

THIS MONTH IN TECHNOLOGY HISTORY

1977 – The Apple II, one of the first personal computers, goes on sale.

1980 – Namco releases the highly influential arcade game *Pac-Man*.

2000 - President Bill Clinton announces that accurate GPS access would no longer be restricted to the United States military.



THIS MONTH IN BUSINESS HISTORY

1927 – The last Ford Model T rolls off the assembly line after a production run of 15,007,003 vehicles.

1980 – Cable News Network (CNN) begins broadcasting.

2009 - General Motors files for Chapter 11 bankruptcy. It is the fourth largest United States bankruptcy in history.

Updated Compliance Requirements

Social Security Number (SSN) Reduction

The Navy has provided guidance and is implementing Phase III of the Social Security Number (SSN) Reduction Plan. Per DON CIO MSG 171625Z FEB 12, "After Monday, 1 October 2012, a disclosure of the last four numbers of the SSN to individuals without a need to know will be treated as a PII breach incident that may result in written notifications to affected personnel. The use of the SSN includes the SSN in any form, including but not limited to: truncated, masked, partially masked, encrypted or disguised SSNs."

Regarding fax machines: "The use of fax machines to send information containing the SSN and other PII by DoN Personnel is prohibited effective Monday, 1 October 2012. External customers such as service Veterans, Air Force and Army personnel, dependents and retirees may continue to fax documents containing the SSN to DoN Activities, but shall be strongly encouraged to use an alternative means. Alternatives to the use of fax machines include United States Postal Service and scanning. Scanned documents shall be transmitted using a secure means such as encrypted emails, safe access file exchange (SAFE), etc. Details regarding the use of SAFE can be found at: DONCIO.NAVY.MIL/PRIVACY/SSN."

The use of network-attached multi functioning devices (MFD) and scanners to scan documents containing the SSN and other PII is restricted to several limitations and prohibitions effective Monday, 1 October 2012.

For details visit:

<http://www.doncio.navy.mil/PolicyView.aspx?ID=3757>

DON CIO Info Alert

DoD to Cease Issuance of Software PKI Certificates to FVEY Partner Nations

The Department of Defense Chief Information Officer has announced a decision to cease the issuance of software Public Key Infrastructure (PKI) certificates to its "Five Eyes" (FVEY) partner nations (Australia, New Zealand, Canada and the United Kingdom). Starting May 31, 2012 Medium Token Assurance PKI certificates will be required.

For details visit:

<http://www.doncio.navy.mil/ContentView.aspx?ID=3983>

DON Secretariat Information Technology Expenditure Approval Authority

To ease transition, these new policy requirements are being implemented in three phases. Phase I focuses on gathering fiscal year 2012 IT planned and actual expenditures. This document was developed to help Secretariat personnel involved with IT resource management understand and successfully execute Phase I Secretariat ITEAA implementation requirements.

For details visit:

<http://www.doncio.navy.mil/PolicyView.aspx?ID=3943>

DON Policy for the Procurement of IT Development and Support Services

This policy emphasizes the mandatory use of the GSA Alliant/Alliant Small Business, DISA Encore II, Army ITES-2S, Air Force NETCENTS, NIH GWAC, and Seaport-E contract vehicles for the acquisition of IT development and support services in varying scenarios.

For details visit:

<http://www.doncio.navy.mil/PolicyView.aspx?ID=3945>

What's New?

Streamlining DON Business Processes for a More Effective and Efficient Future

During the next five to 10 years, the Department of the Navy is facing significant budget constraints. To support vital warfighting capabilities that protect the safety of the nation, it is necessary to find efficiencies in other areas. As part of this effort, the DON Chief Information Office and its information technology partners, such as internal stakeholders and industry, will thoroughly review all operations from an enterprise perspective.

Speaking to more than 400 people at the DON IT Conference in Virginia Beach on May 16, 2012, Terry Halvorsen, DON CIO, outlined his strategy for the future of DON IT. Halvorsen's strategy consists of aligning enterprise business operations through data standardization and transparency, streamlined processes and leveraging the power of the DON enterprise.

When asked about the scope of changes, Halvorsen stated: "We will be looking both at larger scale initiatives such as data center consolidation and seemingly smaller scale changes that will result in a big return on investment – the change between the couch cushions is as valuable as single big spends. For instance, we released a policy on more efficient printing. The DON currently spends \$100 million a year on total printing cost. This new policy has the potential to save \$30 million per year in printing alone. That is significant couch cushion change."

To view more, visit:

<http://www.doncio.navy.mil/ContentView.aspx?ID=3984>

NGEN RFP Released

The Naval Enterprise Networks (NEN) Program Management Office/Next Generation Enterprise Network (NGEN) Program has released the final Request for Proposal (RFP) for transport and enterprise services.

The RFP release was announced via <https://e-commerce.spawar.navy.mil> or www.fbo.gov. The closing date for the proposal solicitation is July 18.

"The release of the RFP is a significant milestone and it reflects critical insight from industry as we compete the world's largest enterprise network," said NEN Program Manager Capt. Shawn Hendricks, U.S. Navy.

The comments from our ongoing dialogue with industry were carefully reviewed and reflected in the government's position in the NGEN RFP."

The NEN Program Office manages the acquisition life-cycle of the Department of the Navy's enterprise-wide information technology networks. NEN's portfolio includes NMCI, the Base Level Information Infrastructure for the Outside of the Continental United States Navy Enterprise Network and NGEN.

To view more, visit:

<http://www.doncio.navy.mil/ContentView.aspx?ID=3961>



State-of-the-Art NMCI Laptops Help NRC Recruit Tech-Savvy Youth

The Navy Recruiting Command (NRC) worked with the Navy Marine Corps Intranet (NMCI) program office to deliver a highly capable tablet-style laptop to support their quest to recruit today's tech-savvy youth. Recruiters' use of state-of-the-art technology helps convey the fact that today's Navy knows how to effectively utilize current and modern information technology.

To fully support the needs of the Navy Recruiter Corps, the new mobile recruiter laptops were custom-configured to support the recruiters' mission as well as to be highly capable in hardware computing power.

Working with the NRC, NMCI began equipping recruiters with a convertible laptop, one in which the screen can swivel 180 degrees to function as a tablet with touch screen capabilities while retaining the full computing power and functionality of a traditional laptop. It comes in a kit with a printer, scanner, speaker and rolling case.

"The capabilities of the Mobile Recruiter solution have allowed us to complete double the tasks in literally half the time, boosting production and improving morale by allowing recruiters to shorten the average workday, all while saving countless dollars in travel and man hours," Naval Aircrewman 2 Mickey Blasingame reported.

Information Technology Areas of Interest

Portfolio Management

IT Vendor Business Case Analyses: Driving Savings Today and Sustaining Relationships in the Future

The BCA methodology was developed collaboratively using an inclusive process to ensure perspectives from stakeholders across the DON's technical and business IT communities, as well as other enterprise stakeholders, who have years of technical and customer experience. Additionally, the BCA methodology ensures the most complete and detailed understanding of the current context of the DON's relationship with any particular high-interest IT vendor with whom the department has invested significant funds in its products, as well as an understanding of the vendor's particular position within its own industry and market.

To view more, visit:

<http://www.doncio.navy.mil/ContentView.aspx?ID=3960>

Information Assurance

Public Key Infrastructure (PKI) refers to the framework and services that provide for the generation, production, distribution, control, and accounting of public key certificates, and provides that critically needed support to applications providing confidentiality and authentication of network transactions as well as data integrity and non-repudiation. The PKI encompasses Certificate Management and Registration functions.

PKI implementation allows individual users to both digitally sign and/or encrypt e-mail messages for transit over the NIPRNET and SIPRNET using their personal COTS e-mail client. Now, more than ever, there is a need for DoD users to have a means for indicating whether e-mail messages are altered during transit. Also of immediate concern is ensuring that hackers are not able to view the contents of Sensitive But Unclassified (SBU) data during transit.

SBU information includes, but is not limited to, contracting documents and unclassified official orders. PKI fills an immediate need to provide a secure means of transport to SBU and routine e-mail messaging between individuals.

Data Management

Federal privacy laws require agencies to "establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records to protect against any anticipated threats or hazards to their security or integrity." The loss or compromise of PII can lead to identity theft and fraud, which directly impacts department personnel, contractors, retirees and their dependents. Safeguards must be applied to IT systems, shared drives, computer networks, email, paper records and websites to prevent unauthorized access. Careful management of this sensitive data will prevent potential PII breaches in the future. A key reference in managing records review and disposal is the Department of the Navy Records Management Manual (SECNAV M-5210.1).

Safeguarding this PII is everyone's responsibility. Use of PII should be reduced to the minimum extent possible. If you do have a need to store PII, here are the steps required to safeguard this type of information.

To password protect a Microsoft Office *document*:

- Open and save the document to the desired location.
- Click on "Tools" in the tool bar at the top of the screen.
- Click on "Options" in the drop down menu.
- Click on the "Security" tab.
- Type in your password and click on "OK."
- Confirm your password and click on "OK."

Architecture

Business process models are the anchor points for associating your department to the BUPERS Enterprise Architecture (BUPERS EA). By documenting your critical business processes and incorporating them into the BUPERS EA, it is possible to analyze the effects that a system or organizational change will have on your business.

The standard for business process modeling is Business Process Modeling Notation (BPMN), which can be obtained at <http://www.bpmn.org>. In addition, the DoD Deputy Chief Management Officer (DCMO) has published a set of standard templates, called BPMN Primitives, that further define how DoD activities should use BPMN to document their processes. The BPMN primitives are available at http://dodcio.defense.gov/Portals/0/Documents/DO_DAF/Primitives_OV-6c_Guidelines.pdf.

Contact the enterprise architect for your Echelon II command for more information on how to develop and incorporate your business processes into the enterprise architecture.

Message from the DON CIO: Keeping PII and PHI Secure

As a department, we like to save our data and records -- to ensure we will have a historical record or to meet a regulatory requirement. And indeed, many of the Department's business processes require the legitimate use of sensitive information. However, there are cases in which personally identifiable information (PII) or protected health information (PHI) should not be used, maintained or collected.

When looking at any piece of PII or PHI, it is important to ask the following questions:

- Is the data needed to perform the mission?
- Do I have the authority to collect it?
- Is it properly protected?
- Is it possible to determine who is collecting the information and who it is being shared with?
- Is it possible for the data to be corrected if necessary?

If the answer to the first question is no, then it is important that the proper steps are taken to eliminate the data. If the answer to the first question is yes, then steps must be taken to ensure all the other responses are also yes.

PII and PHI should only be saved for specific mission requirements, by specific organizations, for a specific purpose and with specific safeguards. A specific mission requirement insists that the user has a specific action that is dependent on that piece of data. Convenience is not a valid excuse for the use of sensitive PII.

To view more, visit:

<http://www.doncio.navy.mil/ContentView.aspx?ID=3963>

Private Eye Keeps Prying Eyes Off Of Your Screen

Anyone who works in the government, or in any organization for that matter, can tell you that information security is a top priority. Countless dollars and hours have been spent securing network traffic, authenticating users, and generally keeping an organization's data safe.

And all of this can be undone by someone looking over a remote user's shoulder at the right moment — or the wrong moment, as the case may be.

Private Eye Software from Oculis Labs can help fill this often-overlooked security gap. Using a computer's Web camera, it's able to tell who is authorized to look at the screen, and make it visible only for those users. Private Eye, developed in the CIA's In-Q-Tel program, uses facial recognition software to keep track of its authorized users. While such a user is looking at the screen, it will remain legible. If that user looks away or leaves, the screen will blur after a predetermined length of time and remain that way until an authorized user is back in position.

It will even detect if there is another person looking over your shoulder. At this point, it will take one of two corrective actions, depending on how it's set. One, it can blur the screen, just like it does when the authorized user leaves. Or, two, it can simply alert the authorized reader to the eavesdropper's presence by showing their image on the display.

Read more:

<http://gcn.com/articles/2012/06/04/private-eye-blurs-screen-to-unauthorized-users.aspx>

EYE ON IT

NIST Guide Explains Cloud in Plain Terms

The National Institute of Standards and Technology has unveiled a guide that explains cloud technologies in "plain terms" to federal agencies and provides recommendations for IT decision-makers, reports **Camille Tuutti** in *Federal Computer Week*.

Read the article here:

<http://gcn.com/articles/2012/05/30/agg-fcw-nist-plain-language-cloud-guidance.aspx#13390978146261&req=rpuPopupResize&len=269>



Pentagon to Update Rules For Using Commercial Social Media Sites

In the wake of a dating site hack that exposed personal information on military subscribers, the Defense Department is planning to put new restrictions on how personnel use commercial social media sites.

DOD will soon issue a new policy directing military personnel to use non-mission related contact information, such as phone numbers and e-mail addresses, when establishing personal accounts, Aliya Sternstein reports in *NextGov*.

Dot-mil e-mail addresses will still be allowed on sites such as Army Knowledge Online, Sternstein writes, but not for commercial sites.

EXTRA BYTES

Popular DoD Desktop App Ready For Mobile Devices

A widely used Defense Department Web application is now available for mobile devices. The Defense Information Systems Agency's Defense Connect Online allows users to host and attend meetings from their Android smart phones and tablets.

Read the article here:

<http://gcn.com/articles/2012/05/24/popular-dod-web-application-ready-for-mobile.aspx#13390994533501&req=rpuPopupResize&len=269>



Navy's New Network Will Cost Half the Previous Estimates

The Navy slashed cost estimates for its Next Generation Enterprise Network contract to between \$4.5 billion and a "maximum value" of \$5.398 billion over five years compared to its October 2011 projections of \$10 billion, an official told reporters Friday.

Read the article here:

<http://www.nextgov.com/defense/2012/05/navys-new-network-will-cost-half-previous-estimates/55819/>

Enabling Business Transformation "On the Go"

Increasing the ability to conduct business on the go, away from a traditional office or desktop environment, can be a key enabler of the Department of the Navy's business transformation process. Arming DON personnel with access to the department's knowledge base regardless of their location will improve effectiveness in any new or improved business process.

A robust enterprise mobility capability can improve communications, save money, enhance the ability to make decisions and facilitate organizational restructuring — all of which are critical business transformation rationales.

Mobility and business transformation can each leverage ongoing Department of Defense (DoD) IT initiatives such as cloud or tablet-based computing. In a cloud environment, an organization's data and applications reside in centralized data centers and are accessed via the Internet or

an intranet such as the Navy Marine Corps Intranet.

There are a number of advantages to this approach. Perhaps the most obvious one from an end user perspective is that the traditional desktop computer with its large disks to store applications and data is replaced with zero- or thin-client devices, which have no or minimal storage, respectively. This is particularly well-suited for a more mobile workforce as mobile devices typically do not have the processing power or storage capacity of a desktop computer.

In this environment, a tablet may be more useful than a standard desktop computer because it can have the same application functionality but with the added benefit of removing the tether from the wall jack.

To view more, visit:

<http://www.doncio.navy.mil/ContentView.aspx?ID=3896>

NMCI's Ever-Improving Security Profile

The Navy Marine Corps Intranet (NMCI) continues to improve its security profile by increasing the use of smartcard credentials for network authentication. The network has established interoperability with Personal Identity Verification (PIV) smartcards issued by non-Department of Defense agencies and departments.

The ability to securely utilize another federal agency's PIV to access NMCI increases productivity and efficiency as a separate DoD Common Access Card (CAC) would not need to be issued to that user. Prior to the successful support of DoD-approved external identity credentials, it would have taken several days for a non DoD user to be issued a DoD CAC. Now when users have non-DoD PIV credentials they can access NMCI and smartcard-enable their NMCI account as soon as their account is provisioned.

This accomplishment is also a significant milestone towards complying with Homeland Security Presidential Directive-12 and numerous DoD and Department of the Navy policies that require the use of a standardized PIV identity credential to access government information systems.

Business IT Transformation Town Hall Transcript Available

At the most recent Department of the Navy Information Technology Conference in Virginia Beach, Va, Terry Halvorsen, DON Chief Information Officer, held a town hall to discuss his strategy for business IT transformation and the future of DON IT. Download the full transcript, which includes questions from the audience.

To view more, visit:

<http://www.doncio.navy.mil/ContentView.aspx?ID=3995>