NAVAL POSTGRADUATE SCHOOL
ITACS
INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES

Technology News August 2009

KUALI FINANCIAL SYSTEM

Ms. Colleen Nickles briefed the IT Task Force at its August meeting on the upcoming launch of the Kuali Financial Management System on October 1, 2009. For ITACS, implementation of the Kuali system is very important because the current system uses aging technology, and the commercial alternatives are expensive and not tailored to NPS requirements. Kuali not only allows NPS to join an open source consortium with some of the best research universities in the nation, but also to benefit from best practices of other research universities' financial processes. It also permits the staff in the Business Solutions Group to develop expertise and marketable skills in this leading-edge technology, a boon to professional staff development efforts within the department.

CYBER SECURITY AND PRIVACY AWARENESS MONTH

In conjunction with the National Cyber Security Alliance's Sixth Annual National Cyber Security Awareness Month in October, NPS will be conducting a local version with an additional emphasis on Privacy. A 1950's horror film has been selected as the main theme; therefore, posters, handouts, and video kiosks with the latest important messages on Cyber Security and Privacy will feature that twist. ITACS will host a kick-off celebration in early October, as well as brown bag discussions and presentations by key NPS faculty whose research involves finding better ways to protect our nation's and your information assets. Special attention will be focused on users and how they can protect sensitive information, both in the home and the work environment. As part of October's Cyber Security and Privacy Awareness Month, Dean Peter Purdue and Vice President Karl van Bibber will be hosting an all-day NPS workshop highlighting faculty research in this important area.

All campus constituents are invited to visit the Technology Assistance Center in October to learn more about cyber security and privacy, and the terrors that threaten us all ……if you dare!

CERTIFICATION AND ACCREDITATION (C&A)

Following a two year effort, ITACS is pleased to announce that the Systems Technology Battle Lab (STBL) has been fully accredited by NAVNETWARCOM for a three year period, expiring in 2012. Due to the lab's dynamic environment, the task was a challenge: with over 60 servers and workstations, a mix of 3 operating systems and dozens of applications. Maintenance will require constant configuration control and monitoring, and working closely with the various research and thesis teams in the STBL that ITACS supports. If you need to modify existing infrastructure or introduce a new capability in the STBL, contact Mr. Ed Nath at Ext. 3014 or Mr. Artie Gross at Ext. 3046. The next project for the C&A team is the Restricted Resources Lab in the Dudley Knox Library.

DATA AT REST (DAR)

You may remember reading in a newspaper when a VA laptop was stolen from the residence of an employee who was not authorized to take sensitive data home. Soon thereafter, the laptop was recovered. The FBI did forensic analysis and was 99% certain the sensitive data were not accessed. The VA settled a class action lawsuit (originally set for $26 billion) for $20 million out of court. A sigh of relief was heard throughout the DC area? Hardly….welcome to the urgent and pressing need for protecting Data at Rest.

Locally, ITACS is addressing this risk by deploying an encryption solution for all authorized government laptop users that process and store sensitive information on their laptops. ITACS will be piloting this solution through September, followed by a wider deployment. If you are a candidate for this technology and have not yet been identified, please have your supervisor reach out to the Privacy Act Coordinator, Mr. Chris Gaucher, at Ext. 3417 and you will be added to the list. Remember: protecting sensitive information is a shared responsibility and there are tools that can assist in meeting that responsibility.

Joint Enterprise Directory Service (JEDS)

The Defense Information Systems Agency has enabled an enterprise-wide directory service that provides DoD People Discovery (i.e. white pages) and DoD identity management attribute services to support DoD access control decisions. The data are available to DoD users through a central public key infrastructure enabled website, https://jeds.gds.disa.mil. The service combines pertinent information from many DoD data sources that provide information on DoD people, objects, and resources within the unclassified environment.

ITACS has posted the JEDS User Guide at: http://intranet.nps.edu/ITACS/Docs/JEDS)_users-guide.pdf.

hamming Update

Currently, there are over 100 active accounts on hamming; users are from GSEAS, GSOIS, CHDS and one is from SIGS.

During the week of August 13, 2009, load on the system, which is typically about 33%, was at 100%.

Mr. Eric Adint, who splits his time equally between GSEAS and ITACS, is currently the only system administrator who, along with Dr. Jeff Haferman, can troubleshoot inquiries. Over 100 items are backlogged for resolution; therefore, Dr. Haferman would like to ask for your patience as work continues to resolve these non-critical incidents.

Common Access Card (CAC)

The DoD and DoN have determined that the Common Access Card (CAC) is more than just a DoD ID card. The CAC contains a computer chip, barcodes, and a magnetic stripe which allows it to be used to access buildings and controlled spaces, to digitally sign and encrypt email messages, and to log in to public key infrastructure access controlled websites.

The DoD and the DoN require that you digitally sign and/or encrypt e-mails when sending:

Digitally-signed Email: Digital signatures must be used whenever email is considered official business and/or contains sensitive information, a file attachment, or an embedded website link. This ensures that the recipient can confidently be assured that the message came from you and not from someone with malicious intent.

Encrypted Email: Email must be encrypted if it contains sensitive information (e.g., FOUO) or information protected by The Privacy Act of 1974 or through The Health Insurance Portability and Accountability Act. Encryption enables users to securely send SSN’s and other sensitive information via e-mail to authorized recipients.

For questions regarding CAC procedures, please contact the Technology Assistance Center at Ext. 1046.

Award to Dr. Peter Denning

The Internet Society announced its award of the 2009 Jonathan B. Postel Service Award to CSNET, which was the experimental networking project that bridged the work done on ARPANET with what we know today as the internet. The Postel Service Award recognizes the pioneering work of the four principal investigators that conceived and later led the building of CSNET – Dr. Peter J. Denning, (member of the IT Task Force, Professor, Chair and Director of the Cebrowski Institute), David Farber, Anthony C. Hearn and Lawrence Landwebber — and the U.S. National Science Foundation program officer and visionary responsible for encouraging and funding CSNET.

Partnerships and Outreach

Dr. Christine Cermak met with representatives from the **Central Coast Broadband Consortium (CCBC)** to finalize the grant proposal being submitted for economic stimulus funding on behalf of the tri-county region. County Administrator Lew Bauman, Asst. City Manager Fred Cohn, and Monterey County CIO Virgil Schwab were in attendance, in addition to representatives from CSUMB and the Monterey County Business Council.

The **Classified Computing Committee**, charged by Dr. Christine Cermak to assess requirements for classified computing at NPS and to provide recommendations for action, began its work, which will be completed in the next several months. Professor Hersch Loomis chairs the committee and members include Professor Chris Eagle, Professor Chris Olsen, Professor Bret Michael, Mr. George Goncalves, and Mr. Joe LoPiccolo.

Dr. Donald Brutzman (MOVES) and Dr. Christine Cermak submitted a proposal to the National Science Foundation, Directorate for Computer Information Science and Engineering Division of Computer and Network Systems, the title of which is *Deploying Ultra High-Quality 4K Digital Video for Archival Science Assets and Distributed Education.* This project proposes a phased evaluation of the complex technology required to realize the vision of ultra high-quality video deployment in the deep ocean. Issues around data preservation and interoperability will be examined, and a prototype workflow for capturing, storing, and archiving digital content will be developed. A digital content repository which can be distributed over partner institutions, a long-term digital library and an archive will also be prototyped. Exploration of the required technologies for deployment of the new camera formats for the MARS Network in the Monterey Canyon — to collect data and to expose the user community to those results — will also be included, so that the techniques developed for the content archive can be utilized successfully in new domains and environments. Finally, best practices will be surveyed and employed for digital distribution to scientists' desktops via desktop visualization, and for public access through exhibitions and outreach. A decision by the National Science Foundation will be made in six months.

Report from the Technology Assistance Center (TAC)

From August 1 through August 28, 2009, TAC received 1,841 requests for assistance, 1,429 of which were resolved by the Tier 1/Tier 2 areas. The remaining 412 were escalated to groups outside of TAC for specialized assistance. This number represents a 12% decrease in requests for assistance from August 2008.

Requests for assistance were categorized as follows:

Phone: 992
Email: 407
Walk-in: 371
Web: 71

This month, 96% of all calls were resolved within the Service Level Agreement (SLA). Those that were carried over are awaiting parts, pending information from the customers, etc.