD data strategy. Potential nonconformances will include a continuing lack of interoperability, duplication of data and effort, and COTS products that, upon fielding, will not conform to current DoD instruction requirements.

Our judgmental selection of systems included:

- 3 ACAT I systems (NMMES-TR, DCGS-N, and ERP). An acquisition program listed as ACAT I is estimated to require expenditure for research, development, test, and evaluation (RDT&E) of more than $480 million or any procurement exceeding $2.79 billion (FY 2014 dollars);
- 1 ACAT II system (ALMDS). Acquisition programs listed as ACAT II require RDT&E expenditure exceeding $185 million or procurement of more than $835 million (FY 2014 dollars);
- 1 ACAT III system (OIS). Acquisition programs listed as ACAT III are those that do not meet the criteria for ACAT II or above; and
- 6 Non-ACAT systems and one system not listed in DITPR-DON.

Recommendations and Corrective Actions

Our recommendations, summarized management responses, and our comments on the responses follow. The scanned text of management responses is in the Appendixes.

We recommend that the Department of the Navy Chief Information Officer and Department of the Navy Deputy Chief Information Officer:

Recommendation 1. Implement a Navy data strategy that:

a. Emphasizes the requirements of the five concepts within Department of Defense Instruction 8320.02 (visible, accessible, understandable, interoperable, and trusted);

b. Implements the Office of Management and Budget Memorandum M-13-13 "Open Data Policy-Managing Information as an Asset," dated 9 May 2013, including using machine-readable and open formats, data standards, ensuring information stewardship through the use of open licenses, and using common core and extensible metadata;

c. Ensures Navy data management strategy and policies include defined goals and benchmarks;

d. Requires all systems that are targeted for replacement to develop the National Information Exchange Model interfaces or a Department of Defense Chief Information Officer-approved alternative. Ensure completion of this step prior to the development of the replacement or redesigned system. This defines data objects (including data elements) and metadata for system development or redesign effort interfaces;

e. Requires all new acquisition programs to follow the National Information Exchange Model methodology (or Department of Defense Chief Information Officer approved alternative) for sharing and re-using data models, and be required to demonstrate the conformity based on a standardized data deliverable as part of the acquisition's Contract Data Requirements List. These accepted data deliverables will be incorporated back into the Department of the Navy enterprise architecture to guide future re-use and data integration;

f. Determines the Navy's strategy for cloud technology. Specifically:

- Determine if the Navy will use commercial cloud services, GovCloud (commercial-off-the-shelf/Government-off-the-shelf), or an internally produced cloud service based on a cost/benefit analysis and risk assessment;
- Determine if the Navy should place multiple systems in the same cloud environment based on a cost/benefit analysis and risk assessment; and

- Require and enforce the use of metadata for all data stored in a cloud environment, in accordance with Department of Defense Instruction 8320.02; and

g. Allows flexibility within the strategy for new and emerging technologies.

Department of the Navy Chief Information Officer (DON CIO) management response. Concur. On 15 September 2017, the DON CIO released the Department of the Navy Strategy for Data and Analytics Optimization. In addition, DON CIO established the Data and Analytics Consortium (DAC) as a forum for data sharing and analytics. The DAC will respond to data and decision demands, share best practices, collaborate on related research, and promote the governance, standards, training, and policies necessary to achieve data and analytics optimization. We will continue to work closely with the DON Deputy CIO (Navy) (DDCIO (N)) and other stakeholders to implement the strategy.

DDCIO (N) management response to Recommendation 1. Concur. To ensure DON alignment, we are working closely with DON CIO and other stakeholders to define the scope of work and spiral-development timeline over the next 18 months, with a targeted completion date of 30 August 2019. In order to ensure full Naval Audit Service insight on addressing recommendations, DON CIO and the Navy Cyber Security Division Director will provide a coordinated status update of progress toward addressing the audit recommendations every 90 days from date of formal issuance of the audit report.

In the near term, we are leveraging existing Department of Defense instructions and industry standards to create an overarching Navy Data Integration Framework to guide on-going data integration and interoperability efforts.

Naval Audit Service comment on management responses. The management responses and corrective actions taken and planned meet the intent of the recommendation.

We confirmed DON CIO developed and promulgated the Department of the Navy Strategy for Data and Analytics Optimization. No further action is required on their part, and the recommendation is considered closed for their purposes.

DDCIO (N)'s planned actions and coordination should result in implementation of the data strategy addressing the elements laid out in the recommendation. The recommendation is considered open until corrective actions are completed. Because the target completion date is more than 1 year in the future, we are establishing an interim reporting date of 7 August 2018; we request that the command provide us with an update on the corrective actions at that time.

We recommend that Deputy Chief of Naval Operations resource sponsors:

Recommendation 2. Require all systems that are targeted for replacement to develop the National Information Exchange Model interfaces or a Department of Defense Chief Information Officer-approved alternative. Ensure completion of this step prior to the development of the replacement or redesigned system. This defines data objects (including data elements) and metadata for system development or redesign effort interfaces.

DDCIO (N) management response. Concur. To ensure DON alignment, we are working closely with DON CIO and other stakeholders to define the scope of work and spiral-development timeline over the next 18 months, with a targeted completion date of 30 August 2019. In order to ensure full Naval Audit Service insight on addressing recommendations, DON CIO and the Navy Cyber Security Division Director will provide a coordinated status update of progress toward addressing the audit recommendations every 90 days from the date of formal issuance of the audit report.

In the near term, we are leveraging existing Department of Defense instructions and industry standards to create an overarching Navy Data Integration Framework to guide on-going data integration and interoperability efforts.

Naval Audit Service comment on the management response. The management response and planned corrective actions meet the intent of the recommendation. This recommendation is considered open until corrective actions are completed. Because the target completion date is more than 1 year in the future, we are establishing an interim reporting date of 7 August 2018; we request that the command provide us with an update on the corrective actions at that time.

Section B: Status of Recommendations

Recommendations							
Finding[6]	Rec. No.	Page No.	Subject	Status[7]	Action Command	Target or Actual Completion Date	Interim Target Completion Date[8]
1	1	23	Implement a Navy data strategy that: a. Emphasizes the requirements of the five concepts within Department of Defense Instruction 8320.02 (visible, accessible, understandable, interoperable, and trusted); b. Implements the Office of Management and Budget Memorandum M-13-13 "Open Data Policy-Managing Information as an Asset," dated 9 May 2013, including using machine-readable and open formats, data standards, ensuring information stewardship through the use of open licenses, and using common core and extensible metadata; c. Ensures Navy data management strategy and policies include defined goals and benchmarks; d. Requires all systems that are targeted for replacement to develop the National Information Exchange Model interfaces or a Department of Defense Chief Information Officer-approved alternative. Ensure completion of this step prior to the development of the replacement or redesigned system. This defines data objects (including data elements) and metadata for system development or redesign effort interfaces;	C O	Department of the Navy Chief Information Officer and Department of the Navy Deputy Chief Information Officer	9/15/17 8/30/19	 8/8/18

[6] "+" = Indicates repeat finding.
[7] O = Recommendation is open with agreed-to corrective actions; C = Recommendation is closed with all action completed; U = Recommendation is undecided with resolution efforts in progress.
[8] If applicable.

Recommendations							
Finding[6]	Rec. No.	Page No.	Subject	Status[7]	Action Command	Target or Actual Completion Date	Interim Target Completion Date[8]
			e. Requires all new acquisition programs to follow the National Information Exchange Model methodology (or Department of Defense Chief Information Officer approved alternative) for sharing and re-using data models, and be required to demonstrate the conformity based on a standardized data deliverable as part of the acquisition's Contract Data Requirements List. These accepted data deliverables will be incorporated back into the Department of the Navy enterprise architecture to guide future re-use and data integration; f. Determines the Navy's strategy for cloud technology. Specifically: • Determine if the Navy will use commercial cloud services, GovCloud (commercial-off-the-shelf/Government-off-the-shelf), or an internally produced cloud service based on a cost/benefit analysis and risk assessment; • Determine if the Navy should place multiple systems in the same cloud environment based on a cost/benefit analysis and risk assessment; and • Require and enforce the use of metadata for all data stored in a cloud environment, in accordance with Department of Defense Instruction 8320.02; and g. Allows flexibility within the strategy for new and emerging technologies.				

Recommendations							
Finding[6]	Rec. No.	Page No.	Subject	Status[7]	Action Command	Target or Actual Completion Date	Interim Target Completion Date[8]
1	2	25	Require all systems that are targeted for replacement to develop the National Information Exchange Model interfaces or a Department of Defense Chief Information Officer-approved alternative. Ensure completion of this step prior to the development of the replacement or redesigned system. This defines data objects (including data elements) and metadata for system development or redesign effort interfaces.	O	Deputy Chief of Naval Operations resource sponsors	8/30/19	8/8/18

Exhibit A: Background and Pertinent Guidance

Background

Department of Defense (DoD) Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," dated 5 August 2013, issued policy that data, information, and IT services are considered enablers of information sharing to DoD. It further states that data, information, and IT services will be made visible, accessible, understandable, trusted, and interoperable throughout their lifecycles for all authorized users. Authorized users include DoD consumers and mission partners, subject to law, policy, data rights, and security classifications. All DoD activities implement applicable standards and specifications as cited in the DoD IT Standards Registry.

The Department of the Navy's (DON's) current policy, Secretary of the Navy (SECNAV) Instruction 5000.36A, "Department of the Navy Information Technology Applications and Data Management," dated 19 December 2005, states that the DON Chief Information Officer (DON CIO) is tasked with developing and maintaining a DON net-centric data strategy to ensure requisite processes, products, tools, and metrics are in place to resolve systems data interoperability and cross-functional issues, including the designation and management of authoritative data sources (ADSs) and the development of integrated service-level and DON data architectures, in accordance with DoD directives and instructions (SECNAV Instruction 5000.36A Section 6.a.(5)).

DON Chief of Naval Operations (CNO) N-codes act as resource sponsors for Navy systems. According to SECNAV Instruction 5000.36A, they shall also serve as Functional Area Managers (FAMs) who develop and manage the information management (IM)/IT system portfolio, application portfolio, and database portfolio to ensure that technology strategies are aligned with DON and Global Information Grid Mission Area strategies. The FAMs are to appoint Functional Data Managers (FDMs) who support FAM organizations in defining requirements for and optimizing the availability of required data while eliminating unnecessarily redundant data in their functional area.

Under this structure the Navy should have implemented DON's latest data strategy released in November 2000, the "DON Data Management and Interoperability Strategic Plan."

Pertinent Guidance

DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology Services in the Department of Defense," 5 August 2013, establishes policies, assigns responsibilities, and prescribes procedures for securely sharing electronic data,

information, and IT services, and securely enabling the discovery of shared data throughout DoD. The instruction also facilitates the shift from the transport medium to a focus on content, and guides the use of resources to implement the secure sharing of data, information, and IT services within DoD information enterprises and with mission partners.

DoD Instruction 8320.07, "Implementing the Sharing of Data, Information, and Information Technology Services in the Department of Defense," 3 August 2015, establishes policy, assigns responsibilities, and prescribes procedures to implement DoD Instruction 8320.02, and enables a secure sharing environment in DoD that supports the warfighting, business, DoD intelligence, and information enterprise environment mission areas. This instruction describes or references key enablers necessary for sharing data, information, and IT services, and ensuring data, information, and IT services are visible, accessible, understandable, trustworthy, and interoperable. Key enablers include, but are not limited to, concepts, processes, governance forums, standards, models, and shared vocabularies. For the purposes of the instruction, data sharing and information sharing are equivalent terms. Service and IT service are used interchangeably throughout this instruction. IT services include DoD Enterprise Services; however, not all IT services are DoD Enterprise Services. Further, this instruction guides the use of resources for implementing the sharing of data, information, and IT services within DoD information enterprises and with mission partners.

SECNAV Instruction 5000.36A, "Department of the Navy Information Technology Applications and Data Management," 19 December 2005, establishes the overarching policy for DON apps and data management. The instruction describes the roles and responsibilities of the DON FAMs, FDMs, and Functional Namespace Coordinators. Also, the instruction establishes roles and responsibilities for the development, execution, and maintenance of DON IT processes and tools to transform apps and data into net-centric Naval capabilities consistent with DoD policy for interoperability and data sharing. The instruction describes the relationships between DON CIO, the Assistant Secretaries of the Navy, Chief of Naval Operations, and the Commandant of the Marine Corps for DON apps and data management.

OMB Memorandum M-13-13, "Open Data Policy-Managing Information as an Asset," 9 May 2013, states, "Information is a valuable national resource and a strategic asset to the Federal Government." It prescribes the use of common core and extensible metadata, and requires agencies to describe information using common core metadata, in consultation with the best practices found in Project Open Data,[9] as it is collected and created. The memorandum also mandates that metadata should include information about origin, linked data, geographic location, time series continuations, data quality, and other relevant indices that reveal relationships between datasets, and allow the public to

[9] Project Open Data was an effort to make data that is releasable by the Federal Government easier to find and use.

determine the fitness of the data source. Agencies may expand on the basic common metadata based on standards, specifications, or formats developed within different communities (e.g., financial, health, geospatial, law enforcement, etc.). Groups that develop and promulgate these metadata specifications must review them for compliance with the common core metadata standard, specifications, and formats. The memorandum also requires that agencies build information systems to support interoperability and information accessibility.

DoD CIO Memorandum, "Adoption of the National Information Exchange Model within the Department of Defense," 28 March 2013, establishes guidance on the adoption of reference information exchanges, and states that DoD will adopt National Information Exchange Model (NIEM) as the best suited option for standards-based data exchanges. This adoption is to involve a series of phased implementations by components and programs using NIEM content, guidance, and tools in an integrated effort to transition current DoD data exchange standards, specifications, and policies to a NIEM-based approach. In addition, DoD is tasked with working with the NIEM Program Management Office to create a Military Operations Domain as part of NIEM.

Exhibit B: Scope and Methodology

We conducted the audit of "Navy Data Strategy" between 1 August 2016 and 4 December 2017. Conditions noted in this report existed at the time of our audit fieldwork. The scope of the audit was derived from the Fiscal Year (FY) 2016 Program Executive Office for Enterprise Information Systems' (PEO EIS's) Risk and Opportunity Assessment submission. To address our audit objective, we evaluated pertinent Department of Defense (DoD) and Department of the Navy (DON) criteria on data management, identified and selected current and planned acquisition category systems, and assessed the plans and implementation schedules for select systems to ensure they reflected industry best practices such as the National Information Exchange Model (NIEM) and Cloud computing.

To determine if DON's data strategy is consistent with DoD guidance and joint information environment (JIE) mandates, we selected a judgmental[10] sample of 12 Navy business and tactical systems contained within the DON Application and Database Management System (DADMS) and DoD Information Technology Portfolio Repository (DITPR) DON registries, which was provided by the DON Chief Information Officer (CIO). Table 3 below shows the 12 selected systems reviewed (Exhibit C identifies the organizations visited and/or contacted during the audit, and Exhibit D details Selected System Results).

Table 3. Selected Navy Systems

System Name (abbreviation)	Tactical/Business	Owner/SYSCOM
Distributed Common Ground System-Navy (DCGS-N)	Tactical	PEO C4I
Maritime Domain Awareness-Non Classified Enclave	Tactical	Office of Naval Intelligence
Airborne Laser Mine Detection System	Tactical	NAVSEA
Navy Tactical Cloud-Reference Implementation (NTC-RI)	Tactical	ONR
Enterprise Procurement System (EPS)	Business	PEO EIS
Navy Maritime Maintenance Enterprise Solution- Technical Refresh (NMMES-TR)	Business	NAVSEA
Maritime Shore Environment	Business	NAVSEA
Navy Enterprise Resource Planning (ERP)	Business	PEO EIS
Enterprise Safety Application Management System (ESAMS)	Business	CNIC
Internet Facilities Asset Data Store (iNFADS)	Business	NAVFAC
Navy Enlisted System (NES)	Business	CNO N1 (N16) BUPERS
Ordnance Inventory System	Business	NAVSUP

Acronym key: BUPERS – Bureau of Navy Personnel; PEO – Program Executive Office; PEO C4I –PEO Command, Control, Communications, Computers, and Intelligence; CNIC – Commander, Navy Installations Command; PEO EIS – PEO Enterprise Information Systems; CNO N1 – Office of the Chief of Naval Operations Manpower, Personnel, Education, and Training; CNO N16 – OPNAV N1-Enterprise; NAVFAC – Naval Facilities Engineering Command; NAVSEA – Naval Sea Systems Command; NAVSUP – Naval Supply Systems Command; ONR – Office of Naval Research; SPAWAR – Space and Naval Warfare Systems Command..

[10] A judgmental sample was selected due to the nature of the audit, part of which was to examine unique information systems and determine whether data strategy considerations were made in accordance with DoD instructions. The sample was selected based on six systems recommended by DON Chief Information Officer (DON CIO), DON Deputy CIO (Navy) (DDCIO (N)), and Space and Naval Warfare Systems Command (SPAWAR); six systems were selected by the team to maximize coverage across Navy system commands.

Our review focused on analyzing supporting documentation to determine compliance with DoD guidance and JIE mandates. This supporting documentation was provided by program and system managers, DON CIO, and DON Deputy CIO (Navy) (DDCIO (N)) subsequent to interviewing personnel and visiting selected system owners. Initially, the audit team met with SPAWAR PEO EIS personnel to confirm the continuing need for the audit. DON CIO was also interviewed to discuss Navy policies and instructions. We selected a sample of 12 Navy systems to determine their data strategy and/or guidance provided concerning the Navy data strategy, and whether their system designs or architecture considered any data strategy elements within DoD instructions.

Internal Controls/Compliance

We evaluated internal controls and reviewed compliance with applicable regulations. Specifically, we compared the data attributes of the systems we audited to laws and regulations. We also reviewed the Managers' Internal Control program at SPAWAR and did not find any issues that relate to this audit.

Data Reliability

We gathered data from DADMS/DITPR-DON that was provided by DON CIO, but did not test the reliability of the data because it was outside the scope of this audit. Although we looked at system data attributes and data structures, we did not test the data reliability of information within the systems we audited.

Followup

We reviewed reports from the Naval Audit Service, Department of Defense Inspector General, and Government Accountability Office, and found there were no reports published in the past 5 years covering Navy data strategy; therefore, no followup was required.

Federal Managers' Financial Integrity Act

The Federal Managers' Financial Integrity Act of 1982, as codified in Title 31, United States Code, requires each Federal agency head to annually certify the effectiveness of the agency's internal and accounting system controls. Recommendations 1-2 address issues related to the internal control over Navy data strategy. In our opinion, the weaknesses noted in this report may warrant reporting in the Auditor General's annual FMFIA memorandum identifying management control weaknesses to the Secretary of the Navy.

Auditing Standards

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Exhibit C: Communications with Management

Noteworthy Accomplishments

During the course of the audit, Department of the Navy Chief Information Officer (DON CIO) personnel took action to initiate the creation of an updated draft Navy data strategy that reflects Department of Defense (DoD) Instruction 8320.02 requirements. We still made recommendations to ensure the implementation of this draft strategy in order that DON complies with the current DoD instructions. At the time of audit publication, the strategy had not been completed.

Meetings with DON Officials

Throughout the audit, we kept DON personnel informed of the conditions noted. Specifically, we conducted site visits at the 12 selected systems' program offices from 16 August 2016 through 28 March 2017 and provided preliminary results to the appropriate personnel at the end of each site visit and/or upon request. We spoke to personnel at Chief of Naval Operations Fleet Readiness and Logistics (CNO N4). Additionally, we provided findings and preliminary recommendations to DON CIO, DON Deputy Chief Information Officer (Navy) (DDCIO (N)), and CNO Manpower, Personnel, Education, and Training (N1).

Activities Contacted and/or Visited During the Audit

- DON CIO, Arlington, VA*
- DDCIO (N), Arlington, VA*
- Space and Naval Warfare Systems Command (SPAWAR), San Diego, CA *
- CNO N1
    - Executive Director CNO Manpower, Personnel, Training, and Education (N1), Arlington, VA*
- CNO N4
    - CNO N4 Functional Area Manager (FAM), Washington, DC*
- CNO N1-Enterprise (CNO N16)
    - CNO N16 Chief Data Steward, Millington, TN *
- Office of Naval Research
    - Program and System Managers for the Navy Tactical Cloud-Reference Implementation, Arlington, VA*
- Office of Naval Intelligence

- Program and System Managers for Maritime Domain Awareness Non-Classified Enclave, Suitland, MD*

- Naval Sea Systems Command
  - Program and System Managers Airborne Laser Mine Detection System, Washington, DC*
  - Program and System Managers Navy Maritime Maintenance Enterprise Solution-Technical Refresh (NMMES-TR), Washington, DC *
  - Program and System Managers for the Maritime Shore Environment, Washington, DC *
- Naval Facilities Engineering Command
  - Program and System Managers for the Internet Facilities Asset Data Store, Washington, DC *
- Naval Supply Systems Command
  - Program and System Managers for the Ordnance Information System, Mechanicsburg, PA and Norfolk, VA*
- Commander, Navy Installations Command
  - Program and System Managers for the Enterprise Safety Application Management System, Washington, DC *
- Program Executive Office (PEO) for Enterprise Information Systems
  - Program and System Managers for the Enterprise Resource Planning, Washington, DC *
  - Program and System Managers for the Enterprise Procurement System, Washington, DC *
- PEO Command, Control, Communications, Computers, and Intelligence
  - Program and System Managers for the Distributed Common Ground System-Navy, San Diego, CA *

**Denotes activity visited.*

Exhibit D: Selected System Results Table

				Visibility	Accessibility
System Number	**System Name (abbreviation)**	**Tactical/ Business**	**Owner/SYSCOM**	**Visible to Authorized Users: Data Dictionary**	**Accessible to Authorized Users: Interface Methods**
Benchmark	NIEM Core	Tactical/ Business	N/A	Has published data dic ionary	XML/Meta data
1	Distributed Common Ground System- Navy (DCGS-N)	Tactical	PEO C4I	Did not provide a complete data dictionary	Data Objects/Meta data
2	Maritime Domain Awareness-Non Classified Enclave (MDA-NCE)	Tactical	Office of Naval Intelligence	Does not store data – provides method of moving data.	NA
3	Airborne Laser Mine Detection System (ALMDS)	Tactical	NAVSEA	Does not store data – creates source data which is provided to another system.	Binary
4	Navy Tactical Cloud (NTC)	Tactical	ONR	Designed to store information from several applications/systems	Data Objects/Meta data
5	Enterprise Procurement System (EPS)	Business	PEO EIS	Early planning phase of development	Early planning phase of development (proposed to have flat-file and XML interfaces depending on system partners)
6	Navy Maritime Maintenance Tech. Refresh (NMMES-TR)	Business	NAVSEA	Early planning phase of development	Early planning phase of development
7	Maritime Shore Environment (MSE)	Business	NAVSEA	No current data dictionary - Provided table layouts	Relational database/Flat file interfaces
8	Navy Enterprise Resource Planning (ERP)	Business	PEO EIS	No current data dictionary - Provided table layouts Stores data as data objects with associated metadata	Relational database/Flat File or XML interfaces
9	Enterprise Safety Applica ion Management System (ESAMS)	Business	CNIC	Has data dic ionary – (Proprietary)	Relational database/Flat File or XML interfaces
10	Internet Facilities Asset Data Store (INFADS)	Business	NAVFAC	Has published data dic ionary	Relational database/Flat file interfaces
11	NAVY ENLISTED SYSTEM (NES)	Business	N1 (N16) BUPERS	Has data dictionary	Flat file/Flat file interfaces
12	Ordnance Inventory System (OIS)	Business	NAVSUP	Has data dictionary	Relational database/Flat file interfaces

				Understandability	Trusted	Interoperability
System Number	System Name (abbreviation)	Tactical/ Business	Owner/SYSCOM	Understandable to Authorized Users and Systems	Does the System Have Sufficient "pedigree" and Metadata	Data Assets Able to Reuse Business and Mission Processes
Benchmark	NIEM Core	Tactical/ Business	N/A	Nc:PersonGivenName Nc:PersonMiddleName	Yes	Yes
1	Distributed Common Ground System- Navy (DCGS-N)	Tactical	PEO C4I	N/A	Yes	Yes
2	Maritime Domain Awareness-Non Classified Enclave (MDA-NCE)	Tactical	Office of Naval Intelligence	MDA-NCE- N/A AMRS (Depends on Table)- FIRSTNM; first_name; last_name, LASTNM GT- N/A	NA	NA
3	Airborne Laser Mine Detection System (ALMDS)	Tactical	NAVSEA	N/A	N/A	Yes
4	Navy Tactical Cloud (NTC)	Tactical	ONR	N/A	Yes	Yes
5	Enterprise Procurement System (EPS)	Business	PEO EIS	Early planning phase of development	Yes	No
6	Navy Maritime Maintenance Tech. Refresh (NMMES-TR)	Business	NAVSEA	Early planning phase of development	Early planning phase of development	No
7	Maritime Shore Environment (MSE)	Business	NAVSEA	Depends on Table FIRST_NM (MID_INITIAL MIDDLE_NM) LAST_NM	No	No
8	Navy Enterprise Resource Planning (ERP)	Business	PEO EIS	First_Name VORNA Middle_Nm MIDNM Last_Nm NACHN	Maybe (Use some metadata)	No
9	Enterprise Safety Application Management System (ESAMS)	Business	CNIC	No current data dictionary – (Proprietary)	Maybe (Use some metadata)	No
10	Internet Facilities Asset Data Store (INFADS)	Business	NAVFAC	N/A	No	No
11	NAVY ENLISTED SYSTEM (NES)	Business	N1 (N16) BUPERS	MEMBER_NAME (Full Name including surname, first, middle, and suffix is within this element)	No	No
12	Ordnance Inventory System (OIS)	Business	NAVSUP	Multiple (43 Instances where "Name" occurs) First_Name, User_First_Name, USER_FIRST_NAME, Last_Name, USER_LAST_NAME Middle name or initial not used	No	No

Acronym key: BUPERS – Bureau of Navy Personnel; PEO – Program Executive Office; PEO C4I –PEO Command, Control, Communications, Computers, and Intelligence; CNIC – Commander, Navy Installations Command; PEO EIS – PEO Enterprise Information Systems; CNO N1 – Office of the Chief of Naval Operations Manpower, Personnel, Education, and Training; CNO N16 – OPNAV N1-Enterprise; NAVFAC – Naval Facilities Engineering Command; NAVSEA – Naval Sea Systems Command; NAVSUP – Naval Supply Systems Command; NIEM – National Information Exchange Model; ONR – Office of Naval Research; SPAWAR – Space and Naval Warfare Systems Command; SYSCOM – Systems Command.

Exhibit E: List of Acronyms

ADS	Authoritative Data Sources
Apps	Applications
CNO	Chief of Naval Operations
CNO N1	Office of the Chief of Naval Operations Manpower, Personnel, Education, and Training
CNO N4	Office of the Chief of Naval Operations Fleet Readiness and Logistics
CNO N16	OPNAV N1-Enterprise
COI	Community of Interest
COTS	Commercial off-the-shelf
CNIC	Commander, Navy Installations Command
DADMS	DON Application and Database Management System
DCGS	Distributed Common Ground System
DCGS-N	Distributed Common Ground System-Navy
DDCIO (N)	Department of the Navy Deputy Chief Information Officer (Navy)
DDMS	Department of Defense Discovery Metadata Specification
DER	Data Engineering Resources
DITPR-DON	DoD IT Portfolio Repository-Department of the Navy
DLMS	Defense Logistics Management System
DMI	Data Management and Interoperability
DoD	Department of Defense
DON	Department of the Navy
DON CIO	Department of the Navy Chief Information Officer
DSE	DoD Data Services Environment
EPS	Enterprise Procurement System
ERP	Enterprise Resource Planning
ESAMS	Enterprise Safety Application Management System
FAM	Functional Area Managers
FDM	Functional Data Managers
FNC	Functional Namespace Coordinators
IE	Information Enterprise
IM	Information Management
iNFADS	Internet Facilities Asset Data Store
IT	Information Technology

IT PfM	Information Technology Portfolio Management
JIE	Joint Information Environment
MOTS	Modified off-the-shelf
N2/N6	Navy Cyber Security Division Director, Office of the Chief of Naval Operations
N4	Fleet Readiness and Logistics
N9	DCNO for Warfare Systems
NAVFAC	Naval Facilities Engineering Command
NAVSEA	Naval Sea Systems Command
NAVSUP	Naval Supply Systems Command
NIEM	National Information Exchange Model
NIPRNET	Non-Secure Internet Protocol Router Network
NMMES-TR	Navy Maritime Maintenance Enterprise Solution- Technical Refresh
NTC-RI	Navy Tactical Cloud-Reference Implementation
OMB	Office of Management and Budget
ONR	Office of Naval Research
PEO	Program Executive Office
PEO C4I	SPAWAR PEO Command, Control, Communications, Computers, and Intelligence
PEO EIS	Program Executive Office for Enterprise Information Systems
PMS 495	Program Manager, Mine Warfare
SECNAV	Secretary of the Navy
SIPRNET	Secret Internet Protocol Router Network
SPAWAR	Space and Naval Warfare Systems Command
XML	Extensible Markup Language

Appendix 1: Management Response from Department of the Navy Chief Information Officer

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

8 February 2018

MEMORANDUM FOR NAVAL AUDIT SERVICE

Subj: DRAFT REPORT 2016-091

Regarding Recommendation 1: Concur. On 15 September 2017, the DON Chief Information Officer (CIO) released the Department of the Navy Strategy for Data and Analytics Optimization. In addition, we established the Data and Analytics Consortium (DAC) as a forum for data sharing and analytics. The DAC will respond to data and decision demands, share best practices, collaborate on related research, and promote the governance, standards, training, and policies necessary to achieve data and analytics optimization. We will continue to work closely with the DON Deputy CIO (Navy) and other stakeholders to implement the strategy.

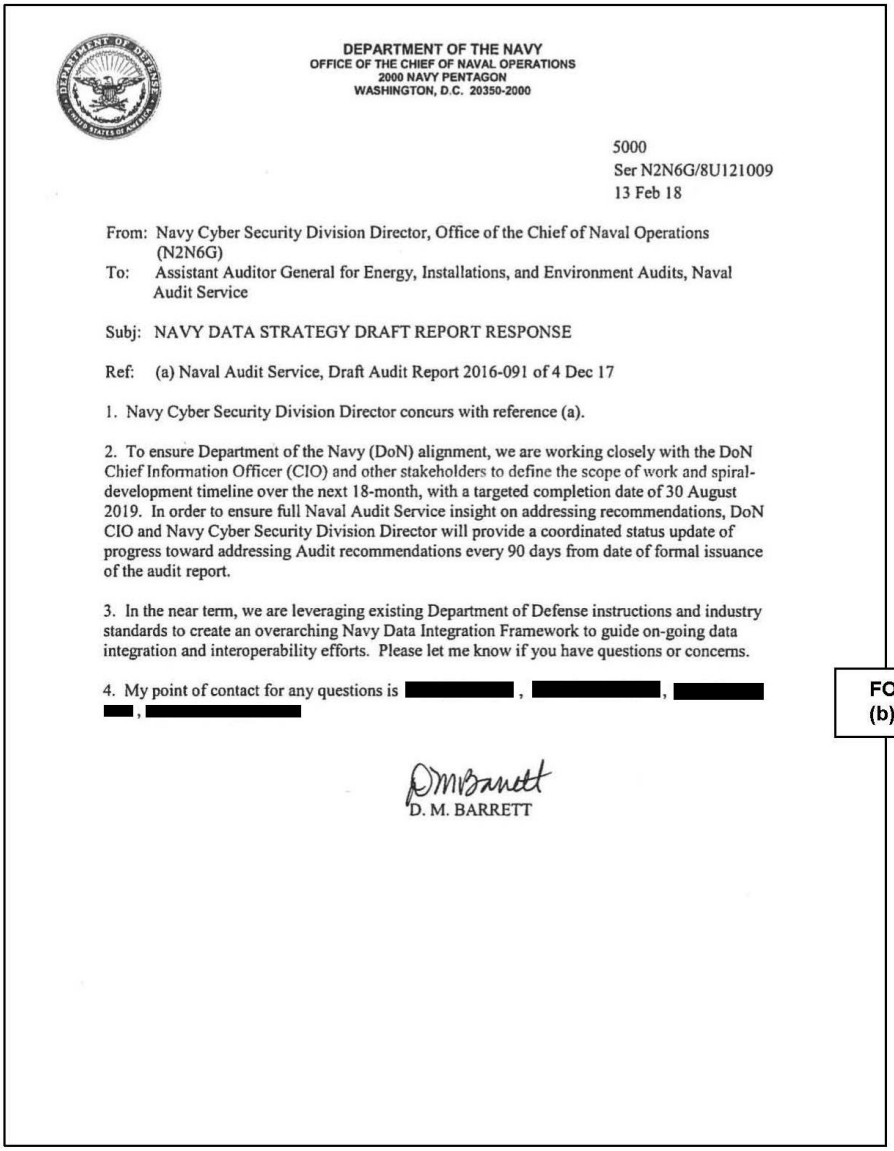
The point of contact is [redacted], [redacted], [redacted].

[redacted]
[redacted]

CAPT, USN
Chief of Staff

FOIA (b)(6)

Appendix 2: Management Response from Navy Cyber Security Division Director, Office of the Chief of Naval Operations (N2N6G)



DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
2000 NAVY PENTAGON
WASHINGTON, D.C. 20350-2000

5000
Ser N2N6G/8U121009
13 Feb 18

From: Navy Cyber Security Division Director, Office of the Chief of Naval Operations (N2N6G)
To: Assistant Auditor General for Energy, Installations, and Environment Audits, Naval Audit Service

Subj: NAVY DATA STRATEGY DRAFT REPORT RESPONSE

Ref: (a) Naval Audit Service, Draft Audit Report 2016-091 of 4 Dec 17

1. Navy Cyber Security Division Director concurs with reference (a).

2. To ensure Department of the Navy (DoN) alignment, we are working closely with the DoN Chief Information Officer (CIO) and other stakeholders to define the scope of work and spiral-development timeline over the next 18-month, with a targeted completion date of 30 August 2019. In order to ensure full Naval Audit Service insight on addressing recommendations, DoN CIO and Navy Cyber Security Division Director will provide a coordinated status update of progress toward addressing Audit recommendations every 90 days from date of formal issuance of the audit report.

3. In the near term, we are leveraging existing Department of Defense instructions and industry standards to create an overarching Navy Data Integration Framework to guide on-going data integration and interoperability efforts. Please let me know if you have questions or concerns.

4. My point of contact for any questions is [redacted], [redacted], [redacted], [redacted]

FOIA (b)(6)

D. M. BARRETT

Contacting the Naval Audit Service About Final Report N2018-0021

(Project Number 2016-091)

Addressees for this Report:

Action Addressees:
Office of the Chief of Naval Operations
Department of the Navy Chief Information Officer
Department of the Navy Deputy Chief Information Officer (Navy)

Copy to (Information) Addressees:
UNSECNAV
DCMO
OGC
ASSTSECNAV FMC
ASSTSECNAV FMC (FMO)
ASSTSECNAV EIE
ASSTSECNAV MRA
ASSTSECNAV RDA
CNO (VCNO, N40, N41)
CMC (DMCS, ACMC)
NAVINSGEN (NAVIG-14)
AFAA/DO
NAVAIR

Actions planned by Department of the Navy Chief Information Officer, Department of the Navy Deputy Chief Information Officer, and Navy Cyber Security Division Director, Office of the Chief of Naval Operations (N2N6G) meet the intent of Recommendations 1 and 2. Recommendation 1 is considered closed for Department of the Navy Chief Information Officer. Recommendations 1 and 2 are considered open for Department of the Navy Deputy Chief Information Officer (Navy) pending completion of the planned corrective actions, and are subject to monitoring in accordance with reference (b). Management should provide a written status report on the open recommendations within 30 days after target completion date. Because the target completion date is more than 1 year in the future, we are establishing an interim reporting date of 8 August 2018; we request that the command provide us with an update on the corrective actions at that time.

Please provide all correspondence to the Assistant Auditor General, Energy, Installations, and Environment Audits, Ronnie J. Booth, [redacted], with copies to the Director of Policy, Oversight, and Information Technology, [redacted]; and the Naval Audit Service Followup Coordinator, [redacted]. Please submit correspondence in electronic format (Microsoft Word or Adobe Acrobat file), and ensure that it is on letterhead and includes a scanned signature.

FOIA (b)(6)

Obtaining Additional Copies

To obtain additional copies of this report, please use the following contact information:

E-mail: NAVAUDSVC.FOIA@navy.mil
Mail: Naval Audit Service
Attn: FOIA
1006 Beatty Place SE
Washington Navy Yard DC 20374-5005

Providing Suggestions for Future Audits

To suggest ideas for or to request future audits, please use the following contact information:

E-mail: NAVAUDSVC.AuditPlan@navy.mil
Mail: Naval Audit Service
Attn: Audit Requests
1006 Beatty Place SE
Washington Navy Yard DC 20374-5005

Naval Audit Service Web Site

To find out more about the Naval Audit Service, including general background, and guidance on what clients can expect when they become involved in research or an audit, visit our Web site at:

http://www.secnav.navy.mil/navaudsvc

Report Front Cover Photograph: *140604-N-CS953-004 WASHINGTON (June 4, 2014) A sea of white uniforms greets visitors to the Navy Memorial in Washington, DC as Sailors gather to celebrate the 72nd anniversary of the Battle of Midway. The celebration held host to Marines, Navy, and Coast Guard service members, Midway veterans and a gathered crowd of onlookers. The Battle of Midway is considered by many to be the turning point of the Pacific theater of World War II and one of the most well-known and revered victories in naval history. (U.S. Navy photo by Mass Communication Specialist 1st Class Tim Comerford/Released)*

Use this page as

BACK COVER

for printed copies

of this document