

Byte Newsletter presented by the BUPERS Information Management Office

Editor: [christopher.sgouros@navy.mil](mailto:christopher.sgouros@navy.mil)

***In this issue:***

Updated Compliance	P.1
What's New?	P.2
IT Areas of Interest	P.3
Cyber Rules Unfinished	P.5
Google Data Secrets	P.5
Eye On IT	P.5
Extra Bytes	P.6
PII Faxed Errantly	P.6

## THIS MONTH IN TECHNOLOGY HISTORY

**1936** – RCA displays first television to press.

**1870** - In the United States, the Weather Bureau (later renamed the National Weather Service) makes its first official meteorological forecast.

**1969** – The first-ever computer-to-computer link is established on ARPANET, the precursor to the Internet.



## THIS MONTH IN BUSINESS HISTORY

**1824** – New York's Fifth Avenue first opens for business.

**1879** - James Ritty, a saloonkeeper and inventor patented the world's first cash register as "Ritty's Incorruptible Cashier."

**1895** – George B. Selden was granted the first U.S. patent for an automobile.

## Updated Compliance Requirements

### ***2012 Annual Records Management Refresher Training***

**DTG 181837Z OCT 12**

This Naval message states that in addition to the basic records management (RM) training requirement, all DON personnel must be reminded, every year, of their RM responsibilities and that this refresher training is mandatory.

**For details visit:**

<http://www.doncio.navy.mil/ContentView.aspx?id=1884>

### ***Release of DON Enterprise Architecture Version 4.0.000***

The purpose of this memo is to announce the release of the Department of the Navy Enterprise Architecture (DON EA) v4.0.000, which updates DON EA v3.1.000. The assessment of compliance with DON EA for FY13 will begin on 1 October 2012. DON Business Mission Area (BMA) investments will be required to complete their program's self-assessment with the DON EA and DoD Business Enterprise Architecture (BEA) version 9.0 no later than 1 February 2013.

**For details visit:**

<http://www.doncio.navy.mil/ContentView.aspx?id=4175>

### ***DON IM, IT, and Cyberspace Performance Measures***

The purpose of this memo is to establish performance measures and their associated reporting requirements in order to assess progress in achieving business information technology transformation.

These measures may be updated in the future to reflect improved reporting/analysis, incorporate feedback, or to respond to changing mission and fiscal requirements.

**For details visit:**

<http://www.doncio.navy.mil/ContentView.aspx?id=4218>

### ***DON CIO Info Alert***

#### **DON Prepares for Audit Readiness**

The first Department of the Navy audit readiness video has been released. Audit readiness is for everyone, not just government financial types. The DON has a requirement to produce certified financial statements by 2017. To attain that goal we must be audit ready. Are you audit ready?.

**For details visit:**

<http://www.doncio.navy.mil/ContentView.aspx?id=4160>

### ***Achieving Measurable Efficiencies Through Data Center Consolidation, System, and Application Rationalization Guidance***

This memo provides details on how the Department of the Navy must engage in the immediate strategic transformation of information technology in business systems, applications, and processes within programs of record and functional area portfolios. It includes applications, networks, and systems classified as Mission Assurance Category II and III, and DON data centers, currently operating on any ashore network.

**For details visit:**

<http://www.doncio.navy.mil/ContentView.aspx?id=4163>

### ***DON CIO Info Alert***

#### **DON to Further Transform Business IT Processes Through Application Rationalization**

This memo provides details on the steps the DON must take to achieve budget savings through application rationalization while ensuring mission needs are met. The scope of the memo includes applications, networks, and systems classified as Mission Assurance Category II and III, and DON data centers ashore.

**For details visit:**

<http://www.doncio.navy.mil/ContentView.aspx?id=4164>

## What's New?

### ***DON Revises Fax Policy on Transmitting PII***

The Feb. 2012 message, Department of the Navy Social Security Number (SSN) Reduction Plan Phase Three, prohibited the faxing of SSNs and other personally identifiable information (PII) in all but a few special cases. Since its release, many processes that require the faxing of PII, specifically the SSN, have been identified. To ensure that business processes continue uninterrupted to the maximum extent possible, the policy has been revised and new policy released.

The new fax policy states, that effective immediately, the use of fax machines to send information containing SSN and other PII by DON personnel is prohibited except under the following circumstances:

- When another more secure means of transmitting PII is not practical.
- When a process outside of DON control requires faxing to activities such as the Defense Finance and Accounting Service (DFAS), Tricare, Defense Manpower Data Center (DMDC), etc.
- In cases where operational necessity requires expeditious handling.
- When faxing PII related to internal government operations only, i.e., office phone number, rank, job title, etc.

**To view more, visit:**

[http://www.doncio.navy.mil/ContentView.aspx?id=4270](http://www.doncio.navy.mil/ContentView.iew.aspx?id=4270)

### ***Message From the DON CIO***

#### ***Building a Strong Foundation for Future Success***

"We can't solve problems by using the same kind of thinking we used when we created them." Albert Einstein said these words two generations ago, and yet they ring even more true today. But, we must not stop there. While it is vital that we use current solutions, best practices and technologies to enable our immediate success, we must also maintain a steadfast eye on the horizon for future requirements, industry trends and threats. Only by balancing the requirements of the present and possibilities of the future, will we become an efficient, effective and forward-looking organization that is positioned for long-term success.

Today's information technology environment is moving at a pace and complexity where data is driving business. Rapid advancements and increased interconnections enable access to information from both desktop and mobile devices. Effective decision making demands an increased focus on understanding and managing vital data to extract meaningful information that will enable intelligent, fact-based decision making to guide the DON in meeting future challenges.

**To view more, visit:**

<http://www.doncio.navy.mil/chips/ArticleDetails.aspx?SectionID=425&IsueID=52>

### ***DON Policies Set Stage for Future IT Efficiencies***

During the past two years, the Department of the Navy laid the groundwork for information technology efficiencies that will enable business operations to better support the department's warfighting and humanitarian missions. In support of the IT efficiencies effort, there were several foundational policies issued that were designed to clarify the DON's goals and prepare for a more streamlined and efficient future. The DON is approaching these efforts from an enterprise-wide perspective with many of the policies signed by leadership from across the department's business operations.

The following is a list of some key policies released during fiscal years 2011 and 2012.

UNDER SECRETARY'S DIRECTION TO DON CIO REGARDING AN EFFICIENCY AND EFFECTIVENESS REVIEW OF IT SYSTEMS: Department of the Navy (DON) Information Technology (IT)/Cyberspace Efficiency Initiatives and Realignment (Dec. 3, 2010) ([www.doncio.navy.mil/ContentView.aspx?id=2061](http://www.doncio.navy.mil/ContentView.aspx?id=2061)) directed the DON Chief Information Officer (CIO) to lead the efficiencies efforts surrounding DON IT procurement and business processes and to define a department strategy to shape the way forward in the information management (IM), IT and cyberspace (excluding intel, attack and exploit), and Information Resource Management (IRM) domains.

**To view more, visit:**

<http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=4226>



# Information Technology Areas of Interest

## Architecture

Modeling your business processes can help your organization improve its efficiency! By documenting your processes through Business Process Modeling (BPM), your organization can easily see the steps and decisions involved in a business process, identify redundant or unnecessary steps, and modify the process to make it more efficient. An example: PERS-97 recently modeled their Career Transition processes for both officers and enlisted personnel. In one of their processes, by making a simple change to the place in the process where a document was created, they were able to eliminate three unnecessary steps; the rest of the processes are under review to identify other efficiencies.

Contact the enterprise architect at [MPTE\\_EA@navy.mil](mailto:MPTE_EA@navy.mil) or business process modeling/improvement team for your Echelon II command for more information on how to document and analyze your business processes.

## Data Management

### Managing Information as an Enterprise Asset

In a knowledge economy, information is one of the most valued enterprise assets. In a transformation economy, proper governance of information becomes a critical success factor. Data and information will outlast applications requiring the management of data and knowledge assets through time as applications, and even business processes change.

Data Governance is essential to ensuring that data is accurate, appropriately shared, and protected. Data is rationalized to create information. Information is rationalized to create knowledge. And knowledge is the basis for wisdom, supplemented by intuition, in decision making. The quality of data and information will certainly impact the quality of the decisions that consume it. However, it can't be assumed that decision making rationale will necessarily make the best use of such information or the best or most appropriate decisions or choose the best course of action. The subject of decision making and decision theory is outside the scope of this report. Nevertheless, positive citizen outcomes are the ultimate objective and this requires government to properly manage data, information and knowledge assets, and to use and manage these assets with the utmost wisdom.

<http://www.nascio.org/publications/documents/NASCIO-DataGovernance-Part1.pdf>

Contact BUPERS Data Management at:  
[MPTE\\_EIM@navy.mil](mailto:MPTE_EIM@navy.mil)

## Information Assurance

### Protecting You Privacy:

With social media, online financial transaction, e-mail and the ease of online shopping, computer user are able to accomplish quite a bit in little time. There are many reasons to be cautious about online personal information. You should be most concerned with keeping personal information from Cybercriminals and Identity thieves. Here are some ways to keep your private information from prying eyes.

Be Anonymous: It is east to give too much personal information online making the work of cybercriminals easier. To protect your online anonymity:

- \* Disclose personal information only when absolutely necessary.
- \* Be cautious of fast friends you have just met online who ask you to reveal personal information
- \* Be cautious of social networking friends you have not seen or heard from in years.
- \* Use a disposable, anonymous e-mail account for websites that require an e-mail to register.

Watch out for Cookies: Cookies are files that websites use to share information about your browsing habits. Most of the time, these files are harmless. For example, a cookie may remember your username and password so you don't have to log in to a website every time you visit. However, some cookies are used to maliciously to track your browsing habits to build a profile of your interests and activities.

Set your browser to warn you when a cookie is installed. Use anti-spyware software that removes tracker cookies. Both Symantec and MacAfee suites offer this capability.

Opt to use a plain text e-mail display instead of HTML e-mail. This way, tracking files and cookies cannot be included in e-mails.

Assume anything sent without encryption can be read by third parties. Always use encryption when sending e-mail containing sensitive information. Never use a work e-mail address for personal use. Have a private e-mail address for private business.

Be extremely careful when using public computers and public wireless networking hotspots as they are more susceptible to malicious behavior.

Contact BUPERS Information Assurance at:  
[BUPERS\\_IA\\_TEAM@navy.mil](mailto:BUPERS_IA_TEAM@navy.mil)

## Portfolio Management

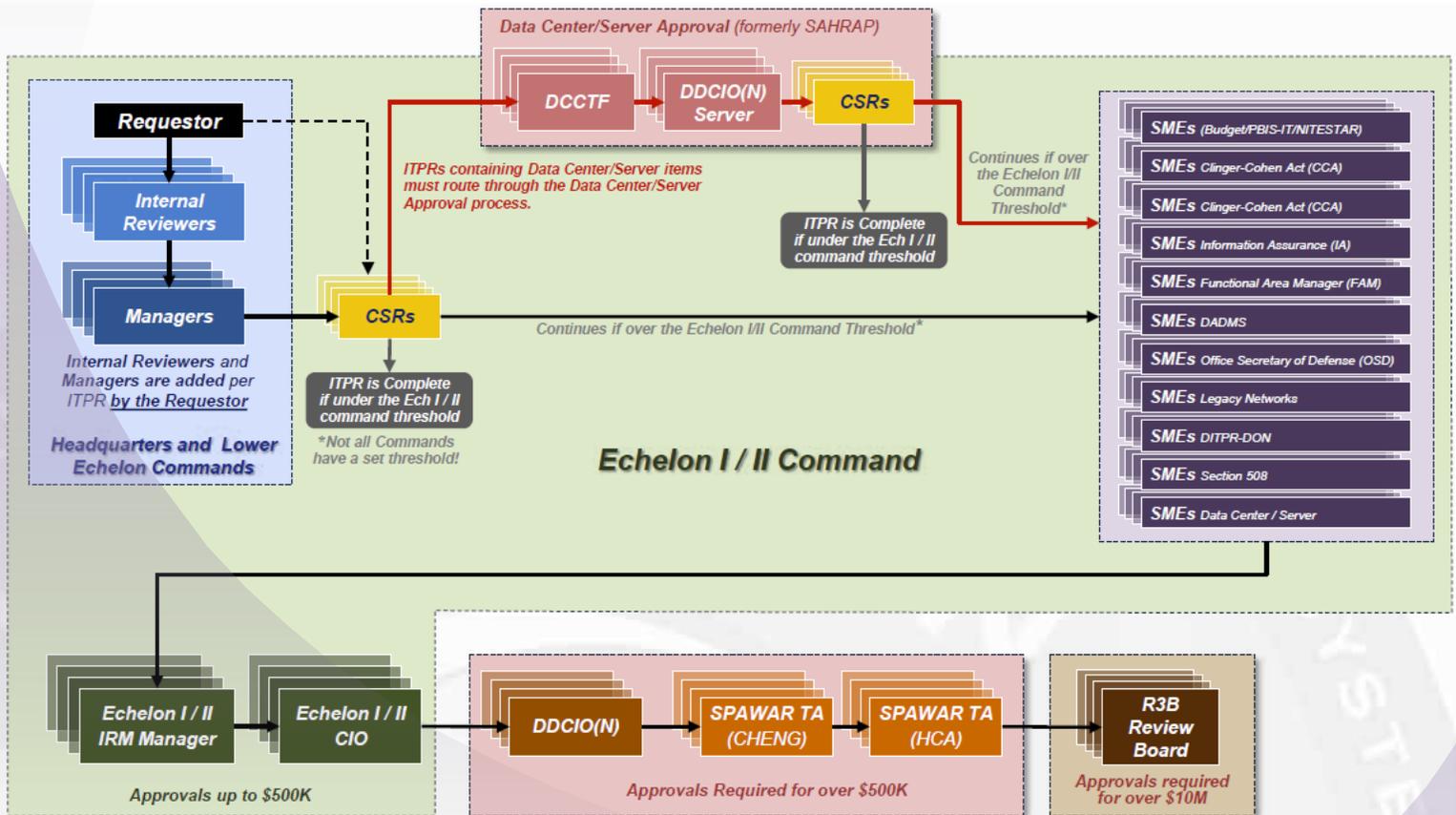
### Basic Navy Information Dominance Approval System (NAV-IDAS) Workflow

This is a basic overview of the NAV-IDAS workflow process. All Echelon I/II Commands have the option of instituting internal Business Rules in regards to policy, processing and information captured outside of the Enterprise-wide required information included and marked within the application. All items that are marked as "Return for Recommendations" by DCCTF, DDCIO(N) Server, SMEs, IRM, Ech I/II CIO, DDCIO(N), SPAWAR TA and R3B will be returned directly to the CSRs for mitigation. If the CSR needs additional edits made by the Submitter, the CSR will "Return with Recommendations" to the submitter for changes and then Submitter will make said changes, resubmit back to the CSR who will then review before approving it to go back to original person who returned the ITPR. Anyone who "Returns" an ITPR for recommended changes MUST review it again and approve it before it will move onto the next group in the approval process. This includes all users that are within the automated workflows as well as any Internal Reviewers, Managers and Ad Hoc users added by the submitter or any persons within the approval process. All

Echelon I/II commands have the authority (if they choose) to set their own Command dollar thresholds. These thresholds represent the dollar amount to which a Manager has final approval authority (some Commands have set the Ech I/II CSRs as an additional approval for all below threshold requests). Each Echelon I/II Command has the option to institute internal business rules and policies in regards to authorizing "Managers" in the NAV-IDAS system to have this approval capability.

To view Frequently Asked Questions, visit: <https://navidas.navy.mil/about.html#faqsContent>

Contact BUPERS Portfolio Management at: [BUPERS\\_PFM@navy.mil](mailto:BUPERS_PFM@navy.mil)



## Cyber Rules of Engagement Still Unfinished

For months, Defense Department officials have been at work establishing the rules of engagement that will govern military action in cyberspace.

Despite recent assurances of their imminence, those rules have yet to be finalized, and some say their absence could affect national security.

Defense Secretary Leon Panetta said in October that Pentagon leaders are close to finishing the rules of engagement, an official doctrine that will likely echo in structure the guidelines that regulate armed conflict. But will that be enough to address, on a national level, the constantly evolving landscape in cyberspace?

"The DOD rules of engagement are important, but there's an issue of whether or not that's suitable for era we're in," said Tim Sample, vice president and sector manager for special programs at Battelle. If the rules are modeled after the traditional rules and assumptions for conventional combat, that would be based on a 'faulty assumption,' he said. "It can be argued whether that's practical [to have] a traditional response to attacks in an era or environment that is by definition very untraditional."

**To view more, visit:**

<http://fcw.com/articles/2012/11/01/cyber-rules-of-engagement.aspx>

## What Agencies Can Learn From Google's Data Center Secrets

For years the federal government has been moving its data into bigger and bigger centers, consolidating servers in the name of efficiency and cost reduction. However, a recent report cast some doubt on whether large facilities were actually a model for efficiency, or simply a growing problem.

In the wake of that, Google, which maintains some of the largest data centers in the world, including many of those behind the often talked-about cloud, has pulled back the veil over how it cools and maintains its facilities. This had been a well-kept secret for a long time and is now revealed in stunning details and photos. It should give feds plenty to think about in terms of how to better maintain and design their own centers.

What Google has showed the world is unique in several ways. The server rooms themselves are rather austere in design, with almost everything being sacrificed in the name of efficiency. Google also is using water cooling more than probably anyone else in the world and is not afraid to put running water pipes directly over top of electronic equipment.

**Read more:**

<http://gcn.com/articles/2012/10/26/agencies-learn-from-google-data-center-secrets.aspx>

## EYE ON IT

### *Election's End Revives Hope for Cybersecurity Action*

For much of the past year, cybersecurity has itself been a battleground – subject to partisan tug-of-war and unsuccessful legislation on Capitol Hill, as well as the possibility of a White House executive order. Now, as Congress is expected to reconvene on Nov. 13 following President Barack Obama's re-election, there is cautious optimism in Washington that there may finally be decisive action.

**Read the article here:**

<http://fcw.com/articles/2012/11/08/cybersecurity-legislation.aspx>



### *5 Tech Priorities for the New Administration*

The Obama administration has made remarkable progress applying IT tools and practices to the problems of making government smarter, faster and cheaper. This has been especially true in its efforts on data center consolidation, the transition to cloud computing and using IT in the push for ever-more government information transparency. To maintain this record, here are five technologies the new administration should keep on the presidential blotter.

**Read the article here:**

<http://gcn.com/articles/2012/11/06/5-tech-priorities-for-the-new-administration.aspx>

## EXTRA BYTES

### Agency Data Centers Will Never Be The Same

Government data centers are entering a period of radical change, triggered by budget limitations, the growth of mobile devices, cloud services and federal mandates for system consolidation.

Read the article here:

<http://gcn.com/articles/2012/10/26/agency-data-centers-idc-report.aspx>



### Proactive, Continuous Monitoring Key to Thwarting Cyber Crime

Continuous monitoring is a critical but often misunderstood component at the epicenter of "proactive" cybersecurity. How do we prevent malicious threats from getting into an organization's network while allowing legitimate data to flow efficiently? How do we monitor data on our storage devices, the data at rest? How do we audit all the devices in our network and their unique configurations?

Read the article here:

<http://gcn.com/articles/2012/10/29/continuous-monitoring-epicenter-proactive-security.aspx>

## DoD Applies Tighter Scrutiny to Business IT Spending

Managers of business IT systems in the Defense Department will face some new hurdles in gaining funding for their projects — even for systems that have been up and running for years.

The changes are part of an overhaul Congress ordered the Pentagon to implement with regard to how it handles investment review boards, the internal overseers federal agencies use to greenlight spending for business IT systems. The biggest change is that the oversight mechanism will now look over both new and legacy IT systems. Virtually every system will get a once-over every year, even if money is only being spent to keep it up and running.

"The status quo can't afford to get a bye, particularly when times are tough," said Dave Wennergren, DoD's assistant deputy chief management officer. "In the IT budget for the Department of Defense, there's over \$7 billion worth of business systems spent every year. Seventy-five percent of that is on sustaining the legacy. Only 25 percent is about building the new. I think that's out of whack, and we aren't forcing ourselves to look at how we're going to spend money in the future. One of the powers of tough financial times is forcing that change in conversation. We have to be able to defend everything."

To view more, visit:

<http://www.federalnewsradio.com/394/3051486/DoD-applies-tighter-scrutiny-to-business-IT-spending>

## Medical Insurance Company Faxes Personal Information to Wrong Number for Three Years

The following is a recently reported personally identifiable information (PII) data breach involving a private medical insurance company that improperly handled PII. Incidents such as this will be reported in each edition of CHIPS to increase PII awareness. Names have been changed or omitted, but details are factual and based on reports sent to the Department of the Navy Chief Information Officer (DON CIO) Privacy Office.

### The Incident

The spouse of a non-appropriated fund (NAF) employee requested a waiver from a medical insurance company for medicine not carried in the Department of Defense formulary. When the spouse did not receive the waiver as expected, it was discovered that the waiver was sent to an incorrect fax number. The medical insurance company's pharmacy reviewer sent the information to a private business. The individual who received the fax stated that the private business had been mistakenly getting faxes from the medical insurance company for the past three years and had tried unsuccessfully to correct the problem. The individual said the faxed documents sometimes contained personal health information (PHI), as well as Social Security numbers (SSN) and other PII.

To view more, visit:

<http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?id=4193>

## Which Paper Shredder Should I Use?

The Department of the Navy Chief Information Officer Privacy Office receives frequent inquiries regarding paper shredding as a means of destroying unclassified documents containing personally identifiable information (PII).

Some commonly asked questions include:

- Which shredder should I purchase? Should I use a straight cut or cross cut shredder?
- What are the DON policy requirements? How small is small enough with regard to shredder residue? Where can I find a list of approved shredders?
- Can I use a shredder service?

To view more, visit: <http://www.doncio.navy.mil/ContentView.aspx?id=4246>