

|                           |     |
|---------------------------|-----|
| Updated Compliance        | P.1 |
| What's New?               | P.2 |
| IT Areas of Interest      | P.3 |
| Consolidating Datacenters | P.5 |
| GSA Cloud Orders          | P.5 |
| Eye on IT                 | P.5 |
| Data Spotlight            | P.5 |
| Network Contract          | P.6 |
| Extra Bytes               | P.6 |
| IT Tips                   | P.6 |

## THIS MONTH IN TECHNOLOGY HISTORY

**1838** – Samuel Morse first successfully tests the electrical telegraph.

**1982** – Richard Skrenta writes the first PC virus code, which is 400 lines long and disguised as an Apple boot program called "Elk Cloner."

**1984** – The first Apple Macintosh computer goes on sale.



## THIS MONTH IN BUSINESS HISTORY

**1881** – Thomas Edison and Alexander Graham Bell form the Oriental Telephone Company.

**1888** – The National Geographic Society is founded in Washington D.C.

**1930** – 3M begins to market "Scotch Tape."

**1957** - U.S. inventor Walter Morrison sells the rights to his flying disc to the Wham-O toy company, who later rename it the "Frisbee."

## Updated Compliance Requirements

### *DON CIO Info Alert*

#### **As NGEN Contract Competition Wages, NMCI Holds Down the Fort**

The transition from NMCI represents the continuous evolution of the DON's enterprise networks. NMCI, in place since 2000, is the largest corporate intranet on the planet, utilizing 384,000 workstations at more than 3,000 locations and representing about 70 percent of all DON IT operations.

*For details about the DON IM/IT Excellence Awards, visit:*  
<http://www.doncio.navy.mil/ContentView.aspx?ID=3229>

### *DON CIO Info Alert*

#### **Master's & Doctorate Level Scholarships Available to DON Personnel**

Scholarships are being offered for Department of the Navy civilian and military personnel through the DoD Information Assurance Scholarship Program (IASP) to meet the increasing demand for cyber/information technology professionals with a cybersecurity/information assurance (CS/IA) focus. These scholarships for master's and doctorate level work cover the cost of tuition, fees and books.

*For details visit:*  
<http://www.doncio.navy.mil/ContentView.aspx?id=535>

### *NAVADMIN 346/11*

#### **IT Procurement Approval and Oversight Authority**

This NAVADMIN (152325Z November 2011) establishes policy for a single IT procurement approval process, under the centralized management of SPAWAR, effective 01 December 2011. The policy requires the use of an Information Technology Procurement Request (ITPR) Smart Form for all IT procurements.

*For details visit:*  
<http://www.public.navy.mil/bupers-npc/reference/messages/Documents/NAVADMINS/NAV2011/NAV11346.txt>

### *DON Moving Toward Greater Efficiencies through Data and IT Consolidation*

The Department of the Navy has a long history of effective information technology solutions that provide the highest level of service and security while being conscious of limited resources. Facing an increasingly resource-constrained future, this commitment to maximizing DON IT support using the most innovative, efficient and effective means will continue.

*For details visit:*  
<http://www.doncio.navy.mil/ContentView.aspx?ID=3508>

### *DON CIO Info Alert*

#### **Department of the Navy in Good Company in IT Efficiencies Way Ahead**

As the quest for cost saving efficiencies rages on, three government officials spoke about the challenges their organizations are facing and their plans to tackle them at the Fifth Annual C5ISR Government and Industry Partnership Conference held recently in Charleston, SC. They described the steps their organizations are taking to deal with the challenges of finding efficiencies and responding to budget cuts.

*For details visit:*  
<http://www.doncio.navy.mil/ContentView.aspx?ID=3288>

### *DON Information Technology Policy Guidance for Fiscal Year 2012*

Since its inception, the focus of the Department of the Navy Information Technology Policy Guidance has been on enabling knowledge dominance by directing that our information management/information technology spending support the creation of a joint, net-centric naval networking environment. The net-centric vision remains a goal, but cutting the Department's IT spending is the priority for 2012.

*For details visit:*  
<http://www.doncio.navy.mil/PolicyView.aspx?ID=3543>

## What's New?

### **Message from the DON CIO:**

This year, the Department of the Navy will build on the efforts of 2011 as we continue on our difficult but necessary journey to transform the way the department manages its business information technology. Finding ways to become more effective in how we acquire and operate IT will lead to decreased costs and ensure we hit the target of reducing the IT budget by 25 percent by 2017.

There is no question that this is a monumental task in an agency as big as the Department of the Navy with more than 800,000 personnel around the world. But the good news is we have already made great strides finding efficiencies and reducing costs by consolidating data centers (see "Consolidating Data Centers Key to Cutting IT Spending"), streamlining processes (see related memos at [www.doncio.navy.mil/efficiencies](http://www.doncio.navy.mil/efficiencies)), "killing" obsolete applications, optimizing systems, leveraging enterprise contracts (see "New DON Mobile Contracts and Tools Drive Savings"), and acting in a more centralized manner. Additionally, stringent approval processes have been put in place to achieve better visibility and to control spending. As a result, we have gained a lot of knowledge about the information technology environment and the true cost of IT.

**To view more, visit:**  
<http://www.doncio.navy.mil/ContentView.aspx?ID=3581>

### **Negotiating Contracts for Cloud-Based Software**

The federal government's "cloud first" policy, as part of the Federal Chief Information Officer's "25 Point Implementation Plan to Reform Federal Information Technology Management," requires federal agencies to consider cloud computing before making new IT investments and to move at least three applications to the cloud by May 2012.

Requests for information, issued by the Department of the Navy in July 2011, indicated that the Next Generation Enterprise Network (NGEN) will transition to a cloud-based delivery model. In an August 2011 media roundtable, the Department of the Navy CIO, Mr. Terry Halvorsen, said cloud computing, along with thin-client and zero-client technologies, are some of the models that the DON can use to cut 25 percent from its business IT budget in the Future Years Defense Program financial plan.

**To view more, visit:**  
<http://www.doncio.navy.mil/ContentView.aspx?ID=3585>



### **Ensuring Spectrum-Dependent Systems are "Up to Code" Saving Time, Money**

To achieve the most efficient use of communications-electronics (C-E) resources, the required capabilities of systems and equipment should be met during the procurement phase — rather than investing in equipment that may require redesign or retrofitting after development. Therefore, it is more critical than ever in these budget constrained times that program offices and procuring officials take advantage of processes that ensure systems and equipment provide their intended capabilities with minimal rework.

The use of electromagnetic spectrum, or radio frequencies, is a common wireless enabler for many, if not most, new C-E systems. The proliferation of wireless spectrum use within the Department of the Navy continues to increase. As a result, access to electromagnetic spectrum for all wireless systems is no longer ensured.

The electromagnetic spectrum is a scarce and highly regulated resource used around the world. Ensuring spectrum support for DON systems is a critical and necessary requirement that must be initiated during procurement and in the earliest stages of system development. Systems must be designed to operate in the proper spectrum, or they may interfere with other systems or violate international treaties and regulations. Retrofitting systems to bring them into compliance with regulations is often much more expensive than properly designing them from the beginning.

**To view more, visit:**

<http://www.doncio.navy.mil/ContentView.aspx?ID=3586>

# Information Technology Areas of Interest

## Portfolio Management

The Annual Reviews for Non-Tier Defense Business Systems to include BMA and EIEMA systems will commence on 01 February 2012 and are due for completion no later than 15 May 2012. The WMA (WARFIGHTER) and DIMA (Intelligence) system review will commence on 21 May 2012 and are due for completion no later than Aug 30 2012. Although the WMA and DIMA review starts later than the BMA and EIEMA if feasible recommend start system review activities soonest but they will not be officially monitored and tracked until 21 May 2012 start date.

All TIER 1 - 4 Defense Business Systems will not be included in the FY12 annual system review just like in the past but they will continue to be reviewed on their Investment Review Board/Certification review schedule.

Concurrent with Non-Tier system reviews the DON Enterprise Architecture Compliance: Pursuant to DON Policy Memorandum of 31 July 2009: Release of the Department of the Navy Enterprise Architecture version 2.1000 (available at <https://www.intelink.gov/wiki/DONEA>), all entities registered in DITPR-DON including, National Security Systems (NSS), will be assessed annually to compliance with the DON Enterprise Architecture (DON EA).

## Architecture

DoD historically spends more than \$6.0B annually developing and maintaining a portfolio of more than 2,000 business systems and Web services. Many of these systems, and the underlying processes they support are poorly integrated. They often deliver redundant capabilities that optimize a single business process with little consideration to the overall business enterprise. It is imperative, especially in today's limited budget environment, to optimize our business processes and the systems that support them to reduce our annual business systems spending.

The Defense Business System Management Committee (DBSMC) embraced the E2E business lifecycle model as a viewpoint to frame and understand our business environment. Further, DBSMC endorsed using and extending the E2E framework to evolve the Business Enterprise Architecture (BEA) within the context of the DoD Enterprise Architecture. This essential framework will be used by the DBSMC and the supporting Investment Review Board (IRB) process to guide and constrain business system investments and conduct business process reengineering determinations as required by statute.

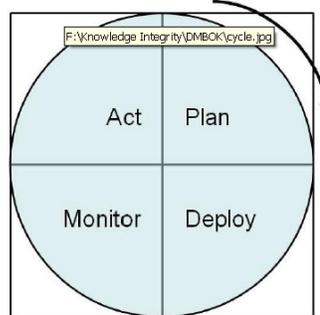
The next version of the Business Enterprise Architecture (BEA 9.0) is scheduled for release in March 2012. In accordance with the 4 April 2011 memo from the DoD Deputy Chief Management Officer (DCMO), in addition to being aligned to the DoD Architecture Framework (DoDAF, currently version 2.0), future BEAs will be described in an ontology using the World-Wide Web Consortium (W3C) open standards Resource Description Framework (RDF)/Web Ontology Language (OWL) and use Business Process Modeling Notation (BPMN) 2.0 Analytic Conformance Class (Primitives) as its modeling language. Architectures wishing to federate with the BEA (including the BUPERS Enterprise Architecture) will be required to do so via an ontology. BEA 10.0 will be the first architecture to be described entirely as an ontology.

The use of ontologies makes it much easier to relate different architectures, and facilitates systematic queries of those relationships. For more information on semantic technology and ontologies, online training is available at the BEA website: <http://www.bta.mil/products/training/SemanticWeb/index.html>

## Data Management

### Data Quality Management

The following figure, based on the Deming<sup>1</sup> model known as "plan-do-check-act", depicts the general approach to Data Quality Management:



**Plan:** Assessing current data quality state and identifying key metrics

**Deploy:** Profiling the data and identifying data issues

**Monitor:** Monitoring and measuring data quality in relation to defined business rules

**Act:** Taking action to resolve data quality issues

*The content of this article was derived from the Data Management Association (DAMA) Data Management Body of Knowledge (DMBOK)*

*The Enterprise copy of the DAMA DMBOK is located on the Enterprise Information Management (EIM) portal on DKO:  
<https://www.us.army.mil/suite/files/23278192>*

*Note: you must have an AKO/DKO account  
To request access, please send an e-mail to: [MPTE\\_EIM@navy.mil](mailto:MPTE_EIM@navy.mil)*

<sup>1</sup>Deming, W. Edwards

## ***Information Assurance***

With TAX season under way, the influx of emails that come in at work and home increase, with more vengeance from years prior. Spammers and Phishers are professionals. They want your data, and they don't care how they get it. The NMCI Email servers block nearly 98% of the SPAM/PHISHING that come our way (often, SPEAR-PHISHING) that target military audience. We are talking millions of emails. Some do make their way through. Alertness at staff and some of our IAM's across the force have bought to my attention some pretty "tempting" emails disguised as banks, department stores, and we still have our friends in "Nicaragua" who are convincing us to send them money so they can send you our "millions."

1) Do NOT CLICK on any emails containing attachments or links, that come in at work, unless they contain a digital signatures. This provides authentication and integrity. (DOD IA training requirements annotate this).

a. The term "CLICKER" is a new term referring to employees that "click" on email links or attachments when they come in and are not verified. Many corporations are implementing "phishing schemes" internally to determine who are the "clickers". (<http://phishme.com/index.php>).

2) Our DOD contractors have NMCI accounts and/or an External Certification Authority (ECA) such as VeriSign and should be conducting official correspondence via a digital certificates from their NMCI or CTR account with the ECA signature. If not, have them re-send, and contact your Command IAM.

3) Review the attached on how to report suspected SPAM/PHISHING. Store for your future reference Do not forward via any other methods. This increases the risk for possible "cyber attacks and/or virus/malware/spyware.

4) Continue being aware of suspicious emails.

5) If an email comes to you with a threat or act of violence against you or family, contact your IAM and/or SECMGR immediately. Threats against the military or anyone is serious.

Closing:

1) Phishing/Scams aren't just related to work email. Be aware at home, and teach your kids and family members about phishing.

2) Assure your computers at home are protected, limited Admin rights, and have current Antivirus software and/or malware protection installed.

3) Be extra careful on Social Networking Sites- (Facebook, MySpace, etc). With Facebook looking at going Public, there will be more Advertisements, More Applications (Apps) which may lead to possible vulnerabilities.

Feel free to contact me or your Command IAM. When in doubt, stay out! (don't click).

### **SPAM/PHISHING Email/POOW Note:**

Spam is unsolicited advertisements sent to an e-mail address. Phishing is a request for personal information disguised as an advertisement, official-looking e-mail, or Web site. The Exchange servers have anti-spam filters to keep spam and phishing to a minimum. When you receive a spam or suspected phishing message, create a new message or forward the entire message, including the original header information, for investigation and to effectively block future messages from the sender.

The current process for reporting spam on NMCI is outlined in the following article on homeport:

<https://www.homeport.navy.mil/support/articles/report-spam-phishing/>

NMCI spam mailbox (nmci\_spam@nmci-isf.com) was designed to specifically address spam and/or phishing emails on NMCI. Please continue to report any spam messages you receive in your inbox within 24 hours of receiving it to this email address (NMCI\_SPAM@NMCI-ISf.com).

## Consolidating Data Centers Key to Cutting IT Spending

To continue supporting the operational forces stationed around the world, protecting the nation and providing humanitarian assistance during these fiscally constrained times, the Department of the Navy is seeking opportunities to increase IT efficiencies while cutting business spending. A primary focus of this effort is data center consolidation, which is essential to reducing the IT budget by 25 percent during the next five years.

To date, there are approximately 150 DON data centers that support delivery of computing capabilities to users. Over the years, the proliferation of Navy and Marine Corps data centers has led to a complex, duplicative and costly network structure.

The goal of the department's data center consolidation initiative is to virtualize and reduce the number of software applications used and select a small number of enterprise data centers for retention and close the remainder. Consolidation of the data centers and reducing the number of applications department-wide will reduce network complexity and the overall cost of purchasing, manpower support, testing, certification, operation and maintenance, while meeting security and operational requirements. Efficiencies are gained by consistently delivering common computing capabilities as services to users.

One such enterprise data center that will be retained is the Space and Naval Warfare (SPAWAR) Systems Center Atlantic data center, which opened this past fall on Joint Base Charleston-Weapons Station.

**To view more, visit:**  
<http://www.doncio.navy.mil/ContentView.aspx?ID=3583>

## GSA Hands Agencies Cloud Security Marching Orders

The General Services Administration released marching orders for a new cloud certification program.

The 47-page "concept of operations" is intended to offer federal agencies and their contractors step-by-step instructions for proceeding with the mandatory authorizations that are slated to start in June.

The Federal Risk and Authorization Management Program, or FedRAMP, is envisioned as a sort of factory line for approving a particular Web-based service once so that any agency can almost immediately adopt it. Certain products will get to be the first in line, according to the document. They include "infrastructure as a service" tools that provide remote storage and networking, email, and other common collaboration applications. Government approved, independent auditors then will evaluate each product's compliance with about 300 controls, such as backup storage requirements.

The new policy fleshes out the role of the Homeland Security Department in the operation. DHS officials will coordinate recovery in the event of an intrusion and develop standards for real-time monitoring of threats, the concept stated.

Agencies, cloud suppliers and auditors recently received from GSA a list of standard protections each service must offer, as well as a memo generalizing the responsibilities of each player.

**To view more, visit:**  
[http://www.nextgov.com/nextgov/n\\_g\\_20120207\\_3832.php?oref=rss](http://www.nextgov.com/nextgov/n_g_20120207_3832.php?oref=rss)

*\*Source: Nextgov website*

## EYE ON IT

### *Pinterest of Interest, But Feds Not Yet Sold On It*

The Pinterest social media service is rapidly gaining in popularity on the Web, and federal agencies are starting to take notice.

**Read the article here:**

<http://fcw.com/articles/2012/02/06/pinterest-generating-feds-interest-but-not-yet-a-groundswell.aspx>



## DATA SPOTLIGHT

Data Management Association (DAMA) defines data governance as:

*The exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets.*

### **What are the goals of data governance?**

- To define, approve, and communicate data strategies, policies, standards, architecture, procedures, and metrics.
- To track and enforce regulatory compliance and conformance to data policies, standards, architecture, and procedures.
- To sponsor, track and oversee the delivery of data management projects and services.
- To manage and resolve data related issues.

To understand and promote the value of data assets.

The content of this article was derived from the Data Management Association (DAMA) Data Management Body of Knowledge (DMBOK)

The Enterprise copy of the DAMA DMBOK is located on the Enterprise Information Management (EIM) portal on DKO: <https://www.us.army.mil/suite/files/23278192>

Note: you must have an AKO/DKO account  
To request access, please send an e-mail to:  
MPTE\_EIM@navy.mil

## EXTRA BYTES

### 5 Technologies on the Way Out in 2012

The technology landscape is changing, with government moving increasingly toward new-school technologies, such as mobile and cloud computing, while cybersecurity concerns rise and budgets shrink.

Read the article here:

<http://gcn.com/articles/2012/01/26/agg-5-technologies-on-the-way-out-in-2012.aspx>



### New Sykipot Variant Can Steal PINs from DOD Smart Cards

A newly discovered variant of the Sykipot Trojan, which has been used for years in attacks originating from servers in China, can be used to compromise the Defense Department's Common Access Cards, according to research by Alienvault Labs.

The variant, which Alienvault says appears to have been around since March 2011, arrives via phishing attacks and uses a keylogger to effectively hijack DoD and Windows smart cards.

Read the article here:

<http://gcn.com/articles/2012/01/13/sykipot-trojan-targets-dod-cac-cards.aspx>

### Northrup Grumman snags \$638 Million Navy Network Contract

The Navy late Wednesday awarded Northrup Grumman Corp. a contract potentially worth \$637.8 million to provide Navy ships with a networked common computing environment.

The Space and Naval Warfare Systems Command awarded Lockheed Martin Corp. and Northrup Grumman prototype contracts for the Consolidated Afloat Networks and Enterprise Services program in March 2010 and Capt. D.J. LeGoff, the CANES program manager, said last week this award represents "a down select to a design, not a vendor."

The Navy will own that design, LeGoff said at a press briefing last week at the Armed Forces Communications and Electronics Association conference in San Diego. He added SPAWAR intends to hold continuous competitions based on that design every two years until all 285 ships and submarines are equipped with the network.

CANES includes servers, computer terminals and software based on commercial standards. SPAWAR plans to award a follow-on CANES contract in the third quarter of fiscal 2013, he said.

The awarded contract will cover installation of CANES on 54 ships, according to LeGoff, with 2,400 computer terminals installed on aircraft carriers, 200 on destroyers and 500 on amphibious ships, which carry Marines. The amphibious ships will have network connections for computers the Marines bring onboard, he added.

CANES will replace decades old shipboard systems installed in an ad hoc fashion over a decade and LeGoff conceded he did not have a good handle on the network infrastructure afloat today. "There's no way we can manage bits and pieces from everyone," he said.

To view more, visit:

[http://www.nextgov.com/nextgov/ng\\_20120201\\_5077.php?oref=rss](http://www.nextgov.com/nextgov/ng_20120201_5077.php?oref=rss)

### DISA Office to Manage Online App Store

The Defense Information Systems Agency has opened a program office that will focus on managing Defense Department mobile devices and the applications that run on them.

The new agency will also run an online store providing DoD users with applications and mobile device management (MDM) services.

"It will be a cross-agency effort that ties in what we're doing on the network side as well as what we're doing on the applications side," said David Bennett, DISA's acting component acquisition executive, who spoke Jan. 24 at the IDGA Network Enabled Operations conference in Alexandria, VA.

To view more, visit:

<http://gcn.com/articles/2012/01/27/disa-launches-program-office-to-manage-mobile-devices.aspx>

## Bi-Monthly IT Tips

### Add a Watermark to a Photo Using Microsoft PowerPoint

Adding a watermark to a photograph by using PowerPoint involves three main tasks: Adding the watermark, formatting it so that it looks transparent, and then grouping and saving the photograph.

<http://office.microsoft.com/en-us/powerpoint-help/add-a-watermark-to-a-photo-with-powerpoint-HA101886853.aspx?CTT=1>

### Create an Easily Customizable Template in Word 2010

This video provides a quick overview of how to create, modify, and save templates in Word 2010. A template is a Microsoft Office document that's been designed with pre-existing themes, styles, and layouts, which has placeholder information instead of real content.

<http://office.microsoft.com/en-us/word-help/video-create-an-easily-customizable-template-in-word-2010-VA101982010.aspx?CTT=1>