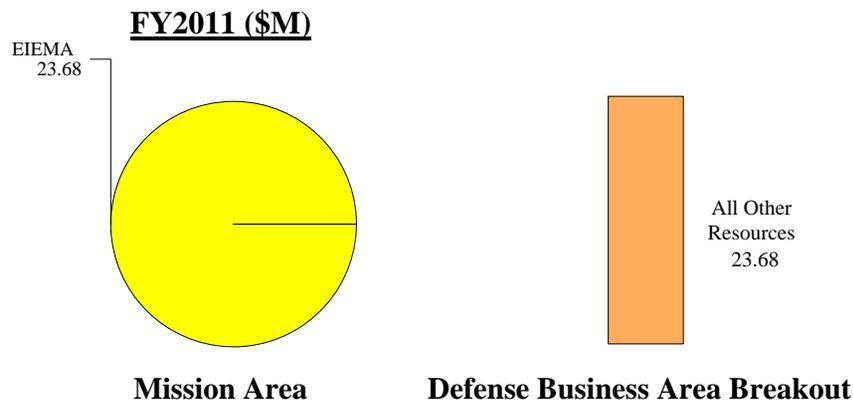


**Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010**



FY10/11PB Comparison (\$M)

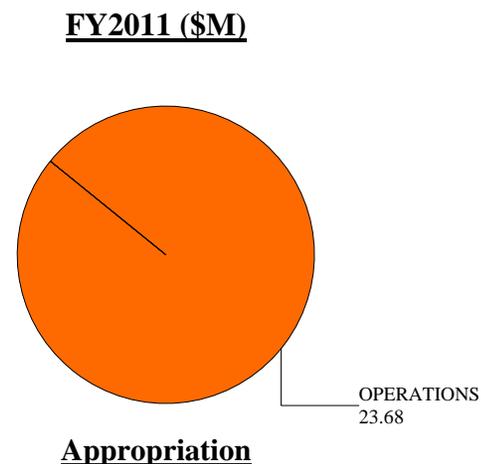
	<u>FY2010</u>	<u>FY2011</u>	<u>Delta</u>
PB FY2010:	\$ 16.67	\$ 17.23	\$ 0.57
PB FY2011:	\$ 25.43	\$ 23.68	-\$ 1.75
Delta:	\$ 8.76	\$ 6.45	-\$ 2.32

Explanation:
The National Defense University (NDU) and Joint Forces Staff College (JFSC) are continuing to work to meet Certification and Accreditation of our network. This includes but is not limited to Information Assurance (IA) continuity of operations (COOP) requirements, developing and implementing policies and procedures, conducting training, and purchasing the necessary equipment to provide an alternate sight for the University's data and critical applications. NDU's Information Technology contract was restructured and re-competed in August 09 as a more detailed definition of the task was identified during the blueprinting phase.

FY10 to FY11 Comparison (\$M)

	<u>FY2010</u>	<u>FY2011</u>	<u>Delta</u>
PB FY2011:	\$ 25.43	\$ 23.68	\$ -1.75

Explanation:
The delta is due to the a new IT support contract which includes changes in the scope of Work from previous years. The National Defense University (NDU) and Joint Forces Staff College (JFSC) provide a reliable and accessible IT infrastructure to support our faculty, staff, and students. The students are senior ranking military officers and high level civilians educated in Joint, National and International Security policy.



**Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010**

Page left intentionally blank

Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010

Executive Summary

The Information Technology Division (ITD) staff preforms research projects, conducts policy analysis, and information assurance program, for the Joint Staff, Secretary of Defense, and National Command Authorities. The CIO manages a Performance Work Statement (PWS) for National Defense University IT Support. The PWS describes in general terms the types of contracted information technology (IT) support required at National Defense University (NDU). Among the key elements contracted out include support for on-site network, database, web, user support, help desk and IT training. Additionally, design, develop, perform initial operational testing and evaluation, transitional hand-off /acceptance of pertinent documentation and implementation of IT changes.

The mission of the Information Technology Directorate, Information Assurance Program is to develop and implement polices and procedures to appropriately safeguard National Defense Information System against external and internal network intruders and security incidents. The key benefits of the Information Assurance Program are to ensure the confidentiality, integrity, and availability of the National Defense University's Enterprise Information Systems. Funding for information assurance categories include: Application security; Computer Operations Security (Intrusion Detection System, Anti-Virus Tools); Manpower (contractor support); Security Application/Software (vulnerability analysis tools); Perimeter Protection Security Architecture (Fire-wall's, Guard); System development security (mobile code development, review, certification); Security Management (IA) Training, IA Workforce certifications, Security Administration (network/system accreditations), Security Test & Evaluation (ST&E), Independent Verification and Validation (IV&V), Computer Network Defense Service Provider; Security policy development and promulgation, and New product security assessment. Due to the increasing magnitude of cyber threats, NDU continues to enhance the security of systems, information and infrastructure components.

Significant Changes

NDU's Information Technology contract was restructured and re-competed in August 09 as a more detailed definition of the task was identified during the blueprinting phase.

Defense Business Systems

All business systems and programs were entered into Defense Information Technology Portfolio Repository (DITPR).

Information Assurance Activities

The National Defense University Information Assurance Program provides information assurance and computer network defense (IA-CND) activities to protect and defend NDU's information and systems by ensuring their confidentiality, integrity, availability, authentication, and non-repudiation.

IA has made significant enhancements to the NDU's defense –in-depth architecture and posture by the deployment and integration of additional IA controls and providing enhance boundary defense, malware protection and system redundancy capabilities.

The over-arching mission of National Defense University is to provide Joint Professional Military Education (JPME) and actively defend information resources, and critical infrastructure to provide assured information delivery, authenticated system and network access, and information protection. To support this mission IA is engaged in efforts to project and defense NDU's networks and information, thereby maximum mission assurance. NDU is:

- Striving to maintain that greater than 90 percent full Federal Information Security Management Act (FISMA) certification and accreditation of NDU's system and networks.

Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010

- Implement enterprise solutions to encrypt NDU's data at rest and ensure protection of sensitive NDU information.
- Enabling and enforcing cryptographic logon on all NDU networks, with the goal of ultimately eliminate reliance on user name and passwords.
- Pilot a Common Access Card (CAC) – enabled blackberry, with plans to follow with an enterprise roll out of this solutions; and
- Improving the protection of sensitive information to reduce that number and frequency of PII (Personal identifying Information) spillages throughout NDU.

NDU is issuing/updating IA policy to provide guidance or direction:

- IA Roles and Responsibilities
- Certification and Accreditation of the NDU's IT system for FISMA NDU's Information Assurance Certification and Accreditation Process (DIACAP) Manual and Guidance; and
- Incident Handling and Response

NDU continues to create an IA empowered workforce initiatives to train and develop its cadre of IA professionals. IA efforts will ensure NDU's network initiative culminate in an architecture with inter-graded IA controls to protect information and systems. Future IA enhancement will build upon achievement and continue to increase the defense-in-depth capabilities of NDU and its component commands.

Major Accomplishments

- Moved our internet service provider to DREN. This is to allow NDU to have a Department of Defense (DOD) compliant, secure, and more reliable infrastructure.
- New applications are (DOD) compliant while meeting customer needs (e.g., flexible and user-friendly).
- Hired IA team. IT policies are generated, current, understood, and enforced.
- Provide prompt and friendly customer help-desk support.
- Implemented Blackberry device data-at-rest encryption.
- Completed the upgrade of the e-mail spam filter system enterprise-wide.
- Implemented CAC logon to the network.
- Implemented Information Assurance Vulnerability Assessment patches accountability and tracking for the network.
- Successfully re-competed the performance-based IT support contract for NDU.
- Migrated the joint professional military education colleges to the Data Enterprise System (DES) for database interface and management

Major Planned Activities

- Change internet service providers to DREN
- Implement Network Access Control, enterprise-wide.
- Implement the host-based security system enterprise -wide.
- Implement a Information Assurance workforce certification program.
- Implement CAC/PKI single sign-on process for all University systems
- Improve configuration management through automation and improved techniques
- Complete the move of the University to DES.
- Implement wireless on campus

Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010

- Complete planned upgrades to video conferencing systems.
- Complete the University's continuity of operations planning
- Upgrade workstation and server operating systems
- Create a standard image for Apple workstations
- Enhance the Remedy application by incorporating asset management
- Continue with certification and accreditation of the network
- Achieve authority to operate (ATO)
- Implement enterprise wide Service Desk ticketing system.
- Deploy domain integrated systems management of Apple computers in the enterprise
- Information Assurance: NDU continue with effort to implement complete network security infrastructure to include but not limited to: PKI Class 3 capability, firewall, DMZ redesign, establish domain infrastructure compliant with DISA STIG policies, and client/server protection suites. Implement the DISA Information Assurance Vulnerability management (IAVM) compliance system Vulnerability Management System (VMS) on NDU's information systems.
- Upgraded and maintained the enterprise anti-virus tool suite, to include pilot testing of the Host Based System Security (HBSS) software and network monitoring tools. Continue with efforts to implement complete network security infrastructure. Continue all defense-in-depth measures. Develop/implement tracking of all NDU's security training as it comes on-line. Maintain and implement technology to refresh IA software and hardware, as necessary. Apply additional security measures to the NDU's architecture with systems like data encryption software and data security and device encryption computer system security software. Maintain the enterprise anti-virus tool suite; implement the DISA Host Base Security system (HBSS) once DISA fields phase two. Continue tracking and updating NDU's system security posture in the VMS tracking database. Continue work on the development and implementation of network appliance tools and software to detect data intrusion and prevent loss of personally identifiable information (PII) in accordance with OMB and directives for the protection of privacy information and PII. Develop and maintain web-enable security documentation repository that includes policies and procedure and security forms.

Global Information Grid (GIG) / Net-Centricity

NDU's efforts to comply with DOD's Net-Centric Goals include the following: system enabled to make use of internal and external network. All business application are web-based registered in the DOD Information Technology Portfolio Repository (DITPR) and are accredited as IATO or ATO. The security of NDU's system and data and infrastructure will continue to improve with the planned enhancement of fire-walls, network, and vulnerability monitoring software.

**Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010**

Page left intentionally blank

**Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010**

Information Technology Budget Exhibit Resource Summary by Initiative (IT-1)

	----- Dollars in Thousands -----		
	<u>FY2009</u>	<u>FY2010</u>	<u>FY2011</u>
NATIONAL DEFENSE UNIVERSITY RESOURCE SUMMARY:	15,174	25,427	23,679

0218 - NDU IT SUSTAINMENT (NDU/IT)

Non-Major

GIG Category: COMMUNICATIONS AND COMPUTING INFRASTRUCTURE - COMPUTING
INFRASTRUCTURE

Operations

			----- Dollars in Thousands -----		
<u>Appropriation</u>	<u>Budget Activity</u>	<u>Budget Line Item</u>	<u>FY2009</u>	<u>FY2010</u>	<u>FY2011</u>
O&M, DW	BA 03 TRN & RECRUITNG	NATIONAL DEFENSE UNIVERSITY	15,174	25,427	23,679
Initiative Resource Summary:			15,174	25,427	23,679

**Department of Defense
Fiscal Year (FY) 2011 IT President's Budget Request
March 2010**

Page left intentionally blank