2013

2013 ITACS Information Technology and Communications Services Naval Postgraduate School Annual Accountability Report

Monterey, California. Naval Postgraduate School

https://hdl.handle.net/10945/56676

Downloaded from NPS Archive: Calhoun
Naval Postgraduate School

Mission Statement

The mission of the Naval Postgraduate School is to provide relevant and unique advanced education and research programs to increase the combat effectiveness of commissioned officers of the Naval Service to enhance the security of the United States. In support of the foregoing, and to sustain academic excellence, foster and encourage a program of relevant and meritorious research which both supports the needs of Navy and Department of Defense while building the intellectual capital of Naval Postgraduate School faculty.
# Table of Contents

Message from the Chief Information Officer .............................................. 4

ITACS Services......................................................................................... 6

Academic Applications............................................................................ 8

Administrative Applications and Services............................................. 10

Cyberinfrastructure............................................................................... 11

Cybersecurity......................................................................................... 13

Resource Management.......................................................................... 15

FY2013 Web Metrics............................................................................. 17

FY2013 Lab and Classroom Metrics..................................................... 18

FY2014 Goals......................................................................................... 19
Introduction

Message from the Chief Information Officer

As with every year, ITACS’ strategic goal is to enable the NPS mission of providing advanced education and research to our officers. Additionally, this year ITACS’ focus was on Cybersecurity and preparing for NPS’ first Cybersecurity Inspection (CSI) by Fleet Cyber Command, Office of Compliance and Assessment in September 2013.

Preparation for the Cybersecurity Inspection started in December 2012. The CSI criteria for evaluation were those used for inspection of a military network, making our EDU inspection more challenging. Our preparation included a dual focus on executing operational commitments for our education and research mission, as well as finding efficiencies and effectiveness in our planning.

ITACS launched a communication campaign ensuring many modes of communication were leveraged, which we called “Swarm Communications.” This campaign was focused on keeping NPS informed about the CSI preparation, communicating any system and network changes, while remaining focused on serving our academic mission. In the end, we were able to pass the CSI—thanks to all the campus support.

The following are a number of initiatives accomplished during FY13:

- **Cybersecurity.** Passed the inspection for the Secret and EDU unclassified networks. This ensured continuation of the .edu network.

- **Video Teleconference (VTC) Bridge.** The seven-year-old Video Bridge was replaced this year, which was a priority for both ITACS and the Comptroller. The new system provides the ability to host both IP and ISDN VTC events. The new equipment allows for more concurrent sessions assisting ITACS in meeting the mission for education, research and the new requirement as an alternative to travel. The new equipment provides more stability and quality in VTC services for our students and faculty.

- **Improving Customer Service.** During FY13 ITACS metrics show a decline in our ability to respond to customer requests. Internal staff were reassigned providing 3 additional personnel available for answering phones. It is expected over time and additional skills the response to customer requests will continue to improve.

- **Network and Server improvements.** The network architecture; server and workstation configurations were reviewed and updated. Monitoring tools were added providing better visibility for all resources on the network. Processes were automated that allow for vulnerabilities to be identified, tracked, mitigated and validated.

- **Cybersecurity training.** ITACS continues to provide an NPS two-hour training session that replaces 5 hours of online. This continues to be well-received by customers, and content is improved and updated on a continuous basis.

- **Procurement.** NPS implemented a workflow for approval of Information Technology Procurement requests aligned with the Navy requirement. Utilizing the KFS systems a workflow was added that routes all IT procurements to the CIO organization for approval. This process became operational in June of 2013 and works well and has allowed opportunities to align requests to existing NPS programs while meeting the needs of the education and research community. It has also alleviated the need to develop a campus-wide constraint that would require each end user to learn a new system to complete additional paperwork to procure IT equipment, software, and services.
Message from the CIO . . .

- **Classified Computing.** Completed the recertification and reaccreditation of the JWICS network.

- **Software Licensing** – ITACS had great success managing the academic software licenses. Using a software management tool underutilized software was identified, and areas where licenses could be pooled were identified resulting in nearly a **$100,000 cost avoidance.**

- **ITACS Team.** The ITACS Team has dedicated time to participate in campus-wide committees with the goal of improving services on campus. These efforts have been related to financial systems, student systems, web applications for academic programs and academic administration. Additionally the team works to stay connected and leverage partnerships on the peninsula, both within DoD and education. These partnerships provide opportunity to leverage resources, stay aligned with best practices and collaborate on innovation that can be applied as each organization serves their customers and their mission.

Cybersecurity is not a one-year commitment for NPS. ITACS continues to build Cybersecurity practices into daily operations. A “new normal” has been established and is part of the way we must do business. We remain focused on our faculty, students and staff and are taking steps to improve our response to customer service, while maintaining a robust security posture.

It was a successful year, and our combined efforts ensured we passed the Cybersecurity Inspection, safeguarding our EDU network. We look forward to FY14 with the same enthusiasm and energy.

Sincerely,

Joseph R. LoPiccolo, Chief Information Officer

---

**ITACS’ Annual Accountability Report: FY2013**

**ITACS’ Strategic Objective: “Enable the NPS Mission”**

FY2014 Initiatives:

- **One Team, One Mission.** Centralize IT by establishing a singular authority to manage IT requirement, aligning with academic, research, and business support units’ mission requirements.

- **Reduce IT Expenditures.** Leverage the Kuali Financial System for Information Technology Procurement Requests (ITPR) to eliminate duplicative IT services and products across campus. Stabilize IT budgeting by determining the cost of doing business and establish IT transparency.

- **Invest in our People.** Provide training opportunities for ITACS staff to gain knowledge and expertise in critical and emerging IT areas.

- **Refine the Cybersecurity Defense-in-Depth Strategy.** Proactively address an increasingly motivated and capable cyber threat. Establish a standardized business protected network on which cybersecurity controls are implemented and monitored to protect our most sensitive data.

- **Collaborate across Campus.** Collaborate with the faculty and staff to identify and improve duplicative or broken business processes that can benefit from the use of IT tools.

- **Simplify the IT Environment.** Promote Virtual Desktop Infrastructure (VDI) as an alternative to the traditional workstation. This can reduce unnecessary risk to unprotected sensitive data across campus and provide a more efficient and resilient client workstation environment that is easier to maintain and responds more quickly to the changing needs of NPS.
ITACS Services

As the Enterprise Information Technology (IT) organization for NPS, ITACS covers a broad spectrum of services including:

**Classified Computing Programs**, which provides staff and infrastructure to support the operations of the university’s five classified networks. Leveraging the expertise found in ITACS’ other functional areas, Classified Computing Programs supports classrooms, computer labs, secure video tele-conferencing, distance learning, conferences, and seminars in the Sensitive Compartmented Information Facility (SCIF), Systems Technology Battle Lab (STBL), the Dudley Knox Library, Watkins Hall, and in various campus auditoriums and lecture halls.

**Cyberinfrastructure**, which includes the Network Operations Center (NOC) that operates seven networks that connect more than 7,500 wired and wireless edge devices to the California Research and Education Network (CalREN), the .mil DOD Research Engineering Network (DREN), and several classified networks. The 10 gigabits per second (gbps) network backbone connects to the Digital California (DC) network backbone for the commercial Internet and the High-Performance Research (HPR) networks for Internet2, U.S. Department of Energy’s Energy Sciences Network (ESnet), National LambdaRail (NLR) and other research capabilities. A redundant 1gbps connection is provided to each network. NPS operates its mainframe on a twenty-four/seven basis. Unified Communications supports all of the email, telephone, Voice over Internet Protocol (VoIP), cell phone, Blackberry and Video Tele-Conference (VTC) communications at NPS. Server management maintains and operates nearly 400 physical and virtual servers, as well as one (1) petabyte (PB) of enterprise storage.

**Cybersecurity and Privacy**, which is responsible for securing the networks and data on campus, including computer network defense and monitoring, antivirus and vulnerability, operating system and application patch management, and certification and accreditation of networks and applications. Staff provide the tools and technologies to find, protect, and react to the unauthorized disclosure of sensitive/privacy data on NPS networks, liaises with third parties throughout the DOD, DON, the greater academic community and state and local government organizations to maintain currency with the latest cybersecurity and privacy policies, guidelines, threats and vulnerabilities; to deliver relevant and timely trainings to the campus user population; and to collaborate with faculty and students on cybersecurity-relevant research topics.

**Education Technologies**, which is responsible for all of the technology, learning spaces, and audio-visual (AV) systems used in teaching both resident and non-resident students, including oversight of 14 computer labs, 10 VTC/Video Tele-Education (VTE) suites, 75 smart classrooms, five auditoria, 20 conference facilities, and 250 software packages. Educational Technologies also maintains the Sakai Collaborative Learning Environment (CLE), web-based collaboration and streaming and on-demand video systems, on-campus podcasting, and the robust video tele-education infrastructure, and has oversight of the TAC, the primary means of IT support for students and faculty.

**Enterprise Information Systems**, which provides integrated, comprehensive technology solutions that enable NPS to streamline and improve its business processes and practices, including the technical implementation of the NPS public (www.nps.edu) and intranet websites, maintenance and administration of over 50 locally developed and commercial web applications, administration of 310 relational databases on 30+ instances of database servers (Microsoft Structure Query Language (SQL) server, Oracle, and MySQL), implementation and maintenance of a web-based issue tracking, project management systems, and collaboration tools such as SharePoint and enterprise JIRA and wiki.

**High Performance Computing**, which manages Linux systems used for teaching and research, provides visualization services that can utilize the Sony 4K projector to render enormous datasets, and oversees the NPS High-Performance Computing (HPC) service. The HPC supercomputer is named "hamming" after the computer pioneer and former NPS professor Dr. Richard Hamming, and has 2,264 computational cores and 11,296 graphical processing unit (GPU) cores.
High Performance Computing

For the past 5 years, ITACS has provided the NPS Supercomputer "Hamming" to all interested NPS researchers, faculty, and staff. The original Hamming, unveiled on January 30 2009, was manufactured by Sun Microsystems (which was purchased by Oracle Corporation on January 27 2010). Beginning in late FY12, and concluding in late FY13, the original Hamming went through a complete system refresh: all Sun/Oracle branded equipment has been completely replaced primarily by compute servers manufactured by SuperMicro Incorporated. The original Hamming was capable of just over 10 billion floating point operations per second; the current Hamming is capable of over 30 billion floating point operations per second, and uses about 1/4 of the power and physical space of the original Hamming. Hamming is primarily used for research, but a growing number of faculty are using the service for teaching.

Oversight of the Hamming SuperComputer is provided by the High Performance Computing (HPC) Advisory Panel. This Panel is comprised of faculty who are experts in the field of HPC and there are representatives from a broad spectrum of campus departments. The HPC Advisory Panel ensures that increasingly scarce HPC funds are spent wisely and are compatible with the needs of HPC researchers. In addition, the HPC Advisory Panel has kept the Hamming SuperComputer on the leading edge of HPC technology by supporting the acquisition of state-of-the-art hardware such as General Purpose Graphical Processing Units (GPGPUs, typically manufactured by NVIDIA); Intel Xeon Phi Many-Integrated Cores (MICs); dense computing nodes = single servers with up to 64 cores and a minimum of 256 GB of RAM, solids state disk drives (SSDs); and more).

The current configuration of the Hamming SuperComputer is well documented on the NPS wiki, and over the last year the stability and overall uptime has improved dramatically. There are over 300 active accounts on the SuperComputer, and it is used for classroom teaching purposes as well as for thesis and research projects. Several years ago, there were over a dozen SuperComputers scattered over campus and maintained by individual investigators. Today, most of those SuperComputers have disappeared in favor of using the ITACS operated and centralized Hamming SuperComputer. There are a couple of smaller SuperComputers still maintained by individual investigators, but these investigators have coordinated with ITACS for support of their systems.

Figures below show the usage of Hamming over FY13 by various customer groups:

- Number of Linux systems campus-wide (virtual + physical and excluding Hamming): 260
- Number of Linux administrators campus-wide: 75
- Number of active accounts on Hamming: 315
- HPC disk space: 200 terabytes (1 terabyte = 1 trillion bytes = 1000 billion bytes)
- HPC tape storage capacity: 1.2 petabytes (1 petabyte = 1 quadrillion bytes = 1000 trillion bytes)
- Number of CPU cores on Hamming: 2,264
- Number of Hamming "compute nodes": 48
- Total memory installed in Hamming (RAM): 8.7 terabytes (1 terabyte = 1 trillion bytes)
Audiovisual

The Audiovisual team began 2013 with the completion of the classroom AV refresh, which included 55 new wide-screen projectors replacing old 4x3 format machines. Aging projector screens and obsolete analog signal routing equipment were also replaced, and the team added support for digital computer video formats (including HDMI and DVI).

The new JIRA-based AV request management system, implemented in late 2012, helped the Audiovisual team support nearly 550 separate AV requests in 2013.

Additionally, the Executive Briefing Center was completed and placed into service, immediately becoming the largest conference room on campus with round-table seating for up to 32 participants. A modern AV presentation and video teleconferencing system (with a hideaway screen and presentation system) provides state-of-the-art support for senior level briefings, meetings and collaboration.

Collaborative Learning Environment/Elluminate

The SAKAI file storage was moved from a dedicated server to the NPS NetApp, allowing for dynamic space allocation and reduced storage requirements. There were also more than eight million Sakai course and project site interactions by 9,918 distinct users throughout the year.

Software/Licensing

The 2013 academic software licensing effort saved NPS over $100,000. Campus-wide duplicative subscriptions were eliminated and we added Dreamspark and VMware Academic Program (VMAP) software licensing programs. These additions provided students, faculty and staff with the ability to download software (e.g. MS Word) for home usage, as well as take advantage of the numerous design and development tools offered on these sites free of charge for the end users. Nearly 315 users have registered since combining the two web stores, completing more than 480 downloads.

Virtual Desktop Initiative (VDI)

ITACS upgraded the VDI hardware, which increased the Virtual Machine (VM) capacity from 64 machines to over 300 while reducing the data center footprint from 40 units of rack space to just two. This also increased the user base, adding virtual desktop capabilities in the Systems Engineering distance learning curriculum, DMAS users, and Information Sciences.

CSI compliance was also achieved, from the servers, database, storage and certificates to all of the desktop images.

Videography & Streaming

A new broadcast and recording system in King Hall was installed, allowing the ability to film and produce the 2013 Summer and Fall Quarter graduation ceremonies, where over 400 remote viewers watched each graduation stream. The installation included three new pan/tilt/zoom (PTZ) high-definition cameras mounted in the auditorium, allowing for one technician to operate the cameras and the Tricaster mixing board from a single station. The video productions are captured with multiple angles and in high definition.

Additionally, upgrades to vBrick and Podcast from a physical server to a virtual server were performed for distance learning student access. This gave students the ability to access DL education from their mobile devices, as well as increased efficiency by decreasing the amount of space utilized to host them.
Video Tele-education/Video Teleconferencing

Over 600 hours of instruction for 148 courses were supported in FY13 along with 268 other video teleconferences for a total of 4,173 video-port-hours of operation.

In order to enable the use of a computer and webcam as a standards-based VTC endpoint, Jabber Video for Telepresence was installed. Jabber supports screen sharing during VTC and reduces the need to ship hardware endpoints to non-resident VTE faculty. The current license supports 25 simultaneous Jabber users.

New Cisco Video Communications Servers were installed, upgrading VTC resources and allowing for a 250% increase in secure firewall traversal resources for VTC/VTE connections. This upgrade enables internal and external users to collaborate more easily and effectively over video.

ITACS also replaced 18 flat screen monitors with high-definition 1080p-compatible units, allowing VTE classrooms and suites to be upgraded to HD video in the future. Firmware updates were also applied to all NPS VTC hardware endpoints to increase resistance to security threats. The benefit of this is to enable participants to communicate and collaborate as clearly as they would in person, without worrying about complicated systems and security threats.

With mid-year OPN funding, ITACS purchased the Cisco MSE8000 Media Services Engine Video Bridge, which provides a more flexible, more efficient VTC experience, including allowing each endpoint to operate at its optimal capability. Faculty now have direct access to control the conference layout, and ITACS staff have the capability to tailor layouts for each endpoint in a conference. Overall, the MSE8000 represents a 33 percent increase in video port capacity.

Classified Computing

In FY 2103 the Classified Computing Programs Staff devoted significant time and energy preparing the Systems Technology Battle Lab (STBL) SIPRNet for a Cyber Security Inspection (CSI) by the Office of Compliance and Assessment (OCA) of Fleet Cyber Command (FCC). This was an in-depth review of the operational posture of the SIPRNet covering physical security, staff qualifications, management programs, network and systems compliance with DoD, DoN, and local security and operational instructions and directives. This was an intensive four day assessment of the preparedness of the SIPRNet to operate safely and securely on the Defense Information Systems Network (DISN) Global Information Grid (GIG). The Classified Computing Programs staff, supported by staff members from all elements of the ITACS department earned a passing score of 90.3%. It was noted by FCC OCA that this was probably one of the three highest scores earned by a Navy SIPRNet during a FCC CSI.

The Classified Computing Programs staff, assisted by the Special Security Officer, successfully completed the rigorous requirements for the recertification and reaccreditation of the NPS JWICS network. This is a tri-annual event requiring a thorough vetting of NPS’ capability to operate the network within prescribed operational and security parameters.
Availability of the JWICS network is a central component of NPS' classified teaching and research strategy and is used to carry NPS distance learning (DL) courses and facilitate collaboration between organizations through the three suite VTCs and two desk top VTCs running on the network.

This year ITACS focused on cybersecurity, mobile access and system improvements for the NPS Administrative Applications and Services.

The Cybersecurity Inspection in September 2013 was an all hands effort, evaluating our systems, scanning them and remediating any configuration or patching requirement. The Administrative Applications and Systems were reviewed to ensure there were no vulnerabilities and that data were adequately protected. These efforts took many hours and contributed to the overall success we had in passing the inspection.

In many ways the bring-your-own-device or BYOD type systems have become the way business is conducted at NPS. There are still many institutional business processes that require a desktop for conducting daily business, but in order to provide information to the students and faculty who at times are very mobile, ITACS has created several mobile interfaces for key applications.

Design of these systems and applications includes the user experience as part of the criteria. During development, the functional business owners, end-user representatives and technical staff meet throughout the process to ensure the solutions meet criteria set for each perspective. The shared goal is effectiveness of service and efficiencies in costs. In this case, costs consider not only the cost of the systems, but also the cost of labor in use of the system.

To meet its goals for FY13, Administrative Applications and Services successfully completed the following initiatives:

Financial Systems

The Kuali Financial System (KFS) Functional and Technical Teams implemented a major change to how indirect cost recovery is calculated during FY 13, as well as numerous enhancements and bug fixes to KFS.

The Memorandum Accounting System (MAS) previously consisted of numerous databases, one for each type of account. During FY 13, these databases were consolidated into one and that one was moved into a Virtual Desktop environment. The end result is a system that is much more stable, easier to use, and easier to maintain.

Kuali Coeus Customization

ITACS began working with the Research and Sponsored Programs Office on customizing Kuali Coeus to provide a research administration system for NPS. Currently, there are several outdated locally developed systems to assist with research administration. These outdated systems will be replaced by Kuali Coeus, an open source research administration system based on a system named “Coeus” that was originally developed by MIT. The target date for launch of Kuali Coeus at NPS is the start of fiscal year 2015.

Nagios Monitoring and Auto-recovery

ITACS continued implementation of Nagios an open source enterprise monitoring system. Accomplishments in FY 13 included employing Nagios for auto-recovery of various services, such as the MFD print spoolers, NetApp, VMware vSphere. Nagios detects problems with these services and remedies them before the problems impact customers.

CAS Enhancements

Implemented a mobile interface for the Central Authentication System (CAS). Implemented password policy warnings in CAS and integrated CAS with MyPassword to provide users feedback regarding login problems and links for taking care of those problems, such as unlocking their computer account using MyPassword.
Enterprise Web Survey Tool Launched

ITACS implemented an enterprise open source web survey tool named “LimeSurvey.” This provides NPS with a much needed web survey capability and meets DoD requirements to provide secure storage of survey data.

Support for Mobile Devices added to Universal Video Embedder

Implemented HTML5 for the “Universal Video Embedder,” which allows videos to be streamed to mobile devices, such as iPads and iPhones.

Deployed Secure Email Gateway

Designed and deployed a secure email gateway to allow applications to send digitally-signed email. It is currently implemented for JIRA and Confluence. More applications will be configured to use it in FY 14.

Puppet Implemented

Implemented the use of Puppet to manage/standardize the configuration of Linux servers. This frees up ITACS and campus system administrators from routine administrative tasks, thus allowing them to spend more time on meeting customer needs.

Cyberinfrastructure

Cyberinfrastructure includes the Server Management, Network Operations Center (NOC), Infrastructure (cable plant), Data Center Operations, and Unified Communications groups. Server management maintains and operates nearly 400 physical and virtual servers, as well as one (1) petabyte (PB) of enterprise storage. The NOC is responsible for seven networks that connect more than 7,500 wired and wireless edge devices to the California Research and Education Network (CalREN), the .mil DOD Research Engineering Network (DREN), and several classified networks. Infrastructure supports all fiber and cable into the campus, across campus and within buildings. The Data Center Operations team ensures continuous operations for all systems within the Data Center. Unified Communications supports all of the email, telephone, Voice over Internet Protocol (VoIP), and cellular communications at NPS.

NetApp

Partnering with the Defense Language Institute, NPS was able to acquire a NetApp storage appliance. This 1.5 Petabyte (1.351e+16 bit) storage device is shared between the two institutions, and has given NPS the ability to expand storage quotas across the board (ranging from 2.5 to 14 times the storage that was available per user). The NetApp has also been put to work as the Storage Area Network (SAN) used to support the Virtual Server Farm that has replaced over 80 physical servers.

NPS Guest Wireless

Since NPS started offering a guest wireless capability years ago the process was cumbersome and involved prior planning and coordination. The new Guest Wireless provides a self-onboarding process. A visitor can obtain an account and connect to the internet over NPS hardware in a matter of a few minutes without needing an NPS account. This capability supports cybersecurity goals by maintaining accountability for devices on the Guest Wireless network. Connections made to this ‘open’ SSID will be captured by SafeConnect, where users can then register themselves and their credentials are sent to a cell phone or email address, enabling the user to log on.

Avaya Servers

The campus telephone system of systems is extensive. The servers have proprietary configurations as well as components NPS manages with privileged accounts. Many months were spent working with the vendor to ensure the STIGs were implemented and security configuration updates done. The work required multiple phone calls with the vendor, testing and then finally coordination to schedule a time for the vendor and NPS administrators to conduct the upgrade. The team selected a time when the outage would cause the least impact to the user community. The upgrades were a success and our security posture was improved.
Microsoft Exchange

In preparation for the CSI, ITACS staff spent months reviewing the server environment for the MS Exchange system of systems, ensuring the Secure Technical Implementation Guides (STIGS) were correct, and scanned and patched any vulnerabilities to the systems. Privileged account structure was reviewed and ensured capabilities met the requirements of the tiered level of permissions specified in the DoD criteria. The team developed a Security Plan, which is extensive documentation about the system to include the concept of operations, and the system diagram. This document served not only the CSI but also was required as a component of the Assessment and Authorization of the EDU Network. Mailbox space increased for students from 100MB to 1GB; faculty from 1GB to 10GB; and staff from 1GB to 5GB.

Active Directory Restructure

Server Management completed a rebuild of the permissions schema internal to Active Directory in order to meet compliance standards for the CSI and ongoing Command Task Orders. This project included breaking out the previous administrative structure into a tiered system, ensuring that a single exploited administrative account would not compromise the entire network. This effort involved careful planning and staged implementation to ensure all operational capabilities were uninterrupted while the changes to configuration, process, and procedure were socialized and completed.

Data Center Virtualization

ITACS purchased VMWare (ESXi hosts) for use in a virtual cloud farm. To date, the 17 servers have alleviated the requirement for over 170 physical servers. The system will be expanded upon in FY14 to allow for greater performance of existing systems, and even more physical server retirement. This effort reduces the data center carbon footprint, as well as operating and life cycle costs.

Hot Aisle Construction

Server Management began a restructuring of the data center to comply with industry best practices. This includes the installation of an over-head power distribution system, and the configuration of server racks to exhaust heat into an aisle between two rows of server racks for better heat removal / cold air intake. This work continues, with another planned hot aisle and HVAC upgrades to improve the efficiency of the NPS datacenter.

Construction/Renovation

The infrastructure team worked with the Naval Facilities, Public Works and contractors to ensure plans appropriately accounted for the cable requirements for each effort. The team worked closely to stay ahead of scheduled work ensuring all parties involved were aware of cable locations, capacity, and utilization before the work began on any site construction. Where coordination was insufficient, the team worked with appropriate authorities and contractors to ensure cable repairs were completed in a timely manner, restoring any lost capabilities.

Upgrade to Wireless 802.11n

ITACS partnered with Brocade to enter an Infrastructure-as-a-Service (IaaS) agreement, in which NPS will be kept on current wireless technology through an ongoing engagement with the Brocade Capital Equipment team. As part of this, ITACS was able to roll out a new fleet of Brocade Motorola Wireless Access Points (WAPs). These WAPs have improved coverage over the older 802.11g models, and support speeds up to 300mbps, which was critical to support our rapidly changing mobile environment.

Wired Port Security

In support of the CSI, ITACS placed port security on all Education and Research Network (ERN) wired ports, requiring either a system be configured and logged in using ERN credentials, or that the system have a machine address to gain access to the ERN. This effort took many weeks of planning, testing and finally implementation. It was a weighted element of the inspection and directly contributed to NPS's passing the CSI.
NPS Networks & Applications Accreditation

Most of the year’s efforts revolved around preparing for the Fleet Cyber Command (FCC)-led Cybersecurity Inspection in September 2013. The NPS ITACS team received a passing score of 76% on the CSI, a combination of the assessments done on both the SIPRNet and the EDU. In fact, we are proud to say that all three Navy Higher Education IT Consortium (NHEITC) members (NPS, Naval War College, Naval Academy) all passed their inspections. The collaborative effort among the ITACS Staff and NPS Faculty, Staff, and Students was the key to our success in passing an inspection whose criteria were more appropriate from an operational Navy network on the DoD Information Network than the NPS EDU network in an academic environment. Regardless, FCC learned a lot about our academic IT environment and will return within the next 18 to 36 months to inspect us again.

The ITACS team worked with the FCC Operational Designated Accrediting Authority (ODAA) to accredit the EDU network under an Interim Authority to Operate. As Educational DAA, each of the NHEITC CIO’s had their local accrediting authorities taken away this fiscal year. As NPS transitioned to this new governance model, an Interim Authority to Operate (IATO) was issued this year for the EDU accreditation that expired in June. Efforts will continue next year to attain a full ATO under this new IT governance model. As part of the annual Information Assurance controls review for the EDU and SIPRNet, the IT Disaster Recovery Plan (DRP) was reviewed and updated. Additionally, the team helped facilitate the SCIF expansion planning which will involve its own set of accreditation challenges.

Regional Security Operations Center (RSOC) Build-out

In addition to a newly engineered TAC Helpdesk, renovations to ITACS spaces included continued expansion of the RSOC. This space is dedicated to monitoring the NPS and DLI-Foreign Language Center (DLI-FLC) networks for performance, operations, and malicious activity giving both organizations a holistic view of our operational IT risk environments. Efforts continued to develop a number of new functionalities including a robust centralized logging capability, near real-time alerts, an issue ticketing system, refined policies and procedures for Incident Management, and a database of all devices on the EDU network. The final architecture will improve on these capabilities and focus on Executive Dashboards, periodic metrics, additional content for the Knowledge Wall, and improved physical security controls for the RSOC and Computer Center.

The additional functionality in the RSOC was demonstrably effective. Last year, ITACS managed 77 internal incidents, but this year, we managed 286 incidents detected by the NPS incident response team. This is an increase of 271% or 2.7 times more incidents detected by and managed by the NPS incident management team. The team did not add additional staff resources, but were able to automate many of the detection and reporting tools and react faster based on this automation, becoming more effective and productive. Additionally, two third party monitoring organizations, the Army High Performance Computer Emergency Response Team (HPC CERT) and the Navy Cyber Defense Operations Command (NCDOC), assisted NPS with the detection and response of 149 other incidents for a total of 435 incidents managed by NPS in response to our extensive sensor grid. Overall, 35% of the total number of incidents were initially detected by external monitoring organizations and 65% were detected internally by NPS staff.

Additionally, the CS team managed 15 incidents involving the electronic spillage of Personally Identifiable Information (PII). This year, NPS received over 30M emails, 55% of which were blocked by our Enterprise Anti-Spam Firewall. Of those, nearly half (45%) were allowed delivery, 2,145 emails picked up by NPS users as suspicious and sent to the abuse@nps.edu mailbox for review. Reviews showed that 58% were spam and 35% were phishing attempts. Since these phishing attempts are not caught by our automated Anti-Spam Firewall, this demonstrates the effectiveness of our knowledgeable user community and their active willingness to help defend the NPS network.
Network Access Control (NAC) Appliance

The NAC was deployed this year throughout the EDU network to enforce Operating System and application patch levels and Anti-virus definitions on systems that join the NPS network. This added extra protections to prevent the NPS user community from introducing malware to others on the network. A cross-organizational ITACS NAC Tiger Team defined the policy, the user requirements and the Standard Operating Procedures, communicated with and trained the end user population, and rolled out the technology across the campus eventually deploying the technology to all end user workstations connected to the network from locally wired, wireless, and remote VPN connections.

An additional benefit to this tool is the ability to understand more about the computers that connect to our EDU network. The NAC assisted with the initial population of a devices database so that we could communicate directly with users who either managed or owned their machines to improve their security posture. The NAC was a tremendous benefit to the incident management team who uses the appliance to immediately block a device that appears to be malware-infected and poses risk to the greater NPS community.

Those systems not appropriately managed can present additional risk to NPS. Over the last year, DoD issued 171 Information Assurance Alerts or Bulletins to the DoD community. Although no one in DoD experienced incidents attributed to the exploitation of these vulnerabilities, there were 30 known successful exploits elsewhere.

Update Anti-Virus Technology

The Cybersecurity team completed deployments of Symantec Endpoint Protection (SEP) to over 90% of end user workstations and deployed Symantec Anti-Virus (AV) to the NetApp filer system. These capabilities protect the NPS end user population from known malware introduced to the campus either from the workstation or directly into storage from remote connections. The team leverages DoD licensing at no cost to the School.

Over 2000 risks were detected and remediated by Symantec Endpoint Protection (SEP). 54% were captured by Scheduled Scans, 2.5% by Manual Scans, 15.1% by Auto-protect.

Cybersecurity Awareness Program

The team refined and updated the content of the Cybersecurity All Hands training, led numerous events during Cybersecurity Awareness Month, and delivered tailored training to small, targeted focus groups. From October 2012 through June 2013, a total of 1748 were trained in fifteen unique sessions of the live All Hands version of the annual Cybersecurity training at NPS. These training sessions were designed to augment annual compliance requirements for cybersecurity awareness. Between online and All Hands training, NPS was able to meet its Cybersecurity Awareness goal.

In FY13 ITACS received 156 Information Assurance Vulnerability Alerts & Bulletins (IAVA/B). An IAVA/B is an announcement of a computer application software or operating system vulnerability notification. These vulnerabilities were announced because they fell below an allowable threshold and were determined to put a network at risk. In FY13 the IAVA/Bs generated the application of over 70,000 critical patches that minimized the risk to the network.

In FY13 16.5M emails were blocked because it was classified as SPAM, phishing, or contained malware.
Resource Management

Resource Management provides support to all operational areas within ITACS in budget, procurement, contracts and some Human Resources-related services. Resource Management specifically manages the finances, personnel, communications, equipment, spaces, travel, training, and professional development for ITACS.

ITACS Expenditures by Area

**Academic Computing** Expenses include classroom and lab refresh initiatives.

**Classified Computing** Expenses include expanded VTC capabilities, additional workstations for classroom support and hardware life cycle refresh for servers and devices.

**Cyberinfrastructure** Expenses include annual maintenance and license renewal, procurement of storage, virtualization and server components, and data center support and refresh related to power and the environment

**Cybersecurity** Expenses include hardware for computer/network defense, costs to implement services and maintain support.

**High Performance Computing** Expenses include hardware replacement and storage expansion for high performance computing.

FY2013 ITACS Expenditures

Provides the summary of the distribution of ITACS non-labor dollars. The “Other” category includes supplies, administrative costs, and non-IT expenditures for the operation of the department.

<table>
<thead>
<tr>
<th>Account Description</th>
<th>FY10</th>
<th>FY11</th>
<th>FY12</th>
<th>FY13</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITACS Non-Labor</td>
<td>$3,737,020</td>
<td>$3,153,739</td>
<td>$2,946,375</td>
<td>$2,793,684</td>
</tr>
<tr>
<td>High Performance Computing (HPC)¹</td>
<td>$0</td>
<td>$159,144</td>
<td>$350,000</td>
<td>$320,000</td>
</tr>
<tr>
<td>Classified Computing (CC)¹</td>
<td>$0</td>
<td>$116,934</td>
<td>$200,000</td>
<td>$200,000</td>
</tr>
<tr>
<td>Total</td>
<td>$3,737,020</td>
<td>$3,429,817</td>
<td>$3,496,375</td>
<td>$3,313,684</td>
</tr>
</tbody>
</table>

¹Prior to FY11 HPC and CC funding came out of the ITACS OPTAR budget
Professional Development

ITACS typically allocates about 5% of its non-labor budget for professional development activities such as technology conferences, technical and management training, as well as education mandated by the Department of Defense for maintaining a cybersecurity workforce. Due to the fiscal and regulatory constraints in FY2013, ITACS was only able to execute a very limited number of professional development opportunities for its staff. The value of our training efforts are vital to the education and research mission. ITACS will make professional development a priority in FY14.

Customer Service Task Force

In FY12 ITACS stood up the Customer Service Task Force and the Customer Service Committee to incorporate service, one of its four core values, into daily operations. The Task Force and the Committee initiated the Customer Account Management program, in which an ITACS staff member interfaces with a campus business unit. The CAM pilot program began with Student Services and the Research Office. The Customer Account Managers had good momentum and plan to expand the effort in future years when fully staffed.

ITACS Staff On Board During FY13*

<table>
<thead>
<tr>
<th>Department</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIO/Executive Director ITACS</td>
<td>1</td>
</tr>
<tr>
<td>Deputy Executive Director ITACS</td>
<td>1</td>
</tr>
<tr>
<td>Senior Leadership Team</td>
<td>6</td>
</tr>
<tr>
<td>Education Technology</td>
<td>13</td>
</tr>
<tr>
<td>Classified Computing</td>
<td>3</td>
</tr>
<tr>
<td>Cybersecurity and Privacy</td>
<td>2</td>
</tr>
<tr>
<td>Enterprise Information Systems</td>
<td>9</td>
</tr>
<tr>
<td>Helpdesk</td>
<td>6</td>
</tr>
<tr>
<td>IT Resources</td>
<td>5</td>
</tr>
<tr>
<td>Network/Server Management</td>
<td>10</td>
</tr>
<tr>
<td>Research Computing</td>
<td>3</td>
</tr>
<tr>
<td>Unified Communications</td>
<td>5</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>64</strong></td>
</tr>
</tbody>
</table>

*GS Staff as of July 2013

Total number of authorized ITACS BINS: 86
In FY13 the majority of users on the NPS network chose to search the internet using Internet Explorer.

An operating system (OS) is software that manages a computer’s hardware and software, enabling it to perform multiple tasks. In FY13 the most commonly used OS on the NPS network was Windows.

Extranet usage refers to users accessing the NPS web site outside of the intranet.

Intranet usage refers to users accessing the NPS internal web site.
ITACS manages 120 classroom and lab spaces used for teaching both resident and non-resident students. Over 90% of these learning spaces contain equipment that captures and stores class content delivered to enable students to access information at any time. Much of NPS curricula requires a collaborative learning environment to deliver on-line courses or enhance on-campus courses.

ITACS recorded nearly 18,000 hours of classroom instruction in FY13 that students were able to retrieve as necessary.

NPS leverages online collaboration tools like Learning Management Systems to enrich the education experience. ITACS coordinated the creation of over 1,900 courses in FY13.

NPS has a robust distance learning program that enables students all over the world to participate in advanced education and research. Providing over 6,600 synchronous sessions has created a learning environment in which participants around the world are able to contribute at the same time.
## FY2014 Goals

**ITACS’ Strategic Objective: “Enable the NPS Mission”**

**FY2014 Initiatives:**

- **One Team, One Mission.** Centralize IT by establishing a singular authority to manage IT requirement, aligning with academic, research, and business support units’ mission requirements.

- **Reduce IT Expenditures.** Leverage the Kuali Financial System for Information Technology Procurement Requests (ITPR) to eliminate duplicative IT services and products across campus. Stabilize IT budgeting by determining the cost of doing business and establish IT transparency.

- **Invest in our People.** Provide training opportunities for ITACS staff to gain knowledge and expertise in critical and emerging IT areas.

- **Refine the Cybersecurity Defense-in-Depth Strategy.** Proactively address an increasingly motivated and capable cyber threat. Establish a standardized business protected network on which cybersecurity controls are implemented and monitored to protect our most sensitive data.

- **Collaborate across Campus.** Collaborate with the faculty and staff to identify and improve duplicative or broken business processes that can benefit from the use of IT tools.

- **Simplify the IT Environment.** Promote Virtual Desktop Infrastructure (VDI) as an alternative to the traditional workstation. This can reduce unnecessary risk to unprotected sensitive data across campus and provide a more efficient and resilient client workstation environment that is easier to maintain and responds more quickly to the changing needs of NPS.