



Calhoun: The NPS Institutional Archive
DSpace Repository

Information Technology and Communication Services (ITACS) Information Technology and Communication Services (ITACS) Public

2006

ITACS Annual Accountability Report: FY2006 Accomplishments and Challenges

Monterey, California. Naval Postgraduate School

<http://hdl.handle.net/10945/37037>

Downloaded from NPS Archive: Calhoun



Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>



ANNUAL ACCOUNTABILITY REPORT: FY2006

ACCOMPLISHMENTS AND CHALLENGES

INTRODUCTION

“Customer Service” was the major focus of the Information Technology and Communications Services (ITACS) department in FY06. ITACS not only met its requirement to provide mission-critical services and equipment to the campus, but also delivered on its commitment to provide expanded and improved services to its customers. Network reliability, essential for educational and research operations at NPS, was 99.96% overall while maintaining a very effective security posture, blocking 1,248 attempted virus infections with the network’s monitoring systems. During this past year, the campus received over 20 million external emails, with 14 million of these classified as spam and blocked by the Barracuda spam filter. The Technology Assistance Center (TAC) responded to 29,146 requests for assistance, and over 500 users were helped in one day during the mandated Security Stand-Down; Instructional Technology supported 150 class segments, 50 video conferences, and responded to 500 audio-visual requests, and more than 2,600 courses, comprising 100 hours weekly, were captured via streaming media.

During FY06, ITACS made decisions that saved measurable dollars and/or reduced staff workload, thereby permitting a reallocation of resources that was used to improve services and to address other institutional requirements. In many cases, the savings were not realized by ITACS, but by the institution or customer’s department, and the budget for ITACS was not reimbursed, neither for the up-front nor recurring costs. All of the projects provided an increase in productivity, higher levels of capability, support for mission accomplishment, and demonstrated cost deference — in either dollars or labor requirements. The following are examples:

- The Technology Assistance Center, which provides Help Desk services to all users, extended their hours of operation from 8:00 A.M - 4:30 P.M. to 7:30 A.M. - 5:00 P.M. These extended hours allow more availability of tiered technical assistance for Distributed Learning students in different time-zones.
- ITACS developed a web-based training interface that supports individually-tailored, specific training requirements. This module has accommodated the Research Principle Investigators and Program Managers, Equal Employment Opportunity, Human Resources, and Privacy Act and Information Assurance Awareness annual mandatory trainings. Because the capability can track and report results, delivery and accountability reporting has been simplified, and hours of staff labor have been reduced.

- ITACS completed the certification and accreditation of the Monterey Peninsula Department of Defense (DoD) Network, the Systems Technology Battle Laboratory (STBL) Secret Internet Protocol Router Network (SIPRNet), and the Library SIPRNet networks and systems. This effort was accomplished in-house, permitting a reallocation of \$150K to be used in support of the general mission of ITACS.

Services were also provided by ITACS on a fee basis to partners of NPS, other DoD sites, the Department of Navy (DoN), and the United States Marine Corps (USMC). The fees collected covered specific training for ITACS and the labor costs associated with the projects, thereby providing benefits both to partners of ITACS and to its staff.

1. ITACS hosted three Web servers for the Defense Language Institute (DLI) on the Education and Research Network, providing an avenue for Americans stationed in remote locations to be able to access DLI materials — without requiring a military network.
2. Blackboard, a Learning Management System (LMS), was expanded to permit both the USMC and the Director of Naval Intelligence to view the features of an LMS system, thereby allowing collaborative work — but independent solutions.
3. The Monterey Peninsula Department of Defense Net (MP DoD-Net) was expanded to accommodate another Department of Defense institution on the Monterey peninsula, the Personnel Security Research Center (PERSEREC). This effort shifted leased circuit costs to the MP DoD-Net equipment, while allowing for increased communications capabilities, benefiting not only PERSEREC, but also the entire Monterey Peninsula Department of Defense community.

In FY06, IMET granted \$300,000 of the \$500,000 requested for wireless network deployment and upgrades, as well as additional data storage capacity. NETC awarded NPS \$500,000 to refurbish 11 classrooms, two study rooms in the library, nine Learning Resource Centers and the smart classroom located in the Graduate School of Business and Public Policy. When presented with the mid-year unfunded budget requests, the Executive Council endorsed the \$3.3 million request for the Telco switch, network upgrade and fiber replacement. ITACS also sought to reduce costs on smaller scales: e.g., in response to the growing demand for Red Hat (Linux) licenses, ITACS negotiated and purchased 500 licenses at a cost of \$7 each, rather than the standard cost of \$50 apiece.

THE EDUCATION AND RESEARCH EDUCATION (ERN) INITIATIVE

The migration of the entire user community to the ERN — which has a total data storage capacity of 18 terabytes but is scalable to a much higher capacity — was staged in three phases. Phase I was completed in FY05, and involved the shift of all users' email addresses from the .mil to the .edu domain. In Phase II, a total of 8.5 terabytes of data files and 823 gigabytes of email were moved to the .edu domain by the Server Management and Network Operations groups — including 1,040 students who were moved in ten days during the summer break. During Phase II, TAC personnel assisted over 700 users before, during and after the transition in archiving email and files, and in various forms of troubleshooting.

Phase III, which includes the hardware-level move to the ERN of computers, printers, scanners and all application servers, began in FY06. To ensure that all web-based

applications and content would be successfully migrated, ITACS staff spent weeks evaluating existing sites and links, as well as testing a migration tool. Only 5% of the migrated web sites had minor problems, and all were resolved very quickly. The Web Operations staff and the Server Management group completed the move of the external military web site, a significant challenge since the upgrade involved both the hardware and server operating system which operates 24 hours a day, 7 days a week. During the Phase III transition from .mil to .edu domain, staff from TAC moved 1,330 machines, which involved coordination between the TAC and the Network Operations Center, as well as site visits by TAC staff of 30-90 minutes for each user.

A major element of the ERN is the high-speed (up to 1Gbps) connection to the Internet, which was made possible by membership in the Corporation for Education Network Initiatives in California (CENIC), funded by a research grant. Connectivity to CENIC provides a redundant communication path that significantly expands the research and educational opportunities for NPS faculty and students.

Benefits to NPS Users of Moving to the Education and Research Network (ERN)

- Profile is smaller, and loads much faster
- Internet throughput is greatly improved
- Domain name change signals the academic affiliation of NPS, and draws attention to its mission of education and research
- Additional bandwidth available
- Improved reliability in NPS network connections to the global Internet and Internet2
- Closer working relationships with institutions of higher education on the Monterey peninsula and beyond
- Provides more efficient peering with higher education and research institutions, both nationally and globally

ABOUT INFORMATION TECHNOLOGY AND COMMUNICATIONS SERVICES (ITACS)

The ITACS department reports to Dr. Christine Cermak, Executive Director of Information Resources, and CIO of the Naval Postgraduate School. The NPS Strategic Plan, *A Vision to the Future*, and the IT Strategic Plan, *The Information Revolution: Planning for Institutional Change*, provided the general framework for operational planning in FY06. The Information Technology Task Force (ITTF), comprised of representatives from every major academic area as well as a number of administrative departments, continued to be the vehicle for policy guidance and the establishment of priorities.

In an effort to realign work centers and to support improved performance, customer service and communications, ITACS was reorganized in FY06. The division now encompasses two major areas: Operations and Technology Services, which falls under the supervision of the Chief Technology Officer and the Director of Technology Services, respectively.

OPERATIONS

- ***Academic and Client Services (ACS):*** Classified Systems; High-Performance Computing; Instructional Technology; Learning Resource

- Centers; Classroom and Laboratory support; New Technology and Innovation Center; PC Shop; Streaming Media
- **IT Administration:** Asset Management; Contract Administration; Financial Management; Human Resources; Policies and Plans
- **IT Infrastructure:** Physical Plant, including construction/remodeling projects across campus
- **Mainframe Operations:** Two IBM mainframe systems, tape and disk subsystems; Operating system (VM, MVS); User Programming support
- **Network Operations Center:** Backup systems; Network; Server Management; Telephones
- **Corporation for Education Network Initiatives in California (CENIC)**
- **Monterey Peninsula Department of Defense Net (MP DoD-Net)**

TECHNOLOGY SERVICES

- **Business Solutions Group (BSG):** Web Services; Blackboard; Administrative Applications (DORS, ETAC, PYTHON, DMAS, MIIS); Content Management System; Application Development
- **Information Assurance**
- **Network Security Group:** Intrusion Detection; Network Monitoring
- **Technology Assistance Center (TAC):** Phone, email and walk-in computer trouble resolution; assistance with applications; virus protection and detection; first stop for new requirements and requests

The five categories of recommendations identified in the IT Strategic Plan — Academic Applications and Services, Administrative Applications and Services, IT Management and Resources, Network Infrastructure and Services, and Partnerships and Outreach and Communications — comprise the main body of this report.

ACADEMIC APPLICATIONS AND SERVICES

CENIC

Affiliation with the Corporation for Education Network Initiatives in California (CENIC) expanded in FY06, beginning with membership privileges. Direct connections to the California Research and Education Network's (CalREN) Digital California (DC) and High-Performance Research (HPR) backbones occurred in the second half of FY06. Because of construction delays affecting both fiber-optic cable and the CENIC node in Salinas, a decision was made to establish the initial connections via a leased AT&T GigaMAN circuit. CENIC affiliation provides over 22 times more bandwidth to support research than was available in past years for approximately 50% less than the cost of direct purchases from a commercial provider.

HIGH-PERFORMANCE COMPUTING (HPC)

High-Performance Computing (HPC) took a leap forward when its website was launched in October. Room 301 in Spanagel Hall became the HPC Center in November, which housed the first cluster, "Anastasia," used by the Oceanography department, and a smaller 5-processor unit for students' use. Physics and Mechanical/Aeronautical Engineering soon added the "Detonation" cluster, and MOVES added the "Wipeout" cluster. In August, Mechanical Engineering added "Cheetah," a new 132-node dual boot-Linux/Windows cluster, with each node having 2 dual-core opteron processors, for a total of 127 processors, making it one of

the top two “supercomputers” currently on campus. Electrical and Computer Engineering is expected to add clusters in early FY07.

Both Dr. Jeff Haferman, Manager of the NPS High-Performance Computing Center, and Dr. John Romo, from the University of Texas Advanced Computing Center, who consults with Fleet Numerical Meteorology and Oceanography Center (FNMOC) through the High-Performance Modernization office, gave presentations on their respective facilities to the IT Task Force. Dr. Haferman also gave an overview of HPC at NPS to the Provost. Both a HPC core support group and a HPC Advisory Group have been formed. Quarterly meetings for the latter began in August 2006.

INSTRUCTIONAL TECHNOLOGY

In December, the Video Tele-Education (VTE) department installed a new videoconferencing bridge, a critical installation because every multi-point VTE class uses this technology to connect. During the winter quarter, 43 course segments were supported by the new bridge, while the audio-visual section of Instructional Technology fulfilled 184 requests for event support, 6 duplication requests and 30 maintenance and/or repair requests. In summer, the Instructional Technology team supported 37 VTE classes, and also began the process of evaluating NPS for IP videoconferencing. More than 100 presentation systems were supported by Instructional Technology in classrooms, Learning Resource Centers and auditoria in FY06. Installation of equipment in the conference room in the School of International Graduate Studies began in late April, and discussions involving plans for the Glasgow extension continue.

The Instructional Technology division also undertook the task of classroom maintenance in FY06. In November, a walk-through of every classroom on campus was conducted, and a report on the inventory was presented to NPS leadership. Of 60 classrooms and 17 Learning Resource Centers evaluated, 21% of ceilings, 53% of carpets, 14% of window coverings, and 45% of chairs needed repair or replacement, while 33% of the facilities needed extensive cleaning. In August, the new Classroom Maintenance Plan was developed and endorsed by NPS leadership. Quarterly evaluations of all classrooms and Learning Resource Centers will be conducted by the Director of Instructional Technology, who will also be responsible for coordinating with key constituents on campus to ensure the plan’s execution.

Additional accomplishments in support of Academic Applications and Services include:

- **Academic Software Licensing:** Reduced images from thirteen to 4; covered all departmental requests, and reduced staff footprint by 5 staff members
- **Sensitive Compartmented Information Facility (SCIF) Computing:** Computer and network connectivity support for 160 faculty/staff and 300 students; migration, implementation, installation and deployment activities; operated all networks without security incidents during the entire year
- **Systems Technology Battle Laboratory (STBL) Secure Computing:** Network connectivity and support for 168 faculty/staff, 546 students, and 80 other users; setup, and configuration of PCs; updating and maintenance, development and implementation of secure web pages and procedures; course, conference and seminar support; installation of software; operated all networks without security incident during entire year
- **Wargaming:** Setup Wargaming center; instruction and execution of scenarios for MOVES, Singapore government San Francisco Bay, merchant ships routing across

- the Pacific Ocean, Stanford University, Baghdad; briefing to distinguished visitors, including Taiwanese Simulation Center
- “Zephyr,” a Windows 2003 server, was brought online to support student web application projects, addressing a long-standing need for a place to host student project/research websites without affecting the NPS production web servers

ADMINISTRATIVE APPLICATIONS AND SERVICES

In addition to launching a new Intranet website design in October, the Business Solutions Group (BSG) partnered with the Human Resources office to update and to improve their New Employee Orientation link; with the Public Affairs Office to create the new photo gallery, which lets NPS archive all photos that it posts to the public in a searchable format, thereby complying with DoD regulations; and the Research Office — to support their integration and the move to convert the spreadsheet system of DORS-DMAS, the NPS financial planning and budgeting systems, to a database system. BSG also teamed with the Dudley Knox Library (DKL) to begin the library’s web re-design project. Last year, a committee from NPS recommended that a Content Management System (CMS) support the project, the result of which was launched in September. An academic catalog system and a sophisticated web-based training capability were also created, and reports for the Provost and Academic Planner regarding faculty pay source, Student Opinion Forms, and teaching awards were also supported by BSG.

In October, 52 students participated in the thesis pilot project of SharePoint, which preceded the NPS requirement that beginning in January 2006, all students use SharePoint for thesis processing. Shortly after the launch of the project, ten students and one faculty member completed SharePoint training. Both SharePoint thesis processing support and training classes continue.

Printing services for the Office of Institutional Advancement were provided by the New Technology and Innovation Center (NTIC) during their 3-month evaluation of Xerox products. During this process, it was determined that the Xerox product was capable of producing high-quality, in-house printing jobs, while reducing both costs and the time lags experienced in waiting for products from DAPS. A contract for a color printer from Xerox was awarded in September 2006, and the new product is expected to be housed in the Office of Institutional Advancement in early FY07. Joint funding of an *Editing Suite* for use with the new printer is expected to help professionalize the NPS video and photographic content.

FY06 marked the first time that ITACS was involved in determining the Functionality Requirements for the copier contract for NPS. The evaluation team reviewed the Xerox Work Centre Pro 265 and Xerox DocuColor 250 multi-function devices, and both received high marks of approval. The combination of scanner, printer, copier and fax multi-function devices will replace the current copiers on campus, and will not only change the way NPS currently provides those services, but also align with the Digitization Committee’s mandate to reduce paper usage on campus. The contract for purchasing the 79 new devices was awarded in September 2006, and the machines will be installed throughout high-volume areas of the campus in early FY07.

Because of the efforts of NTIC, the Center for Executive Education (CEE) will save \$196,880 on paper, printing, labor and mailing costs over a three-year period when it replaces its current 4-inch binders of copied class documents with Gateway’s convertible tablet PC,

installed with DYKnow software. Using a SQL server web application hosted through DYKnow Vision, thumb drives will replace the Center's binder system, while providing state-of-the-art tools to ensure ease of use, and enhanced teaching and learning capabilities.

Requests for streaming live events increased in FY06. ITACS captured not only all of the graduations in the 40 events it streamed, but also:

- Admiral Patrick Dunne's retirement ceremony
- Admiral Wayne Meyer's induction into the NPS Hall of Fame
- Nobel Laureate Dr. Reinhard Selten: "Game Theory Applied to Kosovo"
- Change of Command ceremony in December 2006
- *Grads in Space*
- *Annual Technology Review and Update* (TRAU) weeklong course
- *7th International Symposium on Technology and the Mine Problem*
- Interview with Colonel Jeff Williams, International Space Station
- Distance Learning Summit, sponsored by the Office of Continuous Learning.

Compared to 368 total viewers in the previous year, 832 viewers watched the winter and spring graduation ceremonies in FY06.

IT MANAGEMENT AND RESOURCES

Accountability and responsiveness to institutional goals remained a high priority for ITACS in FY06. Continuing its efforts from last year, including the reorganization of key functions and the development of an annual training plan, ITACS became a higher-quality, more responsive and better-focused organization. The emphasis on establishing baseline metrics for charting progress — with a focus on future efforts — continued. Oversight reporting also remained a priority.

Financial management improvements continued in FY06: monthly IT financial reports of all operating funds by major expense categories were improved and reviewed by senior leadership on a monthly basis; IT management met and reviewed actual-to-planned expenditures on a quarterly basis; NPS leadership was briefed on ongoing operations and the progress of ITACS toward reaching its strategic plan's goals, and financial information was made available to all levels within ITACS.

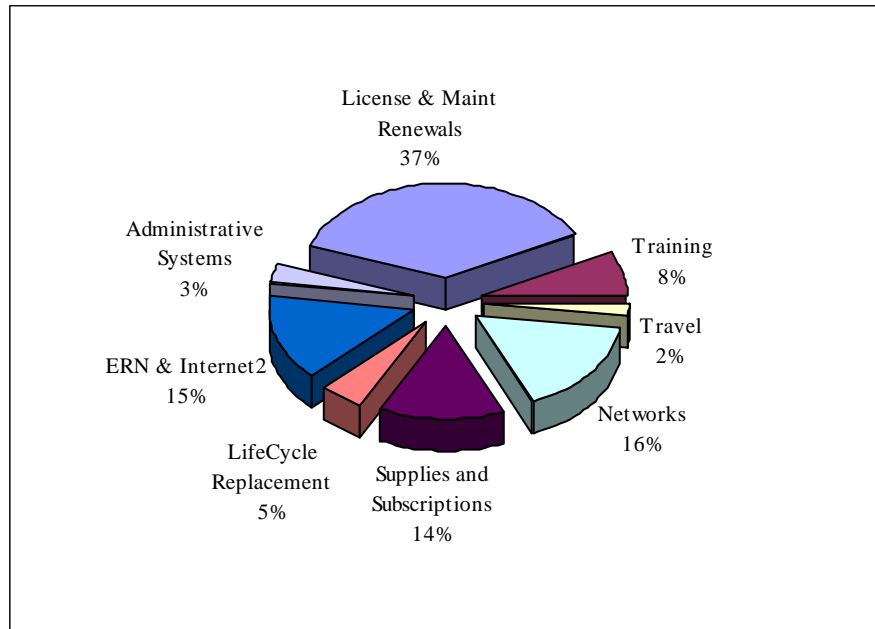
Implementation of IT management software, received via a grant from the NPS Foundation, continued. The software provides additional management controls for governance, asset management, and linkage to the Remedy ticket system, thereby establishing more accurate reporting within ITACS as well as faster responses to data calls.

Indirect Cost Recovery remained a critical concern for ITACS. In October 2005, Dr. Christine Cermak presented data to the Research Advisory Board, noting that 21% of ITACS costs are directly attributable to research; however, ITACS receives 5-6%. The Research Office supported an increase in that amount to 10%. Nearly all costs for Video Tele-Education (VTE) courses are attributable to reimbursable education, but only 31% of those costs are covered by Indirect Cost Recovery. An increase to 42% was recommended. Compliance with Department of Defense mandates, as well as telephone and network equipment, software licensing, memberships and upgrades to Hermann Hall will need to be

funded; therefore, Indirect Cost Recovery and/or re-allocation of internal funds will continue to be a major topic of discussion for ITACS in FY07.

The total ITACS operating budget for FY06 was \$1.42 million. The total ITACS labor budget in FY06 was \$5.71 million (direct and indirect funds), which supported 78 full-time staff.

The following chart shows the FY06 use of operating funds by general categories of expenditures:



The Information Technology Task Force (ITTF) approved the following policies in FY06:

- VTE Central Coordination policy: authorizes the Director of Instructional Technology to have signature authority and responsibility for all of the Video-Tele-Education (VTE) and Video-Teleconferencing (VTC) classrooms at NPS
- Virtual Private Network (VPN) Access policy
- Local Administrative Rights policy: provides the process for users to request an administrative account on their Windows workstations, and outlines user support expectations
- PDA policy/ITACS Policy 903: states services offered by ITACS to PDA users
- “IT Requirements and Support” technology plan, which summarizes all the IT requirements of the Fleet Concentration Area offices, and the IT support necessary to sustain operations at those remote sites

ITACS personnel also joined in the NPS Property Management working group, formed to establish a campus policy for all minor “pilferable” property at NPS.

A Lifecycle Management Plan was presented to the IT Task Force in December, identifying the total replacement costs for all classrooms, Learning Resource Centers and portable equipment at \$4,440,820. Annual recap costs for the same was estimated at \$998,141, and \$66,000 was identified as necessary for an annual recap cost of maintenance for the physical environment of the classrooms. Three areas — environment, audio-visual and equipment — and remaining IT-related items were evaluated and identified, and funds were allocated for a six-month pilot project to begin to rectify this campus-wide problem. Using \$10,000 from the IT budget, two classrooms in Spanagel Hall were selected for renovation during the summer break. Once completed, another \$112,000 was added from the campus budget to assist with further renovations.

Improved processes were also developed for the Lab Recap Plan, which outlines the procedures on purchasing, tracking, and planning of needed items.

NETWORK INFRASTRUCTURE

Maintaining a highly reliable, secure and robust network infrastructure that provides high-speed access to the Internet and enables collaboration with other research universities and activities remained the highest priority of ITACS. Remote access to internal content and services was greatly expanded this year with the installation of hardware-based Virtual Private Network technology. Increased throughput to the Internet was made possible by the installation of Cisco 6509-E switch, which is capable of throughput up to ten gigabits per second. This switch supports the external connection of the ERN of NPS to CENIC's High-Performance Research (HPR) Network and CalREN's Digital California (DC) Network. This new switch provides redundant firewall and supervisor services and 48 switch fabric-enabled 10/100/1000 Ethernet ports for local connections. The new hardware and software supports multiple firewall instances (virtual firewalls), both IPv4 and IPv6, throughput requirements for the existing CalREN DC connection and the HPR connection, and will support the next incremental increase in wide-area bandwidth requirements.

Apple Computer, Inc. was chosen to provide the Storage Area Network (SAN) variant for resolving the user home directory and group share storage challenges at NPS. At a cost of about \$2 per gigabyte, the Apple variant can move files at about half the speed of the high-end SAN, which costs \$14 per gigabyte.

While continuing to expand the reach and throughput of network infrastructure, ITACS also continued to manage the Information Assurance posture. In FY06, there were no major virus infections on the NPS networks. The external boundary of NPS network continued to log multiple attempted intrusions daily. There were 84 client systems infected by a virus in FY06, but the multiple layers of defense implemented on the NPS networks provided excellent protection to both its systems and its information.

The DoD requires mandatory patching of all its systems, as vulnerabilities are identified. Notification of such comes in three forms: the Alert, which requires the patch to be installed within 2 weeks; the Bulletin, which usually has a deadline of within 30 days; and the Technical Advisory, which does not require a patch, but one should be considered. Additionally, Computer Network Defense Task Orders (CTOs) are issued, which usually add criteria both to mitigate a problem and to expedite the installation of an existing alert or

bulletin. A significant workload is associated with managing and executing the installation of each of these patches. During FY06, NPS maintained compliance on all networks.

The Network Security Group (NSG) was realigned from the Security directorate to the Information Resources directorate in FY06. Although the NSG has retained its focus on network security, the inclusion of the group into ITACS provides a valuable opportunity to leverage resources to accelerate progress on the Information Assurance program. In addition to their regular duties, NSG also completed the rebuilding, reconfiguring and hardware improvement of the Computer Network Defense (CND) tools used on the NPS networks. The new systems, used for back-up and recovery of the servers, were built to the standards used on all the ITACS enterprise systems. Six new services were established.

Additional accomplishments related to Network Infrastructure include:

- Enhanced systems monitoring and outage reporting
- Expansion and enhancement of the LANDesk client management software
- Pushing of updates to 2,161 NPS computer systems, including automated fixes and patches to operating system and applications; reporting on inventory, product numbers, software licensing, managing and troubleshooting remote capability; saved hundreds of staff hours, and reduced overall support costs per client
- Implemented the IA Vulnerability Management (IAVM) program
 - IAV Alerts – 42; Bulletins – 18; Technical Advisories – 32; CTOs – 20
- Patches Installed based on IAVM program:
 - Alerts – 5,287; Bulletins – 3,672; Technical Advisories – 9,920
 - Total = 18,879
- 2,566 system hours spent applying patches
- Resolution of **11** Information Assurance Incidents for FY 2006:
 - **2** incidents: classified information sent to NPS unclassified system
 - **1** incident involved Privacy Act data
 - **5** incidents: requests to investigate suspicious activity
 - **1** incident: NCIS noted malicious code
 - **2** incidents involved e-mail services
- Resolution of **22** Information Technology Outages for FY 2006:
 - **8** outages: limited e-mail service interruptions
 - **6** outages: telephone system or the voice mail
 - **2** outages each: firewall and DNS
 - **1** outage each: web system, fire alarm signal; network looping; external CalREN connection
- Annual all users Information Assurance training; 98% compliance
- Registered all networks, servers and business applications in the DoN database
- Continued to deploy new and update expiring DoD Public Key Infrastructure (PKI) certificates for Secure Socket Layer (SSL) for web servers
- Continued participation in the design and implementation of the ERN architecture
- Completed: System Security Authorization Agreements for the two SIPRNet sites at NPS and the Monterey Peninsula Department of Defense Net
- Conducted the IA review of the ITACS and NPS project plans to ensure IA is planned up-front
- Adjusted the formal process for handling, documenting and reporting Security incidents and service interruptions

- Monitoring: All external and internal traffic via various tools, both within the Network Operations Center (NOC) and Network Security Group
- Weekly vulnerability assessment for all servers and clients that are using both NPGS and ERN IP address space
- Continuation of the Navy's milestones for PKI implementation
- Management of the anti-virus solution: deployed to 2,161 clients
- Regular patching of the enterprise servers, with the critical patches identified for their operating systems
- Deployed UNIX Lightweight Directory Access Protocol (LDAP) server for ERN
- Implemented Spotlight on Exchange and Active Directory software: monitors Exchange and servers for performance
- Moved Earth UNIX home file storage to SANS
- Supported student research projects: implemented TNT network with NPS
 - Assisted: Remote call management through VPN for COAST
 - Server consolidation project; wireless implementation project
 - Defense Advanced Research Projects Agency (DARPA) Advanced Terminator project
- Implemented: audio visual connection from San Diego to NPS
- Implemented: monitoring capability for Intrusion Detection on ERN
- Continued support for DMDC customer VPNS: 15 VPNs supported
- EIQ software implemented: analyzes firewall traffic from ERN and MIL
- Five additional T1 pairs for new Tandberg MCU Video Bridge
- CISCO VPN capability for reach back for MIL Domain Name Services (DNS) and CAC Card authentication
- Retired 4 Remote Access Service (RAS) T1 lines
- Deployed thirteen NPGS (MIL) Servers
 - Three Active Directory, Domain Name Service (DNS), Dynamic Host Configuration Protocol (DHCP) servers
 - Intranet, Second front-end Exchange, Student Web, Internet Web, Breeze, Anti-Virus, Applications, Audio-visual servers; two File servers for transition purposes; Ironview server for NOC; Hive server with disk array; two Activity Base Cost servers

New technologies related to Network Infrastructure that were tested/evaluated in FY06:

- Helium Networks Wireless Scout, which maps wireless signals and prints a physical map — evaluated for three months
- In response to a request from the Center for Executive Education and the Admiral's office, a 30-day evaluation and trial of eInstruction's Classroom Participation System (CPS), a form of "clicker technology" that allows polling, was made available during the NPS Submarine Flag Officer's Conference
- In November, Xerox agreed to lend multi-function devices to NPS for 90-day tests
- For Homeland Security and the MOVES Institute, Apple Xserve and MACPro were evaluated
- ForeScout Technologies and Accordant Technologies, conducted demonstrations in compliance appliances and risk media webcasting solutions, respectively

- Cisco Systems provided the equipment by which NTIC evaluated Voice-Over IP (VOIP) video phones; further testing of this technology will be included in the campus-wide evaluation of VOIP
- Apple visited NPS in April to discuss Apple's Storage Area Network (SAN) technology
- Bradford Networks demonstrated their compliancy/admissions control products
- Cisco System showcased its Distance Learning Management System, which includes Cisco's Virtual Classrooms, Video Management and Content Delivery programs
- The NTIC staff visited UC-Davis, where they toured the university's immersive visualization facilities, and saw demonstrations of the university's PowerWall and Keck Caves systems

A project plan for Thin Client technology began in FY06, which proposes appropriate locations on campus for further piloting of this technology. The advantages of Thin Client technology are that it is quiet, has no moving parts, and consumes one-tenth the power of a traditional desktop computer. Development of the plan will continue in FY07.

MONTEREY PENINSULA DEPARTMENT OF DEFENSE NET (MP DoD-NET)

The MP DoD-Net provides fiber-optic connectivity from NPS to local DoD assets: the Defense Language Institute Foreign Language Center and Presidio of Monterey (DLIFLC & POM), the Defense Manpower Data Center (DMDC), Fleet Numerical Meteorology and Oceanography Center (FNMOC), the Naval Research Laboratory (NRL), the National Weather Service, and the Personnel Security Research Center (PERSEREC), enabling several of these properties to abandon commercial leased services and save resultant costs.

In FY 06, Defense Biometric Identification System (DBIDS) connections were extended to all local DoD organizations that use the system for access control. Moving DBIDS onto the MP DoD-Net increased the reliability of access to the system and allowed its data to be made available at all access control points of those organizations using the system. A new node was established at PERSEREC, which supports multiple 100 Mbps circuits in place of a single T1 (1.5 Mbps) circuit. This enables increased bandwidth between PERSEREC and the DMDC, and supports termination of a costly low bandwidth connection through NPS to DoD-wide area networks. The MP DoD-Net partners agreed to assist in funding equipment to extend the full wavelength capability to all sites; passive wave division multiplexing equipment is being ordered as funds are received. Completion of the wavelength build-out to all MP DoD-Net nodes will support increased use for applications such as distributed storage area networking, for recovery from site specific local disasters, and for the transfer of additional traffic off local leased circuits. During the year NPS avoided the cost of two leased T1 circuits; DMDC avoided the cost of a single T1 circuit; DLIFLC & POM avoided the cost of a GigaMAN circuit and maintenance cost of a duplicate CATV head end; and FNMOC and the NRL obtained direct circuits to NPS which were not possible within their budgets prior to establishment of the MP DoD-Net.

The MP DoD-Net received an Institutional Excellence Honorable Mention Certificate at the 35th Annual Association of Communications Technology Professionals in Higher Education (ACUTA) Conference and Exhibition, held on July 26th in San Diego.

Circuits, an e-newsletter produced by the Department of the Navy, Office of the Deputy Chief of Information, highlighted the MP DoD-Net in their September 15, 2006 issue.

WIRELESS

The New Technology and Innovation Center evaluated vendors and products in FY06, and devised a solution to the current wireless network at NPS.

- Only 45% of the NPS campus currently has wireless access
- Current equipment is reaching the end of its lifecycle
- There is a heterogeneous mix of equipment that comprises the network; no central management system exists
- Over 100 access points have been created
- Security compliance is done manually, which produces vulnerabilities
- Guest access to multiple clients is cumbersome and labor-intensive
- Demand for a high-bandwidth wireless network is increasing

Criteria, which were determined through consultation with ITACS leadership, vendor partners, and the NOC, were met by two vendors, Mesh Dynamics and Bradford Networks, and include:

- 98% coverage for the campus
- Reduction of the number of access points
- Reliable transmissions
- Centralized management
- Future-proof capabilities
- Network access control
- Ability to verify compliance
- Compatibility with the wireless infrastructure provider
- Ability to provide varying levels of success
- Zero client footprint
- Out-of-band solution
- Price and serviceability
- Decreased loads on the TAC

Mesh Dynamics will build a modular infrastructure using access points that are not hard-wired into the NPS network, and four radios: one for backhaul and three for downstream use. Bradford Networks will provide the network access control appliance. Mesh Dynamics' plan will reduce the number of access points to eleven, all of which will be outdoors. Bradford Networks will enforce security policies, control network access and measure guest access. Mercury Data Systems will install the wireless components and make any needed adjustments. Contracts for each were awarded in September 2006, and will be funded by IMET. Completion of the build-out is expected in FY07.

COMMUNICATIONS, PARTNERSHIPS AND OUTREACH

During FY06, ITACS continued to expand upon its relationships with SUN Microsystems, CISCO Systems, Apple, Inc., and Foundry Networks. Bi-annual meetings between ITACS leadership and NPS key constituents also continued in FY06.

Technology News, a monthly newsletter which outlines the progress and achievements of ITACS, continued to be produced and distributed to campus leadership throughout FY06. In addition, *Staff News*, a monthly publication highlighting aspects of the IT staff, was produced and distributed to ITACS personnel.

Initiatives:

- Lawrence Livermore National Laboratory (LLNL) visited NPS; discussed collaborations in areas cyber-security, HPC, visualization capabilities, IPv6 transition, and high-speed connectivity
- Ms. Mary Phillips, IT Director of Monterey Peninsula Unified School District (MPUSD) visited NPS IT facilities; received an overview of the IA program and NOC; began discussions to share plans, policies and technology strategies
- Dr. Christine Cermak presented an overview of the NPS Network Capabilities and the MP DoD-Net and Mr. Joe LoPiccolo, ITACS, presented on Streaming Media — to Defense Language Institute leadership
- Navy Higher Education Information Technology Consortium (NHEITC), which includes NPS, the Naval War College and the U.S. Naval Academy, discussed its charter, governance for the group, and the grid proposal
- ITACS team visited Silicon Graphics, Inc.
- Graniterock CIO Mr. Ken Schipper met with Dr. Christine Cermak; received an overview of NPS, including policies, plans and practices
- ITACS sponsored the Cisco Government Network Express Truck on March 14th; dedicated to both federal and public-sector customers, the Network Express Truck boasts a series of specialized stations throughout the exhibit space
- ITACS team conducted an extensive tour of universities in Southern California to collect data for inclusion in the next IT Strategic Plan
- ITACS participated in the Distance Learning Summit; Dr. Christine Cermak presented an EDUCAUSE video providing a future vision of higher education through the year 2020; Mr. Tracy Hammond presented on the use of Video Tele-Education, and Mr. Joe LoPiccolo talked about Streaming Media
- September 26th marked the launch of the Library's new website/Content Management System, the result of a collaboration between the DKL and ITACS

CONFERENCES/SEMINARS

- ITACS team attended the EDUCAUSE Conference in Orlando, Florida
- Dr. Christine Cermak, Mr. Hank Hankins and Mr. Bill Hogan attended the CENIC Advisory Board meeting at UC-Davis
- Association of Communications Technology Professionals in Higher Education (ACUTA) Conference in Palm Springs, Under the Mobility and Wireless issues track, Dr. Christine Cermak and Mr. J.P. Pierson presented *Wireless Implementation and Management at NPS*
- CENIC Conference in Oakland, California: Dr. Cermak and Mr. Joe LoPiccolo, ITACS, spoke on *Streaming Media Deployment in a Research University*
- MINE Conference: ITACS provided support for 7 classrooms and 3 auditoria during the 5-day event; over 400 participants and 29 presenters; zero problems
- MP DoD-Net CIO Council met to plan collaboration on video initiatives
- DoD CIO Council met at NRL and discussed video streaming initiatives, AMP and the Pentagon channel, and streaming as a possible platform for training; DLI began to

work with NPS on instructional content capture and in sharing storage costs; an IPv6 working group was formed

- Dr. Christine Cermak attended the Joint Annual Conference for the Society for Colleges and University Planning and the National Association of College and University Budget Officers (SCUP); Theme: *The Campus of the Future*

INFORMATION TECHNOLOGY DATA

- Accounts: 6,828
- Active Phone Lines: 500 digital; 100 VoIP; 2,400 analog
- Audio-Conferencing Ports: 24
- Backup Data: 66 terabytes (100,000 CDs)
- E-Mail Stored: 820 gigabytes
- External E-Mail Received: 20.2 million per year
- Forty-Eight Point Multipoint Control Unit (MCU)/Video Bridge: 1
- Internet Traffic: 146 gigabytes per day
- ISDN Video-Conferencing Circuits: 165
- Mainframe Data: 130 terabytes
- Multimedia Presentation Systems: 100+
- Network Attached Systems: 5,425
- Networks: 7
- Software Applications: 800
- Technology Assistance Center: received 29,146 requests for assistance; 21,999 were resolved by the Tier 1 and Tier 2 areas; other areas of ITACS helped the remaining 7,147 customers
- Technology Assistance Center: completed 75% of all cases in Remedy in FY06, an increase of 13% from FY05
- User Data: 8.5 terabytes
- Video-Conferencing Facilities: 2
- Video Tele-Education Systems: 6
- Web Services:
 - Extranet: Successful requests: 53,715,232 per day
 - Intranet: Successful requests: 81,866,976 per day
- Number of Remedy cases
 - Urgent – 1,271 (7% > FY 05)
 - High – 6,039 (4% >FY 05)
 - Medium – 20,505 (77% > FY 05)
 - Low – 4,308 (26%> FY 05)
 - Total= 32,123 (32% > FY 05)
- Remedy Cases by Major Categories
 - IA – 3,180 (69%> FY 05)
 - Hardware -1,800 (16% > FY 05)
 - IT Services- 10,399 (123% > FY 05)
 - Networking – 5,149 (4%< FY 05)
 - Software – 4,676 (17%> FY05)
 - Web support- 3,255 (28%> FY 05)

INFORMATION TECHNOLOGY RESOURCES DIRECTORY

Christine Cermak	Executive Director, Information Resources, and Chief Information Officer
Tom Halwachs	Chief Technology Officer
Hank Hankins	Director, Operations
Joe LoPiccolo	Director, ACS and NTIC
Jim Hall	Director, Portfolio Management
Terri Brutzman	Director, Technology Services
Tracy Hammond	Director, Instructional Technology

INFORMATION TECHNOLOGY TASK FORCE COMMITTEE

Chris Abila, ITACS	Hank Hankins, ITACS
Alex Bordetsky, Information Science	Jeff Knorr, Electrical Engineering
Doug Brinkley, GSBPP	Robert Koyak, Operations Research
Terri Brutzman, ITACS	Patrick Leary, Director, IPCOR
Christine Cermak, CIO	Joe LoPiccolo, ITACS
Peter Denning, Computer Science	Tom Mastre, IT Specialist
Douglas Fouts, Electrical Engineering	Rudy Panholzer, Space Systems
Jeff Haferman, ITACS HPR	Alan Pires, ITACS
Jim Hall, ITACS	Megan Reilly, CFO
Tom Halwachs, CTO	Judit Sedillos, Library
Tracy Hammond, Instructional Technology	Jack Shishido, Deputy CFO

APPENDICES

GOALS COMPLETED: FY2006

- Activated and tested Secure File Transfer Protocol (SFTB)
- Added twenty five users to Connect Direct Secure+ for better data transfer security
- Campus-wide implementation of SharePoint capabilities which will assist collaboration, reduce need for paper copies, and reduce need for redundant storage of the same document (reports, files, presentations, spreadsheets, thesis)
- Collaboration on new I-Net project
- Collaboration with county leadership: fiber installation from NPS to the Monterey County facility, using the existing single mode fiber cable; extensive research allowed the work to be accomplished with no downtime to the existing end users
- Collaboration with Director of Operations: NPS point-of-contact for pole-leasing purposes with PG&E
- Collaboration with Force Protection group from San Diego: 6 strands of single-mode fiber laid with the 6 strand of multi-mode fiber, allowing NPS to move the gates off the DSL connections
- Collaboration with ROICC and PW I: fiber to La Mesa rerouted to accommodate fiber needs for the new DMRI building Result: all 36 strands will terminate in building 330 instead of the antenna, allowing NPS more flexibility in establishing connectivity to La Mesa and the Monterey County building
- Complete staffing action for full time HPC technician
- Completed ERN transition of users (email and H drive) – 4000+ accounts

- ☑ Completed Human Resources Management training for seven ITACS supervisors
- ☑ Executed a successful training plan for ITACS employees, providing specific technical training for Email, Share Point and Web Content Management
- ☑ Completed Microsoft online training for 20 ITACS employees
- ☑ Completed the upgrade of Backup Servers, NDSM1 and NDSM2 for expanded backup capability
- ☑ Conduct the Certification Test and Evaluation for the SIPRNet and the Monterey Peninsula Department of Defense Net (MP DoD-Net) for Phase III of the DITSCAP, obtaining an Interim Approval to Operate and the Approval to Connect
- ☑ Continued to provide support for classified thesis assistance and processing
- ☑ Continued to provide training in MS Office suite, MS Share Point and Thesis template use
- ☑ Continue training curriculum for IT professional staff
- ☑ Continuing to operationalize the Information Assurance Manager's role
- ☑ Deployed ERN (EDU) Servers: two ITM servers; Smartboard server for CCMR; InfoWorkSpace Distance Learning Server and two file servers for CCMR; two LanDesk Servers; two file servers with disk arrays for students and group shares; Windows Update, NOC File, Crystal Reports, Python, Blackberry and second front-end Exchange servers; two server management test servers
- ☑ Deployed two Barracuda SPAM filters on ERN
- ☑ Deployment of a second Microsoft Exchange server in Secure Computing facility
- ☑ Designed, developed and established a maintenance schedule for several NPS web sites for conferences and events
- ☑ Developed a template and process for capturing project requirements, including functional area responsibilities, resource requirements, timelines, and expectations. Projects completed include:
 - Thesis SharePoint Pilot
 - DORS-DMAS financial systems improvement
 - Alumni Database transition
 - ITACS/Library Content Management System Pilot
 - Academic Catalog Project
- ☑ Documented the IA and ITACS manning discrepancies, to reallocate both NSG and ITACS personnel to more fully support expanding ITACS needs within the Business Solutions Group, (BSG), the Network Operations Center (NOC), and the Information Assurance (IA) programs
- ☑ Expanded Glasgow network for building extension
- ☑ Expanded Glasgow phone capacity by adding SCC expansion cabinet and 144 ports
- ☑ Expanded original file server SANS configuration from 2.5 TB to 5 TB
- ☑ Finished installation of Automated Tape Library for the ZVM System
- ☑ Implemented CISCO 6509 as border router for HPR and Digital California (DC) connectivity for ERN network
- ☑ Implemented CISCO Secure Socket Layer (SSL) VPN capability to Python and SharePoint resources
- ☑ Implemented HPR network connectivity with internal IP space and De-Militarized Zone Internet Protocol (DMZ IP) space
- ☑ Implemented public network within EDU for guests
- ☑ Implemented virtual redundant firewalls for the HPR and DC networks
- ☑ Increased the number of jobs running under CA-7 scheduler
- ☑ Installed and configured customer requested software products

- ☑ Installed, configured and started maintenance for the Activity Analysis software used by leadership
- ☑ Installed or updated 13 Department of Defense Public Key Infrastructure (PKI) certificates for NPS web servers
- ☑ Installed Tape Encryption Software for mail-away tapes
- ☑ Installed the second Video-Teleconferencing (VTC) suite in the Secure Computing Lab
- ☑ Moved Group Shares to ERN
- ☑ Monterey Peninsula Department of Defense Net
 - Connectivity for DLI for DBIDS to DMDC server and PERSEREC
 - Fleet test project to provide Technical Assistance to remote clients
 - Phone connectivity for DLI to OMC
- ☑ Moved Wireless network to ERN
- ☑ Obtained Microsoft Certified Systems Administrator (MCSA) certification for six ITACS employees
- ☑ Obtained Microsoft Certified Software Engineer (MCSE) certification for three ITACS employees
- ☑ Operationalized the Information Assurance (IA) Training program, certification and accreditation documentation
- ☑ Purchased and installed a new Multipoint Control Unit (videoconferencing bridge)
- ☑ Ran approximately 60,000 jobs per month
- ☑ Redesigned and updated several of the upper levels of the NPS Intranet web presence
- ☑ Refreshed 20 classroom media systems
- ☑ Renovated Technology Demonstration area
- ☑ Requested funds from NETC, based on the Instructional Technology Lifecycle Management plan requirements
- ☑ Taught weekly classes on TSO usage and operation
- ☑ Transition of Python-related e-mail requests from the Python support team to the Technology Assistance Center (TAC)
- ☑ Updated the Instructional Technology Lifecycle Management Plan
- ☑ Upgraded equipment and rebuilt the network scanning and monitoring tools

GOALS : FY2007

ACADEMIC APPLICATIONS AND SERVICES

- ☐ Complete the first annual Classroom Maintenance Plan
- ☐ Complete the Learning Object Repository Pilot (Hive)
- ☐ Complete the Streaming Portal Phase I
- ☐ Complete the third annual classroom equipment inventory, including descriptions of the related environmental areas that affect instruction
- ☐ Conduct the third annual classroom Lifecycle Management Plan (LMP), linking the plan requirements directly to the inventory
- ☐ Develop a project plan for High Performance Computing
- ☐ Develop capability for automated monitoring of classroom and laboratory computer systems
- ☐ Develop the next stage of PYTHON – include online Distance Learning (DL) registration and improved secure data exchange with other NPS systems
- ☐ Evaluate the PC Tablet deployment in CEE for use in the LRC and classrooms

- Evaluate and select a Video Tele-conferencing to the Desktop solution
- Improve HPC infrastructure by:
 1. Upgrading electrical and cooling capacity
 2. Full utilization of the CENIC connection
 3. Improving overall aesthetics of the HPC space
- Replace facility media systems, based on the LMP, as resources are available

ADMINISTRATIVE APPLICATIONS AND SERVICES

- Complete the Xerox Multi-Functional System deployment
- Conduct an IA and a Privacy Act audit of public data
- Conduct the annual IA Awareness Training
- Conduct the annual review of the DoD IA Controls
- Configure and install the Information Assurance Compliance Appliance (Bradford Networks)
- Continue developing Frequently Asked Questions (FAQs) for common TAC assistance calls
- Develop a knowledge base of solutions within the Remedy system
- Develop a staff Cross-Training Initiative
- Evaluate a File Transfer Protocol-like appliance
- Evaluate an Identity Management Appliance
- Evaluate the IA and the Computer Network Defense posture of NPS
- Evaluate the Technology Assistance Center campus service level agreement for all services
- Implement file aging migration capability
- Implement SharePoint capabilities campus-wide
- Implement SIP (Session Initiation Protocol) server for expanding VoIP capability
- Implement Virtual Server Infrastructure
- Investigate additional hardware encryption options for remote access
- Investigate and recommend an Email Attachment Storage Solution
- Upgrade Definity G3R PBX to Communications Manager PBX
- Upgrade Intuity Audix voicemail to Modular Messaging

IT MANAGEMENT AND RESOURCES

- Assist in the development of POM and PR submissions
- Develop a streamlined process for contract renewal and tracking of department purchases
- Finalize standard weekly budget reporting process
- Formalize Lifecycle Management Plan
- Implement and test an ITACS Disaster Recovery Plan
- Institutionalize the use of the ITM software for the decision making process
- Update policy inventory
- Update space inventory records
- Facilitate the update to the IT Strategic Plan

NETWORK INFRASTRUCTURE

- Complete planning and conduct a storage area network test across the MP DoD-Net
- Complete the Certification and Accreditation of unclassified networks, enterprise systems and applications

- Complete the Cisco Video Phone evaluation
- Complete the move of client systems and application servers to the Education and Research Network (ERN)
- Complete the build-out to full capacity on all MP DoD-Net nodes
- Conduct the review of the Minimum Security Checklist on each Network and business application.
- Expand Monterey Peninsula Department of Defense Net capability to include classified data delivery – Secret Internet Protocol Router Network (SIPRNET)
- Implement new Wireless network for campus
- Implement RAS server access for ERN network
- Implement seamless network access for Distance Learning students
- Increase user file storage
- Move primary circuits to the CalREN backbones onto the NPS-Monterey County Education Network
- Negotiate agreements with California State University – Monterey Bay (CSUMB), the California State University System, and CENIC for NPS and CSUMB to provide alternate routes to CalREN for each other
- Provide network access in the wings of Herrmann Hall
- Replacement network infrastructure and equipment for 10G and IPV6 capability
- Submit plans to DISA for transfer of local NIPRNET and SIPRNET circuits from leased lines for review and approval
- Transfer Defense Language Institute Foreign Language Center and Presidio of Monterey telephone trunks from leased T1 lines onto the MP DoD-Net
- Upgrade to the current level ZOS, ZVM and Linux software on the mainframe
- Work with Public Works to establish appropriate cabling and electronics in the new Glasgow (P205) building
- Work with Public Works to remove unnecessary cabling and electronics at fire station

COMMUNICATIONS, PARTNERSHIPS AND OUTREACH

- Continue partnerships/outreach activities with City of Monterey, CSUMB, DoD Monterey Peninsula, EDUCAUSE, DoN CIO, NETWARCOM, Internet2 and CENIC
- Create or strengthen partnerships with:
 1. Calit2 (California Institute for Telecommunications and Information Technology)
 2. UC San Diego
 3. UC Irvine
 4. Lawrence Livermore National Laboratory
 5. UC Santa Barbara
 6. FNMOC
 7. MBARI
 8. High-Performance Modernization Office
- Expand the existing partnerships with Cisco, Foundry and Sun
- Finalize the Higher Educational IT Consortium with the Naval Academy and Naval War College and incorporate within the Navy Educational Enterprise
- Participate in implementing the Regional International Outreach Program
- Strengthen IT collaboration with departments and campus leadership

LOCAL ADMINISTRATIVE RIGHTS POLICY

ITACS Policy Series 900 – Client System Support
Policy 902 – Local Administrator privileges for an end-user

Request for Workstation Local Administrator Privilege

Name (print)

Date

I agree to the Guidelines contained in ITACS policy 902

Signature

Computer(s) for which local administrator privilege is requested:

Computer name(s)

PDA POLICY 903

ITACS Policy Series 900 – Client System Support
Policy 903 – *Use of PDA Privileges Granted to an End-user*



NPS ITACS Policy

Category: 900 – Client System Support

ITACS Policy: 903 - *Use of PDA Privileges Granted to an End-user*

Approval: ITACS and the IT Task Force

Timeline:
Effective date: 1 August 2006

Definitions: Applicable to NPS Network Users

The term “typical end-user” refers to a computer end-user that expects the system level configuration of their computer to be maintained by a member of the IT technical support staff. Typical end-users envision their computer as a business tool and do not want to be concerned with the details required to keep the computer functional.

The term “local administrator” refers to a special, privileged end-user that has inherent operating system configuration rights and capabilities not available to a typical end-user. Local administrators have rights to change system-level parameters.

Local administrator privileges are normally reserved for the IT system administrators (staff) or for an *expert* end-user.

Personal Digital Assistant (PDA) refers to any Government or Private Device.

ITACS Policy Series 900 – Client System Support
Policy 903 – *Use of PDA Privileges* Granted to an End-user

Policy:

If a typical end-user chooses to use a PDA other than a Government purchased Blackberry approved device with an Exchange license for email and related services, the following procedure will be in effect for support of such device by ITACS:

- The device must not redirect NPS mailbox data to a 3rd party server
- The device must not beam email or data to the PDA
- All exchange of NPS information must be done locally by cable, cradle or otherwise, with the exception of the use of NPS wireless services
- Secure POP-ing (downloading) of NPS mailbox data is allowed
- Configuration details for Secure POP are given out at Technology Assistance Center (TAC).

For the initial installation of the PDA (or troubleshooting which entails a software reinstall):

- The end-user (utilizing a government PC) may be granted temporary Administrator Rights in order to Self Install and Configure the device
- Once the PDA is working correctly, the end-user will contact the TAC and will be returned back to User Level Privileges.

ITACS does not provide any hands-on technical assistance for these devices. If the end-user wants full support of a PDA, we recommend obtaining a Blackberry device through our ITACS cell phone department.

Technical:

Because of the system-level “power” given to an end-user having local administrator privileges and the fact that end-users with local administrator privileges are able to damage their own software environment (even destroy all functionality), it is necessary to limit the amount of IT staff labor time spent trying to recover any such end-user damaged system. Therefore, recovery is limited to the re-installation of a standard baseline software image (applications and configuration).

Expectations/

Responsibilities: End-users will be expected to Secure PDA’s both physically and with appropriate Anti-virus and Spyware protection if available.

VIRTUAL PRIVATE NETWORK (VPN) ACCESS POLICY

ITACS Policy Series 200 – Communications Network
Policy 205 – Virtual Private Network (VPN) Policy



205 – Virtual Private Network (VPN) Policy

Approval: ITACS and the IT Task Force

Timeline: Revision date: 12 April 2005
Effective date: 30 April 2005
Review due: 1 April 2006

Purpose: This policy applies to all Naval Postgraduate School staff, students, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing a VPN to access the Naval Postgraduate School network. This policy applies to implementations of VPN that are directed through the CISCO PIX firewall for the nps.navy.mil network, through the CISCO VPN Concentrator connected to the Netscreen firewall device for the nps.edu network, and through the CISCO VPN concentrator designated for site to site connection to the nps.navy.mil network.

Definitions: **Client:** Software that allows a single computer to initiate an IPSec connection to a VPN concentrator, and thus access a Naval Postgraduate School internal network.

Dual Homing: Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP); Being on a Naval Postgraduate School-provided Remote Access home network, and connecting to another network, such as a spouse's remote access; Configuring an ISDN router to dial into Naval Postgraduate School and an ISP, depending on packet destination.

Naval Postgraduate School User(s): Naval Postgraduate School staff, students, contractors, vendors and agents

Site to Site VPN: A VPN between two VPN devices (Router, Firewall or VPN appliance) that connect internal hosts from both networks using IPSec protocols.

Split-tunneling: Simultaneous direct access to a non-Naval Postgraduate School network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Naval Postgraduate School's corporate

ITACS Policy Series 200 – Communications Network
Policy 205 – Virtual Private Network (VPN) Policy

network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

VPN: Virtual Private Network is the use of IPSec protocols to provide a secure connection over an unsecured network.

VPN Concentrator: A device in which VPN connections are originated and terminated.

Client Access

Policy: The purpose of this policy is to provide guidelines for Remote Access IPSec Virtual Private Network (VPN) client connections to the Naval Postgraduate School Network.

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Naval Postgraduate School internal networks.
2. VPN use is to be controlled by requiring user authentication. Users must provide the name and password of a valid user account with VPN authorization.
3. When actively connected to the Naval Postgraduate School network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by the Naval Postgraduate School network operations center.
6. All hosts including personal computers that are connected to Naval Postgraduate School internal networks via remote access technologies must use the most up-to-date anti-virus software. This software can be checked out at the Technology Assistance Center.
7. All hosts including personal computers that are connected to Naval Postgraduate School internal networks via remote access technologies must be up-to-date on all system security patches.
8. VPN users will be automatically disconnected from Naval Postgraduate School's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
9. The VPN connection is limited to an absolute connection time of 8 hours per day.
10. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Naval Postgraduate School's network, and as such are subject to the same rules and regulations that apply to Naval Postgraduate School-owned equipment, i.e., their machines must be configured to comply with InfoSec's Security Policies and are subject to monitoring.

**Client
Connection
Criteria:**

ITACS Policy Series 200 – Communications Network
Policy 205 – Virtual Private Network (VPN) Policy

A VPN user connects directly to internal network firewall and the following traffic is allowed:

1. Web browsing to any internal (NPS) or external site over https, http, or 8080/tcp
2. DNS and WINS from the internal Windows servers
3. NTP from the internal time server
4. Access to Windows home files on internal file and profile servers
5. SSH to any internal NPS address, or any external (non-NPS) address
6. Access to Windows application servers
7. Windows Remote desktop to internal addresses
8. Outlook Email access
9. Citrix access to DORS and Paris

Additional port requirements would be addressed through the Configuration Change Board process.

**Site to Site
Access Policy:**

The purpose of this policy is to provide guidelines for Site to Site IPSec Virtual Private Network (VPN) connections to the Naval Postgraduate School Network.

1. Requests for site to site access to Naval Postgraduate School internal networks must obtain approval from our Configuration Control Board before such access will be allowed.
2. External entities requesting site to site access to the Naval Postgraduate School internal networks must provide the VPN Concentrator equipment, equipment maintenance funding, and any training required by network operations staff.
3. External entities requesting site to site access to the Naval Postgraduate School internal networks must designate a contact person. This person will be responsible for requesting each site to site connection, and will provide the technical point of contact for each such connection.
4. All site to site connections will be configured such that only connections between designated hosts and specified protocols can pass between the sites.
5. Authentication between site to site VPN concentrators will be via a pre-shared key. The key will be at least 16 characters in length and be composed of random combinations of numbers, lower case letters, and upper case letters. Pre-shared keys will be different for each site to site VPN.
6. The encryption level on a site to site VPN will be at 3DES or greater. Authentication algorithms may be 128 bit MD5 or 160 bit SHA.

**Site to Site
Connection
Criteria:**

ITACS Policy Series 200 – Communications Network
Policy 205 – Virtual Private Network (VPN) Policy

A VPN Site-to-Site Authorization Access Questionnaire must be filled out by the requesting site and will be submitted to the Configuration Change Board for approval. The questionnaire will address the ISAKMP policy to be put in place. Site to site VPNs will terminate at a CISCO VPN Concentrator that connects to the nps.navy.mil network. Protocols will be limited to only those required through access filters maintained on the VPN Concentrator.

Enforcement:

Any Naval Postgraduate School user found to have violated this policy may be subject to corrective action, up to and including termination of all remote access privileges.

“IT REQUIREMENTS AND SUPPORT” TEMPLATE



IT Requirements and Support – date

Purpose

The goal of this document is to provide a summary of the IT requirements of the _____ and the resultant ITACS support necessary to maintain operations.

Background

Summary

Requirements

The IT requirements of the _____ are as listed below. These requirements will be reviewed annually by _____ and ITACS for continued applicability.

- 1.

ITACS Support

The IT requirements of the _____ will be met by ITACS as listed below.

- 1.

Resources

The following table provides the resource requirements for the IT support of the FCA offices.

Resource requirement	Office Responsible
TAC support	ITACS

Evaluation

The _____ IT requirements and support are to be continually monitored by _____ and ITACS. This document shall be reviewed annually for continued applicability and any issues not addressed

Attachment 1

Specific _____ requirements